UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Identificación Electrónica y Confianza en las Transacciones Electrónicas: la Regulación Jurídico-Administrativa de las Instituciones de Acreditación de la Actuación Electrónica

D. Ignacio Alamillo Domingo

2018

UNIVERSIDAD DE MURCIA

FACULTAD DE DERECHO

IDENTIFICACIÓN ELECTRÓNICA Y CONFIANZA EN LAS TRANSACCIONES ELECTRÓNICAS: LA REGULACIÓN JURÍDICO-ADMINISTRATIVA DE LAS INSTITUCIONES DE ACREDITACIÓN DE LA ACTUACIÓN ELECTRÓNICA

Tesis Doctoral dirigida por

Prof. Dr. D. Julián Valero Torrijos

D. Ignacio Alamillo Domingo

2018

A Roser, por su infinita paciencia conmigo,
que no podré compensar en una vida.

A nuestros tres hijos, por las horas robadas.

Tesis para la obtención del grado de Doctor presentada por el Licenciado IGNACIO ALAMILLO DOMINGO y realizada bajo la dirección del Prof. Dr. D. Julián Valero Torrijos, Catedrático de Derecho Administrativo de la Universidad de Murcia.

Murcia, 2018

ÍNDICE DE CONTENIDOS

ACRÓNIMOS

AENOR	Asociación Española de Normalización.
BGB	*Bürgerliches Gesetzbuch*.
CAD	Código (italiano) de la Administración Digital – *Codice dell'amministrazione digitale*, Decreto Legislativo de 7 de marzo de 2005, n. 82, modificado por Decreto Legislativo de 26 de agosto de 2016.
CCRA	*Common Criteria Recognition Agreement*.
CEF	*Connecting Europe Facility*.
CEN	*European Committe for Standardization.*
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.
CSV	Código Seguro de Verificación.
CWA	*CEN Workshop Agreement.*
Decisión de cooperación eIDAS	Decisión de Ejecución (UE) 2015/296 de la Comisión, de 24 de febrero de 2015, por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al artículo 12, apartado 7, del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Texto pertinente a efectos del EEE).
Decisión de listas de confianza eIDAS	Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
Decisión de listas de confianza ventanilla única	Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior [notificada con el número C(2009) 7806].

Decisión IDABC	Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC).
Decisión ISA	Decisión Nº 922/2009/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas (ISA) (Texto pertinente a efectos del EEE).
DFE	Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
DSP2	Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.
EA	*European Accreditation*.
eIDAS	Identificación, autenticación y firma electrónicas.
EIF	*European Interoperability Framework.*
EN	*European Norm.*
ENAC	Entidad Nacional de Acreditación.
ETSI	*European Telecommunications Standards Institute*.
HSM	*Hardware Security Module.*
IDA	*Interchange of Data between Administrations*.
IDABC	*Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens*.
IEC	*International Electrotechnical Commission.*
IETF	*Internet Engineering Task Force.*
ISO	*International Standardization Organization.*
LAE	Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

LCGC	Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación.
LCSP/2007	Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.
LCSP/2017	Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
LFE	Ley 59/2003, de 19 de diciembre, de firma electrónica.
LMCE	Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996), junto con su nuevo artículo 5 bis aprobado en 1998.
LMFE	Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001).
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LOPSC/2015	Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
LPAC	Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
LRJSP	Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
LUTICAJ	Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
MCE	Mecanismo Conectar Europa.
NTI	Norma Técnica de Interoperabilidad.
OID	*Object Identifier.*
OTP	*One Time Password.*
PDF	*Portable Document Format*.
PEGS	*PanEuropean Government Service*.
PEPS	*PanEuropean Proxy Server*.

QAA	*Quality Authentication Assurance*.
RDENI	Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
RDENS	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
RDLAE	Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
RDLFE	Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.
RDLOPD	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
Reglamento de interoperabilidad eIDAS	Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Texto pertinente a efectos del EEE).
Reglamento de normalización europea	Reglamento (UE) Nº 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión Nº 1673/2006/CE del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE).
Reglamento de seguridad eIDAS	Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Texto pertinente a efectos del EEE).

Reglamento eIDAS	Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Texto pertinente a efectos del EEE).
Reglamento etiqueta eIDAS	Reglamento de Ejecución (UE) 2015/806 de la Comisión, de 22 de mayo de 2015, por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados.
RFC	*Request For Comments.*
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
SAML	*Security Assertions Markup Language*.
SOG-IS	*Senior Officials Group Information Systems Security.*
STORK	*Secure idenTity acrOss boRders linKed*.
SVG	Ley Federal (austríaca) sobre Firmas Electrónicas y Servicios de Confianza para Transacciones Electrónicas – *Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG),* promulgada por artículo 1 de la Ley Federal de 8 de julio de 2016.
TC	*Technical Committee.*
TIC	Tecnologías de la Información y Comunicación.
TL	*Trusted List*.
TRLCSP	Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
TRLGDCU	Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
TS	*Technical Specification.*
UNE	Una Norma Española.

VDG	Ley (alemana) de Servicios de Confianza – *Vertrauensdienstegesetz* (VDG), promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017.
XML	*eXtensible Markup Language.*

INTRODUCCIÓN

Este trabajo surge de la hipótesis de que existe una relación entre la intervención del derecho público y el valor jurídico de los instrumentos que empleamos, en el entorno digital, para generar prueba de la actuación de las personas y otros hechos jurídicamente relevantes.

La digitalización de la sociedad, mediante la adopción de las tecnologías de la información y las comunicaciones –las cuales han sido frecuentemente denominadas "nuevas", con respecto a las tecnologías "viejas" del soporte papel– conduce de forma inevitable a la adaptación de las instituciones jurídicas preexistentes, de modo que se mantenga su función social en el nuevo escenario; o, alternativamente, a su sustitución por instituciones jurídicas nuevas, impulsadas por la aparición de innovaciones tecnológicas que permiten, en el espacio digital, actuaciones que eran impensables en el mundo físico, conduciendo a una mayor transformación de los procesos.

La institucionalización de la firma electrónica de documentos es buena muestra de la primera posibilidad, en que se adopta una tecnología que ofrece una funcionalidad equivalente a la firma manuscrita, aunque lógicamente las tecnologías de ambas en nada se parezcan, para su uso en aquellos documentos electrónicos o comunicaciones electrónicas en que se hubiese requerido, de ser sustanciados en soporte físico, una firma manuscrita.

Respecto a la segunda posibilidad indicada, la amortización de la tarjeta postal de acuse de recibo propia del envío postal y, por tanto, también de la notificación administrativa o judicial en soporte papel, firmada manuscritamente por el receptor de dicho envío constituye un excelente ejemplo de innovación sustitutiva. En efecto, cuando trasladamos el envío postal al entorno electrónico no será preciso mantener esta tarjeta con firma manuscrita, sino que será prueba suficiente el registro de acceso del destinatario de dicha comunicación, debidamente identificado electrónicamente; posibilidad ya acogida en nuestro ordenamiento, tanto en las notificaciones administrativas como en sus equivalentes privados, que se sustancian mediante la entrega electrónica certificada.

El objeto de interés en este trabajo orbita, pues, alrededor de las instituciones jurídicas que sirven para la acreditación de la actuación electrónica de las personas, incluyendo su régimen jurídico propio (definiciones, requisitos de validez y efectos jurídicos sustantivos y, en su caso, procesales), su régimen de utilización sectorial y, lo que es más importante, el modelo regulatorio diseñado por el legislador en orden a establecer un valor reforzado para estas instituciones, que incluye el régimen jurídico de los prestadores, eminentemente privados, que con sus servicios y productos ofrecen soporte a estas instituciones.

En un primer momento, que puede situarse en el decenio de 1995 a 2005, la firma electrónica fue objeto de estudio principalmente por parte de la doctrina mercantilista y procesalista, seguramente por sus orígenes ligados al comercio electrónico, tanto en el nivel internacional, donde son referencia ineludible los trabajos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, como en el de la, entonces, Comunidad Europea. Estas reflexiones iniciales también se extendieron a otras tecnologías que no habían sido aún institucionalizadas jurídicamente, al menos en España, como el sello de tiempo electrónico o los servicios que permitían la acreditación

de la remisión y recepción de las comunicaciones.

Se trata de un periodo que coincide con la recepción jurídica de las tecnologías de autenticación de datos, sustrato tecnológico de la institución en que la firma electrónica consiste, y el inicio de su uso en el comercio electrónico –caracterizado por un fuerte rechazo al uso de la firma electrónica avanzada basada en certificado electrónico reconocido e, incluso en mayor medida, a la firma electrónica reconocida, y la aparición de instituciones complementarias, como la del tercero de confianza–, y, de forma más tímida, también en el procedimiento administrativo electrónico.

Dicha recepción jurídica se produce de forma algo peculiar, al aprobarse en España el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica (en adelante, RDLFE), en base a la posición común relativa a la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica, norma que se aprueba sólo tres meses después –Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (en adelante, DFE)– incluyendo diferencias significativas en relación al RDLFE que no serán resueltas (y no todas) hasta la aprobación de la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE).

Las contribuciones académicas de esta primera etapa no prestaron, en mi opinión, la suficiente atención al modelo de supervisión y control de los prestadores. Aunque en la mayoría de casos se analizaron los diferentes modelos regulatorios previstos por el legislador, de configuración diversa en el RDLFE y la LFE, así como el estatuto de obligaciones de los prestadores de servicios de certificación, en dichas contribuciones no se profundizó suficientemente, a mi juicio, sobre la propia justificación de la existencia de un sistema público de supervisión y control (el porqué es preciso un régimen administrativo a estos efectos), menos aún sobre la relación que pueda presentar la existencia de este sistema en relación con el valor reforzado de la firma electrónica (qué aporta la existencia de este régimen a la prueba).

Con algo de posterioridad, motivada por la progresiva adopción de estos mecanismos y servicios en el ámbito del sector público, una parte de la doctrina administrativa que, con gran visión de futuro, decidió abordar los retos del que se convertiría en el único procedimiento administrativo, aportó una segunda gran oleada de contribuciones alrededor de las instituciones de acreditación electrónica de la actuación, estudiando la problemática que genera su uso para la actividad administrativa.

Esta reflexión se intensifica con la aprobación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (en adelante, LAE) y su normativa de desarrollo, tanto en el ámbito de la Administración General del Estado cuanto en diversas Comunidades Autónomas y en la Administración Local, todas ellas en el marco de la importantísima normativa común de interoperabilidad y seguridad dictada al albur de la LAE.

Se trata de una reflexión que ha resultado de extraordinaria relevancia, dado que, a diferencia del sector privado, la firma electrónica avanzada basada en certificado reconocido iba a constituir un verdadero derecho de los ciudadanos en sus relaciones con el sector público, tanto en el ámbito administrativo, como en el judicial, derecho que se iba a ejercer de forma correlativa a la obligación de relacionarse de forma exclusivamente electrónica con dichas entidades que progresivamente se ha extendido a gran parte de

ciudadanos, en especial personas jurídicas y profesionales.

Por ello, no es arriesgado afirmar que la administración electrónica ha sido el sector en que se ha realizado un mayor grado de uso de los certificados electrónicos, incluso cuando la reforma del sector público, sustanciada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPAC) y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP), ha apostado por una mayor neutralidad y flexibilidad en el uso de estas instituciones en la actividad administrativa.

Estas contribuciones, enfocadas en las complejas particularidades que presentan las instituciones de acreditación electrónica de la actuación por parte de los interesados, de los órganos administrativos y del personal al servicio de la Administración, que plantean retos de extraordinario interés para la transformación de la actividad administrativa y el modelo de relación interadministrativa, no han abordado, tampoco, el estudio del papel que juega el Derecho administrativo en relación con la eficacia jurídica de estas instituciones.

Con la aparición del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS), se ha ampliado el número de instituciones jurídicas para la acreditación de la actuación que, además de la firma electrónica de persona física, ahora incluye el sello electrónico de persona jurídica, el sello de tiempo electrónico, la entrega electrónica y la autenticación de sitio web.

El Reglamento eIDAS ha adoptado un enfoque de armonización, al objeto de eliminar las numerosas disfunciones identificadas en relación con la DFE, principalmente producidas por la trasposición en sede nacional, en especial en el ámbito de la Administración electrónica y su dimensión transfronteriza, pero también para crear un marco jurídico común a todos los servicios que aportan confianza a las transacciones, algo que resulta imprescindible para lograr un Mercado Único Digital que funcione correctamente.

En el Reglamento eIDAS se apuesta, en reacción al marco anterior, por un régimen de control previo y reforzado en relación con las modalidades "cualificadas" de la mayoría de instituciones jurídicas de acreditación de la actuación electrónica, que constituye una base fundamental para la confianza que en los mismos depositan ciudadanos e instituciones, creando un segundo régimen jurídico específicamente diseñado para el reconocimiento transfronterizo de los sistemas de identificación electrónica utilizados por los Estados miembros.

De todo ello nace un reduplicado interés por el estudio de las estructuras jurídicas reguladoras de las instituciones jurídicas de acreditación de la actuación electrónica, incluyendo las actualmente previstas pero también aquéllas que en el futuro puedan aparecer, posiblemente en los Estados miembros, y que con una elevada probabilidad acabarán por incorporarse al acervo de la Unión, siguiendo la misma lógica de reconocimiento transfronterizo interoperable que actualmente informa el Reglamento eIDAS.

Una lectura inicial de la normativa, que vamos a analizar en este trabajo, ya genera la intuición de que existe una conexión profunda entre los efectos jurídicos de las instituciones jurídicas de acreditación de la actuación electrónica y la intervención del Estado mediante un régimen de supervisión y control; como si, de algún modo, este

régimen de Derecho administrativo fuera consustancial al otorgamiento de una cierta fehaciencia probatoria de dicha actuación, establecida por vía de presunción legal, sea en el Derecho de la Unión o en las legislaciones nacionales.

Si ello es así, podríamos afirmar que la eficacia de estas pruebas tecnológicas depende del correcto funcionamiento de estas estructuras normativas, pero también debería preocuparnos que las presunciones que se puedan establecer sean apropiadas, dado que podrían eventualmente afectar al derecho constitucionalmente garantizado a la tutela judicial efectiva.

Ello es así porque estas instituciones jurídicas se corresponden con fuentes de prueba electrónica –no con los medios de prueba previstos en la legislación procesal– que van a producir una especial eficacia, invirtiendo la carga de la prueba en cuanto a las actuaciones y hechos que acrediten. De lo cual se deduce, incluso de forma intuitiva, que esa inversión de la carga de la prueba, ese efecto procesal de la institución, sólo debe producirse cuando existen garantías objetivas que lo justifiquen, y no en caso contrario.

También podemos intuir que no es ésta la única justificación para la existencia de las actuales estructuras normativas de las instituciones de acreditación de la actuación electrónica, sino que también presenta una gran importancia la protección de los usuarios de los servicios sin cualificación y, también, garantizar un nivel adecuado de interoperabilidad de dichas instituciones en el territorio de la Unión.

Por tanto, y sin perjuicio del indudable interés que presenta conocer el elenco de instituciones jurídicas empleadas para la acreditación de la actuación electrónica, será objeto de especial interés caracterizar el papel específico que cumplen las diferentes modalidades de intervención administrativa, en orden a poder realizar una valoración global crítica sobre la adecuación de este modelo a las premisas anteriormente expuestas y, en su caso, realizar propuestas.

No se ha abordado en este trabajo el estudio de todas las cuestiones relacionadas con la prestación de los servicios de confianza, por considerarse tangenciales al objeto que acabamos de exponer, sin afectación al mismo. En concreto, se ha considerado innecesario abordar el estudio acerca del régimen de responsabilidad por la prestación de servicios de confianza, dado que, por otra parte, resultan plenamente vigentes las aportaciones doctrinales realizadas con ocasión de los servicios de certificación regulados en la DFE y la LFE.

Tampoco se han estudiado las cuestiones referidas a la responsabilidad patrimonial de la Administración que pudieran darse en relación con sus actividades de supervisión, ni en relación con la expedición o uso de sistemas de identificación ni por el uso de las restantes instituciones de acreditación, dignas de una investigación específica al respecto. No se ha procedido, finalmente, al estudio detallado de dos instituciones de acreditación de la actuación electrónica, muy novedosas, principalmente debido a su escasa madurez y grado actual de adopción.

Conforme a cuanto se acaba de exponer, el trabajo se ha estructurado en siete Capítulos y unas conclusiones finales.

En el primer Capítulo presentamos las instituciones jurídicas que se emplean para la acreditación de la actuación electrónica, sin perjuicio de que las mismas se puedan emplear, también, para la acreditación de otros hechos jurídicamente relevantes; así como el modelo regulatorio de los servicios de confianza.

En los Capítulos segundo a quinto estudiamos las tres principales instituciones de acreditación de la actuación electrónica; a saber, la identificación electrónica, la firma electrónica de persona física y el sello electrónico de persona jurídica. En este sentido, en el Capítulo segundo se caracterizan los servicios de identificación y autenticación electrónicas, presentándose aquéllos basados en los tres servicios de confianza de expedición de certificados, y también los servicios públicos establecidos en España para dicho propósito; mientras que, en el tercero, se presenta el uso de estos mismos medios de identificación para el acceso transfronterizo a los servicios públicos en los Estados miembros de la Unión y, en su caso, también servicios privados. A continuación, en el Capítulo cuarto se estudia en profundidad el régimen jurídico general de la firma electrónica y del sello electrónico, y también se presentan los tres servicios de confianza en soporte de estas instituciones de prueba electrónica; a saber, la creación, la validación y la conservación de la firma electrónica y del sello electrónico; para abordarse, en el quinto Capítulo, las regulaciones sectoriales del uso la firma electrónica y el sello electrónico, tanto en el sector privado cuanto en el ámbito del sector público español, con mucho la más significativa.

Por último, en los Capítulos finales se trata el régimen jurídico general aplicable a los prestadores de servicios de confianza. De este modo, el Capítulo sexto se ocupa del estatuto jurídico de prestación de servicios de confianza, diferenciando las obligaciones comunes a todos los servicios de aquéllas que únicamente aplican a los servicios cualificados; ocupándose el séptimo y último Capítulo del régimen de supervisión y control aplicable a dichos servicios.

Finalmente, respecto a la metodología empleada para la realización de la investigación, resulta preciso hacer notar que se ha adoptado un enfoque basado en la combinación del análisis de las fuentes normativas, tanto jurídicas como técnicas, dado que ambas son imprescindibles para comprender el modelo regulatorio de estas instituciones, con las aportaciones de la doctrina científica y de la experiencia práctica derivada de la realización de proyectos reales para diversos prestadores de servicios de confianza que han debido obtener la cualificación de sus servicios conforme al Reglamento eIDAS, así como una larga experiencia previa, superior a veinte años, como profesional de este sector.

Se trata, por tanto, de una aproximación al objeto de estudio muy cercana a la práctica profesional, que ha buscado no sólo la explicación teórica del modelo regulatorio de estas instituciones, sino asimismo explorar su aplicabilidad inmediata para ofrecer soluciones fundadas a los problemas y desafíos a los que se han de enfrentar los actores que participan en este mercado.

CAPÍTULO 1. LAS INSTITUCIONES JURÍDICAS DE ACREDITACIÓN DE LA ACTUACIÓN ELECTRÓNICA Y LOS SERVICIOS QUE LAS SUSTENTAN

En este primer Capítulo nos proponemos presentar los aspectos más generales de nuestro objeto de estudio, que son las instituciones jurídicas creadas para la acreditación de la actuación electrónica, en general.

La legislación que ha regulado la acreditación de la actuación electrónica, sus efectos y sus garantías, parte de la existencia de mecanismos y de servicios de seguridad[1] en el ámbito de las tecnologías de la información y la comunicación, para construir un modelo en el que, dependiendo del uso que se haga de una parte de los mismos –entre otros muchos factores–, se establecen determinadas consecuencias jurídicas.

Como es lógico, la juridificación[2] o normativización legal se produce a partir de una realidad previa[3], que en este caso presenta una gran amplitud y riqueza, y en relación con la cual se determinarán reglas imperativas –de mandato, de prohibición– y otros tipos de reglas –de consenso, de interoperabilidad…– en función de muchos parámetros, entre los cuales indudablemente ideológicos y sociológicos, como ha mostrado de forma clara el tridimensionalismo jurídico[4].

Podemos, por tanto, afirmar que se ha producido una verdadera recepción jurídica de estas tecnologías, en respuesta a la progresiva extensión de su uso, que ha resultado en la creación de verdaderas instituciones jurídicas, tributarias de la realidad tecnológica de la que proceden[5], de la que son una abstracción legal.

Por ello, nuestro análisis deberá considerar también la autorregulación que el sector tecnológico ha venido creando desde hace ya bastantes años, fuera del sistema formal de fuentes del Derecho, pero de indudable valor regulador, en especial desde una concepción sociológica de lo normativo, que se muestra con especial intensidad en el modelo

[1] Se suele hablar de servicios de la seguridad de la información, de seguridad informática o de las TIC o, más recientemente, de servicios de ciberseguridad, términos todos ellos extraordinariamente relacionados, y que plasman dimensiones diferentes de una misma realidad.

[2] Para el Real Diccionario de la Lengua, juridificar es "regular en derecho una situación anteriormente no prevista en las normas".

[3] Se suele decir, y no sin razón, que el Derecho siempre va detrás de la realidad. No es excepción, desde luego, nuestro objeto de estudio.

[4] Para Miguel Reale, citado por (García Medina, 1995, pág. 20), "debemos entender el término derecho tanto como expresión del valor delo que es justo, como norma ordenadora de conducta, e incluso como hecho social e histórico", por lo que "[e]n definitiva, y combinando esas posibles apreciaciones de la palabra derecho, debemos concluir que el Derecho tiene una estructura tridimensional, en la que la norma se encargará de la regulación de las actividades tanto individuales como colectivas, teniendo siempre en cuenta las distintas circunstancias fácticas u orientándose a la realización de ciertos y concretos valores".

[5] Se trata de un buen ejemplo de "la fuerza normativa de lo fáctico" (Blanquer, 2006, pág. 408). Como es lógico y razonable, sólo nos centraremos en presentar aquellos servicios y técnicas de seguridad de la información que se han sido objeto del reconocimiento o la institucionalización por el Derecho.

regulador de estas instituciones[6], caracterizado por un intenso protagonismo de las normas técnicas.

Este Capítulo se estructura en cuatro epígrafes. En el primero de ellos, nos centraremos en el ya aludido proceso de institucionalización jurídica de los mecanismos y servicios de seguridad de las tecnologías de la información empleados en la acreditación de la actuación electrónica de las personas, que necesariamente inscribimos en nuestro entorno, que no es otro que el de la Unión Europea. En este sentido, y dado que este proceso no ha sido, en términos históricos, lineal ni homogéneo, presentaremos la recepción jurídica de las tecnologías para la autenticación de los datos, la primera que aparece en el nivel europeo, y posteriormente, la recepción jurídica de las tecnologías, adicionales a las anteriores, para la autenticación de entidades. Este primer epígrafe también presenta, por su influencia en el proceso de institucionalización jurídica a que nos estamos refiriendo, las iniciativas referidas a la interoperabilidad lideradas desde el ejecutivo comunitario en orden a la construcción y correcto funcionamiento del Mercado Único Digital.

En el segundo epígrafe de este Capítulo, presentaremos el concepto de identificación electrónica institucionalizado en la normativa europea, el alcance de la regulación armonizada en el nivel de la Unión y sus relaciones con los Derechos nacionales; tratamiento que se realiza de forma individualizada para reflejar que esta institución recibe un régimen netamente diferenciado del de las restantes instituciones jurídicas para la acreditación de la actuación electrónica, y que se agrupan en la categoría de servicios de confianza.

Precisamente, la presentación de estos servicios de confianza se realiza en el epígrafe tercero de este Capítulo, en el que se introduce su caracterización en la normativa de la Unión, que armoniza en gran medida el régimen aplicable a estos servicios, y se discute el aparente descuadre de la identificación electrónica a la luz de la aludida caracterización. En el mismo epígrafe se analiza el modelo regulatorio diseñado por el legislador de la Unión en relación con los servicios de confianza, y la posibilidad de que, en el nivel nacional, se puedan regular otros servicios de confianza.

Finalmente, el cuarto epígrafe de este Capítulo se dedica a presentar a los diferentes actores de este modelo regulatorio, un marco de gobernanza multinivel, incluyendo al prestador del servicio y a los agentes públicos y privados que intervienen en el mismo, con especial detalle de las competencias de cada uno de éstos, buena muestra de la complejidad de la construcción de los bloques fundamentales que deben sustentar el correcto funcionamiento del Mercado Único Digital a que antes nos hemos referido.

1.1 LA INSTITUCIONALIZACIÓN JURÍDICA DE LOS MECANISMOS Y SERVICIOS DE SEGURIDAD DE LAS TIC PARA LA ACREDITACIÓN ELECTRÓNICA DE LA ACTUACIÓN

El 23 de julio de 2014 el Consejo de la Unión Europea aprobó en lectura única el Reglamento (UE) Nº 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, el

[6] Esto es así especialmente en el caso de los denominados "servicios de confianza". Sobre su modelo regulador, cfr. el epígrafe 1.3.2 de este trabajo.

"Reglamento eIDAS"), un importante y transformador[7] hito en la juridificación de las garantías del tráfico jurídico sustanciado electrónicamente.

Dicho Reglamento tiene, conforme declara su artículo 1, un objeto triple y aparentemente heterogéneo, en cuya virtud "a) establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro, b) establece normas para los servicios de confianza, en particular para las transacciones electrónicas, y c) establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web".

Los numerales a) y c) del artículo 1 enumeran diferentes tipos de "pruebas electrónicas" de la actuación de las personas –o de los sistemas informáticos que las mismas utilizan, inclusive sin intervención directa en cada caso singular–, posicionando el Reglamento como norma fundamental de la acreditación electrónica de la actuación jurídicamente relevante, de alcance general y no sectorial[8], en especial en las transacciones en el mercado interior, aunque no se limita exclusivamente a las mismas.

En efecto, las instituciones jurídicas[9] enumeradas en estos dos numerales –el medio de identificación electrónica de persona física o jurídica, la firma electrónica de persona física[10], el sello electrónico de persona jurídica, el sello de tiempo electrónico, la certificación de la entrega electrónica y la autenticación de sitio web– se corresponden con artefactos técnicos que permiten la acreditación de actos, pero también de otros hechos[11], con una indudable relevancia probatoria en el ámbito electrónico; esto es, son

---

[7] Para (De Miguel Asensio, 2015, págs. 969-970) destaca "[l]a profunda transformación del modelo previo […] por el abandono como instrumento normativo de la directiva y su sustitución por un reglamento, de modo que el nuevo marco jurídico resulta directamente aplicable en todos los Estados miembros", así como que "el Reglamento 910/2014 responde en su contenido a una orientación sustancialmente diferente a la que inspiró la Directiva", dado que, además de la firma electrónica, "comprende en su objeto otros mecanismos de gran relevancia para la seguridad, confianza y fiabilidad del comercio electrónico, como es el caso de los sellos electrónicos y de la autenticación de sitios web".

[8] (Illescas Ortíz, 2001, pág. 89) ya hizo notar, aunque en relación en el RDLFE que "no estamos por consiguiente ante una norma destinada en exclusiva a regular el C-E sino a reconocer jurídicamente un nuevo soporte, distinto del oral o del escrito, hábil para la emisión de declaraciones de voluntad y de ciencia por parte de las personas".

[9] Empleamos el término de institución jurídica en el sentido indicado por (Boer, 2009, pág. 89 y ss.), que se refiere a la ley como una institución cuyo propósito principal es crear un orden normativizado mediante la formalización –el autor se adhiere a la concepción de (MacCormick, 1998)–, lo cual sucede normalmente cuando el orden normativo informal, que suele aparecer de forma espontánea, fracasa en alcanzar sus objetivos pretendidos. En el sentido expuesto, podemos ver la firma electrónica como una institución relativa al orden normativo establecido por la ley.

[10] (Galindo, 1998, pág. 99) identifica a la firma digital como una "institución de confianza", si bien también emplea el término para referirse a las autoridades de certificación y de registro. También (Couto Calviño, 2007, pág. 6) indica que "cuando hablamos de firma electrónica nos encontramos ante una verdadera institución jurídica, singular y autónoma, netamente diversa de la firma manuscrita, sujeta a un régimen peculiar, legal o convencional".

[11] Sobre los diferentes tipos de hechos, cfr. (Blanquer, 2006, pág. 76 y ss.).

artefactos que sustentan la prueba electrónica[12], de modo funcionalmente análogo a como ha venido sucediendo en el mundo físico, en especial en las transacciones acreditadas mediante el uso del soporte papel.

Así, mientras que la firma electrónica, al resultar equivalente a la firma manuscrita, acredita el hecho en el que un acto jurídico consiste (la emisión de una declaración de voluntad, por ejemplo), el sello de tiempo electrónico, al vincular una serie de datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante, acredita un hecho bruto, del mundo físico[13], que permitirá sustentar, en su caso, un hecho jurídico o institucional concreto (la emisión de dicha declaración antes de un momento concreto, a determinados efectos legalmente previstos).

A estas instituciones nos vamos a referir como fuentes de prueba electrónica[14] desde un punto de vista procesal, para diferenciar su régimen jurídico propio de la regulación de los medios de prueba prevista en las leyes procesales. Basta con decir ahora[15] que se trata de instituciones jurídicas que nacen de la existencia de mecanismos y servicios de seguridad tecnológica referidos a la autenticidad de entidad, del origen de los datos, de la integridad y en soporte del no-repudio o no-rechazo, con la finalidad de que dichas tecnologías puedan gozar de un reconocimiento jurídico que permita su uso en sustitución de sus correlatos en soporte papel. Por este motivo, y para diferenciarlas de otras finalidades de uso de las mismas tecnologías, nos referimos a ellas, colectivamente, como instituciones de acreditación de la actuación electrónica[16].

Cuando decimos que estas instituciones se corresponden con artefactos técnicos que constituyen fuentes de prueba electrónica lo hacemos en el mismo sentido que, en realidad, ya sucede con las tradicionales fuentes de prueba "no electrónica". En efecto, el trazo en el que consiste una firma manuscrita es un artefacto técnico[17], por más que se

---

[12] Hay que aclarar ya en este momento que nos estamos centrando en el ámbito del objeto de la prueba, que se refiere a los hechos, aunque parte de la doctrina considera que el verdadero objeto de la prueba es, realmente, las afirmaciones de las partes respecto a los hechos, debiéndose entender que "[l]a palabra *hechos* se está empleando aquí en su sentido más amplio, comprendiendo todo lo que por el derecho material puede establecerse como contenido del supuesto fáctico de una consecuencia" (Montero Aroca, 2007, pág. 70 y ss.).

[13] Esto explica que en la legislación belga se diga, en relación con el sello de tiempo electrónico, que el mismo no confiere fecha cierta, sin perjuicio de lo previsto en el artículo 1328 del Código Civil, puesto que en realidad el sello de tiempo sólo acredita la existencia de esta declaración cuando se pone el sello, pero no puede acreditar cuándo se emitió. Se puede ver, de forma clara en este ejemplo, la diferencia entre el hecho en bruto y el hecho jurídico.

[14] Como explica (Montero Aroca, 2007, pág. 151), "[l]as partes en sus actos de alegación realizan afirmaciones de hechos y la prueba de esas afirmaciones no podrá lograrse si no se cuenta con algo que, preexistiendo al proceso, puede luego introducirse en éste", por lo que "[c]onceptualmente hay que distinguir, pues, entre lo que ya existe en la realidad (fuente) y el cómo se aporta al proceso (medio) con el fin de obtener el certeza del juzgador", por lo que "[f]uente es un concepto extrajurídico, metajurídico a a-jurídico, que se corresponde forzosamente con una realidad anterior al proceso y extraña al mismo; mientras que medio es un concepto jurídico y, más específicamente, procesal".

[15] En posteriores Capítulos de este trabajo procederemos al estudio detallado de cada una de estas instituciones jurídicas, por evidentes razones metodológicas.

[16] No se trata, en este momento, de crear un concepto formal y acabado, sino que emplear una categoría conceptual que nos permite agrupar estas instituciones en atención a su uso.

[17] Resulta innegable que la firma manuscrita es también un artefacto técnico, aunque el mismo se encuentre

base en la tecnología de la tinta y el papel, a la que tan acostumbrados estamos, y que ha sido claramente institucionalizado jurídicamente. Igualmente, los documentos acreditativos de la identidad constituyen artefactos físicos con mayores o menores medidas de seguridad, diseñados para su exhibición personal en procesos que exigen la determinación de dicha identidad[18].

Sin embargo, es preciso llamar ya la atención sobre dos cuestiones, sobre las que volveremos más adelante. En primer lugar, el diferente objeto del Reglamento eIDAS en relación con el medio de identificación y las restantes fuentes de prueba electrónica[19]; mientras que en el primer caso el objeto de la norma se limita a "las condiciones en que los Estados miembros deberán reconocer los medios […] pertenecientes a un sistema […] notificado de otro Estado miembro", en el segundo el objeto es el "marco jurídico para" dichas pruebas electrónicas, incluidos los documentos electrónicos.

En ambos casos, además, el artículo 46 del Reglamento eIDAS ordena taxativamente que "[n]o se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en formato electrónico", una referencia que refuerza claramente la finalidad de la norma de sustentar la prueba de la actuación electrónica, cuya fuente y medio más reconocido es, precisamente, el documento[20].

En segundo lugar, el numeral b) del artículo 1 del Reglamento eIDAS se refiere al establecimiento de "normas para los servicios de confianza, en particular para las transacciones electrónicas"[21], anunciando la conexión entre las fuentes de prueba

---

basado en la tecnología de la escritura personal, de la autografía. Ciertamente se trata de una tecnología, creada a lo largo de un periodo histórico, y que tenemos absolutamente interiorizada. (Fraenkel, 2008, p. 17) caracteriza la firma manuscrita como un "signo notable, que combina cuatro elementos: la función individualizadora de un nombre propio, el efecto de presencia de un grafismo trazado por la mano, la prominencia visual de un signo personal y la fuerza de un acto de lenguaje" (la traducción es mía). (Muñoz Machado, 2000, pág. 119) inicia su reflexión sobre la firma electrónica recordando que "[e]l soporte papel sustituyó al apretón de manos y a la palabra dada, que eran ley en los pequeños y grandes contratos de la sociedad agraria; cuando el conocimiento directo entre los contratantes desapareció, las normas aplicables a cada contrato se hicieron más precisas, exigiendo para algunos de ellos la forma escrita".

[18] Por ello, podemos caracterizar la identidad digital como "un artefacto humano, un documento electrónico con una serie de informaciones referidas a una personal –no la persona en sí– emitido por la propia persona o per terceros, incluyendo al Estado, organizaciones públicas y privadas, y otros ciudadanos" (Alamillo Domingo, 2010a, pág. 19), en una visión bastante más amplia que la recogida en el Reglamento eIDAS.

[19] (Graux, 2011, pp. 21-22) se ha referido a todos estos servicios como "servicios de autenticación electrónica", entre los que incluye la "identificación cualificada", en su estudio sobre una posible evolución de la DFE.

[20] Aquí empleo la noción de documento en un sentido muy amplio, que incluye también los contenidos de las comunicaciones o mensajes de datos. (Rodríguez Ayuso, 2018, pág. 80) también adopta esta visión muy amplia del "documento como contenido", prescindiendo del soporte físico continente del mismo como elemento necesario del mismo.

[21] No resulta tan evidente como pueda parecer que deba existir un marco regulador de las actividades del denominado, en sentido amplio, como comercio electrónico. Para (Ortega Díaz, 2008, pág. 28), "[a] pesar de las tendencias libertarias que se preconizaban, y aún preconizan, que el espacio virtual debe ser un espacio pleno de libertad donde no debe existir ningún tipo de regulación ni control, olvidando que la auténtica libertad se fundamenta en el concepto de seguridad, lo cierto es que la existencia de un marco jurídico que generara confianza en este nuevo espacio virtual se manifestaba como una necesidad incontestable".

electrónica –así como de su validez y efectos– y los servicios de confianza que las van a sustentar, servicios que podemos adelantar se confían eminentemente al sector privado[22] y tienen un marcado carácter de actividad económica mercantil.

El Reglamento eIDAS no es, en absoluto, la primera norma jurídica que regula la prestación de los servicios a que nos acabamos de referir. En efecto, el citado Reglamento no es el punto de partida en la institucionalización legal de las fuentes de prueba electrónica, sino que parte de la existencia de importantes antecedentes –tanto en el nivel nacional, como en el nivel de integración europea, y desde luego en el plano internacional– que han influido decisivamente en la normativa actual[23].

Tampoco es, desde luego, el punto final de recepción jurídica de estas fuentes de prueba, porque el imparable proceso de innovación tecnológica ya ha superado las instituciones y servicios regulados en el mismo. Así sucede con novedosos servicios electrónicos regulados en sede nacional en conexión con la prueba electrónica[24], y también con las tecnologías de registro distribuido, como *blockchain*[25], que basándose igualmente en criptografía de clave pública –pero no en certificados, mucho menos conformes con las prescripciones del Reglamento eIDAS–, permite la creación de un suerte de libro mayor inalterable y gestionado de forma absolutamente descentralizada[26] que puede emplearse

[22] Se trata de un modelo que encaja bien en el denominado Estado garante, en contraposición al Estado prestaciona, y que se caracteriza por el protagonismo de la actividad de garantía –y de la actividad de regulación, subespecie de la anterior– en relación con prestaciones entregadas al mercado que, de otro modo, hubieran sido retenidas por el Estado. Como ha dicho (Esteve Pardo, 2015, pág. 26), "[l]a función que le cumple a la actividad garante es la de mantener o recuperar la atención de los intereses generales en sectores y actuaciones situados de lleno bajo la iniciativa y dirección privada pero que tienen una dimensión pública por afectar a estos intereses", lo que a mi juicio resulta plenamente aplicable a lo que, en definitiva, no deja de ser un modelo de privatización de las fuentes de prueba electrónica. Para (Gamero Casado, 2015, págs. 118-119), "[e]n la actual tesitura la Administración recibe mandatos contradictorios: por una parte se desea que su interferencia sea mínima, pero al mismo tiempo se le responsabiliza de cualquier fallo del sistema y se le atribuye una capacidad salvadora ilimitada […] De tal manera que la dogmática clásica del Derecho Administrativo, asentada sobre la potestad, el acto unilateral y el monopolio, desplaza sustancialmente su centro de gravedad como consecuencia de una reinterpretación del papel que corresponde al poder público en general y a la Administración en particular, incorporando en su lugar las técnicas y potestades de ordenación de la economía generadas en el ordenamiento norteamericano, conocidas como *regulación*".

[23] En efecto, hay que reconocer ya que el Reglamento eIDAS es, igual que anteriormente su Directiva antecedente, tributario de las normas nacionales, que son las que producen el proceso inicial de institucionalización jurídica de los mecanismos y servicios de seguridad objeto de nuestro estudio. Si nos interesa especialmente el proceso de institucionalización en el nivel europeo es, en parte, por el parejo proceso de desestatalización de las fuentes de prueba electrónica que viene a suponer, derivada de la conexión de estos instrumentos con las necesidades del Mercado Único Digital, que ha sido observado por la doctrina el hilo del fenómeno de aparición del denominado Derecho Administrativo Global, como por ejemplo puede verse en (Darnaculleta Gardella, 2016, pág. 22 y ss.).

[24] Como, por ejemplo, el archivo electrónico seguro de documentos, ya regulado en Bélgica y Francia.

[25] Para una introducción técnica detallada del funcionamiento de este sistema aplicado a la criptomoneda Bitcoin, cfr. (Nakamoto, 2008), *in toto*. Aunque el sistema de cadenas de bloques se desarrolla inicialmente en este ámbito de aplicación en concreto, se puede emplear para cualquier otro tipo de transacción.

[26] (Swan, 2016, pág. 186) caracteriza la tecnología de cadenas de bloques como un protocolo de software y un libro de registro distribuido para registrar transacciones, que puede actuar como sustrato computacional a escala global para el procesamiento de cualquier tipo de actividad digitalizada. La tecnología de cadenas de bloques permite la actualización de todos los nodos de una red en un entorno de computación distribuida con el estado actual del mundo, por lo que permite conferir un estado compartido

para la acreditación de la actuación por vía electrónica.

Pero sí podemos decir que el Reglamento eIDAS supone un hito más que notable en este proceso de institucionalización jurídica de los mecanismos de acreditación de la actuación electrónica en que consisten estas fuentes de prueba electrónica, y los servicios en que las mismas se sustentan; en especial atendiendo a los grandes objetivos que subyacen a su aprobación[27].

En cualquier caso, no resulta del todo innecesario decir que el Reglamento emplea profusamente el término "confianza", pero lo hace de forma muy específica, muy enfocada en una categoría de servicios prestados por vía electrónica que, de algún modo, aportan confianza a las transacciones, sin abordar otras dimensiones de este fenómeno, ampliamente analizadas, especialmente desde la sociología del riesgo y la seguridad[28].

1.1.1 La recepción jurídica de las tecnologías de autenticación del origen de los datos

Desde una óptica estrictamente cronológica, podemos observar cómo el Derecho regula, inicialmente[29], los mecanismos y servicios de seguridad de las tecnologías de la información y las comunicaciones que se emplean para la autenticación del origen de los datos[30], que frecuentemente permiten también la garantía de la integridad de los mismos datos[31].

En relación con estas tecnologías, el antecedente más directo del Reglamento eIDAS se encuentra, en el nivel de la Unión Europea, en la Directiva 1999/93/CE, del Parlamento

---

de confianza a un sistema distribuido. Para esta autora, "una cadena de bloques es como un gigantesco documento de hoja de cálculo interactiva de Google que cualquier persona puede ver bajo demanda, donde administradores independientes (mineros) verifican y actualizan constantemente el libro para confirmar que cada transacción es válida. Se denomina cadena de bloques porque se publican secuencialmente bloques o lotes de transacciones a un libro mayor, de forma que se crea una cadena de bloques. El resultado es la creación de una red segura en la que se puede, de forma independiente, confirmar cada transacción como única y válida sin la intervención de un intermediario centralizado como un banco, un gobierno u otra institución" (la traducción es mía), por lo que se trata de un sistema que ya no se basa en la confianza entre las partes, sino en el propio sistema de cadenas de bloques.

[27] Para (Gobert, 2015, p. 4 y ss.), el Reglamento eIDAS presenta tres grandes objetivos; a saber, remover obstáculos al funcionamiento del mercado interior; reforzar la confianza y, finalmente, reforzar la seguridad jurídica.

[28] Como, por ejemplo, puede verse en (Pelletan, 2017) *in toto*, que contrapone la dialéctica de la sociedad de la seguridad frente a la sociedad de la confianza.

[29] (De Miguel Asensio, 2015, pág. 958) ha indicado que "[e]l empleo efectivo de muchas de las posibilidades de comunicación de Internet aparece subordinado a la presencia de mecanismos que permitan comprobar el origen y la integridad de los datos comunicados, así como acreditar la identidad del transmitente y, en ocasiones, manifestar su voluntad de formular la declaración contenida en la información", por lo que considera que "[a]nte esa realidad no resulta extraño que el sector de las firmas electrónicas es el que fue objeto de una regulación más temprana en el conjunto de las actividades relacionadas con Internet, tanto en el ámbito estatal, como comunitario europeo e internacional".

[30] Puede verse una completa introducción a estas tecnologías en los Anexos A.3.1, en cuanto a su concepto y diferenciación de la autenticación de entidades, y A.5, en cuanto al denominado "no repudio", ambos de este trabajo.

[31] En relación con la misma, cfr. el Anexo A.4 de este trabajo.

Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica (en adelante, DFE), a la que de hecho ha derogado mediante su artículo 50.1, con efecto de 1 de julio de 2016[32].

A la DFE nos referiremos a lo largo del trabajo, pero antes conviene mencionar un antecedente más lejano, puesto que en cierto modo también lo fue de la citada Directiva, que es la importante Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para la Codificación del Derecho Mercantil Internacional (en adelante, CNUDMI) en 1996[33] (en adelante, LMCE), a partir de la cual se decide incluir en el programa de trabajo de la CNUDMI las cuestiones referidas a las firmas numéricas y las entidades certificadoras, con el objetivo de preparar legislación uniforme sobre los siguientes aspectos: la base jurídica que sustenta los procesos de certificación, incluida la tecnología incipiente de autenticación y certificación digitales; la aplicabilidad del proceso de certificación; la asignación del riesgo y la responsabilidad de los usuarios, proveedores y terceros en el contexto del uso de técnicas de certificación; las cuestiones concretas relativas a la certificación mediante el uso de registros y la incorporación por remisión[34]; propuesta que se concretó en la Ley Modelo de Firma Electrónica (en adelante, LMFE), de 2001.

Nos encontramos en un momento en el que la tecnología de autenticación –de entidades, pero también de mensajes de datos; esto es, documentos electrónicos– se encontraba ya disponible y presentaba un grado importante de normalización técnica dentro de la (hoy) Unión Internacional de Telecomunicaciones, organismo de Naciones Unidas especializado en las TIC, por lo que existía la expectativa de que se produciría un incremento significativo de su uso, especialmente con el advenimiento de las relaciones comerciales en la era de los proveedores de servicios de información[35].

Además, existía ya un mercado incipiente de autoridades de certificación en diversos Estados; entre ellos, España, con entidades como la Fábrica Nacional de Moneda y Timbre (FNMT)[36], la entidad financiera Banesto[37] o la Agencia de Certificación Electrónica (ACE)[38], que en 1997 se encontraban ya plenamente operativas.

En consecuencia, los Estados percibían que la promulgación de leyes sobre firmas digitales y que reconocieran la actividad de las autoridades de certificación podía ser un elemento esencial para el desarrollo del comercio electrónico, así como la posibilidad de

---

[32] Conforme al epígrafe 2 del mismo artículo 50, todas las referencias que se realicen a la DFE deben entenderse desde dicha fecha realizadas al Reglamento eIDAS, de modo que una norma sustituye a la otra.

[33] La LMCE fue aprobada por la CNUDMI en su 29º período de sesiones.

[34] Cfr. la Guía para la incorporación de la Ley Modelo de Firma Electrónica, página 14.

[35] Cfr. documento A/CN.9/421, página 28.

[36] En el caso de la Fábrica Nacional de Moneda y Timbre, entidad pública empresarial, cfr. el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

[37] Esta entidad financiera fue la primera entidad en expedir certificados de propósito general a sus clientes, y mantuvo su actividad hasta 2013, en que cesa la misma debido a la absorción de la entidad financiera dentro del Banco Santander. Cfr. http://ca.banesto.es/index.htm

[38] ACE era una compañía de titularidad compartida entre Telefónica y los tres procesadores de medios de pago españoles, y fue la primera entidad española dedicada a la prestación de servicios de certificación para transacciones electrónicas seguras (de acuerdo con el protocolo SET, de Visa y Mastercard).

que en el marco de Naciones Unidas se pudiera intentar armonizar las nuevas leyes de firma digital[39], o al menos establecer principios comunes en este campo, proporcionando una infraestructura internacional a dicha actividad[40].

Como se puede ver, y desde una óptica eminentemente política, se consideró la necesidad de crear instituciones jurídicas reguladoras de las garantías de seguridad de la actuación electrónica, si bien alrededor del concepto troncal de autenticación del documento[41].

Se trataba de una cuestión que que constituía un reto importante[42], sin que tampoco se pueda ignorar, sin caer en la más evidente ingenuidad, el indudable interés de los Estados en moldear el funcionamiento de las técnicas criptográficas en las redes[43].

---

[39] Se suele considerar al Acta de Firma Digital de Utah como la primera legislación de firma electrónica, que adoptaba un enfoque tecnológico concreto, no neutral, pero que sigue percibiéndose en la legislación posterior, incluida la europea. Sobre esta ley, en cuanto a este modelo de regulación y su crítica, cfr. (Richards, 1999) y, en la doctrina española, (Ortega Díaz, 2008, págs. 76-78).

[40] Cfr. documento A/CN.9/438/Add.2, página 3.

[41] En este sentido, como se explica en el Informe "Planificación de la labor futura sobre comercio electrónico: Firmas digitales, autoridades certificadoras y asuntos jurídico conexos", Documento A/CN.9/WG.IV/WP.71, de 31 de diciembre de 1996, del Grupo de Trabajo sobre Comercio Electrónico de la CNUDMI, durante la preparación de la Ley Modelo de comercio electrónico, "el Grupo de Trabajo examinó las siguientes funciones tradicionales de las firmas manuscritas: identificar a una persona, proporcionar la certidumbre en cuanto a su participación personal en el acto de la firma, y vincular a esa persona con el contenido de un documento", añadiendo que "una firma podría cumplir otras diversas funciones, según cual fuera la naturaleza del documento firmado. Por ejemplo, una firma podría constituir un testimonio de la intención de una parte de considerarse vinculada por el contenido de un contrato firmado, de la intención de una persona de respaldar la autoría de un texto, de la intención de una persona de asociarse al contenido de un documento escrito por otra persona, y del hecho de que una persona estaba en un lugar determinado a una hora determinada". Lo interesante es que este informe adopta un enfoque amplio acerca de lo que puede denominarse firma electrónica, en el sentido de incluir aquellas tecnologías que permiten cumplir, en el medio electrónico algunas o todas las funciones identificadas como características de las firmas manuscritas. Y aunque el citado informe se centra casi en exclusiva en las técnicas basadas en criptografía –y en particular, en firmas digitales refrendadas por certificados–, presenta también otras técnicas que pueden resultar apropiadas, al objeto de que la futura legislación no desaliente su uso, en especial si la misma opta por regular el uso de la tecnología de firma digital mencionada. Y, en concreto, cita la autentificación mediante un dispositivo biométrico basado en las firmas manuscritas, sistema de autentificación que exige el análisis previo de muestras de firmas manuscritas y su almacenamiento utilizando el dispositivo biométrico.

[42] Como explica (Ortega Díaz, 2008, pág. 30), "[o]torgar la misma validez jurídica a la firma electrónica que a la firma manuscrita era una tarea que había que emprender con cautela. En efecto, esta equiparación era imprescindible pero debía hacerse de manera que generara en el mercado la confianza necesaria para que su implantación fuera una realidad", lo que venía dificultado por "el concepto impreciso que a finales de los años noventa se manejaba al hablar de firma electrónica, que aglutinaba desde el simple nombre del signatario mecanografiado en el documento hasta la firma digital basada en criptografía asimétrica".

[43] Con ocasión del análisis de las que denomina "arquitecturas de seguridad y garantía", (Galindo, 1998, págs. 99-100) indica que "se manifiestan socialmente cuatro posiciones sobre la filosofía o política técnico-jurídica que puede estar presente en la construcción de una arquitectura de seguridad y garantía de las comunicaciones electrónicas que permita el funcionamiento de las técnicas de cifrado", incluyendo "las tendencias fundamentales siguientes: 1.ª la propuesta de políticas que ponen un mayor énfasis en el diseño de redes de seguridad y confianza destinadas fundamentalmente a la protección de la seguridad del Estado o a propiciar un funcionamiento centralizado/jerárquico de las instituciones de garantía; 2.ª la propuesta de políticas que ponen un mayor énfasis en lograr la libertad y autonomía del ciudadano o individuo; 3.ª la propuesta de políticas que centran sus tesis en la aceptación de que el presente es un mundo plural y complejo, que cuenta con múltiples culturas, las cuales quedan mínimamente satisfechas con la

Como punto de partida para dichos trabajos, la LMCE había incluido un artículo 7 en el que se establecía una regla de equivalencia funcional[44] entre la firma electrónica y la firma escrita, norma de neutralidad técnica plena que tendría la virtud de informar los incipientes trabajos de la que sería, posteriormente, la DFE[45], aunque la misma no fuera especialmente respetuosa con dicha neutralidad tecnológica.

La LMFE desarrolló las cuestiones relativas a la firma electrónica atendiendo a estos mismos principios, especialmente en su artículo 6, y en cierto modo análogo a la DFE, aprobada dos años antes, resultando especialmente interesante para nuestro trabajo el contenido de su artículo 7, que se enfoca a establecer, conjuntamente con el artículo 6, "un mecanismo mediante el cual las firmas electrónicas que reúnan criterios objetivos de fiabilidad técnica puedan beneficiarse de una pronta determinación de su eficacia jurídica"; de modo que en la Ley Modelo encontramos dos regímenes diferenciados "según el momento en que se tiene la certeza de que una firma electrónica se reconoce como equivalente funcional de una firma manuscrita"[46].

Se inauguró en el plano internacional del comercio electrónico, de esta forma, la contribución del derecho administrativo a la validez y eficacia de la firma electrónica, que posteriormente –significativamente, en la Unión Europea, en las leyes nacionales y, en un momento posterior, en el Reglamento eIDAS– se iba a extender a las restantes instituciones de prueba electrónica de la actuación de las personas.

Volviendo al ámbito de la, entonces aún, Comunidad Económica Europea, la Comisión reconocía ya en su comunicación titulada "Iniciativa Europea de Comercio Electrónico", presentada el 16 de abril de 1997 al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, que las firmas digitales constituían un mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas; mientras que, en la Declaración Ministerial de Bonn, se enfatizaba que las firmas

---

participación de todas ellas en la organización heterogénea de las sociedades democráticas. Esta es la propuesta democrática o comunicativa; y 4.ª la propuesta de políticas que se fijan en la existencia de entidades de certificación tradicionales". A ésta última tendencia, se refiere el autor como "la posición positivista, o lo que es lo mismo, la que contempla al sistema legislativo, que si atiende al fenómeno tecnológico en cambio no regula por su novedad a las arquitecturas de seguridad y confianza de las comunicaciones electrónicas a las que aquí se hace referencia", aludiendo expresamente a registros públicos y notarías, a los que asimila a "todas las instituciones que, en cuanto servicios u oficinas de confianza, tienen atribuidas las funciones de identificar y certificar a personas u ordenadores" (Galindo, 1998, pág. 101).

[44] Sobre este principio aplicado a la firma electrónica, cfr. (Cruz Rivero, 2005). Para este autor, "la equivalencia funcional es la capacidad de un instrumento electrónico de satisfacer la misma necesidad que un instrumento tradicional", capacidad de que "llevado a denominar al instrumento electrónico con el mismo nombre que al clásico (firma) y ha justificado la atribución de los mismos efectos jurídicos".

[45] (Cruz Rivero, 2005) se refiere a la LMCE y la LMFE como los antecedentes remotos de la DFE, aunque ciertamente la LMFE es posterior, por lo que más bien estos antecedentes podrán encontrarse en sus trabajos preparatorios.

[46] Cfr. el epígrafe 76 de la Guía para la incorporación al derecho interno de la LMFE. En efecto, como ha indicado (Cruz Rivero, 2005), "la regulación de la LMFE tiene la ventaja de reconocer la posibilidad de que el Estado que acoja la Ley Modelo defina supuestos concretos de firmas electrónicas que cumplen los requisitos del art. 6", con la "ventaja de preconstituir la fiabilidad de las firmas electrónicas, de modo que la equivalencia con las firmas tradicionales desde el punto de vista formal no quede pendiente de un pronunciamiento judicial posterior en tal sentido, como ocurría bajo el régimen de la LMCE".

digitales resultaban una cuestión clave para el comercio electrónico; todo ello en un momento en el que diversos Estados miembros se encontraban ya legislando en el nivel nacional el uso de firma digital, como eran Alemania e Italia[47].

En su consecuencia, la Comisión presentó el 8 de octubre de 1997 al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación "El fomento de la Seguridad y la Confianza en la Comunicación Electrónica – Hacia un Marco Europeo para las Firmas Digitales y el Encriptado", donde se indicaba la necesidad de un planteamiento coherente en este ámbito, propuesta que el Consejo acogió favorablemente el 1 de diciembre de 1997, invitando a la Comisión a presentar, en la mayor brevedad posible, una propuesta de Directiva del Parlamento Europeo y el Consejo sobre firmas digitales.

La Comisión Europea publicó el 13 de mayo de 1998 la propuesta de Directiva de Firma Electrónica, que finalmente se aprobó el 13 de diciembre de 1999, con los objetivos de aumentar la confianza en las nuevas tecnologías y la aceptación general de las mismas (considerando (4) de la DFE), de promover la interoperabilidad de los productos de firma electrónica (considerando (5) de la DFE), o de estimular la prestación de servicios de certificación en toda la Comunidad a través de redes abiertas (considerando (10) de la DFE), contribuyendo al uso y al reconocimiento legal de la firma electrónica en la Comunidad.

En su consecuencia, la DFE creó un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior[48], y que supuso, como la LMFE, una importante contribución del derecho administrativo a la eficacia de la firma electrónica, desde una doble perspectiva: en primer lugar, mediante el establecimiento de un régimen de supervisión *a posteriori* de la actividad de las personas, físicas o jurídicas, que ofrecían al público servicios en soporte de la firma electrónica, y que agrupó alrededor del concepto legal de "servicio de certificación"; en segundo lugar, al prever sistemas voluntarios de acreditación destinados a un nivel reforzado de prestación de servicios, que "pueden aportar a los proveedores de servicios de certificación un marco apropiado para aproximarse a los niveles de confianza, seguridad y calidad exigidos por un mercado en evolución" (Considerando (11) de la DFE), normalmente regulados por el sector público, aunque no de forma exclusiva.

Por lo que se refiere a la primera cuestión, la DFE no contenía una definición de "servicio de certificación", sino que lo caracterizaba al indicar que un proveedor de servicios de certificación era "la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica", en una concepción muy amplia y que destacaba por asumir la ausencia de reserva a las autoridades públicas en relación con la prestación de estos servicios; más aún, apostando ya por la prestación privada de estos

---

[47] Cfr. (De Miguel Asensio, 2015, pág. 958).

[48] El considerando (3) del Reglamento eIDAS indica que la Directiva "se refiere a las firmas electrónicas, sin ofrecer un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso. El presente Reglamento refuerza y amplía el acervo que representa dicha Directiva". Como ya se avanzó, no resulta procedente entrar, en este momento, en el análisis detallado de sus contenidos, dado que lo realizaremos a lo largo del trabajo, con ocasión del estudio del Reglamento eIDAS.

servicios dentro del mercado interior[49].

Quizá la DFE adoptó esta denominación, que en algunos casos ha resultado confusa, porque la firma electrónica avanzada, que es la que recibe un efecto jurídico determinado, se debe basar de forma necesaria en un certificado electrónico reconocido; y desde luego, la prestación de servicios como el sellado de la fecha y hora de una firma electrónica, o la generación, validación o custodia de una firma electrónica no parece tener nada que ver con los certificados electrónicos, por lo que su inclusión en este concepto resulta extraña, y más cuando la Directiva no establece obligaciones para dichos servicios. A pesar de ello, resulta interesante que la DFE ya venga en crear una suerte de clase de servicios, que van a tener en común entre ellos "que utilicen firmas electrónicas o se sirvan de ellas, como los servicios de registro, los servicios de estampación de fecha y hora, los servicios de guías de usuarios, los de cálculo o asesoría relacionados con la firma electrónica" (Considerando (9) de la DFE).

Estos servicios serán, como se ha avanzado, objeto de supervisión –normalmente por parte de la correspondiente autoridad administrativa, aunque la DFE permitía también el establecimiento de sistemas de supervisión basados en el sector privado (Considerando (13) de la DFE–, aunque únicamente cuando los mismos sean ofrecidos al público, al objeto de garantizar el cumplimiento de las exigencias jurídicas de las firmas electrónicas que deban ser jurídicamente equivalentes a las firmas manuscritas; muestra indubitada de la aportación del derecho administrativo a la eficacia de la prueba electrónica correspondiente, en clara conexión con los indudables intereses generales[50] a que la misma sirve.

A modo de resumen, la DFE constituyó el primer ejercicio de institucionalización jurídica y armonización inicial, en la actual Unión Europea, de los mecanismos y servicios de seguridad de la TIC empleados para la actuación electrónica, ejercicio que se amplía en el Reglamento eIDAS, como veremos inmediatamente, en gran medida por la necesidad de cubrir nuevos servicios, que a lo sumo estaban sólo institucionalizados en las legislaciones de algunos Estados miembros, y cuyos efectos debían poderse extender a todos los Estados miembros de la Unión, al objeto de garantizar el funcionamiento del mercado interior, y sin perjuicio de la necesidad de resolver las no pocas disfunciones[51] que se habían puesto de manifiesto en la aplicación de la DFE.

---

[49] Así se desprende del Considerando (10) de la DFE, así como del modelo regulatorio de la norma.

[50] Sobre la caracterización del interés general, cfr. la reciente reflexión de (Gamero Casado, 2015, pág. 15 y ss.). En el caso que nos ocupa, resulta fácil apreciar diversos intereses generales alrededor de las fuentes de prueba, como la seguridad o la facilitación de la actuación transfronteriza.

[51] La valoración del funcionamiento de la DFE no ha sido positiva para la doctrina. (De Miguel Asensio, 2015, pág. 969) ha llegado a afirmar, al respecto, que "[e]n no pocos sectores la elaboración en el seno de la UE de un complejo marco normativo creado al hilo del desarrollo de la sociedad de la información ha resultado tan poco operativo en la práctica como en el ámbito de las firmas electrónicas", añadiendo que "la orientación y el contenido de la normativa de armonización adoptada mediante la Directiva 1999/93/CE determinaron que los mecanismos de firma electrónica típicamente utilizados en el ámbito del comercio electrónico prácticamente no fueran objeto de atención legislativa así como que otros posibles mecanismos tecnológicos relevantes para aportar seguridad al comercio electrónico quedaran al margen de ese régimen legal", considerando causa de esta falta de inoperancia "las dificultades de aplicación o el carácter innecesario de ciertos requisitos legales, la inadecuación de algunas de las limitaciones previstas, o el carácter inviable de ciertos elementos básicos de la Directiva". Se trata de un panorama más desolador, ciertamente, que el de la administración electrónica, aunque tampoco mucho más.

1.1.2 La recepción jurídica de las tecnologías de autenticación de entidades

En un momento posterior, y en cierto modo, de forma paralela a la institucionalización de las tecnologías de autenticación del origen de los datos, hemos asistido también a la aparición de otro tipo de prueba electrónica, que también es objeto de regulación –más limitada, en este caso– en el Reglamento eIDAS, y que recibe un tratamiento legal diferenciado.

Nos estamos refiriendo a la recepción jurídica de los mecanismos y servicios de autenticación de entidades, pero considerados de forma autónoma a aquellos empleados para la autenticación del origen de los datos, de los que se van a diferenciar funcionalmente, al objeto de garantizar exclusivamente la identidad de una entidad, habitualmente una persona (que actúa a través de un agente informático) o un sistema de información que funciona automatizadamente.

En definitiva, nos referimos al uso de estas tecnologías para acreditar la identidad, en sus múltiples manifestaciones[52], pero no para la atribución del origen de los datos a dicha entidad.

Desde la perspectiva del Reglamento eIDAS, que resulta parcial, normalmente nos vamos a referir a los sistemas de identificación electrónica establecidos o utilizados por los diferentes Estados miembros, frecuentemente como servicio público reservado, como por ejemplo, con base en las capacidades técnicas de los documentos nacionales de identidad electrónicos[53], o sus documentos análogos para extranjeros residentes, de obtención y uso obligatorio en conexión con la seguridad pública[54]; pero también a otros servicios electrónicos empleados para la identificación frente a las entidades del sector público, de obtención voluntaria, y que en muchas ocasiones han sido regulados como instrumento auxiliar al procedimiento administrativo electrónico[55].

---

[52] Como he tenido ocasión de indicar en otro momento, la identidad electrónica se encuentra compuesta por una colección de atributos que permiten a los terceros reconocernos, pudiendo expresarse en forma de identidad personal, corporativa, de cliente, etc. (Alamillo Domingo, 2010a, págs. 17-18)

[53] (Merchán Murillo, 2016, págs. 50-51) establece una conexión entre la nacionalidad y los atributos de identidad, especialmente aquellos acreditados mediante los documentos nacionales de identidad, indicando que "en la mayoría de los casos, los ciudadanos de un Estado no pueden utilizar su identificación electrónica para autenticarse en otro país porque los sistemas nacionales de identificación electrónica en su territorio no son reconocidos en aquel. Dicha barrera electrónica excluye a los prestadores de servicios del pleno disfrute de los beneficios del propio mercado".

[54] (Beltrán de Felipe, 2010, pág. 42) ha destacado la diferente percepción que tienen los ciudadanos acerca del uso de determinados datos de su identidad, de modo que "la identidad (en concreto: las técnicas de identificación por parte de las autoridades) levantan rechazo y sospecha en algunos sectores y en algunos países entre personas que piensan que la existencia de datos acerca de ellas es una amenaza para su intimidad o privacidad, o para sus derechos en general", por lo que considera que "[l]os sistemas públicos de identificación […] son entonces considerados como algo peligroso, tendencialmente incompatible con la democracia y con las libertades porque permiten a las autoridades controlar a las personas, recabar datos sobre su vida, costumbres, etc., e invadir su intimidad".

[55] Sobre la conceptualización y análisis general de los instrumentos de procedimiento administrativo electrónico, cfr. (Martínez Gutiérrez, 2009), *in toto*.

Estos servicios de seguridad de la TIC[56] han sido institucionalizados de forma diferente a los mecanismos de firma electrónica y a los servicios de certificación (en el Reglamento eIDAS, servicios de confianza), sin integrarse en la misma categoría, algo que únicamente parece responder a la voluntad política de los Estados miembros de que no sean privatizados[57].

Ello no ha impedido la aparición de modalidades privadas de prestación de servicios de identificación electrónica[58], que actualmente funcionan en base a las reglas del derecho privado –con sujeción, en todo caso, a la normativa general reguladora de los servicios de la sociedad de la información– y a la que, en su caso, se disponga en cada Estado miembro[59]; ni afecta a las mismas. Y tampoco afecta a normativas sectoriales, como la regulación aplicable a los servicios de autenticación reforzada, en relación con la prestación de servicios de pago en el mercado interior[60].

En todo caso, resulta evidente que el Reglamento eIDAS no debe ser considerado como una regulación autónoma de la identidad digital[61], sino sólo de una de las capacidades de la misma ofrece, como es la posibilidad de autenticarse frente a terceros empleando un conjunto concreto de datos de identidad.

1.1.3 La influencia decisiva de la interoperabilidad en el proceso de institucionalización jurídica en el nivel de la Unión Europea

La importancia de la interoperabilidad no es una novedad del Reglamento eIDAS en absoluto, y ya se deducía de la DFE[62], aunque se trata de uno de los grandes problemas que precisamente han afectado a la efectividad en la aplicación de dicha norma[63].

Ello es así hasta el punto de que, en mi opinión, no puede entenderse el proceso de institucionalización jurídica de estas categorías de servicios, públicos o privados, sin

---

[56] Cfr. el Anexo A.1 de este trabajo.

[57] Cfr. el epígrafe 3.1.1, en relación con los epígrafes 2.2 y 2.2 de este trabajo.

[58] Cfr. el Anexo A.3.4 de este trabajo.

[59] Así ha sucedido, por ejemplo, en Finlandia, a partir del Acta de Autenticación Reforzada y Firmas Electrónicas, 617/2009.

[60] Cfr. los artículos 97 y 98 de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n o 1093/2010 y se deroga la Directiva 2007/64/CE, y el Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros.

[61] (Lusoli, Maghiros, & Bacigalupo, 2008, p. 178 y ss.) han analizado la necesidad de un nuevo marco regulatorio para la identidad digital, partiendo de la existencia de los derechos a la intimidad y a la protección de datos, concluyendo en la conveniencia de un marco basado en la autonomía.

[62] De este modo ha sido puesto de manifiesto por (Merchán Murillo, 2012, pág. 15), en conexión con el uso transfronterizo de las firmas electrónicas.

[63] Muy crítico se muestra (Krawczyk, 2010, p. 17), en especial con la firma electrónica cualificada.

atender a uno de los grandes objetivos del Reglamento eIDAS[64], en el marco de integración de la Unión Europea, como es la construcción de un Mercado Único –ahora– Digital, del cual el sector público es un actor de extraordinaria relevancia, que se basa ineludiblemente en la noción de interoperabilidad como instrumento habilitador del reconocimiento transfronterizo[65], pero que al tiempo contribuye, indirectamente, a una cierta armonización de los sistemas jurídicos de los Estados miembros, al menos en las zonas de contacto.

Con carácter general, hay que recordar que la interoperabilidad de las redes nacionales constituye uno de los objetivos de la acción de la Unión, en el marco de las redes transnacionales previstas en los artículos 170 y 171 del Tratado de Funcionamiento de la Unión Europea, una verdadera competencia del legislador de la Unión en relación con las redes transeuropeas de comunicaciones electrónicas.

Ha sido la consideración de la administración electrónica dentro del ámbito de estas redes, que se evidencia –entre otros– en el sistema de financiación del Mecanismo Conectar Europa, la que ha permitido a la Unión intervenir en un espacio en el que de otro modo posiblemente no hubiera resultado competente[66]. Y ello a pesar de que el actual artículo 6 del Tratado de Funcionamiento de la Unión Europea prevea la competencia de la Unión "para llevar a cabo acciones con el fin de apoyar, coordinar o complementar la acción de los Estados miembros", en el ámbito de la "cooperación administrativa".

Por este motivo, la interoperabilidad ha sido tratada, en el nivel de la Unión Europea, en múltiples instrumentos, de los cuales –y en relación con los servicios públicos electrónicos–, podemos destacar algunos de los más relevantes. Éstos han influido de forma decisiva en el actual Reglamento eIDAS[67].

---

[64] Para (Gobert, 2015, pp. 8-9), la elección de un reglamento como instrumento es juiciosa, porque "[d]esde el punto de vista legal, permite una mayor armonización y evita diferencias tanto en la interpretación legal como en la forma en que se llevan a cabo los controles", mientras que "[d]esde un punto de vista operativo, obliga a los Estados Miembros y a los proveedores de servicios a cooperar más eficazmente para resolver los problemas actuales de interoperabilidad técnica y para garantizar que los sistemas nacionales, que a veces son diferentes, puedan «entenderse y hablarse entre sí»".

[65] Para (Gamero Casado, 2016, pág. 24), "[l]a interoperabilidad es complicadísima de conseguir, y constituye la barrera más relevante para la generalización de la administración electrónica en este primer cuarto del Siglo XXI", idea que ya había manifestado el mismo autor con bastante anterioridad (Gamero Casado, 2009, pág. 294).

[66] Como explica (Cerrillo i Martínez, 2010, pág. 767), "[l]a Unión Europea ha facilitado el desarrollo de la administración electrónica en Europa, a pesar de no tener una competencia específica en la materia" y "ha estado siempre sensibilizada por la interoperabilidad al considerar que existe un alto riesgo de que surjan barreras electrónicas debido a la dimensión nacional de la administración electrónica y a la escasa interoperabilidad a escala europea".

[67] Como ha indicado (Merchán Murillo, 2018, pág. 8), en la construcción del mercado único digital, "[e]n definitiva, lo que se pretende es hacer plenamente interoperables los servicios de e-Administración, superando las barreras organizativas, técnicas, semánticas y jurídicas, para garantizar que los puntos de contacto únicos funcionen como verdaderos centros de e-Administración, permitiendo el acceso a los ciudadanos y empresas y que se cree una lista común de servicios públicos transfronterizos esenciales, que correspondan a necesidades bien definidas", por lo que "[s]olo de esta manera, se puede determinar un sistema jurídico específico, que permita a los actores actuantes en el mercado comunicarse, intercambiar información, ofrecer y usar servicios y productos en tiempo real", notando que "[s]i echamos la mirada a la normativa anterior, la citada interoperabilidad no existía, en relación a la identificación y la autenticación electrónica. En especial, a lo que se refiere la a la dimensión jurídica de la interoperabilidad y, por ende, a

Sin ánimo de exhaustividad, nos podemos referir ya a la Decisión Nº 1720/1999/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 1999, por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA), así como el acceso a las mismas, modificada por Decisión Nº 2045/2002/CE, del Parlamento Europeo y del Consejo, de 21 de octubre de 2002, apuesta por la actuación de la Comunidad en el ámbito de las redes telemáticas transeuropeas para las administraciones[68], con el objetivo, entre otros, de "lograr un alto nivel de interoperabilidad, dentro de cada sector administrativo, y entre sectores administrativos diferentes y, en su caso, entre éstos y el sector privado, de las redes telemáticas establecidas en los Estados miembros y entre la Comunidad y los Estados miembros con el fin de apoyar el establecimiento de la unión económica y monetaria y de realizar las políticas y actividades comunitarias, contempladas en los artículos 3 y 4 del Tratado, teniendo en cuenta el trabajo ya en curso en los programas existentes de la Comunidad o de los Estados miembros".

En la Comunicación de la Comisión al Consejo, al Parlamento europeo, al Comité Económico y Social Europeo y al Comité de las Regiones – El papel de la administración electrónica en el futuro de Europa, COM (2003) 567 final, de 26 de septiembre de 2003, se conceptúa la interoperabilidad como la forma o el medio en que debe tener lugar la interconexión de sistemas, información y formas de trabajar, dentro de una administración o entre administraciones, a nivel nacional o europeo, e incluso con el sector empresarial, y se aclara, de forma significativa, que "la interoperabilidad no es una mera cuestión técnica de conexión de redes informáticas, sino que también afecta a cuestiones de organización, tales como la coordinación de procesos que no se quedan dentro de los límites de una entidad, sino que suponen interfuncionar con otras entidades que bien pueden tener una organización interna y unas operaciones diferentes". La interoperabilidad debe ser, en opinión de la Comisión, cuestión de una política que considere su dimensión europea, complementaria de las actuaciones en sede nacional[69].

La noción de marco de interoperabilidad se desarrolla ya en detalle, en 2003, en el importante documento titulado precisamente "Marco de Interoperabilidad Europea" o EIF[70] 1.0, publicado en 2004, marco que se había previsto ya en el Plan de Acción eEurope 2005, acordado en 2002, y que sirve de referencia para el ya mencionado Programa IDABC. La interoperabilidad se define, en el EIF 1.0, como "un conjunto de estándares y guías que describen la forma en la que las organizaciones han acordado, o

---

la falta de neutralidad tecnológica; pues, si hubiera una verdadera neutralidad tecnológica significaría que los ciudadanos tienen el derecho a elegir las soluciones técnicas que quieran utilizar, en las relaciones que mantienen con la Administración pública, que bien podría ser la de otro Estado miembro".

[68] El Considerando (9) de esta Decisión defiende la necesidad de crear sistemas integrados de comunicación de datos entre administraciones –a los que denomina redes telemáticas–, mientras que su Considerando (10) se refiere a la necesidad de conectar dichas redes, por lo que las mismas serán transfronterizas. Esta argumentación sirve para legitimar jurídicamente la actuación en el nivel de la entonces Comunidad Europea, de acuerdo con los artículos 3.1.o), y 154 a 156 del Tratado constitutivo de la Comunidad Europea (versión consolidada de 1997).

[69] En España, hasta 2010 no se aprueba un marco de interoperabilidad para todos los niveles de administración, actualmente contenido en el Real Decreto 4/2010, de 8 de enero.

[70] Acrónimo del título en inglés del documento, que es "European Interoperability Framework".

deberían acordar, interactuar entre ellas"; y, en concreto, el EIF define un conjunto de recomendaciones y guías para los servicios públicos electrónicos, que permita a las administraciones públicas, las empresas y los ciudadanos interactuar de forma transfronteriza, en un contexto pan-Europeo.

El EIF parte, para su diseño, de una serie de principios para el diseño de servicios públicos electrónicos, incluyendo la accesibilidad, el multilingüismo, la seguridad, la privacidad, la subsidiariedad, el uso de estándares abiertos, la evaluación de los beneficios del uso de aplicaciones de fuentes abiertas y el uso de soluciones multilaterales[71]; y considera tres dimensiones de la interoperabilidad, incluyendo la organizativa, la semántica y la técnica[72].

Desde una óptica más jurídica, el artículo 3.f) de la Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (en adelante, "Decisión IDABC"), de nuevo legalmente fundamentada en las redes transeuropeas de telecomunicaciones, define la interoperabilidad como la "capacidad de los sistemas de tecnologías de la información y las comunicaciones (TIC), y de los procesos empresariales a los que apoyan, de intercambiar datos y posibilitar la puesta en común de información y conocimientos", una definición que pone el acento en un enfoque más bien tecnológico como base de la interoperabilidad.

Por su parte, la Comunicación de la Comisión al Consejo y al Parlamento Europeo, "Interoperabilidad de los servicios paneuropeos de administración electrónica", COM (2006) 45 final, de 13 de febrero de 2006, considera a la interoperabilidad como una condición de cara a la mejora de las condiciones para una Europa competitiva e innovadora; que requiere estrategias comunes e inversiones sustanciales de todas las partes interesadas en infraestructura de colaboración e infraestructura operativa, atendiendo a una visión a largo plazo de servicios paneuropeos de administración electrónica viables; en definitiva, como un objetivo europeo que deben perseguir las instituciones europeas en estrecha colaboración con los Estados miembros, y que se canalizará a través de las iniciativas i2010 e IDABC.

Más recientemente, el artículo 2.a) de la Decisión Nº 922/2009/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas (en adelante, Decisión ISA), de nuevo con base legal en la redes transfronterizas de telecomunicaciones, define la interoperabilidad como "la capacidad de que organizaciones diversas y dispares interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y que hayan sido acordados previa y conjuntamente, recurriendo a la puesta en común de información y conocimientos entre las organizaciones, a través de los procesos empresariales a los que apoyan, mediante el intercambio de datos entre los sistemas de TIC respectivos", en un cambio de enfoque notable, que se aleja de los aspectos tecnológicos –que lógicamente continúan teniendo un protagonismo notable–, para incorporar elementos de colaboración y gobernanza sobre procesos con base tecnológica.

[71] Estos principios han sido acogidos por el Esquema Nacional de Interoperabilidad español.

[72] Estas dimensiones de la interoperabilidad se citan también en el artículo 6 del RDENI, el cual agrega la dimensión temporal de la interoperabilidad, que ha de garantizar "el acceso a la información a lo largo del tiempo".

La Decisión ISA se refiere, en su artículo 2.c), a los marcos comunes (de interoperabilidad) como "estrategias, especificaciones, metodologías, directrices, así como enfoques y documentos similares", definición que se concreta en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Hacia la interoperabilidad de los servicios públicos europeos", COM (2010) 744 final, de 16 de diciembre de 2010, que se refiere a un marco de interoperabilidad como "un enfoque concertado con respecto a la interoperabilidad para las organizaciones que desean colaborar en favor de la prestación conjunta de servicios públicos", de forma que "dentro de su ámbito de aplicabilidad, especifica un conjunto de elementos comunes, tales como vocabulario, conceptos, principios, políticas, directrices, recomendaciones, normas, especificaciones y prácticas", constituyendo un poderoso instrumento de *soft law* –en este caso, público–, cuya legitimidad nace del consenso, desde abajo hacia arriba, más que del sistema clásico de jerarquía de fuentes, de arriba hacia abajo.

Estos marcos comunes deben ser objeto de creación y mejora dentro del programa ISA, tanto desde la perspectiva transfronteriza como intersectorial[73], y complementados mediante servicios comunes –aplicaciones e infraestructuras operativas de naturaleza genérica que satisfagan las necesidades comunes del usuario en los distintos ámbitos políticos– y herramientas genéricas –plataformas de referencia, plataformas compartidas y de colaboración, componentes comunes y módulos similares que satisfagan las necesidades comunes del usuario en los distintos ámbitos políticos[74]–; todo ello de acuerdo con los principios que informan el programa ISA: neutralidad con respecto a la tecnología y adaptabilidad, apertura, reutilización, privacidad y protección de los datos personales, y seguridad.

Finalmente, la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Una Agenda Digital para Europa", COM (2010) 245 final/2, de 26 de agosto de 2010, eleva el valor político de la interoperabilidad a un lugar sin precedentes anteriores, afirmando que "la finalidad genérica de la Agenda Digital es obtener los beneficios económicos y sociales sostenibles que pueden derivar de un mercado único digital basado en una internet rápida y ultrarrápida y en unas aplicaciones interoperables".

En este sentido, la falta de interoperabilidad se ha identificado, nada más y nada menos, como uno de los siete obstáculos al círculo virtuoso de la economía digital en la Unión Europea, los cuales "socavan gravemente los esfuerzos realizados para explotar las TIC, evidenciando la necesidad de una respuesta política global y unificada a nivel europeo", por lo que no sorprende que dicha Agenda establezca una línea específica de actuaciones referidas a la interoperabilidad[75], así como un refuerzo político notable a la aplicación de la Estrategia Europea de Interoperabilidad y del Marco Europeo de Interoperabilidad.

Como se puede ver de este sucinto repaso –que se puede ver en detalle en la Ilustración 1–, y partiendo de la fundamentación jurídica de la competencia de actuación de la Unión

[73] Cfr. el artículo 3.a) de la Decisión ISA.

[74] Cfr. el artículo 3.c) i 3.d) de la citada Decisión.

[75] Incluyendo la mejora del marco europeo de normalización, ya que las normas se califican como esenciales para la interoperabilidad; la promoción de un mejor uso de las normas; o la interoperabilidad de las tecnologías de identidad y firma electrónica.

Europea en relación con las redes transeuropeas de telecomunicaciones, podemos afirmar que la interoperabilidad se ha convertido en una potente línea política de las instituciones europeas.

Uno de las nociones interesante del EIF es su naturaleza de "meta-marco de interoperabilidad"; esto es, su orientación a ser un marco de referencia para los restantes marcos de interoperabilidad, en especial los que se establezcan en sede nacional, en aplicación del principio de subsidiariedad; de modo que constituye un modelo con el que se pueden alinear todos los marcos de interoperabilidad, facilitando el diseño de los servicios públicos europeos.

De hecho, el EIF es sólo una de las iniciativas de interoperabilidad, que ofrece soporte a la estrategia de interoperabilidad, y es soportado por guías ulteriores, así como por servicios y herramientas[76]. Como tal marco de marcos de interoperabilidad, el EIF define principios, un modelo conceptual, niveles de interoperabilidad, acuerdos de interoperabilidad y normas de gobernanza de la interoperabilidad; aspectos que se proyectan también en marcos sectoriales, como el de interoperabilidad de la identificación electrónica transfronteriza o el del uso transfronterizo de los servicios de confianza, desarrollados en el marco del Mecanismo Conectar Europa. A ellos nos referiremos en su debido momento.

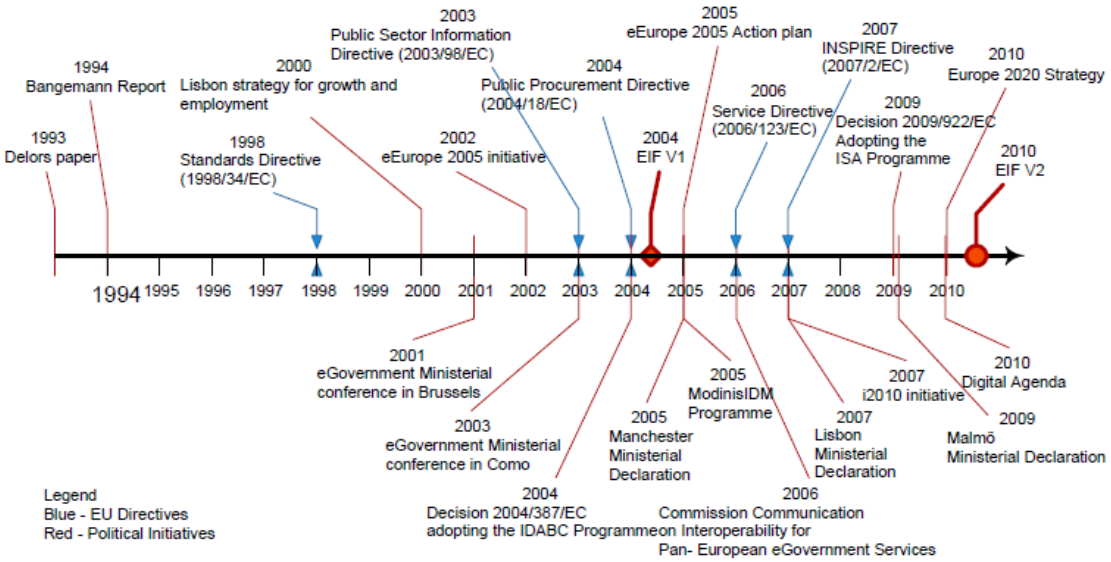


Ilustración 1. Cronología de iniciativas de la UE en interoperabilidad (fuente: EIF 2.0)

Precisamente en estos marcos de interoperabilidad se sustenta la aplicación del Reglamento eIDAS, con su fuerte enfoque de reconocimiento transfronterizo, tanto en relación con los sistemas de identificación electrónica cuanto por lo que se refiere a los servicios de confianza –en especial en el ámbito de los servicios públicos electrónicos–, todo ello con la base legal de la necesaria aproximación de las legislaciones de los Estados miembros al objeto de garantizar el funcionamiento del mercado interior.

[76] Cfr. (European Interoperability Framework (EIF). Towards Interoperability for European Public Services, 2011).

1.1.4 La interoperabilidad también influye, en el nivel nacional, en la regulación del uso de las instituciones de acreditación de la actuación electrónica

El interés por la interoperabilidad también se encuentra en el nivel nacional, al menos en el caso de España, y presenta una influencia más que notable, aunque, como es lógico, sólo en el ámbito que no se encuentre armonizado en cada momento por la normativa de la Unión Europea.

Por lo que se refiere a las instituciones de acreditación de la actuación electrónica, la interoperabilidad también ha jugado un rol fundamental, aunque limitada al "sector" de la administración electrónica[77], como posteriormente veremos, tanto en relación con la identificación basada en certificados como en cuanto a la firma electrónica[78].

En ambos casos, podemos avanzar que nos encontramos ante un detallado marco normativo, que complementa el régimen general, que inicialmente parte del establecimiento de condiciones adicionales para el uso de la firma electrónica en el sector público, para posteriormente regular nuevas instituciones para la acreditación de la actuación electrónica; en especial, nuevos medios de identificación electrónica[79] y sistemas de firma para la actuación administrativa automatizada.

Dicho marco fue establecido en España, en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (en adelante, LAE), y desarrollado primeramente, y para el ámbito de la Administración General del Estado, por el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (en adelante, RDLAE) y, posteriormente con alcance para todas las Administraciones Públicas, por el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (en adelante, RDENI), y ha sido objeto de un detallado y prolijo desarrollo posterior mediante las Normas Técnicas de Interoperabilidad que el mismo prevé; constituyendo el soporte para disponer de un conjunto de "reglas del juego"[80] que garanticen la correcta actuación

---

[77] Los sistemas deben alcanzar un nivel mínimo de interoperabilidad para que los ciudadanos puedan ejercer sus derechos en las relaciones electrónicas con las Administraciones Públicas, exigencia que resulta especialmente importante cuando dichas relaciones se imponen con carácter obligatorio a los interesados. Como gráficamente ha denunciado (Gamero Casado, 2016, pág. 21), "en la fase estricta de presentación, es frecuente tropezarse con graves problemas de interoperabilidad, de suerte que no puede completarse el trámite porque se actualizó la versión de Java, porque no se ha descargado el *applet* de firma electrónica, o porque la versión del navegador es incompatible", lo que implica que "[s]i el sufrido ciudadano no supera en plazo esta peculiar gymkhana, y no logra finalmente completar el trámite de presentación, perderá todos sus derechos", resultado que califica de inaceptable.

[78] Cfr., respectivamente, los epígrafes 2.1.4 y 5.2 de este trabajo.

[79] Cfr. los epígrafes 2.2.2 y 2.2.3 de este trabajo, en relación con el régimen originario y su posterior alineación con el Reglamento eIDAS, con ocasión de la denominada "reforma del sector público".

[80] Para (Gamero Casado, 2016, pág. 25), se trata de un modelo brillante y que constituye un verdadero referente mundial, aunque, como he puesto de manifiesto con ocasión de la Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración, existen no pocas dudas jurídicas en relación con los instrumentos normativos adoptados (Alamillo Domingo, 2012, pág. 83 y ss.).

electrónica en este sector.

La aproximación a la interoperabilidad en el enfoque español es sensiblemente diferente al de la Unión Europea que hemos examinado anteriormente, al presentar un fuerte componente de coordinación[81], pero sin una base legal del todo clara en este sentido, dado que no nos encontramos ante el ejercicio de una competencia formalmente atribuida, sino más bien en el ámbito de la cooperación[82] en orden a la efectividad de la interoperabilidad, que se ha convertido en un verdadero principio legal[83], hoy recogido expresamente en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP)[84], pero con insuficiencias de tipo procedimental bastante importantes en comparación con la LAE[85].

En todo caso, y atendiendo a que a lo largo de este trabajo deberemos analizar las previsiones del esquema español de interoperabilidad, sólo resulta preciso tomar consciencia del importante papel de esta normativa, adicional y complementaria de la general que rige las instituciones de acreditación de la actuación electrónica, cuando las mismas se utilizan en el dominio de la administración electrónica.

1.2 LA IDENTIFICACIÓN ELECTRÓNICA EN EL REGLAMENTO EIDAS

Una de las novedades más importantes del Reglamento eIDAS es la regulación de la identificación electrónica para la autenticación transfronteriza[86], que se encuentra

---

[81] En opinión de (Cerrillo i Martínez, 2010, pág. 787), "[l]a regulación que hace la LAE del ENI permite observar algunos elementos que lo identifican como un mecanismo de coordinación interadministrativa aunque la finalidad última no puede ser la homogeneización de los servicios y las infraestructuras que desarrolla cada administración pública".

[82] (Cerrillo i Martínez, 2010, pág. 788).

[83] Sobre la noción de interoperabilidad, cfr. el completo estudio realizado en el ámbito de la Administración electrónica, que es una de las iniciativas con mayor capacidad de tracción para la incorporación de ciudadanos y empresas a la Sociedad de la Información, realizado por (Martínez Gutiérrez, 2009, pág. 256 y ss.), autor que considera a la interoperabilidad como un nuevo principio jurídico (Martínez Gutiérrez, 2016b, pág. 2899). Nótese que la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP) así lo ha recogido en su artículo 3.2, para las relaciones electrónica de las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes. Cfr. también (Gómez Puente, 2011).

[84] Nótese que la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP) así lo ha recogido en su artículo 3.2, para las relaciones electrónica de las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes.

[85] Así lo ha hecho notar (Gamero Casado, 2016, pág. 25), para quien la reforma "ha incurrido en una omisión asombrosa e imperdonable: la determinación de su procedimiento de aprobación […] [d]e tal manera que las nuevas leyes invocan y remiten incesantemente a la interoperabilidad, pero no se sabe quién ni cómo establecerá en lo sucesivo sus contenidos", añadiendo que "[s]e trata de un grave defecto de técnica normativa que debe subsanarse antes de la entrada en vigor de estas leyes, pues podría incluso ponerse en entredicho la validez del RD 4/2010, al desaparecer su Ley de cobertura", subsanación que jamás se ha producido.

[86] (Aavik & Krimmer, 2016, pp. 151-152) se refieren a la necesidad de los Estados de desarrollar, a medida que el mundo se digitaliza, formas de integrar a los "emigrantes digitales", considerando a tales a los ciudadanos sin residencia en el país, pero que desean involucrarse electrónicamente en sus servicios

principalmente contenida en el capítulo II del Reglamento eIDAS, así como en diferentes actos de ejecución dictados por la Comisión Europea.

La posibilidad de uso de la identificación electrónica personal en las operaciones transfronterizas constituye una de las principales herramientas de habilitación del Mercado Único Digital, lo que exige el desarrollo de un marco legal que la conceptúe y dote de efectos.

En este epígrafe estudiaremos el marco conceptual de la identificación electrónica en la normativa de la Unión, y caracterizaremos el modelo regulatorio de la misma, al objeto de obtener una visión general, y contraponerla a la de los servicios de confianza.

1.2.1 El concepto de identificación electrónica en el Reglamento eIDAS

Abordar el estudio de este concepto en la normativa de la Unión Europea es una tarea compleja, para lo cual nos ayudará la representación gráfica del mapa de conceptos empleados por el Reglamento eIDAS que se muestra en la Ilustración 2.

Por identificación electrónica, el artículo 3.1 del Reglamento eIDAS se refiere al "proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica", que, aunque la definición no lo explicite, sirve principalmente para la autenticación transfronteriza en el acceso electrónico a servicios ofrecidos por los organismos del sector público[87].

Se trata de una definición ciertamente escasa, para cuya concreción debemos acudir a otras definiciones del mismo texto legal y apoyarnos en la autorregulación previamente existente[88] y en la autorregulación del sector público creada específicamente para esta institución[89].

El artículo 3.3 del Reglamento eIDAS define los datos de identificación de la persona como "un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica"; es decir, un identificador digital[90], como por ejemplo un nombre, uno o dos apellidos o un número de registro asignado por el Gobierno (en el caso de España, uno de los más empleados, pero no el más extendido, es el número del Documento Nacional de Identidad).

Dada la existencia de diversos conjuntos de datos que identifican, y la complejidad jurídica que presentaría crear una identificación única agregada con todos los posibles

---

públicos, como en el caso del programa de e-Residencia de Estonia.

[87] Cfr. artículo 6.1 del Reglamento eIDAS.

[88] Como, por ejemplo, las normas ISO/IEC 24760-1:2011 o 29115:2013. Cfr. el Anexo A.3.6 de este trabajo.

[89] En este sentido, resulta muy notables los trabajos de la iniciativa STORK, o del grupo de trabajo franco-alemán referido al eIDAS Token.

[90] (Dumortier, 2016, p. 5) opina que no tienen por qué tratarse de datos que identifiquen unívocamente a la persona, lo que permite disponer de identidades parciales, sino que es el proceso lo que debe identificar al usuario de forma única.

datos[91], nos referiremos con carácter general a identidades electrónicas parciales.

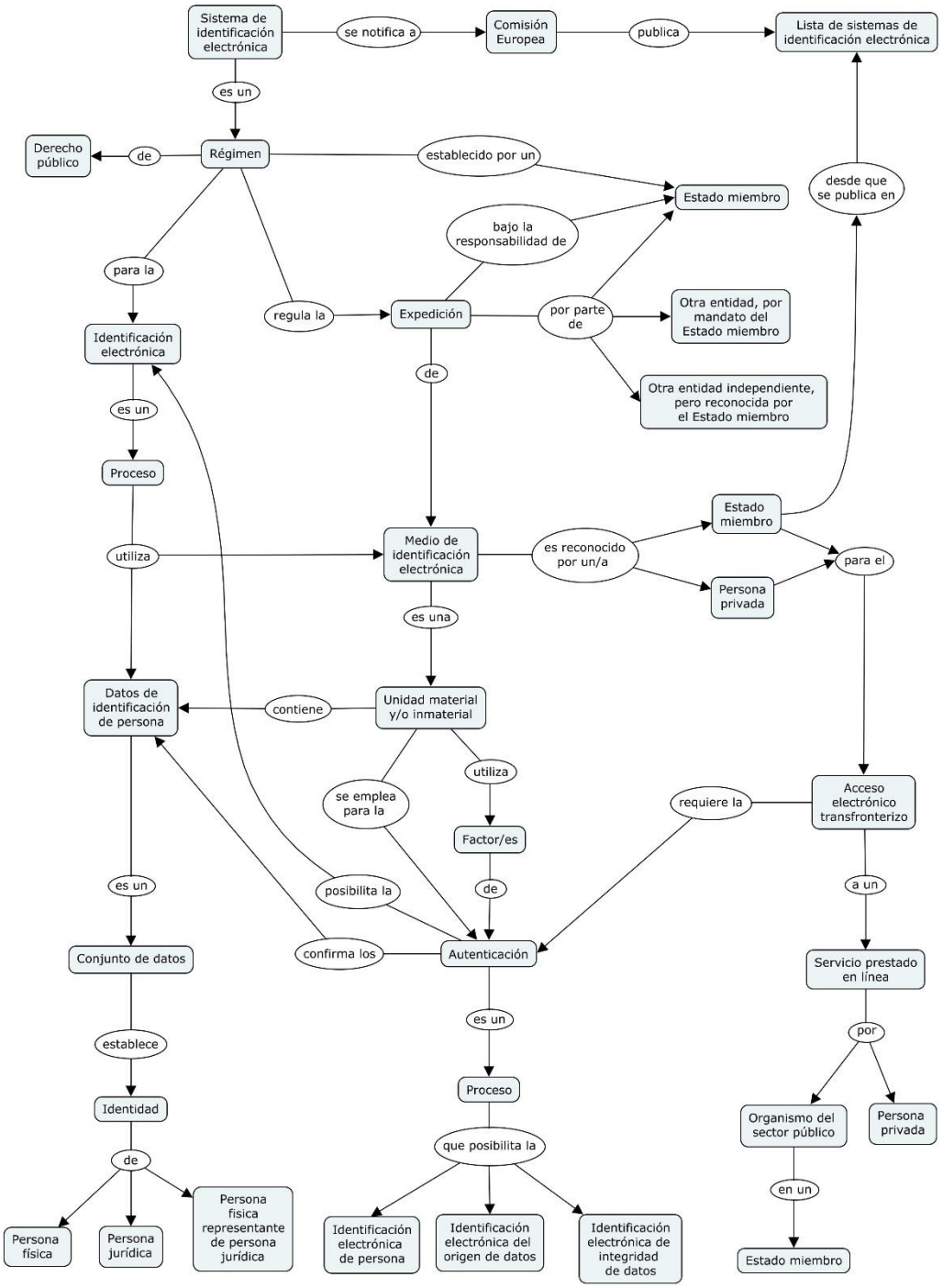


Ilustración 2. Mapa conceptual de la identificación electrónica (elaboración propia)

[91] Dada la aplicación indiscutible de la normativa de protección de datos, a mayor agregación de datos en una identidad, mayores restricciones se deben establecer a su utilización. Ello sin perjuicio, además, de la existencia de prohibiciones constitucionales a los identificadores únicos globales que existen en algunos Estados de la Unión Europea.

Hasta aquí, la identificación electrónica consiste en un proceso donde se emplean identificadores de personas físicas o jurídicas, pero aún no se ha establecido ni qué tipo de proceso es, ni para qué finalidad, por lo que debemos seguir profundizando en el Reglamento eIDAS.

En este sentido, el artículo 3.4 del mismo define el sistema de identificación electrónica como "un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica"[92], añadiendo el artículo 3.2 del mismo texto legal que por medios de identificación electrónica debemos entender "una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea".

A partir de estas definiciones podemos empezar a comprender algo mejor el concepto de identificación electrónica, ya que se caracteriza por tratarse de un régimen que sustenta el proceso de identificación electrónica mediante la expedición de unidades que contienen datos de identificación y que sirven para la autenticación transfronteriza.

La necesidad de proceder a esta conceptualización procede de la importante cantidad de medios de identificación electrónica que se encuentra a disposición de los Estados miembros, que introduce un elemento de fuerte diversidad entre los mismos[93], tanto en términos de seguridad como de interoperabilidad, dificultando o directamente impidiendo las operaciones transfronterizas.

Asimismo, es más que necesario reseñar que, de acuerdo con el artículo 3.5 del Reglamento eIDAS, la autenticación se define como "un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico", definición de la que resulta muy destacable el hecho de que se refiere a tres servicios de seguridad anteriormente presentados: la autenticación de entidad[94], la autenticación del origen de los datos y la integridad de los datos, algo que puede generar confusión[95].

---

[92] Lo que supone que el enfoque de la normativa se limita a los sistemas de identidad de tercera parte, dado que se emplean para relacionarnos con organizaciones y personas diferentes a las que nos los ha suministrado (Alamillo Domingo, 2010a, pág. 19).

[93] Buena muestra de dicha diversidad se encuentra reflejada en (Graux & Majava, 2007), actualizado en (Graux, Majava, & Meyvis, 2009). Véase también (Leitold, 2010).

[94] En este sentido, y según dispone el artículo 7.f) del Reglamento eIDAS, la autenticación en línea sirve para que una parte usuaria establecida en un Estado miembro pueda confirmar los datos de identificación de la persona recibidos en forma electrónicamente.

[95] Así sucede en el caso de (Merchán Murillo, 2016, pág. 57), que en mi opinión mezcla, en un razonamiento circular, la autenticación de entidad (ligada a la identificación) con la autenticación del origen de los datos (propia de la firma electrónica, que de algún modo siempre exige también alguna identificación), cuando se plantea que "[s]i decimos que una firma electrónica es cualquier medio de autenticación electrónica de la identidad de un sujeto y de la intención de éste, indicando aprobación y asociación con un registro electrónico; o sea, podemos decir que la autenticación electrónica es un término utilizado para referirse a diversas técnicas destinadas a reproducir en un entorno electrónico las funciones señaladas como característica de las firmas manuscritas", por lo que "cabría decir que la autenticación es firmar, para establecer como verdadero o asociarse asimismo con un documento, lo que nos permite llegar a la afirmación, con la que empezamos este capítulo: autenticación es el proceso de verificación de una identidad".

La autenticación de entidad sería, por tanto, el núcleo esencial de esta nueva regulación[96], ya que la anterior normativa cubría suficientemente la autenticación de datos, así como la integridad, pero es muy destacable que la definición también incluya a estos dos servicios de seguridad, porque si comparamos esta definición con la de sello electrónico contenida en el artículo 3.25 del propio Reglamento eIDAS, veremos que también el sello sirve para exactamente los mismos propósitos de garantía del origen de los datos y de la integridad de los mismos datos. Y que el sello electrónico avanzado, además, identifica a su creador (cfr. artículos 3.26 y 36.b del Reglamento eIDAS).

No parece, sin embargo, que sea obligatorio que el medio de identificación electrónica sustente todos estos servicios de seguridad, en atención al uso de la conjunción "o" empleada en la definición, por lo que nos encontraremos frente a medios de identificación que permitirán sólo la autenticación de entidades –lo que comúnmente se percibe como "identificación"– mientras que otros podrán también ofrecer la garantía de autenticación de origen de datos e incluso de la integridad[97].

En cambio, para que una tecnología se pueda calificar como sello electrónico es necesario que la misma permita la garantía del origen de los datos y de la integridad de los datos, por lo que sólo en algunos casos se va a producir este solapamiento.

Un fenómeno similar se produce con la firma electrónica avanzada[98], dado que la misma exige la identificación del firmante, la vinculación unívoca con el firmante, y la posibilidad de detectar la modificación ulterior de los datos; esto es, la autenticación de la entidad, la autenticación del origen de los datos y la integridad de los datos; servicios que se pueden sustentar tecnológicamente en un medio de identificación electrónica, tal y como el mismo se define en el Reglamento eIDAS.

Es decir, que en ambos casos (firma electrónica avanzada y sello electrónico avanzado), nos vamos a encontrar con la posibilidad de que algunos sistemas de identificación electrónica ofrezcan exactamente sus mismas funcionalidades, como por ejemplo en el caso del uso de la firma digital basada en certificado no cualificado –en su caso, con el concurso de una tarjeta criptográfica– como medio de identificación electrónica[99].

En efecto, es evidente que las tecnologías como la firma digital basada en certificado, que hemos presentado con cierta extensión anteriormente, pueden funcionar de forma indistinta como medio de identificación electrónica y como servicio de confianza, por lo que cabe preguntarse entonces de qué depende que cierta tecnología reciba la denominación de sistema de identificación electrónica, de servicio de confianza (de firma o sello electrónico), o de ambas a la vez, a lo cual encontramos respuesta que en la simple voluntad política de cada Estado miembro, que en ejercicio de su soberanía puede decidir que dicho sistema lo sea –en virtud de su reconocimiento como tal–, e incluso los efectos

---

[96] Más en concreto, la autenticación transfronteriza para el acceso a servicios públicos que, como veremos, se considera un servicio público reservado a la autoridad pública competente de cada Estado miembro.

[97] Por este motivo, para (Dumortier, 2016, p. 6) el concepto de autenticación es más amplio que el de identificación.

[98] Pero no con la firma electrónica (no avanzada), en cuya definición sólo se exige que se pueda emplear para firmar (cfr. artículo 3.10 del Reglamento eIDAS).

[99] Por ejemplo, en el caso de las personas físicas, el DNI electrónico; mientras que, en el caso de las personas jurídicas, el certificado expedido por la FNMT-RCM podría ser un excelente candidato.

jurídicos que le quiera dar[100]. Y si la única diferencia es el cumplimiento de las condiciones de uno u otro régimen jurídico, ello implica que todos los certificados cualificados que se expidan en España, con independencia de la titularidad del servicio, pública o privada, son candidatos potenciales a ser reconocidos como medios de identificación electrónica por el Estado[101].

Ciertamente parece poco interesante, desde una perspectiva de mercado único digital, que un Estado miembro se limite a la expedición de estos medios de identificación electrónica, por mucho que los mismos permitan la autenticación del origen de los datos y la integridad de los datos, sin que los mismos cumplan también lo estipulado para ser considerados como firma o sello electrónico avanzado o cualificado, básicamente porque –como veremos posteriormente con mayor detalle– estos sistemas no serían reconocidos en los restantes Estados miembros y, por tanto, su valor sería claramente inferior a los servicios de confianza técnicamente equivalentes[102].

Más común será, sin embargo, la existencia de otros escenarios de interrelación entre los medios de identificación electrónica y los servicios de confianza. Por ejemplo, determinados medios, como el DNI electrónico español, contienen un certificado de identidad (utilizable como medio de identificación electrónica) y, además, un certificado de firma electrónica cualificada (servicio de confianza, sujeto a la regulación). Otra posibilidad es que un mismo mecanismo técnico sirva para las dos funcionalidades a la vez, en cuyo caso debe cumplir con la regulación prevista para la identificación electrónica y para el servicio de confianza correspondiente, de forma acumulativa.

Finalmente, serán también frecuentes los medios de identificación electrónica que simplemente no sean técnicamente idóneos para cumplir con los requisitos de los servicios de confianza cualificados, por lo que podrán emplearse para firmar, pero sin que resulte necesario que el emisor se someta al régimen previsto para este tipo de servicios. Éste sería el caso, por ejemplo, de medios de identificación basados en contraseñas de un solo uso, que no se basan en certificados y, por tanto, no pueden sustentar una firma electrónica cualificada[103].

1.2.2 El alcance de la regulación de la Unión y su relación con la legislación nacional

Presentado el concepto de identificación electrónica en el Reglamento eIDAS, conviene delimitar el alcance de la regulación por parte del citado Reglamento, y su relación con

---

[100] En efecto, igual que por Ley formal se pueden establecer los efectos jurídicos sustantivos de la firma electrónica, inclusive su equiparación previa con la firma escrita, y presunciones procesales que favorezcan su utilización, también se puede hacer en relación con los sistemas de identificación si se considera oportuno.

[101] De esta forma ha ido ocurriendo hasta la fecha en la participación de España en el proyecto STORK, y también así parece haber sido recogido en la reforma de la legislación de procedimiento administrativo común, que regula la identificación electrónica.

[102] Desde luego, sería poco comprensible que una empresa de un Estado miembro pudiera acceder a un procedimiento de contratación electrónica empleando su identificación electrónica, pero que después no pudiera sellar electrónicamente la proposición económica.

[103] Algo que la experiencia del sector privado ha mostrado claramente innecesario, desde luego.

la regulación en el nivel nacional, a la que nos referiremos –en el caso de España– posteriormente con mayor detalle[104].

Lo primero que hay que decir es que el Reglamento eIDAS se limita a establecer "las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro", según dispone su artículo 1.a), condiciones que orbitan fuertemente alrededor de las cuestiones de seguridad e interoperabilidad[105] de los sistemas y medios de identificación electrónica, como tendremos ocasión de analizar en detalle infra[106], resultando, sin embargo, muy notable que el Reglamento eIDAS no haya establecido ningún régimen jurídico de supervisión y control[107] en relación con el uso de estos medios.

Como el propio Reglamento eIDAS indica, uno de sus objetivos es "eliminar las barreras existentes para el uso transfronterizo de los medios de identificación electrónica utilizados en los Estados miembros para autenticar al menos en los servicios públicos" (Considerando 12), por lo que el Reglamento parte de una realidad preexistente, que son estos sistemas de identificación que los Estados miembros habían ido estableciendo, en el pasado, para sus ciudadanos, principalmente en relación con el acceso a los servicios públicos, y que no se encontraban cubiertos por la DFE[108], en lugar de apostar por un sistema estandarizado de identificación electrónica europea, para todos los ciudadanos y empresas o por el desarrollo de una identificación electrónica europea común[109].

En el mismo sentido, el propio Considerando 12 del Reglamento eIDAS aclara que "lo que pretende es garantizar que sean posibles la identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros", en respuesta a las necesidades de realización del mercado interior[110], que se han ido plasmando en diferentes instrumentos legislativos, entre los cuales revisten especial importancia la Directiva 2006/123/CE del Parlamento Europeo y

---

[104] Cfr. el epígrafe 2.2 de este trabajo.

[105] Como he tenido ocasión de indicar en otro lugar (Alamillo Domingo, 2010b, pág. 52), "[e]l nuevo contexto de actuación se encuentra marcado por la heterogeneidad y la complejidad", incluyendo "[m]uchas identidades (pese a ser de más calidad): públicas, privadas, nacionales, regionales, locales, sanitarias, financieras... con tendencia a la reducción y generalización de las identidades en algunos espacios, y al incremento de las identidades de primera parte (en redes sociales, donde los usuarios se identifican a sí mismos)", y "[m]uchos proveedores en red sobre atribuciones y capacidades de personas: Administraciones Públicas, registros jurídicos y notariales, y de entidades privadas, con tendencia a la alta especialización y consumo en línea, mediante servicios web automatizados".

[106] Cfr. los epígrafes 3.1.3 y 3.1.7 de este trabajo.

[107] Así lo ha indicado (Gobert, 2015, p. 11).

[108] Cfr. el apartado 1 de la exposición de motivos de la Propuesta de Reglamento eIDAS.

[109] (Merchán Murillo, 2018, pág. 14).

[110] En opinión de (Aavik & Krimmer, 2016, p. 160), no resultaría posible un Mercado Único Digital sin la existencia de herramientas como el eIDAS, que al menos "teóricamente permitiría crear un sistema en el que los Estados podrían hacer uso de los mejores servicios públicos electrónicos existentes (p.ej. el sistema tributario creado en un Estado, un sistema de pensiones de otro y un registro de salud de otro) haciendo la administración electrónica significativamente más eficaz y eficiente en costes" (la traducción es mía).

del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior[111], y la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza[112], ambas citadas expresamente en el Reglamento eIDAS, pero sin que tengan menor importancia otros instrumentos de relación transfronteriza entre los ciudadanos y el sector público.

Así sucede en determinados casos en el ámbito de la contratación pública electrónica[113], de la facturación electrónica[114], del derecho societario[115] o de la gestión tributaria electrónica[116]; o incluso para el acceso a los datos personales oficiales o para el voto electrónico[117].

---

[111] En relación con esta Directiva, el Considerando 9 del Reglamento eIDAS indica que "en la mayoría de los casos, los ciudadanos de un Estado miembro no pueden utilizar su identificación electrónica para autenticarse en otro Estado miembro porque los sistemas nacionales de identificación electrónica en su país no son reconocidos en otros Estados miembros. Dicha barrera electrónica excluye a los prestadores de servicios del pleno disfrute de los beneficios del mercado interior. Unos medios de identificación electrónica mutuamente reconocidos facilitarán la prestación transfronteriza de numerosos servicios en el mercado interior y permitirán a las empresas actuar fuera de sus fronteras sin encontrar obstáculos en su interacción con las autoridades públicas".

[112] En relación con esta Directiva, el Considerando 10 del Reglamento eIDAS indica que "el reconocimiento mutuo de la identificación y la autenticación electrónicas es esencial para que la atención sanitaria transfronteriza de los ciudadanos europeos se haga realidad", especificando que "cuando una persona se desplaza para ser tratada, sus datos médicos deben ser accesibles en el país que dispense el tratamiento. Para ello es necesario contar con un marco de identificación electrónica sólido, seguro y confiable".

[113] Aunque la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE, regula en su artículo 22.6 el uso de sistemas de firma electrónica avanzada para la transmisión y recepción electrónica de las ofertas y propuestas de participación, en otros muchos casos se puede acudir al empleo de medios de identificación electrónica por parte de los licitadores, ya que en todo caso los requisitos de seguridad de las comunicaciones deben establecerse de acuerdo con criterios de proporcionalidad (cfr. Considerando 57). Una posibilidad particularmente interesante la encontramos en la subasta electrónica (cfr. artículo 35 de la Directiva).

[114] En este sentido, la Directiva 2014/55/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la facturación electrónica en la contratación pública no incluye entre sus requisitos el de la firma electrónica de la factura (cfr. el Considerando 25), por lo que la entrega de la misma por el contratista al organismo del sector público se podría realizar perfectamente mediante un sistema de identificación. En sentido similar, la Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido, en su redacción por Directiva 2010/45/UE del Consejo, de 13 de julio de 2010, indica en su artículo 233 que se deberá garantizar la autenticidad del origen y la integridad del contenido de la factura por los medios elegidos por el sujeto pasivo, entre los que, desde luego, se puede emplear el medio de autenticación de que haya sido dotado.

[115] La Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las sociedades unipersonales privadas de responsabilidad limitada (COM/2014/0212 final), prevé en su artículo 14.5 la posibilidad de que dichas los socios fundadores de dichas sociedades puedan emplear, para su registro en el Estado miembro donde tengan su domicilio social, cualquier identificación expedida en otro Estado miembro por las autoridades de dicho Estado o en su nombre, incluida la identificación expedida por vía electrónica.

[116] Por ejemplo, la Propuesta de Directiva del Consejo por la que se modifica la Directiva 2006/112/CE, relativa al sistema común del impuesto sobre el valor añadido, en lo que respecta a una declaración de IVA normalizada (COM/2013/0721 final), finalmente retirada por la Comisión el 30 de abril de 2016, previó la presentación por vía electrónica empleando los sistemas previstos en el Reglamento eIDAS.

[117] Cfr. el epígrafe 30 del Dictamen del Comité de las Regiones – La política y la gobernanza de internet

Desde una perspectiva formal, la regulación del Reglamento eIDAS es extraordinariamente respetuosa con las competencias de los Estados miembros en materia de identificación electrónica, limitándose a establecer un marco para el reconocimiento mutuo de los sistemas en cuestión[118] y, en relación con el mismo, legitimar la prestación, por parte del ejecutivo europeo y de los Estados miembros, de un servicio público europeo en soporte de la autenticación en línea transfronteriza.

Muestra de este respeto es que la norma "no se propone intervenir en los sistemas de gestión de la identidad electrónica e infraestructuras conexas establecidos en los Estados miembros" (Considerando 12), que resultan, por tanto, competencia exclusiva de los Estados miembros; o que "los Estados miembros deben seguir siendo libres de utilizar o introducir, a efectos de identificación electrónica, medios de acceder a los servicios en línea [… y] poder decidir si interviene o no el sector privado en la prestación de estos medios" (Considerando 13), cuestiones que de nuevo quedan en la esfera de competencia propia y exclusiva de cada Estado miembro de la Unión.

Finalmente, el Considerando 13 del Reglamento eIDAS también dice que "los Estados miembros no deben estar obligados a notificar sus sistemas de identificación electrónica a la Comisión", por lo que "corresponde a los Estados miembros decidir si notifican todos, algunos o ninguno de los sistemas de identificación electrónica utilizados a nivel nacional para el acceso al menos a los servicios públicos en línea o a servicios específicos", de forma que nos encontramos frente a una regulación con un fuerte elemento de voluntariedad.

Podemos, en su consecuencia, encontrar un segundo elemento de diversidad entre los diferentes Estados miembros de la Unión Europea, incluyendo Estados que introducen sistemas de identificación electrónica y que los notifican para su uso transfronterizo, frente a Estados que introducen estos sistemas de identificación electrónica sólo para su uso interno.

En realidad, desde la perspectiva del Reglamento eIDAS, veremos que la identificación electrónica se enfoca como una colección de servicios públicos electrónicos, a diferencia de los servicios de confianza –de carácter marcadamente mercantil–, que pueden ser prestados en régimen de gestión directa o indirecta[119], aunque también podría ser un

---

(2015/C 019/14), de 4 de diciembre de 2014, emitido con ocasión de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: La política y la gobernanza de internet – El papel de Europa en la configuración de la gobernanza de internet, COM (2014) 72 final/2, de 12 de febrero de 2014.

[118] (Merchán Murillo, 2016, págs. 35-36), sin embargo, considera que "habían sido los Estados miembros los que habían tomado la iniciativa, proponiendo los sistemas de identificación a los ciudadanos, así como a los sistemas nacionales de gestión de identidades, siendo muchos países los que han desarrollado e implantado (o están en proceso de hacerlo) tarjetas de identidad electrónicas (Alemania, España, Italia, entre otros); dado que la UE no había hecho uso del poder concedido en el Tratado de Lisboa", razón por la que "surge la necesidad de armonizar la amplia y diversa gama de leyes nacionales sobre e-ID, como un imperativo del mercado interno, lo que ha justificado, a nuestro juicio, la aprobación del Reglamento 910/2014 relativo a la identificación electrónica y servicios para las transacciones electrónicas en el mercado interior". Formalmente no puede hablarse de dicha armonización, menos aún a la luz de las diferentes experiencias legislativas posteriores al propio Reglamento eIDAS, sin perjuicio de que las normas de reconocimiento mutuo e interoperable, que sí se encuentran armonizadas, generen también un impacto en el nivel nacional, acercando los diferentes sistemas.

[119] En función de la personificación jurídica de la entidad prestadora del servicio, nos podríamos encontrar

servicio privado reconocido por el Estado (cfr. artículo 7.a) del Reglamento eIDAS), aunque siempre bajo su responsabilidad.

Como consecuencia de esta orientación, el Reglamento eIDAS no será aplicable a los sistemas de identificación electrónica prestados por entidades públicas o privadas que no hayan sido reconocidos por el Estado en cuestión, que quedarían fuera de regulación del Reglamento eIDAS[120]. Esto no significa que no se pueda expedir identificación electrónica por el sector privado, ni que la misma no obtenga reconocimiento alguno, sino que dicha actividad se realiza de forma autorregulada, basada en acuerdos entre las partes, y sin perjuicio de que la misma pueda ser objeto de legislación sectorial en el nivel de la Unión Europea, o de legislación nacional.

En definitiva, el Reglamento eIDAS no constituye la base legal para la regulación de los sistemas de identificación electrónica en los Estados miembros, sino sólo para su reconocimiento mutuo en las operaciones transfronterizas, por lo que la verdadera regulación de dichos sistemas la encontraremos en el nivel nacional. Ciertamente, la libertad que tendrá cada Estado para regular su/s sistema/s de identificación electrónica vendrá condicionada por las reglas del Reglamento eIDAS, porque el cumplimiento de las mismas es condición para el dicho reconocimiento mutuo, de modo que su eficacia como instrumento regulador es innegable.

Finalmente, es preciso reseñar que del análisis del Reglamento eIDAS se deriva con claridad que sus previsiones sólo se aplican a la autenticación en línea[121], por lo que también quedaría potencialmente excluida la autenticación presencial, lo cual es relevante desde la perspectiva de la libre circulación de personas que se desplazan físicamente al territorio de otro Estado miembro[122].

Esto tiene una explicación bastante evidente, que viene dada por el hecho de que no siempre sucederá que un mecanismo de autenticación en línea se encuentre sustentado por un instrumento físico que acredite la identificación presencial. En efecto, aunque esto es así en el caso de instrumentos como los documentos nacionales electrónicos de identidad o los pasaportes electrónicos, que son instrumentos de viaje, que permiten los desplazamientos fuera del territorio nacional, y que también pueden incorporar medios de identificación electrónica, no lo será en otros casos, como por ejemplo en medios de identificación electrónica (por ejemplo, suministrados por entidades privadas) sustentados en dispositivos móviles como los teléfonos inteligentes.

---

ante un nuevo caso de ejercicio de potestades administrativas por parte de sujetos privados, resultando que, a juicio de (Gamero Casado, 2018), cito por la versión electrónica, "no debe resultar inaceptable que la Administración transfiera el ejercicio de potestades administrativas a sus medios propios, aunque tengan forma de personificación jurídico-privada, siempre y cuando su ejercicio se siga sometiendo al Derecho administrativo, tal y como pretende la disposición en examen", refiriéndose a la Ley 39/2015, de 1 de octubre, la cual valora positivamente, al menos en este aspecto.

[120] Aunque no necesariamente fuera del alcance de la regulación del nivel nacional, que teóricamente podría establecer reglas al respecto, algo que en España no ha ocurrido hasta la fecha.

[121] Cfr. artículos 6.1 y 7 del Reglamento eIDAS.

[122] Sin perjuicio de que en una transacción presencial se pueda producir, si resulta preciso, una autenticación en línea, de forma que por ejemplo el ciudadano desplazado a otro Estado pueda intercambiar atributos de forma transfronteriza con dicho Estado. Esta posibilidad resultaría posible en el modelo distribuido de STORK, si el ciudadano es dotado de un medio físico de identificación con el software intermedio.

Por más que estos medios de identificación electrónica sean habilitados, conforme a las reglas del Reglamento eIDAS que luego analizaremos[123], para la autenticación transfronteriza en línea, de ello no se va a derivar que los mismos puedan sustituir a los documentos públicos oficiales a que nos acabamos de referir, a efectos de la identificación personal.

No debemos cerrar este análisis inicial de la identificación electrónica en el Reglamento eIDAS y su relación con el Derecho nacional sin indicar que el Reglamento se abstiene de establecer obligación alguna de uso de los medios de identificación electrónica, cuestión que queda completamente en manos del legislador nacional, y que presenta delicados y polémicos interrogantes de orden constitucional, en la medida en que un exceso de identificación supone una evidente afectación al denominado anonimato en la red, reconducible a los derechos a la intimidad o a la protección de datos[124].

1.3 LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS

1.3.1 La "definición" de los servicios de confianza en el Reglamento eIDAS

El artículo 3.16) del Reglamento eIDAS no contiene, propiamente, una definición o concepto de servicio de confianza, sino más bien una enumeración de servicios de la sociedad de la información que, precisamente por ser incluidos en dicha lista cerrada, se consideran "servicios de confianza".

Estos servicios son "a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios".

Antes de entrar en la presentación, sucinta en este lugar, de los servicios de confianza, es preciso indicar que esta denominación de "servicio de confianza" contenida en el Reglamento eIDAS constituye una evolución y, al tiempo, ampliación semántica sobre la denominación de "servicio de certificación", y se puede fundamentar en el hecho de que estos servicios permiten aportar confianza a los procesos de negocio en los que se emplean, en gran medida gracias a los efectos jurídicos que se asocian a dichos servicios.

Muestra de ello es que la exposición de motivos del Reglamento eIDAS manifieste que "el presente Reglamento se propone reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la

[123] Cfr. el epígrafe 3.1 de este trabajo.

[124] Sobre esta cuestión, puede verse las contribuciones de (Roig Batalla, 2007, pág. 322 y ss.), y de (Barrat Esteve, 2010, pág. 823 y ss.), éste último, en referencia expresa a los que denomina "entificadores".

Unión"[125], para lo cual se precisa ir más allá de la regulación de firma electrónica, la cual no ofrecía "un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso"[126].

El Reglamento eIDAS, por tanto, persigue la creación de una ley uniforme para el mercado interno, proporcionando las normas jurídicas armonizadas en relación con varios servicios, que de hecho ya operaban en los estándares técnicos similares, y ofrece la posibilidad de coordinar las diferentes bases legales para el gobierno electrónico y sociedad digital de forma global, aunque también plantea retos importantes[127].

La propuesta de Reglamento[128], de hecho, se justifica por la Comisión Europea tanto desde la perspectiva de resolver las barreras *de facto* creadas por las legislaciones nacionales a la interoperabilidad de la firma electrónica, creando una situación de igualdad entre los prestadores de servicios de confianza (prueba de necesidad), así como considerando que no es esperable que estas dificultades sean superadas por la coordinación voluntaria entre los Estados miembros de la Unión (prueba de eficacia).

Esta noción de "servicio de confianza", también referido como "servicio confiable"[129] o "servicio en el que se confía", no es invención del Reglamento eIDAS, sino que puede encontrarse referenciada con bastante anterioridad por agentes del mercado, así como en la literatura académica, que la ha tratado desde una variedad de perspectivas[130], en una

---

[125] Considerando (2) del Reglamento eIDAS.

[126] Considerando (3) del Reglamento eIDAS.

[127] (Borges, 2012), cito la versión electrónica, en referencia a la Propuesta de Reglamento, critica la mezcla de la regulación de servicios de confianza y de identidad electrónica, la posibilidad de exclusión de la aplicación de algunos servicios de confianza basados en acuerdos de derecho privado de la regulación, o la insuficiente regulación de la identidad electrónica, especialmente en el caso de mal uso de dicha identidad.

[128] COM (2012) 238 final, sección 3.2.

[129] Para algunos autores, no se debería hablar tanto de "servicios de confianza" (*trust services*) como de "servicios confiables" (*trustworthy services*), como argumentan (Dumortier & Vandezande, 2012b).

[130] Así podemos citar, a título ejemplificativo, a (Olnes, 2001), que define la confianza como la percepción de ausencia de vulnerabilidades y, después de distinguir entre la confianza técnica y organizativa, ofrece una taxonomía de servicios en los que se confía en atención a características de dichos servicios, como el tipo de servicio, la calidad del servicio, la gestión de evidencias, la comunidad de usuarios, el modelo de confianza, los aspectos jurídicos y el patrón de comunicaciones. (Baldwin, Shiu, & Cassasa Mont, 2002) se refieren a los servicios de confianza como habilitadores del comercio electrónico e indican la existencia de servicios de confianza ampliamente instalados en los procesos en soporte papel, considerando que los prestadores de estos servicios son expertos en la gestión de riesgos referidos a los servicios que ofrecen, y aportan un listado de servicios candidatos a entrar en esta calificación: servicios de identidad, de autorización, de anonimato, de calificación y recomendación de confianza, de garantía de entrega de comunicaciones, de generación de acuses de recibo auditables, de almacenamiento y de notaría. Asimismo, estos autores se refieren también a la existencia de determinados servicios de componentes de confianza, que no tienen sentido para los usuarios finales, pero que se emplean en los restantes servicios de confianza, incluyendo los servicios de almacenamiento de claves, los servicios de archivo y los servicios de sellado de fecha y hora. Por su parte, para (Dumortier & Vandezande, 2012b), la confianza en las operaciones de comercio electrónico funciona de forma similar a una caja negra de avión: el usuario confía en que la máquina registrará todos los procesos y mantendrá una evidencia suficiente para poder reproducir lo que realmente sucedió; una aproximación que consideran puede resultar más efectiva que el empleo de documentos firmados electrónicamente. En su opinión, y con independencia de cuál sea la definición para el concepto de confianza, ésta siempre consiste en un estado interno del usuario evocado por las características de fiabilidad de la tecnología, una aceptación informada de la vulnerabilidad.

evolución a la luz de la cual, podríamos conceptualizar los servicios de confianza como aquellas tecnologías en las que se puede confiar, por lo que modifican la percepción del usuario con respecto a la vulnerabilidad de un proceso al que se incorporan; para lo cual el usuario debe poder reconocer un servicio de confianza, de hecho, como suficientemente confiable.

Esto implica la existencia de una relación de transitividad que conecta la confianza en un proceso o una transacción con el uso de uno o varios servicios de confianza; a su vez, la confianza en los servicios de confianza conecta con la regulación de la actividad del prestador y, más en concreto, en su fiabilidad; y la fiabilidad de la prestación del servicio conecta con la regulación de la fiabilidad de los productos y, en último término, de la criptografía empleada por dichos productos, como se puede ver en la Ilustración 3.

A los efectos indicados, podemos entender la aproximación del Reglamento eIDAS en orden a la creación de un nivel reforzado de servicios de confianza[131], lo cual no deja de llamar la atención, en el sentido de que realmente la confianza en dichos servicios parece nacer el hecho de que los mismos se encuentran regulados por el ordenamiento jurídico[132], más que de sus propias características técnicas.

Ilustración 3. Cadena de valor en el mercado de la confianza (elaboración propia)

En este sentido, el artículo 3.17) del Reglamento eIDAS nos aporta la noción de un "servicio de confianza cualificado", que define como "un servicio de confianza que cumple los requisitos aplicables previstos en el presente Reglamento", distinción relevante porque permite establecer, con carácter general, dos niveles de servicios "de confianza".

---

[131] (Rico Carrillo, 2015, pág. 4) opina que "[l]a confianza se refiere principalmente al grado de percepción en la seguridad del servicio prestado. La confianza y seguridad en las transacciones electrónicas han sido consideradas fundamentales en el desarrollo del comercio electrónico y de las operaciones con Administración pública; consumidores y usuarios demandan seguridad técnica y jurídica a efectos de poder confiar en los diferentes servicios de la sociedad de la información", especificando que "[l]La seguridad técnica se refiere principalmente a la utilización de mecanismos seguros que garanticen la autenticidad y confidencialidad de las transacciones (protocolos de seguridad, claves, servicios de certificación, etc.) mientras que la seguridad jurídica implica la definición de las obligaciones de las partes, principalmente de los prestadores de servicios a efectos de determinar la responsabilidad frente a una determinada actuación", y que "[l]a combinación de estos dos elementos provee un alto grado de seguridad a los usuarios de los servicios electrónicos", para concluir que "[e]stos dos factores son tomados en cuenta en la redacción del Reglamento, a efectos de proporcionar servicios de confianza de alta fiabilidad y cumplir el objeto primordial de la norma comunitaria".

[132] Una regulación que, desde luego, deberá incorporar unos mínimos para generar esta confianza. Entre otras cuestiones que veremos en su momento, resultan especialmente relevantes los aspectos de responsabilidad por la prestación de los servicios, y los instrumentos para asegurar ésta, como ha puesto de manifiesto (Ortega Díaz, 2008, pág. 149).

En primer lugar, nos podemos referir a un nivel "ordinario" de servicio de confianza, que no se encuentra prácticamente regulado, y que no recibe ningún reconocimiento legal en particular; en cuyo caso, el usuario debe construir su propio estado interno de confianza respecto al servicio. En este sentido, un usuario puede reconocer una contraseña de su entidad financiera como suficientemente segura para autorizar transacciones, pero no un servicio de almacenamiento de documentos en la Nube.

En segundo lugar, el Reglamento eIDAS se refiere al nivel "cualificado" de servicio de confianza, que se encuentra altamente regulado, y que recibe un reconocimiento particular de efectos legales, lo cual debería suponer un incentivo a su adopción[133]. En este caso, este reconocimiento legal explícito es el que permite al usuario reconocer el servicio como confiable, por lo que podemos asumir[134] que estos servicios se desarrollarán antes y en mayor volumen que los que no gocen de esta condición.

Es preciso también comentar que el Reglamento eIDAS contiene una lista cerrada de servicios de confianza, al objeto de delimitar el alcance de la regulación uniforme europea, pero que los Estados miembros pueden definir otros servicios de confianza[135], así como mantener (o introducir) disposiciones nacionales, acordes con el Derecho de la Unión, relativas a los servicios de confianza[136], siempre que tales servicios no estén plenamente armonizados por el Reglamento, consideraciones que muestran uno de los objetivos centrales de la regulación, como es garantizar la libre circulación de estos servicios en el mercado interior[137], mediante el establecimiento de un conjunto mínimo de normas armonizadas.

Una consecuencia de esta previsión es la más que posible divergencia en el catálogo de servicios de confianza en las diferentes jurisdicciones de la Unión Europea, a medida que el sector empresarial vaya generando nuevos servicios, a partir de la innovación tecnológica[138].

---

[133] En realidad, la dificultad de demostrar que un servicio es realmente cualificado puede llegar a eliminar todo el incentivo que ofrece el "reconocimiento" legal del servicio cualificado (Dumortier & Vandezande, 2012b), lo cual se intenta solventar, como veremos, mediante la imposición de la evaluación de la conformidad del servicio.

[134] Podría tratarse, sin embargo, de una apuesta arriesgada, dada la experiencia previa de la firma electrónica reconocida, que ha tenido una escasa adopción, por inhibidores de diversos tipos (Srivastava, 2011), o (Roβnagel, 2006). En efecto, hay que reconocer que el mayor uso de la firma electrónica basada en certificado electrónico se observa en los escenarios donde la Administración ha impuesto este mecanismo (como en el ámbito tributario) o bien ha ofrecido un incentivo extra para su uso (para habilitar usos privados como la factura electrónica, por ejemplo).

[135] En este sentido, el Considerando (25) del Reglamento eIDAS indica que "[l]os Estados miembros deben conservar la libertad para definir otros tipos de servicios de confianza, además de los que forman parte de la lista cerrada de servicios de confianza prevista en el presente Reglamento, a efectos de su reconocimiento a nivel nacional como servicios de confianza cualificados".

[136] Cfr. Considerando (24) del Reglamento eIDAS.

[137] El Considerando (24) el Reglamento eIDAS indica, *in fine*, que "los productos y servicios de confianza que se ajusten al presente Reglamento deben poder circular libremente en el mercado interior", algo que desde luego no sucede en la actualidad.

[138] Como han explicado (Ballbé & Padrós, 1997), la subsidiariedad provoca un proceso de competencia vertical entre los poderes centrales (de la Comunidad Económica Europea, hoy Unión Europea) y los Estados. Como en el modelo norteamericano, en este tipo de sistemas se puede visualizar la legislación

Respecto a la lista cerrada de servicios de confianza, la misma deriva de la propia definición del servicio de confianza cualificado que acabamos de ver y, en cuya virtud, sólo puede ser cualificado un servicio en relación con el que el Reglamento eIDAS ha establecido requisitos concretos. De ahí se desprende que, en realidad, disponemos de dos listas de servicios de confianza, dado que no todos los servicios de confianza pueden ser objeto de cualificación.

Más en concreto, los nueve servicios de confianza tipificados en el Reglamento eIDAS que pueden ser objeto de cualificación son los siguientes:

- Tres servicios de expedición de certificados electrónicos cualificados, para la firma electrónica de persona física, de sello electrónico de persona jurídica y de autenticación de sitios web, dado que el artículo 28 y el Anexo I del Reglamento eIDAS, el artículo 38 y el Anexo III del Reglamento eIDAS, y el artículo 45 y el Anexo IV del Reglamento eIDAS establecen, respectivamente, los correspondientes requisitos.
- Un servicio de expedición de sellos electrónicos cualificados de tiempo, dado que el artículo 42 del Reglamento eIDAS establece los correspondientes requisitos.
- Un servicio cualificado de entrega electrónica certificada, dado que el artículo 44 del Reglamento eIDAS establece los correspondientes requisitos.
- Dos servicios cualificados de validación de firmas electrónicas cualificadas y de sellos electrónicos cualificados, dado que el artículo 33 y el artículo 40 del Reglamento eIDAS establecen, respectivamente, los correspondientes requisitos, aplicándose el artículo 33 *mutatis mutandis* en el caso del sello.
- Dos servicios cualificados de conservación de firmas electrónicas y de sellos electrónicos cualificados, dado que el artículo 34 del Reglamento y el artículo 40 del Reglamento eIDAS establecen, respectivamente, los correspondientes requisitos, aplicándose el artículo 34 *mutatis mutandis* en el caso del sello.

En cambio, los servicios de confianza no cualificados incluyen, adicionalmente a las versiones no cualificadas de los nueve servicios contenidos en el listado anterior, también los siguientes[139], puesto que expresamente se citan en la definición de servicio de confianza contenida en el Reglamento eIDAS:

- Un servicio de creación de firma electrónica (ordinaria y avanzada) y de sello electrónico (ordinario y avanzado) a distancia.
- Un servicio de validación de certificados de firma electrónica, de sello electrónico y de autenticación de sitio web.
- Un servicio de conservación de certificados de firma y sello electrónico.

No parece razonable que deba existir esta diferenciación, al menos desde un punto de

---

nacional como un laboratorio de innovación normativa, que en su caso cristalizará en regulación armonizada en el ámbito de la Unión Europea. Desde luego, esto es precisamente lo que ha sucedido en el ámbito de los servicios de identificación y de confianza, y puede anticiparse que posiblemente continuará siendo así en el futuro, con los servicios emergentes en algunos Estados, como por ejemplo en el caso del archivo electrónico de documentos, ya regulado en Bélgica.

[139] El órgano de supervisión español, sin embargo, no incluye estos servicios en su listado, que se limita a las modalidades no cualificadas de los nueve servicios referidos.

vista teórico, dado que, en la lógica de doble nivel que se establece en el Reglamento eIDAS, cualquier servicio de confianza debería poder ser objeto de cualificación.

Sin embargo, es cierto que, si no se establecen requisitos específicos para un servicio de confianza, no existe el presupuesto para esta cualificación, al menos en la definición legal actual, que en definitiva es el cumplimiento de unas condiciones de fiabilidad mínimas que permitan establecer la confianza a la que antes nos referíamos.

Esta diferenciación puede producir, en definitiva, problemas de consistencia en el mercado, generando confusiones en los usuarios. Por ejemplo, con esta interpretación legal, resulta perfectamente imaginable que un prestador de servicios de confianza ofrezca el servicio (no cualificado) de creación de firma o sello electrónica/o avanzada/o a distancia, en su caso generando o gestionando los datos de creación de firma o sello correspondientes, mientras que la prestación del mismo servicio, pero en relación con la firma o sello electrónica/o cualificada/o, quedará reservada a cualquiera de los prestadores cualificados (para cualquiera de los servicios susceptibles de cualificación, claro), porque sólo quien gestiona los datos de creación correspondiente puede permitir la creación de la firma o sello.

Una posibilidad, más que razonable, es que el prestador que expide el certificado cualificado de firma o sello electrónica/o cualificada/o sea también el que ofrezca el servicio de generación o gestión de los datos de creación correspondientes, dado que dicho prestador precisamente resulta responsable, frente a terceros, de que el dispositivo empleado sea cualificado, pero también resulta imaginable un modelo en el que otro prestador cualificado de servicios de confianza realice esta generación o gestión de los datos de creación de firma o sello electrónica/o cualificada/o, como en el caso de un prestador que ofrezca servicios de validación y/o conservación de firma o sello.

1.3.2 El aparente descuadre de la identificación electrónica en la categorización de los servicios de confianza

Aparentemente descuadra, en esta construcción, que la regulación de la prueba de la identificación no se haya tipificado como servicio de confianza típico[140], dado que en efecto no se incluye de forma expresa en la definición de estos servicios, sino que tiene la suya propia, pero en realidad esto no es del todo cierto.

En primer lugar, sucede que existen servicios de confianza armonizados en el Reglamento eIDAS que tienen, entre sus efectos jurídico típicos, el de permitir la identificación electrónica. Éste es el caso de la expedición de certificados de firma electrónica de persona física, un servicio de confianza armonizado por el Reglamento eIDAS, confirma la identidad de dicha persona física; y de la misma forma ocurre con el certificado de sello electrónico de persona jurídica, que confirma su identidad. Por ello, estos servicios de confianza, que pueden ser objeto de cualificación, permiten la identificación electrónica[141].

---

[140] (Kennedy & Millard, 2016, p. 102).

[141] Es cierto que se puede argüir que esta función de identificación electrónica lo es en conexión con la firma electrónica o el sello electrónico, por lo que un certificado que no tuviera el propósito de permitir generar firmas o sellos electrónicos estaría fuera del ámbito de los servicios de confianza armonizados por el Reglamento eIDAS, por lo que debería ser definido como servicio de confianza en sede nacional,

De forma similar ocurre con la autenticación –que cumple realmente la función de identificación– de los sitios web, que se trata en el Reglamento eIDAS, a diferencia de la identificación electrónica de las personas, como un servicio de confianza armonizado, inclusive con cualificación.

En segundo lugar, el motivo por el que no se trata la identificación electrónica como servicio de confianza en el Reglamento eIDAS es su consideración como prerrogativa nacional[142], que permite su mantenimiento por el Estado como servicio público, sin que se encuentre obligado a autorizar su prestación por operadores privados, y menos como actividad económica, puesto que esa es la implicación directa de su tipificación como servicio de confianza. Pero de ello no se desprende que no pueda adoptarse esta decisión en sede nacional, aunque no parece que de momento se esté incluyendo este servicio en la categoría de servicio de confianza, cuando se regula su prestación por empresas privadas[143].

En todo caso, lo que sucede es que la identificación electrónica de las personas –que no de los sitios web– realmente tiene diversos regímenes jurídicos aplicables, que resultan plenamente alternativos, y que pueden incluso convivir en un mismo Estado miembro, pudiendo ser tratada como un servicio público, como un servicio de confianza, o como incluso como un tercer tipo de servicio privado, en función de lo que decida cada Estado miembro.

Sin embargo, dado que existen servicios de confianza que permiten, en todos los casos, la identificación electrónica –en concreto, los de expedición de certificados de firma electrónica de persona física, de sello electrónico de persona jurídica y de autenticación de sitio web–, hay que concluir que los servicios de confianza van a permitir cubrir todas las necesidades de generación de prueba de la actuación electrónica, sin perjuicio de que la prueba de identificación electrónica se va a poder sustentar, además de en algunos servicios de confianza típicos, en mecanismos que no se sujetan a la normativa de servicios de confianza, cuando el Estado en cuestión decida adoptarlos.

Todo esto explica, en realidad, que la normativa contenida en el Reglamento eIDAS no sea aplicable a la identificación electrónica excepto en cuanto a su reconocimiento transfronterizo entre los Estados miembros, lo cual ciertamente implica establecer un efecto jurídico típico para estos sistemas, que es "servir para el acceso transfronterizo a servicios públicos y, eventualmente, privados", pero nada más.

Desde esta perspectiva, la regulación de la identificación electrónica contenida en el Reglamento eIDAS presenta una extensión diferente a la regulación de los servicios de confianza, porque sólo regula su dimensión de uso transfronterizo, mientras que la regulación de los servicios de confianza se refiere tanto al uso transfronterizo de los servicios, como al régimen para su prestación y a sus efectos jurídicos sustanciales.

---

limitando sus efectos a la misma – excepto su notificación como medio de identificación electrónica conforme al Reglamento eIDAS. Pero no es menos cierto que desde luego la prueba que sustentan, de forma primaria, es la de identidad. Cfr. el epígrafe 2.1.3 de este trabajo.

[142] Cfr. el Considerando (12) del Reglamento eIDAS.

[143] A título de ejemplo, tanto Finlandia como Italia han regulado la prestación de este servicio por parte de empresas privadas, pero sin denominarlo como "servicio de confianza".

1.3.3 El modelo regulatorio de los servicios de confianza tipificados en el Reglamento eIDAS

Desde el punto de vista de la teoría de las fuentes, los servicios de confianza se rigen, con carácter general, por el Reglamento eIDAS y por las leyes nacionales que lo complementen en cuanto a dicha categoría de servicios. Adicionalmente, estos servicios de confianza, sean o no cualificados, pueden también ser considerados como una subespecie de los servicios de la sociedad de la información[144], por lo que resultarán aplicables a los mismos, cuando sean ofrecidos por prestadores españoles, las reglas de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, si bien únicamente en la parte que no entre en conflicto con la normativa armonizada. Y, por supuesto, formarán parte del marco aplicable todas las restantes normas del ordenamiento jurídico que resulten procedentes, como por ejemplo en el ámbito laboral, tributario, etc.

A partir de las fuentes jurídicas ya mencionadas, y desde la óptica de los diversos modelos jurídicos que emergen de las mismas[145], el Reglamento eIDAS –a diferencia del enfoque

---

[144] Cfr. (Pérez Pereira, 2009, pág. 29). En efecto, estos servicios encajan perfectamente bien en la definición del artículo 2.a) de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, que remite a la Directiva 98/34 del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, referencia que hoy debe entenderse realizada a la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, que ha derogado a la citada Directiva 98/34. También (Rodríguez Ayuso, 2018, pág. 150 y ss.) considera que los servicios de confianza pueden ser considerados servicios de la sociedad de la información, añadiendo que resultan encuadrables en los servicios de intermediación, al resultar instrumentales para la contratación electrónica.

[145] Es preciso recordar, siguiendo a Miguel Reale, la diferencia entre las fuentes jurídicas y los modelos jurídicos. Como explica (García Medina, 1995, pág. 181) "la idea de modelo, por el contrario, «nos sitúa ante un momento autónomo de la vida del derecho», momento en el que la experiencia jurídica pasa a «formas objetivadas y positivas, consubstanciándose en esquemas o estructuras racionales, en las que los elementos de la estructura social son enfocados a través de un repertorio o clase de comportamientos válidos en una totalidad de sentido»", por lo que, mientras que "la fuente sea legislativa, consuetudinaria, etc., es una estructura social que, en función de las competencia previamente determinadas, posibilita la instauración o singularización de otras estructuras que son los modelos legales, consuetudinarios, etc.", sucede que "[e]l modelo jurídico se separa de la fuente de la que procede, debido a la exigida y constante adecuación a los diversos hechos sociales", por lo que el modelo tiene naturaleza prospectiva y un marcado carácter operacional, frente a la naturaleza retrospectiva de la fuente, en la que predomina el sentido técnico-formal de la vigencia de las normas. Cuanto se acaba de decir refleja perfectamente bien el modelo de los servicios de confianza. En este sentido, (De Miguel Asensio, 2015, pág. 959 y ss.) aprecia, a partir del análisis del derecho comparado, "básicamente la existencia de tres modelos diferentes de regulación, según el nivel de intervención […] un primer enfoque [que] se caracteriza por ser reglamentista, al atribuir reconocimiento legal en determinadas circunstancias a una modalidad específica de creación de firma electrónica –basada en el uso de la criptografía asimétrica de clave pública–, regularen detalle los requisitos a los que se subordina el funcionamiento de las entidades de certificación así como su régimen de responsabilidad, y atribuir derechos y obligaciones a los titulares de las claves […] un segundo modelo [que] pretende facilitar en términos generales el empleo de las firmas electrónicas para eliminar dudas y obstáculos acerca de su eficacia, pero sin regular las especificaciones de medidas tecnológicas previstas a ese fin, limitándose a lo sumo a enumerar los requisitos que esas firmas deben satisfacer para ser equiparadas a las incluidas en soportes materiales […] y […] un tercer modelo normativo [que] contempla

de la DFE, y lógicamente, de lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE), donde la prestación de los servicios de certificación era completamente libre[146], aunque matizada por la figura de la acreditación[147]–, opta por una orientación regulatoria de control previo en relación con la prestación de los servicios de confianza cualificados que el mismo regula, si bien con alguna particularidad que resulta interesante comentar; al tiempo que mantiene la supervisión *a posteriori* en relación con los sistemas sin cualificación, y deja plena libertad a los Estados miembros en relación con el modelo regulatorio de los servicios de confianza que establezcan en sede nacional.

Se trata, por tanto, de un sistema mixto, en el que se gradúa la intensidad de la intervención administrativa en función, en definitiva, de los efectos asociados a los servicios de confianza, y que supone un retorno parcial a modelos regulatorios preexistentes a la propia DFE, que sometían a licencia previa la oferta de estos servicios[148].

Efectivamente, y sólo en relación con los servicios cualificados de confianza tipificados en el Reglamento eIDAS, su artículo 21.1 dispone que el prestador, que no disponga de cualificación, para poder iniciar su actividad relativa a servicios cualificados, debe presentar al organismo de supervisión una notificación de su intención[149] junto con un informe de evaluación de la conformidad expedido por un organismo de evaluación de la

---

la eficacia legal de las firmas electrónicas en términos muy amplios y flexibles, pero [que] de otra parte regula de manera detallada los requisitos que deben cumplir ciertas firmas electrónicas a las que se atribuye una eficacia reforzada y que se vinculan en la práctica con el uso de técnicas de criptografía asimétrica".

[146] Algo que no estuvo exento de polémica, dada la existencia de un sector de la doctrina, de corte fedatarista, que defendía la existencia de un régimen de reserva de actividad en favor de los notarios, dada su función tradicional de identificación personal, como han explicado (Huerta Viesca & Rodríguez Ruiz de Villa, 2001, pág. 93).

[147] En la regulación anterior a la LFE; esto es, en el Real decreto-ley 14/1999, de 17 de septiembre (RDLFE), existía un sistema voluntario de acreditación de la actividad de los prestadores y de certificación de los productos de firma, cuyo efecto jurídico era precisamente el de presumir el cumplimiento de los requisitos por parte del sistema de firma electrónica avanzada; sistema que fue desarrollado por Orden del Ministerio de Fomento de 21 de febrero de 2000 y que podía considerarse como un sinónimo a una autorización, al menos en relación con los certificados reconocidos (Martínez Nadal, 2001, pág. 167 y ss), jamás derogada y, por tanto, todavía formalmente vigente. (Alonso Ureba & Alcover Garau, 2000, pág. 203) criticaron "la opción de la Posición Común y, por ende, del Real Decreto-ley de establecer que no es precisa la autorización previa para poder ejercer la actividad certificadora: la señalada importancia pública de ésta para el buen funcionamiento del tráfico electrónico debería llevar a la necesidad de la previa autorización, a la que además se podrían conectar los efectos que ahora se enlazan a la acreditación voluntaria", algo que pasaría, como hemos visto, catorce años más tarde con la aprobación del Reglamento eIDAS.

[148] Como explica (Galindo, 1998, pág. 119), en relación con la legislación alemana de firma electrónica preexistente a la DFE, "[l]o más interesante a reseñar de esta regulación es que ésta no es una normativa de firma digital simplemente, como es lógico abarca a la arquitectura de red necesaria para el mantenimiento de la firma", resaltando que "[l]as disposiciones muestran la constitución por la legislación alemana de una red de seguridad y garantía de las comunicaciones electrónicas de carácter mixto: dependiente de la voluntad de los particulares al tener libertad para contratar con uno u otro servicio de certificación, y de la voluntad política del Estado ejercida mediante el otorgamiento de licencias para los servicios de certificación y el establecimiento de medidas de seguridad por parte de la Autoridad regulativa en materia de Telecomunicaciones", modelo que resulta ciertamente parecido al finalmente adoptado en el Reglamento eIDAS, aunque sólo para los servicios cualificados.

[149] Cfr. el epígrafe 7.1.2.1 de este trabajo.

conformidad[150], mientras que el artículo 17, en sus epígrafes 3.a) 4.g), determina que dicho organismo nacional realizará actividades de supervisión previa y de concesión de la cualificación[151], no pudiéndose iniciar la prestación del servicio hasta haber obtenido dicha cualificación (artículo 21.3), y que la misma haya sido difundida públicamente mediante el mecanismo de lista de confianza[152] previsto en el artículo 22 del Reglamento eIDAS.

Este enfoque se justifica en el Considerando (45) del Reglamento eIDAS, cuando indica que "[a] fin de permitir un proceso de puesta en marcha eficiente, que lleve a la inclusión de los prestadores cualificados de servicios de confianza y de los servicios de confianza cualificados que prestan en listas de confianza, deben fomentarse las interacciones preliminares entre los candidatos a prestadores cualificados de servicios de confianza y el organismo de supervisión competente con vistas a facilitar la diligencia debida que lleve a la prestación de servicios de confianza cualificados", proceso previo que, aunque con una terminología algo oscura, materialmente se trata de una autorización[153], que deberá concederse en aplicación del correspondiente procedimiento administrativo, en el marco de la legislación nacional.

Además, el prestador cualificado de servicios de confianza deberá superar una evaluación de la conformidad al menos cada dos años, y remitirla al supervisor, tal como determina el artículo 20.1 del Reglamento eIDAS, así como soportar las auditorías que le realice el supervisor, o las evaluaciones adicionales de la conformidad que el mismo le imponga, en virtud de lo dispuesto en el apartado 2 del propio artículo 20 del Reglamento eIDAS.

Esta nueva orientación regulatoria, que se muestra en la Ilustración 4, supone una clara excepción al enfoque de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la

---

[150] Cfr. el epígrafe 7.1.1 de este trabajo.

[151] Cfr. el epígrafe 7.1.2 de este trabajo.

[152] Cfr. el epígrafe 7.1.4.1 de este trabajo.

[153] Conforme a la caracterización contenida en el Considerando (39) de la Directiva 2006/123/CE, del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior, la cualificación debe considerarse como un régimen de autorización, a los efectos de la norma europea. Para (Mora Ruiz, 2016, pág. 1121) en la autorización se muestra "la necesidad de una intervención previa de las Administraciones para constatar la legalidad de la actividad", de modo que "la construcción dogmática de estos títulos ha tenido dos consecuencias inmediatas: En primer lugar, la actividad resulta clandestina si no se ha sometido al control previo (y preventivo) de la Administración. Y, en segundo lugar, se ha aceptado generalmente una intensidad diferente en cuanto a la intervención de la Administración en la esfera de derechos de los ciudadanos atendiendo a los efectos de la misma, de forma que el término autorización-licencia se ha asociado a los supuestos en los que la Administración contrasta, *grosso modo*, que el particular cumple los requisitos exigidos por el Ordenamiento para la realización de una actividad o el ejercicio de un derecho", caso al que se contrapone la concesión; sin perjuicio de la necesidad de adecuar esta construcción a los principios dimanantes de la Directiva de Servicios. En este sentido, (Rico Carrillo, 2015, pág. 8) considera que "[e]n el caso previsto en el Reglamento para los prestadores de servicios de confianza cualificados, aunque no se trata en sí de una autorización previa al inicio de la actividad (en el entendido que estos sujetos ya se encuentran prestando servicios), sino de una cualificación administrativa a efectos de prestar servicios de confianza cualificados, el acto administrativo en cuestión podría ser catalogado como una autorización, en este caso, el régimen de autorización encuentra su justificación en la finalidad primaria de la norma, que como ya hemos indicado, se centra la necesidad de reforzar la seguridad y confianza en los servicios electrónicos". También considera (Gobert, 2015, p. 27) que nos encontramos ante una autorización.

sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), que en su artículo 4 prohíbe la sujeción de los servicios de la sociedad de la información a autorización previa ni a ningún otro requisito con efecto equivalente, y de la Directiva 2006/123/CE, del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior, que limita la posibilidad de restringir el acceso de las actividades de servicios y su ejercicio a un régimen de autorización únicamente cuando se den determinadas circunstancias[154].

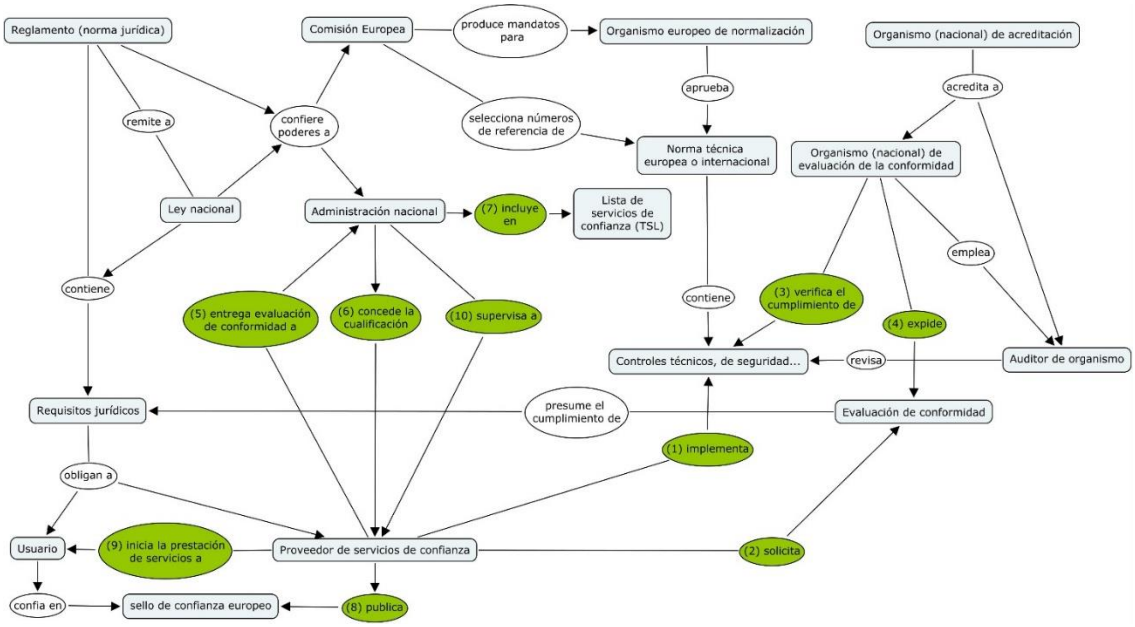


Ilustración 4. Estructura regulatoria de los servicios de confianza (elaboración propia)

Aunque dicha Directiva no impide que sea una norma jurídica europea la que establezca dicha autorización administrativa previa[155], resultaría razonable que dicha restricción, en especial cuando supone un cambio tan importante con respecto a la regulación anterior[156], encontrase acomodo en alguna de dichas condiciones.

---

[154] De acuerdo con el artículo 9.1 de la Directiva 2006/123, dichas condiciones incluyen que el régimen de autorización no sea discriminatorio para el prestador de que se trata; la necesidad de un régimen de autorización esté justificada por una razón imperiosa de interés general; y que el objetivo perseguido no se pueda conseguir mediante una medida menos restrictiva, en concreto porque un control *a posteriori* se produciría demasiado tarde para ser realmente eficaz.

[155] Cfr. el artículo 9.3 de la Directiva 2006/123/CE, que establece claramente que la presente sección no se aplicará a los regímenes de autorización regidos directa o indirectamente por otros instrumentos comunitarios. Como recuerda (Linde Paniagua, 2008, pág. 44), "la Directiva de servicios en el mercado interior no afecta a los servicios y profesiones reguladas por el Derecho comunitario. Esto es, si un acto comunitario regula aspectos concretos que conciernen al acceso o al ejercicio de actividades, o el ejercicio en sectores concretos, o en relación con profesiones concretas, dichos actos comunitarios primarán en su aplicación sobre la Directiva de servicios en el mercado interior".

[156] (Ortega Díaz, 2008, pág. 90 y ss.) explica la influencia de las tendencias liberalizadoras de los mercados, que conducen al fenómeno de la neorregulación, sobre el mercado de los servicios de certificación, que llevan al legislador comunitario a combinar un modelo de libre acceso con la existencia de mecanismos de control que garanticen el funcionamiento de este mercado y su fiabilidad.

Una posible explicación del cambio de modelo jurídico se puede encontrar en el asunto DigiNotar, un prestador de servicios de certificación holandés que sufrió un importante ciberataque en 2011, presuntamente perpetrado por ciberguerreros iraníes[157], que permitió el ciberespionaje a los ciudadanos. Algo que afecta con toda claridad a la seguridad de las comunicaciones electrónicas de ámbito global.

Otro motivo por el que se encuentra justificado un enfoque de supervisión reforzada puede ser la conexión entre el servicio de confianza y la eficacia de la prueba electrónica que el mismo genera o sustenta, que en último término afecta al derecho a la defensa, a la tutela judicial efectiva prevista en el artículo 24 de nuestra Constitución, pero también a la seguridad jurídica[158], de todo lo cual se desprende un innegable interés público en garantizar que dichas pruebas electrónicas sean, en definitiva, dignas de los efectos que producen.

Y es que, en efecto, el legislador –sea el de la Unión Europea o el nacional– asocia efectos jurídicos a los servicios de confianza que coadyuvan al valor y la eficacia probatorias de los diferentes elementos de las actuaciones electrónicas que acreditan los mismos, como la atribución del mensaje o documento, la declaración de voluntad, el momento de existencia de un mensaje, etc. Muestra de esto es el segundo párrafo del artículo 3.2 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, que establece que "[s]i se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados", presunción en sentido estricto, y que debe admitir prueba en contrario[159].

---

[157] Cfr. el informe del equipo de investigación, en (Hoogstraaten, y otros, 2012). La consecuencia directa para el prestador fue la pérdida de confianza y posterior cierre de la empresa, pero la afectación a los derechos y libertades de los ciudadanos fue potencialmente muy superior.

[158] (Rodríguez Ayuso, 2018, pág. 308) encuentra "comprensible en aras de otorgar una mayor seguridad jurídica (probablemente también técnica) a los DSSIisc [destinatarios de los servicios de confianza] que contraten con el PSSIisc [prestador de los servicios de confianza] aquellos SSIic [servicios de confianza] cualificados", aunque también que esta previsión "debería haber ido precedida de una previa adaptación de la normativa comunitaria de referencia, personificada en la DCE. En efecto, si lo que se pretende es alterar el principio, tradicional en el ámbito de la sociedad de la información, de no sujeción a autorización previa, únicamente para aquellos PSSI que ejerzan funciones de naturaleza intermediadora consistente en la prestación de SSIisc, hubiera sido aconsejable, para una mayor certeza y seguridad en el jurista y en todo aquel que se vea afectado por la nueva regulación, dotar de una mayor coherencia la relación entre ambas normas, bien estableciendo en la general la excepción referida, bien haciéndola constar en la específica; de lo contrario, la seguridad jurídica perseguida con la alteración del mencionado principio puede verse anulada con la inseguridad jurídica propiciada por esta incongruencia o incompatibilidad".

[159] De otro modo, nos encontraríamos, a juicio de (Blanquer, 2006, pág. 162 y ss.) en el ámbito de las ficciones legales, entre las que sitúa a las presunciones *iuris et de iure*, como la establecida para la veracidad de los documentos públicos, que hacen prueba plena, sin perjuicio de la posibilidad de demostrar la falsedad de documento público, que hace decaer el presupuesto de dicha presunción legal. En el caso de la firma electrónica, a partir de la existencia de la firma electrónica cualificada (que puede afirmarse a partir del hecho bruto de una firma digital con las propiedades legalmente previstas) puede presumirse el hecho incierto de que dicha firma electrónica fue realmente creada por el titular del certificado, y no por otra persona. Para este autor, la diferencia entre la ficción legal y la presunción está en que la primera no existe

Y, en sustento de estos efectos jurídicos, el Reglamento eIDAS –y la ley nacional que lo completa en cada Estado miembro– regula cómo debe ejercerse la actividad de los prestadores que ofrecen dichos servicios, partiendo siempre de la base de que se trata de una actividad económica, ofrecida indistintamente por operadores privados o públicos.

Lo anterior parte de una orientación de privatización de determinadas actividades de seguridad informática[160], en soporte a la prueba electrónica de la actuación, que resulta muy notable, aunque desde luego no es innovación del Reglamento eIDAS, sino de la DFE, y que se contrapesa mediante un sistema de control[161] que resulta justificado por trascender de la esfera de intereses privados de los particulares, en especial en presencia de una parte débil, y también en atención al reconocimiento transfronterizo que se desea para dichos servicios.

Hay que notar, finalmente, que el artículo 2.2 del Reglamento eIDAS excluye de su aplicación a "la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes", concretándose en el Considerando (21) que el Reglamento "no debe cubrir la prestación de servicios utilizados exclusivamente dentro de sistemas cerrados entre un conjunto definido de participantes, que no tengan efectos en terceros", por lo que "[p]or ejemplo, los sistemas establecidos en empresas o administraciones públicas para gestionar procedimientos internos que hagan uso de servicios de confianza no deben estar sujetos a las obligaciones del presente Reglamento". De ello se deriva que "[ú]nicamente los servicios de confianza prestados al público que tengan efectos en terceros deben cumplir las obligaciones establecidas en el presente Reglamento"[162], sin

---

un hecho incierto que requiera de prueba, sino que tiene por objeto un hecho cierto.

[160] Esta orientación a la privatización de la seguridad muestra una fuerte dependencia del origen anglosajón de estas tecnologías, especialmente de Estados Unidos, que se caracteriza por la influencia del protestantismo, que conduce a Estados individuocéntricos, con una mayor privatización de la función de seguridad, en contraste con los Estados de base católica, como ha mostrado (Martínez Quirante, 2002, pág. 23 y ss.) en su estudio de los modelos de seguridad y las armas, y que desde luego resulta perfectamente observable en la seguridad informática.

[161] Como ha explicado (Ortega Díaz, 2008, pág. 173), a pesar de que la creación del espacio de comunicación conocido como "ciberespacio" lleva, a mediados de los noventa, a la defensa por el movimiento ciberutópico de la eliminación de gran parte de las normas que puedan afectar a dicho espacio, dando total libertad a los operadores del mercado, "el pensamiento ciberutópico no tarda en entrar en crisis. Por un lado, la generalización del desarrollo tecnológico no es el esperado y, por otro, el ámbito empresarial y el académico comienzan a percatarse de que, si bien la tecnología puede ser revolucionaria, no puede ser utópica", y, añade, "[l]a existencia de un espacio virtual absolutamente libre, sin reglas, implica una panacea libertaria que no tiene espacio en una economía de mercado", lo que dará lugar a una exigencia de regulación y a la aparición del denominado "pensamiento tecnorrealista".

[162] Con respecto a la LFE, (Martínez Nadal, 2009, págs. 65-66) se planteaba la duda acerca de si la LFE se aplicaba a todos los prestadores de servicios de certificación domiciliados o establecidos en España o, por el contrario, si sólo se aplicaba a determinados prestadores en función de su actividad, dado que tanto el RDLFE como la DFE permitían entender que su ámbito de aplicación se limitaba sólo a los prestadores que expedían certificados al público. Esta autora concluye que la LFE, sin embargo, resulta aplicable a todos los prestadores, sin perjuicio de que determinadas previsiones sólo resultaran aplicables a los que expedían al público. En mi opinión, aunque tampoco el artículo 2 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, como en la LFE, no distingue entre prestadores que expiden al público y otros prestadores, parece que no debería darse esta problemática de nuevo, al encontrarse la exclusión incluida expresamente en el artículo 2.2 del Reglamento eIDAS.

perjuicio de que, en dichos casos, y como es lógico, dichos servicios no gozarán de los efectos jurídicos correspondientes[163], por lo que esta autorregulación privada no será especialmente atractiva, y no podrá acudirse a ella en los casos en que la normativa exija, directa o indirectamente, una prueba basada en un servicio cualificado, como por ejemplo en el caso de una firma electrónica cualificada, o cuando dicha prueba resulte conveniente.

También permite el Reglamento eIDAS la exclusión de los servicios públicos que se encuentren regulados por el Derecho nacional, pero parece que sólo cuando se gestionen procedimientos internos que hagan uso de los servicios de confianza, y de nuevo, en este caso, sucederá que estos servicios no gozarán de los efectos jurídicos previstos, en el Reglamento eIDAS, para los servicios de confianza cualificados[164].

1.3.4 La posibilidad de establecer otros servicios de confianza en la legislación nacional

De acuerdo con el Considerando (25) del Reglamento eIDAS, "los Estados miembros deben conservar la libertad para definir otros tipos de servicios de confianza, además de los que forman parte de la lista cerrada de servicios de confianza prevista en el presente Reglamento, a efectos de su reconocimiento a nivel nacional como servicios de confianza cualificado", lo que permite un elevado grado de innovación jurídica en la creación de nuevos servicios, o en el mantenimiento de instituciones actualmente existentes restringiendo su reconocimiento jurídico estricto al ámbito del Estado; servicios que, en ambos casos, lógicamente no gozarán de libre circulación dentro de la Unión, por no

---

[163] Para (Gobert, 2015, p. 24), "[a]unque esto no está expresado en el Reglamento, parece evidente que si un prestador ofrece sus servicios en un «sistema cerrado», no debería poder ofrecer servicios de confianza «cualificados» en el marco de este sistema cerrado y, al mismo tiempo, reclamar el beneficio de la excepción. En nuestra opinión, el hecho de declarar que se ofrecen servicios de confianza «cualificados» implica que el proveedor del servicio acepte implícitamente cumplir con los requisitos del Reglamento relativos a esta categoría de servicios y, por lo tanto, renunciar implícitamente al beneficio de la excepción establecida en beneficio de los «sistemas cerrados». Un razonamiento diferente equivaldría a vaciar el Reglamento de su contenido, al menos en lo que respecta a los requisitos y el régimen de control aplicables a los servicios «cualificados»" (la traducción es mía), análisis con el que estoy plenamente de acuerdo, al constituir un evidente fraude de ley.

[164] Un ejemplo de este tipo de exclusión lo podemos encontrar, en Bélgica, en el artículo XII.24 §3 del *Code de droit économique*, incorporado por la *Loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique; 21 julliet 2016*, que dispone que "[d]e conformidad con el artículo 2, apartado 2, del Reglamento 910/2014, todos los componentes utilizados para las firmas electrónicas, las entregas electrónicas certificadas, los sellos electrónicos de tiempo y para el archivo electrónico, proporcionados de forma gratuita o mediante pago por una autoridad administrativa […], en ejecución de las tareas que le hayan sido encomendadas por o en virtud de una ley, quedan excluidas del ámbito de aplicación del Reglamento 910/2014, de este título y sus anexos", pero añadiendo inmediatamente que "[s]in embargo, los artículos 25 (1), 41 (1) y 43 (1) del Reglamento 910/2014 se aplican a los componentes utilizados para las firmas electrónicas, las entregas electrónicas certificadas y los sellos electrónicos de tiempo a que se refiere el párrafo primero" (la traducción es mía).

encontrarse tipificados en el Reglamento eIDAS.

La presencia de este Considerando denota que el Reglamento eIDAS no agota, mediante su armonización, los posibles servicios que se pueden incluir en esta categoría, seguramente por la voluntad de los Estados miembros de continuar legislando al respecto, como ha sucedido en el pasado con la mayoría de los servicios que actualmente se han incorporado al Reglamento eIDAS.

Un ejemplo de servicio de confianza previsto en el plano nacional lo encontramos en el Derecho belga, que regula el servicio de confianza de archivo electrónico, que "consiste en la conservación de datos electrónicos o la digitalización de documentos en soporte papel, y que es ofrecido por prestador de servicios de confianza en el sentido del artículo 3, epígrafe 19, del Reglamento eIDAS o que es explotado por su propia cuenta por un organismo del sector público o por una persona física o jurídica"[165], servicio que puede ser objeto de cualificación, en cuyo caso recibe el efecto jurídico de presumirse el cumplimiento de cualquier obligación legal de conservación de un documento si el mismo ha sido incorporado a este servicio, y de que el mismo no ha sido alterado, sin perjuicio de los cambios que se realicen en su soporte o formato electrónicos.

Nótese que, de hacerse uso de esta posibilidad de regular nuevos servicios de confianza, en especial si los mismos se sujetan a cualificación, la misma quedará incluida en el alcance de la norma nacional de transposición de la Directiva de Servicios, en nuestro caso, en la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio, por lo que se deberán aplicar los criterios previstos en dicha normativa, principalmente la determinación de la razón imperiosa de interés general que justifique el régimen en que la cualificación consiste, que conecta con la ya mencionada afectación al derecho fundamental a la tutela judicial efectiva derivada del establecimiento de presunciones legales.

1.4 LOS ACTORES DEL MODELO REGULATORIO DE LOS SERVICIOS DE CONFIANZA

Aunque posteriormente nos referiremos con detalle a los principales contenidos del régimen jurídico del nuevo modelo regulatorio, conviene en este momento previamente presentar a los actores del mismo, y sus funciones y competencias, que se muestran en la Ilustración 5.

Los actores con protagonismo más remarcado en el modelo regulatorio de los servicios de confianza son el prestador de servicios de confianza, que ofrece los servicios que sustentan la prueba electrónica, de una parte, y la Comisión Europea, el legislador nacional y el organismo nacional de supervisión, de la otra.

También son relevantes, en este modelo regulatorio, las organizaciones competentes en el ámbito de la normalización, los fabricantes de tecnologías, los organismos de

[165] La traducción es mía. Sobre este servicio, cfr. (Gobert, 2016, pp. 5, 31-36) y la *Loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique ; 21 juillet 2016*.

certificación de la seguridad de los productos empleados en los servicios de confianza y los organismos de evaluación de la conformidad de la prestación del servicio de confianza, en especial dada la intervención necesaria de estos últimos.

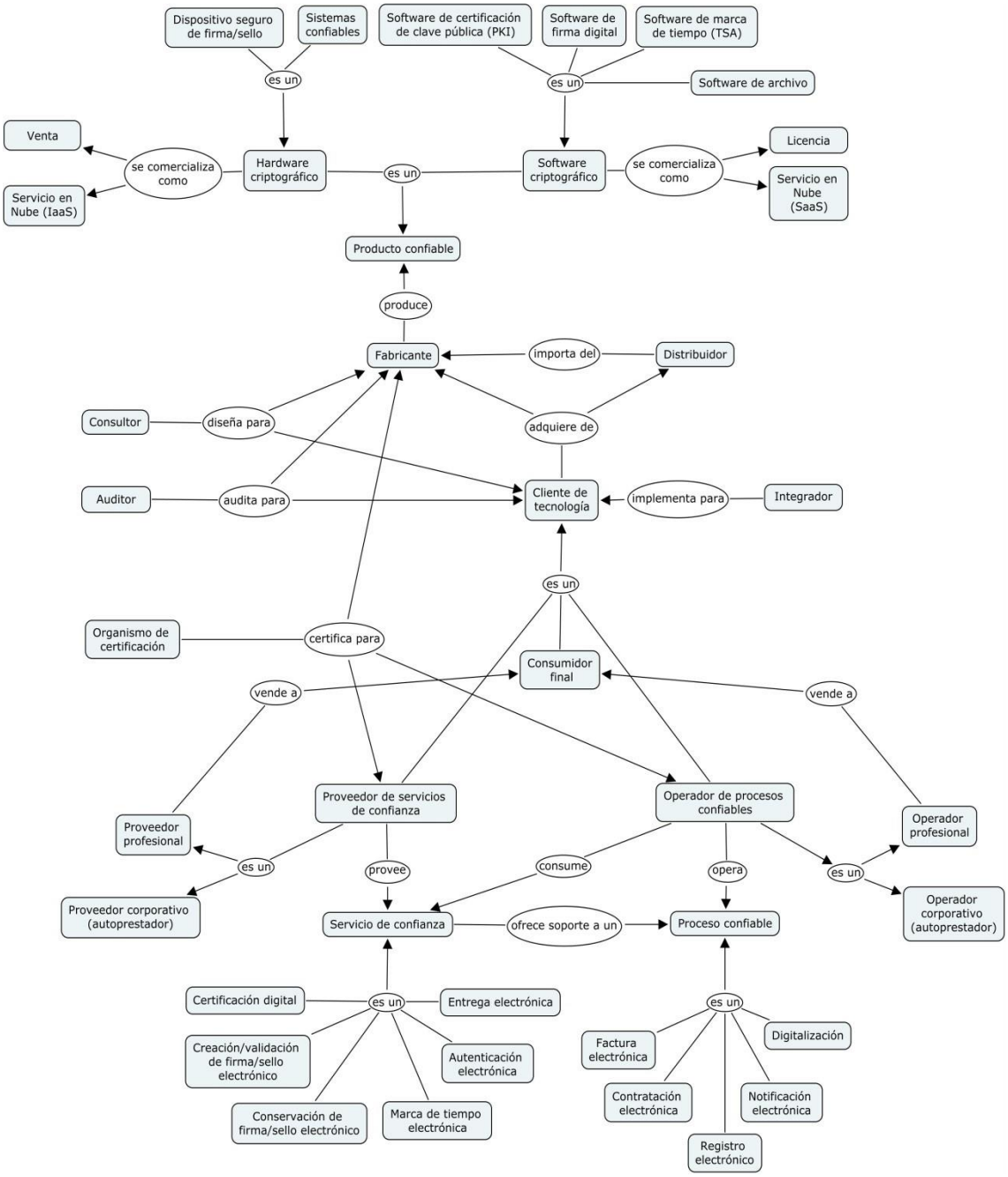


Ilustración 5. Mapa de actores del mercado de la confianza (elaboración propia)

Como se puede ver, nos encontramos en un modelo de gobernanza multinivel, formado por diversos planos de regulación, incluyendo la regulación uniforme contenida en el Reglamento eIDAS, la regulación específica de cada legislación nacional complementaria, el *soft law* público y la autorregulación de la industria, que presentan complejas interacciones entre sí, y que suponen una clara afectación al principio de

seguridad jurídica[166], algo que no deja de ser una cierta ironía precisamente cuando nos referimos a la juridificación de las tecnologías para la seguridad.

1.4.1 La caracterización del prestador de servicios de confianza

El artículo 3.19 del Reglamento eIDAS, define al prestador de servicios de confianza como "una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza", mientras que su artículo 3.20 indica que es un prestador cualificado de servicios de confianza "un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación", definición de la que ya se infiere la sujeción de la actividad a una autorización administrativa previa, como veremos posteriormente con detalle.

Anteriormente, la LFE se refería al prestador de servicios de certificación electrónica, como la persona física o jurídica que expedía certificados o prestaba otros servicios en relación con la firma electrónica (artículo 2.2 de la LFE), en una denominación, que era equivalente a la contenida en la DFE, que podía dar lugar a confusiones, ya que existían servicios relacionados con la firma electrónica que no tenían por qué tener nada que ver con la certificación digital, como por ejemplo la emisión de sellos de tiempo de documentos, o la custodia de documentos firmados electrónicamente, y aún en este caso los prestadores de estos servicios eran legalmente denominados "prestadores de servicios de certificación", incluso aunque dichos prestadores no expidieran certificados[167].

A la vista de este enfoque amplio de servicio de certificación, podemos considerar que todos los servicios de certificación han sido absorbidos dentro de la categoría de los servicios de confianza, aunque no a la inversa.

Un elemento importante a tener en cuenta en relación con los prestadores de servicios de confianza es el lugar de su establecimiento, ya que el Reglamento eIDAS se aplica sólo "a los prestadores de servicios de confianza establecidos en la Unión" (artículo 2.1), y sin perjuicio del mecanismo de reconocimiento de servicios de confianza ofrecidos por prestadores establecidos en un tercer país conforme al artículo 14 del propio Reglamento eIDAS.

Por lo que respecta a la concreción de la ley nacional aplicable[168], la española se aplica a

---

[166] (Gamero Casado, 2015, pág. 114 y ss.) se refiere al "desordenamiento jurídico", que desde luego en nuestro caso es fácilmente apreciable, y que ha generado la potente disfunción de que "[n]o sólo los ciudadanos carecen de la pericia necesaria para identificar las normas vigentes en cada momento en un sector determinado de ordenación: la tarea resulta asimismo inviable en la actualidad para los operadores jurídicos más avezados, que pueden verse sorprendidos al descubrir modificaciones sustanciales en una determinada materia articuladas mediante leyes cuya rúbrica poco o nada tiene que ver con semejante contenido".

[167] Así lo ha denunciado (Martínez Nadal, 2009, págs. 310-312).

[168] Para (Rodríguez Ayuso, 2018, pág. 293), "dentro de nuestro ordenamiento jurídico interno, el lugar de establecimiento del PSSI ejerce una triple finalidad: en primer lugar, dispone el ámbito de aplicación de la normativa en materia de contratación y firma electrónicas; en segundo lugar, determina también la aplicación adicional de todas las demás disposiciones del ordenamiento jurídico español que les resulten de aplicación en función de la actividad específicamente desarrollada, y, en tercer lugar, precisa la ley y las

los prestadores de servicios de confianza que estén establecidos en el Estado español y a los que, no siendo residentes o no teniendo domicilio en el Estado español, operen mediante un establecimiento permanente (en aplicación analógica del criterio contenido en el artículo 2.1 de la LFE, que lo ha establecido en relación con los servicios de certificación de firma electrónica).

Este criterio se ha mantenido en el artículo 2 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, pero con el matiz de que, en el caso de los prestadores de servicios residentes o domiciliados en otro Estado que tengan un establecimiento permanente situado en España, sólo se encontrarán sujetos a la Ley española siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea, una previsión que puede generar dudas a la vista del artículo 17.1 del Reglamento eIDAS, que limita las funciones del organismo de supervisión al Estado miembro que lo designa, salvo la cooperación prevista en la misma norma.

La LFE consideraba que un prestador de servicios de confianza estaba establecido en el Estado español cuando tuviera la residencia o el domicilio social en territorio español, siempre que éstos coincidieran con el lugar en que esté efectivamente centralizada la gestión administrativa y la gestión de sus negocios (artículo 2.3 de la LFE), que era el criterio ya clásico de la jurisprudencia europea, hoy reflejada en el Reglamento (CE) Nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I); y adicionalmente, la LFE presumía que existía establecimiento en el Estado español cuando el prestador o alguna de sus sucursales estuvieran inscritos en el Registro Mercantil o en otro Registro constitutivo (artículo 2.5 de la LFE). Finalmente, se consideraba que un prestador opera mediante un establecimiento permanente en territorio español cuando disponga habitualmente de instalaciones o lugares de trabajo en que realice la totalidad o una parte de los servicios (artículo 2.4 de la LFE), incluyendo, por tanto, las oficinas comerciales; y que la simple utilización de medios técnicos situados en el Estado español para la prestación del servicio no implicaba establecimiento en el Estado español[169].

Todas estas previsiones han decaído en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, lo cual debe ser objeto de valoración positiva, si bien sorprende la no incorporación, al Anteproyecto de Ley, de los epígrafes 5.2 y 5.3 de la LFE, lo que supone su pérdida de vigencia.

Recuérdese sólo que, conforme al artículo 5.2 de la LFE, "[l]os órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas", previsión que en cierto modo resulta innecesaria, dado que de todos modos resulta aplicable la legislación de defensa de la competencia, principalmente contenida en la Ley 15/2007, de 3 de julio y el Real Decreto 261/2008, de 22 de febrero.

---

autoridades encargadas del control de su cumplimiento, de acuerdo con el principio de la aplicación de la Ley del país de origen que inspira la DCE y, consecuentemente, la LSSICE".

[169] Para (Martínez Nadal, 2009, pág. 65), esta previsión "debería ser objeto de una interpretación a contrario, en el sentido de que el simple hecho de que un prestador establecido en España […] utilice medios tecnológicos situados fuera de España no excluye la aplicación de la Ley española de firma electrónica".

Por lo que se refiere al epígrafe 3 del artículo 5 de la LFE, el mismo establecía que "[l]a prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación", previsión que parecía dimanar del artículo 3.7 de la DFE, en cuya virtud "[l]os Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales", de modo que "[t]ales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate", y siempre que, en lo que ahora nos interesa especialmente, "[e]stas prescripciones no deberán obstaculizar los servicios transfronterizos al ciudadano".

Aunque no se encuentra expresamente indicado en este epígrafe, y debido a su ubicación sistemática en la LFE, la doctrina ha indicado que la prestación de servicios de certificación por parte de las Administraciones Públicas no debía afectar a la libre competencia, excluyendo a los restantes prestadores de servicios[170], disfunción que se ha producido con bastante claridad en algunos casos, a los que posteriormente nos referiremos.

Podía entenderse, en efecto, que el régimen de prestación de servicios de certificación por parte de la Administración Pública constituía un conjunto de prescripciones adicionales (al régimen general, se debe entender), por lo que resultaba exigible que dicho régimen fuera compatible con la DFE, en especial desde la perspectiva de la no discriminación a otros prestadores de servicio establecidos en otros Estados miembros. A este régimen, que desde luego ha existido, y no siempre ha cumplido con estas exigencias, nos referimos posteriormente con detalle[171].

En todo caso, y dado que el Reglamento eIDAS ha eliminado la noción de las prescripciones adicionales para el uso de la firma en el sector público, parecería innecesario mantener el epígrafe 3 del artículo 5 de la LFE en el ordenamiento jurídico español –mediante su incorporación al Anteproyecto de Ley–, especialmente en el caso de la actividad de prestación de servicios por las Administraciones Públicas excluida del Reglamento eIDAS, pudiendo reconducirse otras disfunciones al derecho de la competencia.

El prestador de servicios de confianza deberá cumplir las obligaciones que le impongan el Reglamento eIDAS y la correspondiente legislación nacional que la complemente, incluyendo determinados reglamentos técnicos, así como –de forma indirecta– las normas técnicas que voluntariamente decida adoptar para poder obtener la cualificación de sus servicios.

1.4.2 Las competencias de la Comisión Europea relativas a los servicios de confianza

En el modelo regulatorio de los servicios de confianza, la Comisión Europea va a tener un relevante papel en orden al funcionamiento del mercado de servicios de confianza,

[170] (Martínez Nadal, 2009, págs. 130-132).

[171] Cfr. el epígrafe 5.2.1 de este trabajo.

función que se va a sustentar en normas y reglamentos técnicos, en relación con tres ámbitos netamente diferenciados.

En primer lugar, la Comisión puede "establecer una mayor especificación de las medidas técnicas y organizativas de seguridad" aplicables a los prestadores y que se prevén en el artículo 19.1 del Reglamento eIDAS[172], debiéndose notar que esta posibilidad existe tanto en relación con los prestadores cualificados como no cualificados.

En segundo lugar, la Comisión puede "establecer números de referencia" relativos a normas relacionadas con la actividad de prestación de los diversos servicios de confianza[173], el cumplimiento de las cuales implicará la presunción de cumplimiento de dichos requisitos por parte de la correspondiente tecnología empleada para la prestación del servicio o la creación de la fuente de prueba electrónica de que se trate.

El elenco previsto incluye aquellas normas referidas a los sistemas y productos fiables correspondientes a los sistemas fiables previstos en el artículo 24.2, letras e) y f) del Reglamento eIDAS[174]; las normas relativas a firmas o sellos electrónicos avanzados[175]; las normas relativas a certificados cualificados de firma o sello electrónico[176]; las normas referidas a los dispositivos cualificados de creación de firmas o sellos electrónicos[177]; las normas relativas a los procesos de validación de firma o sello electrónico[178]; las normas

---

[172] Artículo 19.4.a) del Reglamento eIDAS. Una de las normas de carácter general referidas a medidas técnicas y organizativas de seguridad para la prestación de servicios de confianza es la norma ETSI EN 319 401 v2.2.1 (2018-02). Electronic signatures and infrastructures (ESI); General Policy Requirements for Trust Service Providers, que define los requisitos comunes que deben cumplir todos los prestadores de servicios de confianza.

[173] El Reglamento eIDAS no contiene, en su texto, las prescripciones técnicas completas referidas a la prestación de los servicios de confianza, sino que emplea el método de la remisión a normas técnicas y, más en concreto, un reenvío formal a las normas que se aprueben, que, en opinión de (Izquierdo Carrasco, 2000, pág. 245 y ss.), es la modalidad "que mayores problemas plantea, pues, en principio, puede suponer que el ordenamiento jurídico pierda el control sobre el contenido de la norma técnica que a él se incorpora".

[174] Artículo 24.5 del Reglamento eIDAS, como por ejemplo sucede con la especificación técnica CEN/TS 419 261:2015, que establece requisitos de seguridad para sistemas fiables que gestionan certificados y sellos de tiempo, o CEN/TS 419 241:2014, que establece requisitos de seguridad para sistemas fiables de firma en servidor. También resulta relevante la norma CEN EN 419 221, partes 1 a 4, que definen perfiles de protección conforme a Criterios Comunes para los bienes de equipo criptográficos (HSM) que gestionan las claves criptográficas de los sistemas fiables.

[175] Artículos 27.4 y 37.4 del Reglamento eIDAS.

[176] Artículos 28.6 y 38.6 del Reglamento eIDAS, como, por ejemplo, ETSI EN 319 411-2 v2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

[177] Artículos 29.2 y 39.1 del Reglamento eIDAS. Cfr. la Decisión de Ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, a la que nos referiremos con detalle posteriormente, y que parece haberlas convertido en obligatorias.

[178] Artículos 32.3, 33.2 y 40 del Reglamento eIDAS. Por ejemplo, ETSI EN 319 102-1 V1.1.1 (2016-05). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital

referidas a los servicios cualificados de conservación de firma o sello electrónico[179]; las normas referidas a la vinculación exacta de la fecha y hora con los datos y a una fuente de información temporal exacta[180]; las normas referidas a los procesos de envío y recepción de datos[181]; y las normas relativas a los certificados cualificados de autenticación de sitio web[182].

En tercer lugar, la Comisión puede "establecer números de referencia" relativos a normas relacionadas con el propio funcionamiento del marco regulatorio de los servicios de confianza, incluyendo las normas para la acreditación de los organismos de evaluación de la conformidad y para el informe de evaluación de la conformidad, y sobre las disposiciones en materia de auditoría con arreglo a las cuales los organismos de evaluación de la conformidad realizarán la evaluación de la conformidad de los prestadores cualificados de servicios de confianza[183]; las normas de formato y procedimiento relativas al inicio de la actividad, incluyendo la notificación de la intención de iniciar la actividad al organismo de supervisión, el informe de evaluación de la conformidad y la verificación y concesión de la cualificación por parte de organismo de supervisión[184]; las especificaciones técnicas y de formato relativas a las listas de confianza de servicios de confianza[185]; las especificaciones relativas a la forma y en particular la presentación, composición, tamaño y diseño de la etiqueta de confianza «UE» para servicios de confianza cualificados[186]; las normas de formatos de referencia de las firmas electrónicas avanzadas o métodos de referencia cuando se utilicen formatos

---

Signatures; Part 1: Creation and Validation.

[179] Artículos 34.2 y 40 del Reglamento eIDAS. Por ejemplo, ETSI EN 319 132-1 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures, define un formato para la conservación a largo plazo de las firmas/sellos electrónicos, que el servicio puede implantar; mientras que ETSI TS 101 533-1 v1.3.1 (2012-04). Electronic signatures and infrastructures (ESI); Data preservation systems security; Part 1: Requirements for implementation and management, establece requisitos para los repositorios de documentos firmados.

[180] Artículo 42.2 del Reglamento eIDAS. Por ejemplo, ETSI EN 319 422 v1.1.1 (2016-03). Electronic signatures and infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, que define, entre otros, los contenidos de un sello cualificado de tiempo electrónico, mientras que ETSI EN 319 421 v1.1.1 (2016-03). Electronic signatures and infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, que define los requisitos que debe cumplir un prestador de servicios de confianza que emite sellos de tiempo electrónico, incluyendo sellos cualificados de tiempo electrónico.

[181] Artículo 44.2 del Reglamento eIDAS. Por ejemplo, ETSI TS 102 640-1 V2.2.1 (2011-09). Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture, y sus partes adicionales – que en el futuro inmediato serán sustituidas por una nueva norma ETSI, definen un sistema de correo electrónico seguro como servicio de entrega electrónica.

[182] Artículo 45.2 del Reglamento eIDAS. Por ejemplo, ETSI EN 319 411-2, ya citada.

[183] Artículo 20.4 del Reglamento eIDAS. En este sentido, se puede mencionar que la norma técnica ETSI EN 319 403 V2.2.2 (2015-08). Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers, define los requerimientos para la evaluación de la conformidad de los proveedores de servicios de confianza con las normas propias de cada servicio.

[184] Artículo 21.4 del Reglamento eIDAS.

[185] Artículo 22.5 del Reglamento eIDAS.

[186] Artículo 23.3 del Reglamento eIDAS.

alternativos[187]; y, por último, las normas para la evaluación de la seguridad de los productos de tecnología de la información a efectos de certificación de los dispositivos cualificados de creación de firma o sello[188].

Como se puede ver del extenso listado anterior, el ejecutivo comunitario tiene una importantísima capacidad de "desarrollo" de la normativa jurídica, mediante la referencia a normas técnicas, lo que denota la relevancia de la autorregulación tecnológica[189] en este ámbito[190], algo que no necesariamente debe ser considerado positivamente[191].

Más aún, en caso de que la Comisión haga uso de su competencia y establezca las normas técnicas anteriormente indicadas en los términos previstos legalmente –que analizaremos en breve–, es preciso hacer notar que el cumplimiento de algunas de ellas pasará a ser legalmente imperativo[192] y objeto de la correspondiente evaluación de la conformidad,

---

[187] Artículos 27.5 y 37.5 del Reglamento eIDAS. Cfr. la Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior; a la que posteriormente nos referiremos con detalle.

[188] Artículos 30.3 y 39.2 del Reglamento eIDAS. Cfr. la Decisión de Ejecución (UE) 2016/650, a la que nos referiremos con detalle posteriormente.

[189] Como ha señalado (Gamero Casado, 2015, pág. 122), "[t]ambién es representativo del Estado garante el paso de la regulación directa por parte de los poderes públicos a una autorregulación en la que se establece toda una estructura de entidades de normalización, acreditación y homologación, en un contexto que se engloba bajo la noción genérica de autorregulación y que en nuestro Derecho descansa esencialmente sobre las determinaciones de la Ley 21/1992, de Industria", modelo en relación con el autor identifica que "[l]os problemas pendientes de resolver son de dos tipos, pero en ambos casos tienen que ver con la preservación de las garantías que son propias e inherentes del Derecho Administrativo, y que se han resquebrajado como consecuencia del nuevo orden de relaciones. Así, debe establecerse, por una parte, la sujeción al Derecho Público de estas relaciones entre sujetos privados, dado que suponen el ejercicio de funciones públicas; y debe regularse, asimismo, el modo en que los sujetos terceros pueden hacer sus derechos e intereses en la medida que se puedan ver lesionados".

[190] (Merchán Murillo, 2018, pág. 6) señala cómo "las referencias a la tecnología aparecen, a veces de manera casi imperceptible en las Leyes reguladoras de la e-Administración", frecuentemente mutando en normas jurídicas, y cuya lectura "permite observar el grado de precisión técnica al que se llega, imposible de alcanzar a través de las normas jurídicas, que les dan amparo. La complejidad técnica y la permanente evolución justifican, plenamente, el recurso a las normas técnicas para fijar estos aspectos, que, por otro lado, tienen un gran impacto en el desarrollo de la e-Administración", en especial en el ámbito de la interoperabilidad.

[191] (Muñoz Machado, 2000, pág. 59) hizo notar que "[l]a remisión a normas técnicas privadas para lograr la reglamentación de una determinada actividad o servicio también se ha desarrollado mucho en los sectores afectados por las nuevas tecnologías en los últimos años", admitiendo que "[l]a utilización de normas privadas […] es casi una necesidad es un mundo en el que el desarrollo de las tecnologías de la comunicación está masivamente entregado a la responsabilidad de corporaciones y establecimientos de base privada", criticando la "dejación por parte de los organismos públicos de cualquier normativa y su sustitución por los acuerdos alcanzados por los agentes interesados, o en el seno de los organismos privados que los representan", opinión que se encuentra plenamente vigente, al menos en relación con el Reglamento eIDAS.

[192] Como ha indicado (Moles Plaza, 2004, págs. 46-47), las normas técnicas, que son por definición de aplicación voluntaria, integran el "derecho blando", de carácter eminentemente supraestatal y naturaleza predominantemente técnica, y que no precisa devenir "derecho duro" u obligatorio, para ser eficaz; todo

tanto de forma previa al inicio de la prestación del servicio (artículo 21.1 del Reglamento eIDAS), como periódicamente durante el tiempo en el que el mismo se preste (artículo 20.1 del Reglamento eIDAS).

Dado que la concesión de la cualificación; esto es, la autorización administrativa, no se puede solicitar ni obtener sin antes superar una evaluación de la conformidad que demuestre el cumplimiento de lo establecido por dichas normas, nos encontramos ante el primer caso donde podemos hablar de la existencia de verdaderos reglamentos técnicos[193], por ser obligatorios, aplicables a servicios de la sociedad de la información[194].

En concreto, se deben considerar reglamentos técnicos las normas que establezcan una mayor especificación de las medidas técnicas y organizativas de seguridad de los prestadores de servicios de confianza (sean o no cualificados)[195]; los formatos y procedimientos (incluidos los plazos) en relación con la notificación de incidentes de seguridad que sufran los prestadores de servicios de confianza[196]; o las normas para la evaluación de la seguridad de los productos de tecnología de la información a efectos de certificación de los dispositivos cualificados de creación de firma o sello[197], dado que limita la posibilidad del prestador de elegir productos no certificados, o certificados conforme a otras normas de evaluación.

Como se ha avanzado, algunas de estas normas técnicas constituyen normas de producto[198] íntimamente ligadas a reglas relativas a servicios[199], en el sentido del artículo

---

ello sin perjuicio de que, en ocasiones, termine convirtiéndose en "derecho duro" mediante la promulgación de leyes y regulaciones. En relación con el *soft law* comunitario y su incidencia en el derecho administrativo español, cfr. (Sarmiento, 2008, págs. 82-89).

[193] Sobre la distinción entre normas técnicas y reglamentos técnicos, cfr. (Moles Plaza, 2001, págs. 147-174). En cuanto ahora interesa, el reglamento técnico se conceptualiza como un acto unilateral concertado que emana del poder ejecutivo, al igual que sucede en los casos de reenvío.

[194] Hasta la aprobación de este Reglamento, se había producido una cierta cantidad de Directivas de armonización para la comercialización de determinados productos que ya permitían a la Comisión pedir a las organizaciones europeas de normalización la adopción de normas armonizadas que confieran presunción de conformidad con los requisitos esenciales aplicables (denominadas con carácter general como "legislación comunitaria de armonización", cfr. la Decisión nº 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos). De forma similar, en el ámbito de los servicios de comunicaciones electrónicas se había previsto ya en la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la posibilidad de que la Comisión, en su caso, solicite a las organizaciones europeas de normalización que elaboren normas, establezca y publique en el Diario Oficial de la Unión Europea una lista de las normas o especificaciones de cara a fomentar su uso, o hacer obligatoria su aplicación, o retire normas o especificaciones de dicha lista.

[195] Artículo 19.1.4.a) del Reglamento eIDAS.

[196] Artículo 19.1.4.b) del Reglamento eIDAS.

[197] Artículos 30.3 y 39.2 del Reglamento eIDAS. Cfr. la Decisión de Ejecución (UE) 2016/650, a la que nos referiremos con detalle posteriormente.

[198] Como en el caso de los sistemas fiables o de los dispositivos cualificados de creación de firma, incluyendo las aplicaciones informáticas empleadas por los prestadores o suministradas a los clientes, que en todos los casos tienen la consideración de "producto".

[199] Dicho artículo define la regla relativa a los servicios como "un requisito de carácter general relativo al acceso a las actividades de servicios contempladas en la letra b) y a su ejercicio, especialmente las disposiciones relativas al prestador de servicios, a los servicios y al destinatario de servicios, con exclusión

1.1.e) de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, aunque la mayoría de las normas anteriormente indicadas se refieren exclusivamente a servicios prestados por vía electrónica, y cuando son obligatorias para poder prestar el servicio – como en el caso de los dispositivos cualificados de creación de firma o sello electrónico cualificado –, constituyen reglamentos técnicos, en el sentido del artículo 1.1.f) de la misma Directiva[200].

Las normas técnicas establecidas por la Comisión Europea en relación con los restantes aspectos de la actividad de prestación de servicios de confianza, sin embargo, continuarán siendo puramente voluntarias, dado que su único efecto jurídico es presumir el cumplimiento, por parte del prestador, de los requisitos establecidos en la norma jurídica, por cuanto que dichas normas técnicas concretan las obligaciones referidas a la actividad de los prestadores de servicios de confianza que voluntariamente decida sujetarse a las mismas. De esta forma, por ejemplo, si la Comisión Europea establece el número de referencia de la norma ETSI EN 319 412, que describe los contenidos de un certificado cualificado –de firma electrónica de persona física, de selo electrónico de persona jurídica o de autenticación de sitio web–, el prestador que cumpla lo ordenado en dicha norma recibirá la presunción legal de estar cumplimiento con las correspondientes obligaciones previstas en el Reglamento eIDAS.

Por tanto, en el Reglamento eIDAS no se impone a los prestadores de servicios de confianza el cumplimiento de lo establecido por estas normas, posiblemente al objeto de preservar la neutralidad tecnológica que el mismo Reglamento declara, de lo que se desprende la posibilidad legal de que el prestador decida emplear otras normas técnicas para demostrar la conformidad de su servicio, o incluso decidir no sujetarse al cumplimiento de ninguna norma técnica en concreto. La única consecuencia jurídica de dichas decisiones, como se ha avanzado, será que el prestador no podrá beneficiarse de la presunción de cumplimiento de los requisitos del Reglamento eIDAS cubiertos por la norma, por lo que deberá acreditar dicho cumplimiento empleando cualesquiera otros medios de prueba.

Es evidente que la decisión de cumplir con las normas técnicas que hayan sido establecidas por la Comisión Europea viene modulada por el incentivo de beneficiarse de esta presunción, en especial porque la citada presunción afecta al organismo de

---

de las normas que no se refieren específicamente a los servicios determinados en dicho punto", debiendo considerarse que "una norma se refiere específicamente a los servicios de la sociedad de la información cuando, por lo que respecta a su motivación y al texto de su articulado, tenga como finalidad y objeto específicos, en su totalidad o en determinadas disposiciones concretas, regular de manera explícita y bien determinada dichos servicios".

[200] El artículo define los reglamentos técnicos como "las especificaciones técnicas u otros requisitos o las reglas relativas a los servicios, incluidas las disposiciones administrativas que sean de aplicación y cuyo cumplimiento sea obligatorio, de iure o de facto, para la comercialización, prestación de servicio o establecimiento de un operador de servicios o la utilización en un Estado miembro o en gran parte del mismo, así como, a reserva de las contempladas en el artículo 7, las disposiciones legales, reglamentarias y administrativas de los Estados miembros que prohíben la fabricación, importación, comercialización o utilización de un producto o que prohíben el suministro o utilización de un servicio o el establecimiento como prestador de servicios".

supervisión, que lógicamente no podrá cuestionarla[201].

Sin embargo, en el caso de que el prestador decida sujetarse a las citadas normas técnicas, su cumplimiento pasa a ser obligatorio para este prestador, y será objeto de la evaluación de la conformidad anteriormente aludida, y de la correspondiente cualificación y supervisión.

Por ello, el papel de las normas técnicas como instrumento regulador (cuando son impuestas de forma obligatoria) o autorregulador (en los restantes casos), es absolutamente crucial, y suele basarse en una gran variedad de instrumentos diferentes de las normas técnicas formales, incluyendo especificaciones técnicas, acuerdos multilaterales de la industria, publicaciones de grupos de trabajo u otras fuentes de gran dinamismo y alcance mundial.

En este contexto, hay que notar que el marco legal europeo referido a la normalización técnica se ha completado con el novedoso Reglamento (UE) Nº 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, que precisamente presta una atención especial a las normas de servicios y la evolución de los documentos de normalización distintos de las normas formales[202].

En especial, se parte de que la Directiva 98/34/CE[203] "solo se aplica a las normas para los productos, por lo que no engloba expresamente las normas para los servicios. Además, la separación entre servicios y bienes resulta cada vez menos pertinente en la realidad del mercado interior. En la práctica, no siempre es posible hacer una clara distinción entre normas para productos y normas para servicios. Muchas normas para productos tienen un componente de servicio, mientras que, a menudo, las normas para servicios se refieren también en parte a productos. Procede, por tanto, adaptar el actual marco legislativo a estas nuevas circunstancias ampliando su ámbito de aplicación a las normas para los servicios"[204], apostando también por la posibilidad de referenciar las denominadas "especificaciones técnicas de la TIC", que son diferentes[205] de las normas europeas desde el punto de vista formal[206].

Dicho Reglamento regula las normas europeas y documentos europeos de normalización en apoyo de la legislación y políticas de la Unión, y precisamente su artículo 10.1 autoriza, dentro de los límites de las competencias que establece el Tratado de Funcionamiento de la Unión Europea, que la Comisión podrá pedir a una o varias

---

[201] Aunque lo que sí podrá hacer es exigir el cumplimiento de otros requisitos que se hayan establecido en el nivel nacional, siempre que los mismos no se refieran a aspectos armonizados por el Reglamento eIDAS.

[202] Considerando (7) del Reglamento (UE) 1025/2012.

[203] Hoy, Directiva (UE) 2015/1535.

[204] Considerando (10) del citado Reglamento.

[205] Y cuyo uso "no debe socavar la coherencia del sistema europeo de normalización. Por lo tanto, el presente Reglamento también debe establecer las condiciones en las que puede considerarse que una especificación técnica no entra en conflicto con otras normas europeas", según el Considerando (36) del citado Reglamento.

[206] Por ejemplo, las especificaciones del IETF, denominadas RFC, y que regulan la mayor parte de los servicios de Internet, incluyendo los servicios de confianza, creadas de forma paralela a la normalización europea institucionalizada.

organizaciones europeas de normalización[207] que elaboren una norma europea o un documento europeo de normalización en un plazo determinado.

En el caso que nos ocupa, esta previsión permite a la Comisión realizar mandatos de normalización en relación con las materias previstas por el Reglamento eIDAS, para posteriormente establecer, también de acuerdo con las previsiones legales expresas del mismo Reglamento, los números de referencia de dichas normas, pudiendo, por tanto, tratarse de verdaderas normas europeas cuanto de otros documentos de normalización.

Y efectivamente, la Comisión Europea, que inicialmente impulsó la normalización a través de la iniciativa conocida como EESSI, mediante especificaciones técnicas sin el rango de norma europea, emitió el Mandato M/460, de 22 de diciembre de 2009, con la finalidad de simplificar y completar, además de elevar a la categoría de normas europeas, las ya citadas especificaciones, todo ello en el plazo máximo de cuatro años, por lo que cabe intuir que esas serán las normas candidatas a ser seleccionadas por la Comisión. Nótese que el Mandato en cuestión es anterior al Reglamento (UE) Nº 1025/2012, por lo que el procedimiento seguido no corresponde al que en futuros mandatos se deberá seguir.

La selección (el establecimiento) de normas técnicas se configura en el Reglamento eIDAS, salvo en el caso de la certificación de los dispositivos cualificados de creación de firma electrónica o de sello electrónico, como actos de ejecución[208], que deberán ser adoptado mediante el procedimiento de examen, todo ello en los términos dispuestos por el Reglamento (UE) Nº 182/2011 del Parlamento Europeo y del Consejo de 16 de febrero de 2011 por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión, lo que denota una fuerte voluntad de los Estados miembros de, por una parte, garantizar unas condiciones uniformes de ejecución por parte de la Comisión y, de otra, mantener un fuerte control sobre la actuación de la Comisión[209].

Esencialmente, en este tipo de procedimientos se actúa mediante la formación de un comité[210] compuesto por representantes de los Estados miembros, con la misión de

---

[207] A las que se refiere, por cierto, (Esteve Pardo, 2010, pág. 235) con epítetos como "tecnocracia" y "expertocracia organizadas", indicando que "los operadores en los diferentes sectores donde la técnica ocupa una posición relevante han alcanzado acuerdos sobre materias de interés común y después han constituido poderosas organizaciones que acaban ostentando una posición muy influyente, en muchos aspectos decisiva".

[208] Por lo que constituye un caso en el que existe una reserva de decisión del procedimiento para decidir al que se ha referido también (Esteve Pardo, 2010, págs. 243-244), en el que el poder legislativo interviene "en el diseño del organigrama, en la determinación y aún configuración de los órganos llamados a adoptar decisiones en las materias sensibles".

[209] Se trata de un importante cambio con respecto a la Propuesta de Reglamento, que contenía una mayor cantidad de actos delegados previstos, como han notado (Dumortier & Vandezande, 2012a, p. 12); cambios que puede ser debido al hecho de que los Reglamentos europeos –y en menor medida, las Directivas– se han considerado muestras de *commandeering* ejecutivo del poder europeo central sobre los Estados miembros, que se ven obligados a aplicar la normativa –en este caso, técnica– aprobada, con independencia de su parecer contrario, algo que, a juicio de (Ballbé & Martínez, 2003, págs. 194-195), vulnera los principios estructurales de la separación de poderes horizontal y vertical, y los valores constitucionales pluralistas.

[210] La Directiva de firma electrónica ya había regulado, en su artículo 9, un comité de firma electrónica, que operaba de acuerdo con la Decisión 1999/468/CE, antecedente inmediato del Reglamento (UE) Nº

alcanzar un acuerdo con la suficiente calidad y consenso sobre el acto en cuestión[211], comité cuyas deliberaciones resultan sujetas al derecho de acceso por los ciudadanos de la Unión[212] y, por tanto, deberían ser transparentes, lo cual se encuentra parcialmente garantizado gracias al acceso al Registro de Comitología[213].

El procedimiento de examen resulta apropiado por tratarse de actos de ejecución de alcance general[214], lo cual implica un régimen específico de adopción de acuerdos por consenso general o por mayoría reforzada[215] y mecanismos para evitar el bloqueo de los actos a adoptar[216], pero no es menos cierto que se trata de un régimen en el que la Comisión sólo puede ejercer sus competencias en la medida en que un número suficiente de Estados miembros lo quieran de forma expresa.

En resumen, nótese que, en este modelo regulatorio, el rol de la Comisión en relación con la actividad de los prestadores de servicios de confianza se centra en gran medida en fomentar la creación de las normas técnicas de servicios de confianza, que son desarrolladas por la industria, a través de las organizaciones europeas o internacionales de normalización; y en establecer posteriormente dichas normas al objeto de facilitar su adopción por la propia industria que las ha producido, aunque siempre con la intervención necesaria y previa de los Estados miembros.

De forma breve, se trata de un enfoque de regulación mínima y autorregulación máxima, pero consensuada con la Administración, y que se presenta, como ya hemos visto, en dos grados de intervención: reglamentos técnicos obligatorios[217] y normas técnicas voluntarias[218].

Este modelo, que formalmente resulta perfectamente defendible, no está exento de problemas, entre los cuales la ausencia de jerarquía normativa entre el Reglamento eIDAS (que es la norma jurídicamente vinculante) y las normas técnicas (que no son

---

182/2011.

[211] Artículo 3 del Reglamento (UE) Nº 182/2011.

[212] Artículo 9.2 del Reglamento (UE) Nº 182/2011.

[213] Disponible en http://ec.europa.eu/transparency/regcomitology/index.cfm?CLX=es. Se debe buscar el "eIDAS Committee".

[214] Artículo 2.2.a) del Reglamento (UE) Nº 182/2011.

[215] Típicamente, dado que será la Comisión la que proponga la norma técnica, dicha mayoría será de un mínimo del 55% de los miembros del comité que represente a Estados miembros participantes que reúnan como mínimo el 65% de la población de dichos Estados (artículo 5.1 del Reglamento (UE) Nº 182/2011, que remite al artículo 238, apartado 3, del Tratado de Funcionamiento de la Unión Europea).

[216] En concreto, la Comisión podrá adoptar el acto referido a la norma técnica cuando no se oponga a ello una mayoría simple de los miembros que componen el comité. Caso de oposición, el presidente podrá, bien presentar al mismo comité una versión modificada del mismo en el plazo de dos meses a partir de la votación, bien presentar al comité de apelación para una nueva deliberación el proyecto de acto de ejecución en el plazo de un mes a partir de la votación.

[217] Como se recordará, entran en esta categoría las normas técnicas y organizativas de seguridad previstas en el artículo 19 del Reglamento eIDAS, así como las normas aplicables a los dispositivos cualificados de creación de firma previstas en el artículo 29 del mismo Reglamento.

[218] Como en el caso de la norma técnica voluntaria que describe el contenido de los certificados cualificados a la que nos hemos referido anteriormente.

jurídicamente imperativas), lo que impide reaccionar legalmente contra el contenido de una norma técnica que se considere contraria a la propia norma jurídica, por ejemplo, por no incorporar reglas técnicas que permitan garantizar el cumplimiento de los requisitos jurídicos mínimos, o cuyos contenidos resulten discriminatorios.

Otra disfunción podría venir dada por el hecho que la norma técnica resulte excesivamente creativa en cuanto a las obligaciones del prestador, estableciendo reglas técnicas de obligado cumplimiento que no tengan base legal en ningún requisito del Reglamento eIDAS; o por el hecho de que una norma técnica, aparentemente genérica, en realidad sólo permita el empleo de una única tecnología, en exclusión de otras mientras el comité no tenga a bien seleccionar otras normas técnicas[219].

Contra dichas disfunciones, hay que entender que la vía de reacción sería atacar el propio acto de ejecución de la Comisión, a través del correspondiente procedimiento judicial contra los actos de la Comisión, en especial un acto de ejecución venga referido a una norma de obligado cumplimiento que entre en contradicción con el Reglamento eIDAS; esto es, cuando nos encontramos en presencia de un verdadero reglamento técnico.

La segunda competencia de la Comisión se refiere a la posibilidad de establecimiento de criterios específicos[220] que deben satisfacer los organismos designados para la certificación de la conformidad de los dispositivos de creación de firma o sello electrónico, según prevé el artículo 30.4 del Reglamento eIDAS, competencia que se ejerce por delegación[221], a tenor del artículo 290 del Tratado de Funcionamiento de la Unión Europea, dada la necesidad de complementar algunos aspectos técnicos concretos del Reglamento de manera flexible y rápida[222], y que se orienta a garantizar unas condiciones uniformes relativas a la actuación de estas entidades, cuya misión es comprobar que los productos empleados para la creación de la firma electrónica cualificada o del sello electrónico cualificado cumplen las exigencias legales.

---

[219] Por ejemplo, el acuerdo de grupo de trabajo CEN CWA 14169, referenciado por Decisión 2003/511/CE de la Comisión, de 14 de julio de 2003, relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, sólo permitía que los chips criptográficos fueran certificables como dispositivos seguros de creación de firma, impidiendo, durante años, que otras tecnologías pudieran acceder a dicha condición, disfunción que se ha tratado de solventar –aunque sólo parcialmente– en el Reglamento eIDAS. Esta Decisión de la Comisión ha sido derogada recientemente, por la Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

[220] Esta competencia no es tan novedosa como podría parecer, ya que la Directiva 1999/93/CE de firma electrónica ya la había previsto en su artículo 3.4, mediante el entonces vigente procedimiento de reglamentación, previsto en la Decisión 1999/468/CE, que dio lugar a la Decisión 2000/709/CE de la Comisión, de 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica.

[221] Las condiciones para el ejercicio de la delegación se contienen en el artículo 47 del Reglamento eIDAS.

[222] Considerando (70) del Reglamento eIDAS.

1.4.3 Las competencias del legislador nacional relativas a los servicios de confianza

El Reglamento eIDAS prevé también competencias de los Estados miembros, que en algunos casos corresponderán al legislador, y en otros, al supervisor o a terceras autoridades, como el supervisor de protección de datos o de consumo, según corresponda.

En el primer caso, sucede que el Reglamento eIDAS, como hemos ido indicando, armoniza determinadas reglas esenciales relativas a los servicios de confianza, pero no afecta a la competencia del legislador nacional, que se mantiene plenamente vigente en aquellos aspectos que no hayan sido objeto de armonización.

En este sentido, cabe indicar que cualquier aspecto no armonizado podrá ser objeto de la legislación nacional. Entre los mismos, destaca con fuerza que el Reglamento eIDAS no haya armonizado la normativa nacional relativa al uso de la criptografía, que por tanto se rige por el Derecho del Estado de establecimiento del prestador del servicio.

En tanto en cuanto los dispositivos de creación de firma y sello como los denominados sistemas fiables hacen uso de la criptografía, la normativa nacional reguladora de su certificación de seguridad podrá introducir la verificación de la calidad de los correspondientes algoritmos,en conexión con la evaluación de la seguridad de los correspondiente productos, materia de especial sensibilidad que podría afectar a los niveles de seguridad efectiva, por lo que los órganos competentes para ello en los diferentes Estados miembros tenderán a consensuar los mínimos deseables para toda la Unión, en foros como el SOG-IS.

De esta forma, las antiguas regulaciones del uso de la criptografía, como la francesa, que cualificaba a las entidades que expedían certificados de firma electrónica como prestadores de servicios de criptología, han quedado absorbidas en un marco específico, relativo a la certificación de la seguridad tecnológica de producto, que es más general y amplio que el de los productos empleados por los prestadores de servicios de confianza, y que progresa para lograr el reconocimiento general de las certificaciones expedidas a dichos productos, al menos en el ámbito de la Unión Europea.

Además de lo anterior, el propio Reglamento eIDAS prevé el desarrollo, en sede nacional, de normas complementarias al Reglamento, en algunos casos con carácter opcional, y en otros, de forma necesaria.

El Considerando (22) del Reglamento eIDAS indica que “corresponde al Derecho nacional definir los efectos jurídicos de los servicios de confianza, salvo disposición contraria del presente Reglamento”, lo que deberá recaer sobre el legislador, mediante la oportuna legislación sustantiva o procesal. Más en concreto, el Considerando (49) del Reglamento eIDAS concreta que “el presente Reglamento debe establecer el principio de que no se deben denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada. Sin embargo, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el presente Reglamento según los cuales una firma electrónica cualificada debe tener el efecto jurídico equivalente a una firma manuscrita”,

como tendremos ocasión de analizar en detalle[223].

Por su parte, el Considerando (24) del Reglamento eIDAS establece que "los Estados miembros podrán mantener o introducir disposiciones nacionales, acordes con el Derecho de la Unión, relativas a los servicios de confianza, siempre que tales servicios no estén plenamente armonizados por el presente Reglamento", añadiendo que "no obstante, los productos y servicios de confianza que se ajusten al presente Reglamento deben poder circular libremente en el mercado interior", posibilidad que, también con carácter general, deberá ser ejercitada por el legislador, y que permite realmente un margen de maniobra importante para que los Estados regulen gran cantidad de aspectos referidos a la prestación de los servicios, si bien con la limitación de que sólo resultarán aplicables a los prestadores instalados en su territorio[224].

Para el tratamiento adecuado de esta cuestión, resulta imprescindible identificar el alcance de las disposiciones armonizadas, identificar las posibles disposiciones adicionales y evaluar su impacto. En muchas ocasiones, las propias normas técnicas seleccionadas por la Comisión remitirán a la legislación nacional para la determinación de determinados aspectos, o bien dejarán aspectos sin definir, por lo que resultará conveniente que el legislador nacional los regule.

A título de ejemplo, podemos citar los periodos de retención de registros por los prestadores (que pueden ser de más o menos años, frecuentemente en atención a las normas jurídicas de prescripción de acciones), o la forma de acreditar la trazabilidad hasta el laboratorio UTC nacional, que se debería establecer en el marco de la legislación metrológica.

Formaría, también, parte de las competencias del legislador nacional, delegable en su caso en el organismo de supervisión, la aprobación de reglamentos y normas técnicas –tanto relativas a las medidas de seguridad[225], cuando al propio contenido de la actividad prestacional[226]– cuando no lo haya hecho la Comisión Europea, con el único límite de que, como acabamos de ver, dichas disposiciones no se opongan al Derecho de la Unión, lo cual incluye que las mismas no infrinjan el principio de neutralidad tecnológica, por lo que se debería considerar contraria al Reglamento eIDAS una disposición que impida absolutamente la elección tecnológica del prestador, en especial en el caso de un servicio armonizado.

Asimismo, y como sabemos[227], los Estados miembros mantienen la libertad para definir y regular nuevos servicios de confianza en sede nacional, siempre que no se solapen con los servicios de confianza tipificados en el Reglamento eIDAS, en cuyo caso es preciso notar que el legislador nacional será libre de establecer el modelo regulatorio de control

---

[223] Cfr. el epígrafe 4.2 de este trabajo.

[224] Lo cual podría situarles en una situación de desventaja competitiva frente a prestadores instalados en otros Estados, que podrán comercializar igualmente sus servicios en toda la Unión Europea.

[225] En este caso, posiblemente con el carácter de reglamento técnico obligatorio, lo que obligaría a su notificación conforme al procedimiento de la Directiva (UE) Nº 2015/1535.

[226] En ese caso debería ser con carácter puramente voluntario, al objeto de cumplir con el principio d neutralidad tecnológica, que impide imponer al prestador el uso de tecnologías o modelos de negocio concretos.

[227] Cfr. el epígrafe 1.3.4 de este trabajo.

que le parezca más adecuado, dentro de las reglas generales del Derecho de la Unión, inclusive mimetizando el concepto de cualificación, pero en sede nacional, estableciendo un régimen de autorización previa[228].

El artículo 16 del Reglamento eIDAS prevé que "los Estados miembros establecerán normas relativas a las sanciones aplicables a las infracciones del presente Reglamento. Las sanciones previstas serán eficaces, proporcionadas y disuasorias", previsión que exige la correspondiente norma con rango de ley formal, en atención al principio de tipicidad, y que se debería sustanciar en la reforma de la LFE para su adecuación al Reglamento eIDAS.

En este sentido, el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza propone un completo cuadro de infracciones y sanciones, al que nos referiremos posteriormente[229].

Asimismo, y esto es más novedoso, el artículo 17.5 del Reglamento eIDAS autoriza que "los Estados miembros podrán disponer que el organismo de supervisión establezca, mantenga y actualice una infraestructura de confianza de conformidad con las condiciones establecidas en la legislación nacional", posibilidad que permite diversos modelos de implementación, como una entidad de certificación raíz nacional que firmase los certificados en soporte de todos los servicios de confianza supervisados en un Estado miembro, como han realizado Alemania o Polonia; una autoridad de certificación que firme todas las autoridades del sector público, como en Portugal; o bien una autoridad de certificación puente, como sucede en Estados Unidos.

Finalmente, los artículos 28 y 38 del Reglamento eIDAS prevén que los Estados puedan fijar, o no, normas relativas a la suspensión de los certificados de firma y sello electrónico, posibilidad que en la DFE y la LFE es obligatoria, algo que posiblemente también deberá ser objeto de la correspondiente actuación del legislador nacional.

El ejercicio de todas estas competencias se va a traducir en una norma legal, que deberá ser objeto de la correspondiente notificación previa a la Comisión, en el marco de la Directiva 2015/1535, ya mencionada.

1.4.4 Las competencias del ejecutivo nacional; en particular, el organismo de supervisión. La cooperación con terceros

Por su parte, al ejecutivo nacional corresponden la mayoría de competencia de ejecución del Reglamento eIDAS, en especial al organismo de supervisión[230], incluyendo el análisis de los informes de evaluación de la conformidad[231]; conceder la cualificación a los

---

[228] Así sucede, por ejemplo, en Italia en relación con los servicios de operador de correo electrónico certificado, de gestor de la identidad digital o de conservador de documentos, que se sujetan a acreditación (cfr. el artículo 29 del Código de la Administración Digital, aprobado por Decreto legislativo de 7 de marzo de 2005, número 82, en redacción dada por Decreto legislativo de 28 de agosto de 2016, número 179), por citar una de las ya diversas experiencias de Estados miembros de la Unión Europea.

[229] Cfr. el epígrafe 7.3 de este trabajo.

[230] Artículo 17.4 del Reglamento eIDAS.

[231] Cfr. el epígrafe 7.1.1 de este trabajo.

prestadores de servicios de confianza y a los servicios de confianza que prestan[232], y retirar esta cualificación; difundir la cualificación de los prestadores mediante listas de confianza[233], realizar auditorías o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la conformidad de prestadores cualificados de servicios de confianza[234]; o requerir que los prestadores de servicios de confianza corrijan cualquier incumplimiento de los requisitos establecidos[235].

Se trata, en definitiva, del régimen de supervisión –reforzada[236], en el caso de los servicios cualificados– instaurado por el Reglamento eIDAS en relación con la prestación de los servicios de confianza.

Obviamente, dichas competencias –que analizaremos con mayor detalle en su momento, por razones sistemáticas– se deberán ejercer de acuerdo con las normas de procedimiento administrativo previstas en el derecho nacional, con especial atención a la aplicación del principio de buena administración, incluida la obligación del supervisor de motivar sus decisiones[237], dados los costes económicos que las evaluaciones de conformidad no periódicas suponen a los prestadores, por ejemplo.

Dada la importancia de esta función, y como se ha avanzado, resulta necesario que en cada Estado miembro exista un organismo de supervisión, algo que –debido a la necesaria especialización del mismo[238]– podría resultar gravoso para los Estados miembros de menor dimensión. Por otra parte, dada la evidente dimensión transfronteriza de estos servicios, podría resultar inviable realizar actuaciones administrativas en el territorio de otros Estados miembros. Todo ello exige el establecimiento de relaciones de colaboración entre los citados Estados miembros en relación a la supervisión.

En dicho sentido, el Considerando (42) del Reglamento eIDAS indica que "[p]ara facilitar la supervisión de los prestadores cualificados de servicios de confianza, por ejemplo cuando un prestador preste sus servicios en el territorio de otro Estado miembro y no esté sujeto a supervisión en este, o cuando los ordenadores de un prestador estén situados en el territorio de un Estado miembro distinto de aquel en el que está establecido, debe crearse un sistema de asistencia mutua entre los organismos de supervisión de los Estados miembros"; mecanismo que se regula en el artículo 18 del Reglamento eIDAS[239], que

---

[232] Cfr. el epígrafe 7.1.2 de este trabajo.

[233] Cfr. el epígrafe 7.1.4.1 de este trabajo.

[234] Cfr. el epígrafe 7.1.1 de este trabajo.

[235] Cfr. el epígrafe 7.2.1 de este trabajo.

[236] Para (Dumortier & Vandezande, 2012a, p. 10), la supervisión de estas actividades por parte del sector público puede ser efectiva, pero únicamente si se ejerce de forma muy estricta y seria, como se ha deducido del incidente de DigiNotar.

[237] Considerando (46) del Reglamento eIDAS.

[238] Especialización que se traduce en coste de personal y, en su caso, de contratación externa. A título de ejemplo, el ejecutivo alemán ha cuantificado aproximadamente en quince personas/año las necesidades totales que se exigen para la supervisión, incluyendo el cumplimiento de las obligaciones mínimas previstas por el Reglamento eIDAS y de las provisiones complementarias de la legislación alemana. Cfr. la notificación a la Comisión Europea del proyecto de Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*).

[239] Recuérdese que, conforme al artículo 4.3 del Tratado de la Unión Europea, "[c]onforme al principio de cooperación leal, la Unión y los Estados miembros se respetarán y asistirán mutuamente en el cumplimiento

prevé tres modalidades de asistencia mutua.

La primera modalidad, prevista en el epígrafe 1 del artículo 18, consiste en la cooperación con vistas a intercambiar información sobre prácticas idóneas.

Se trata de una previsión lógica, dada la complejidad técnica de la actividad administrativa de supervisión, en especial en atención a la diferente tipología de servicios de confianza tipificados en el Reglamento, y su origen histórico en las leyes nacionales. Por ejemplo, en Alemania se institucionaliza el servicio de confianza de sellado electrónico de tiempo mucho tiempo antes de incorporarse al Reglamento eIDAS, por lo que el organismo alemán tiene gran experiencia en la supervisión de dicho tipo de servicio, y en su consecuencia puede fácilmente cooperar con otros organismos de supervisión.

Hay que entender que nos encontramos ante una cooperación adicional a la que se prevé en el artículo 48 del propio Reglamento eIDAS, y a la que ya nos hemos referido, y que podrá sustanciarse, conforme al Derecho nacional, mediante las diferentes fórmulas, inclusive informales, previstas en el mismo.

En concreto, estas relaciones de cooperación podrán ser bilaterales o multilaterales, de las cuales la más notable –por su larga duración– es el Foro de Autoridades Europeas de Supervisión[240], establecido en 2002 para la cooperación multilateral en el ámbito de los servicios de certificación regulados en la DFE, y que se mantiene plenamente operativo.

Cuenta con supervisores de veintiséis Estados, no tiene personalidad jurídica propia y se presenta como un cuerpo con experiencia para sustentar la cooperación, el intercambio de información y la asistencia entre los miembros, de forma alineada con los mandatos del artículo 17.4.a) y c), y 18.1 del Reglamento eIDAS. Será preciso ver, sin embargo, si realmente recupera la relevancia que tuvo en su día.

La segunda modalidad prevista es la colaboración en cuanto a las funciones de supervisión, prevista en el segundo párrafo el artículo 18.1 del Reglamento eIDAS, que establece que "[u]n organismo de supervisión, previa solicitud justificada de otro organismo de supervisión, deberá prestar asistencia a dicho organismo con el fin de que las actividades de los organismos de supervisión pueden realizarse en forma coherente", la cual "podrá incluir, en particular, las solicitudes de información y las medidas de supervisión, tales como las peticiones para que se lleven a cabo inspecciones en relación con los informes de evaluación de la conformidad a que se refieren los artículos 20 y 21".

Nos encontramos, en este caso, ante un organismo de supervisión que realiza tareas para otro organismo, a petición del mismo, siempre que las mismas cumplan dos condiciones: la primera, que se trate de una función competencia del organismo requirente; la segunda, que la función encomendada entre dentro de las competencias del organismo requerido. Por ejemplo, el organismo de supervisión español podría precisar asistencia del organismo húngaro, en caso de que los sistemas fiables de un prestador establecido en España se encuentren en Hungría, asistencia que podría referirse, por ejemplo, a la

---

de las misiones derivadas de los Tratados", que "[l]os Estados miembros adoptarán todas las medidas generales o particulares apropiadas para asegurar el cumplimiento de las obligaciones derivadas de los Tratados o resultantes de los actos de las instituciones de la Unión" y que "[l]os Estados miembros ayudarán a la Unión en el cumplimiento de su misión y se abstendrán de toda medida que pueda poner en peligro la consecución de los objetivos de la Unión".

[240] Cfr. http://www.fesa.eu/.

inspección presencial de las instalaciones donde se encuentran dichos sistemas fiables.

En efecto, el epígrafe 2 del artículo 18 del Reglamento eIDAS prevé tres casos en los que se podrá denegar la asistencia: el primero de ellos resulta aplicable cuando "el organismo de supervisión no es competente para prestar la asistencia solicitada", como por ejemplo, si la petición de asistencia se refiere a la verificación técnica del cumplimiento de requisitos técnicos de los productos empleados en los sistemas fiables del prestador, ya que dicha competencia recae sobre un organismo de evaluación de la conformidad de productos de seguridad, conforme a Criterios Comunes de Seguridad, o cuando la solicitud de asistencia se refiera a elementos fuera de territorio de dicho organismo de supervisión; el segundo de los casos resulta aplicable cuando "la asistencia solicitada no guarda proporción con las actividades de supervisión del organismo de supervisión realizadas de conformidad con el artículo 17", y se dirige claramente a evitar una sobrecarga injustificada de trabajo sobre el organismo de supervisión requerido para asistencia; finalmente, el tercero de los casos resulta aplicable cuando "la prestación de la asistencia solicitada sería incompatible con el presente Reglamento", que constituye un escenario de carácter general en el que pueden caber diversos motivos de denegación, por ejemplo en caso de referirse a aspectos no armonizados.

La tercera modalidad se encuentra prevista en el artículo 18.3 del Reglamento IDAS, en cuya virtud, "[c]uando proceda, los Estados miembros podrán autorizar a sus respectivos organismos de supervisión para que lleven a cabo investigaciones conjuntas con participación de personal de los organismos de supervisión de otros Estados miembros", constituyendo la posibilidad más intensa de las tres y que, por el evidente elemento de actuación administrativa extraterritorial, requiere de la autorización previa de los Estados miembros, así como de "acuerdos y procedimientos para dichas actividades conjuntas", que "serán aprobadas y establecidas por los Estados miembros de que se trate de conformidad con sus legislaciones nacionales".

Adicionalmente a estas tres modalidades de cooperación, el artículo 19.2 del Reglamento eIDAS ordena que "[c]uando proceda, en particular si una violación de la seguridad o pérdida de la integridad afecta a dos o más Estados miembros, el organismo de supervisión notificado informará al respecto a los organismos de supervisión de los demás Estados miembros de que se trate", lo que realizará a los efectos oportunos, que normalmente se traducirá en la correspondiente actuación de supervisión[241] por el organismo que reciba la información.

El Reglamento eIDAS no prevé únicamente relaciones administrativas entre organismos de supervisión, sino también entre éstos y otros organismos, significativamente la autoridad de protección de datos personales, dada la importancia de estos datos en los servicios de confianza, como por ejemplo en el caso de la expedición de certificados electrónicos de firma electrónica.

De esta forma se prevé, por ejemplo, en el artículo 20.2 del Reglamento eIDAS, en cuya virtud "[e]n caso de posible infracción de las normas sobre protección de datos personales, el organismo de supervisión informará a las autoridades de protección de

[241] Por ejemplo, imaginemos que en Alemania se detecta un incidente motivado por una vulnerabilidad en una aplicación informática muy ampliamente empleada por prestadores de otros Estados miembros, algo que por cierto es el caso, dado el relativamente escaso número de fabricantes de estas tecnologías, e informa de dicho problema a sus iguales. Sería razonable que el organismo español de supervisión pidiera a los prestadores que mitiguen dicha vulnerabilidad.

datos de los resultados de sus auditorías", para respetar el principio de competencia.

Una segunda relación interadministrativa es la que se establece entre el organismo de supervisión y la Agencia Europea de Seguridad de Redes y de la Información (ENISA) al amparo de lo establecido en el artículo 19 del Reglamento eIDAS, referida a dos casos.

En primer lugar, el epígrafe 2, tercer párrafo, del artículo citado ordena que "[c]uando proceda, en particular si una violación de la seguridad o pérdida de la integridad afecta a dos o más Estados miembros, el organismo de supervisión notificado informará […] a la ENISA", dada la dimensión trasfronteriza del incidente, que puede requerir de la coordinación de la citada Agencia.

En segundo lugar, el epígrafe 3 del propio artículo 19 también ordena, esta vez con carácter estable, que "[e]l organismo de supervisión facilitará a la ENISA anualmente un resumen de las notificaciones de violación de la seguridad y pérdida de la integridad recibidas de los prestadores de servicios de confianza", cabe imaginar que al objeto de que por dicha Agencia se pueda evaluar la conveniente de establecer guías de seguridad voluntarias, o proponer a la Comisión la adopción de los reglamentos técnicos de seguridad a que antes hemos hecho referencia.

CAPÍTULO 2. LOS SERVICIOS DE IDENTIFICACIÓN Y AUTENTICACIÓN ELECTRÓNICA

En este Capítulo abordamos el análisis de los servicios electrónicos que permiten la acreditación de la identidad por vía electrónica, y que, como ya hemos visto, se corresponden con los servicios de identificación y autenticación electrónicas, en su caso con intervención directa de terceros a los que se "delega" la operativa[242].

Nos centraremos en los dos servicios actualmente regulados para dicha función en España, como son los certificados electrónicos (en sus diferentes modalidades, que acreditan la identidad de una persona física, de una persona jurídica o de un sitio web), de un lado, y los sistemas de identificación ofrecidos al amparo de la normativa de administración electrónica, de otro, que son servicios de delegación de la autenticación, como Cl@ve.

Esto no significa que no puedan existir –y, de hecho, existen– otros servicios de acreditación de la identidad mediante la delegación de la autenticación, pero los mismos no disponen actualmente de un marco regulador diferente del previsto para los servicios de la sociedad de la información, y no gozan de un reconocimiento específico, por lo que quedan fuera de nuestro objeto de estudio.

Por tanto, en el primer epígrafe de este Capítulo abordamos el estudio del servicio de confianza de expedición de certificados, el único servicio privatizado de identificación electrónica que ha sido institucionalizado por la ley y que recibe efectos jurídicos concretos que lo hacen útil como herramienta para la acreditación de la actuación electrónica. En el mismo presentamos la caracterización del servicio y sus requisitos jurídicos correspondientes, establecidos tanto en la normativa de la Unión como por la normativa española que la complementa. Asimismo, se presenta su efecto jurídico y, finalmente, se estudian en profundidad las particularidades, que no son pocas, de este servicio en el ámbito de la administración electrónica.

En cambio, en el segundo epígrafe nos centramos en el análisis de los servicios públicos de identificación electrónica desarrollados en España, incluyendo el DNI electrónico, instrumento de identificación electrónica de carácter general, y otros servicios implementados para el desarrollo de la administración electrónica, en especial al objeto de facilitar al máximo la accesibilidad a los servicios públicos electrónicos.

Ambos tipos de servicios puede ser objeto de notificación, como veremos en el Capítulo 3, a la Comisión Europea a los efectos de su reconocimiento para las transacciones transfronterizas vinculadas a servicios públicos electrónico y, en función de la decisión de cada Estado miembro notificante, también en relación con relaciones jurídico-privadas, por lo que resulta preciso conocer su régimen jurídico con detalle.

[242] Cfr. una introducción a las técnicas relativas al servicio de seguridad de autenticación, en el Anexo A.1 de este trabajo.

2.1 EL SERVICIO DE CONFIANZA DE EXPEDICIÓN DE CERTIFICADOS DE IDENTIDAD PERSONAL Y DE SITIOS WEB

En este epígrafe nos vamos a referir a uno de los elementos que sustentan la acreditación electrónica y, por tanto, la prueba, de la identidad, como es el certificado de clave pública, y el correspondiente servicio de confianza. Se trata de un instrumento que es diseñado y autorregulado con la función de identificación y autenticación, aunque posteriormente su uso se ha asociado más con la validez de la firma digital de documentos y comunicaciones electrónicas, especialmente desde la óptica de la normativa legal que procede a su institucionalización.

Sin embargo, lo cierto es que el certificado digital, y el servicio de confianza que lo sustenta, constituye una prueba electrónica de la identidad, sea de persona física[243] o jurídica, y con independencia de si el certificado se emplea para avalar una firma electrónica, un sello electrónico o un nombre de dominio en Internet, motivo por el que procede su estudio en este momento.

2.1.1 Caracterización del servicio: el certificado electrónico

Debemos, en primer lugar, caracterizar los certificados de firma y sello electrónico, objeto de este servicio de confianza, que la legislación regula como componente imprescindible de las modalidades más robustas de la firma y sello electrónico –avanzada y cualificada–, para, posteriormente, presentar los certificados de sitio web.

De todos los tipos técnicos de certificados de clave pública que la autorregulación ha producido[244], el certificado cualificado de clave pública para la firma de las personas físicas ha sido el paradigma legal de certificado electrónico regulado[245], al cual se han acabado asimilando los restantes certificados de firma y sello electrónico, como ha sucedido en el caso de los certificados de sello electrónico para la actuación automatizada, administrativa o judicial.

El artículo 3.14) del Reglamento eIDAS se refiere al certificado de firma electrónica como "una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona", y el artículo 3.15) del mismo, al certificado cualificado como un "certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I"[246]. De forma análoga, en el caso del

---

[243] Como indica (Martínez Nadal, 2009, pág. 117), "[l]a principal función del certificado es asociar la identidad de una persona determinada a una clave pública concreta (e indirectamente a una clave privada)", por lo que "[e]l destinatario de un certificado que desee confiar […] puede usar la clave pública incluida en el certificado para verificar que la firma digital fue creada con la correspondiente clave privada", de modo que "[s]i tal verificación realizada utilizando un certificado es satisfactoria, se obtiene la seguridad (razonable, pero no absoluta, como veremos) de que la clave privada es poseída por la persona mencionada en el certificado, y que la firma digital fue creada por esa persona determinada".

[244] Sobre estos tipos de certificados, cfr. el anexo A.2.

[245] Y es que, como veremos en su momento, para que una firma o sello electrónico se pueda considerar cualificado, se debe basar en un certificado electrónico cualificado.

[246] La LFE definía, por su parte, el certificado electrónico, en su artículo 6, como "un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de

sello, el artículo 3.29) define el certificado de sello electrónico como "una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona", mientras que el artículo 3.30) se refiere al certificado cualificado como "un certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III".

Por su parte, el artículo 3.38) del Reglamento eIDAS define el certificado de autenticación de sitio web como "una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado", definiendo el artículo 3.29) de la misma norma el certificado cualificado como "un certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV".

Esta identificación, que es la finalidad principal de los certificados[247], se expide en relación con diversos propósitos legales previstos en el Reglamento eIDAS, principalmente para respaldar la firma o el sello electrónico avanzado –a los que posteriormente nos referimos con detalle[248]–, al confirmar la identidad de la persona correspondiente, y para la autenticación de los sitios web; esto es, para que se pueda identificar a los citados sitios web en las conexiones realizadas con los mismos, o también desde los mismos.

Para sustentar la confianza de las partes usuarias, el Reglamento eIDAS establece un conjunto de normas mínimas referidas al contenido de cada uno de estos certificados y a las obligaciones mínimas de los prestadores de que los expiden, configurando, por tanto, los correspondientes servicios de confianza de expedición de certificados, tipificados en el Reglamento eIDAS.

Debido a que los tres servicios son muy similares, los trataremos conjuntamente. Y lo hacemos en este capítulo, porque el servicio de confianza de expedición de certificados tiene la finalidad de aportar prueba electrónica acerca de la identidad de la persona indicada en el mismo.

La duda que se puede plantear, aunque sólo en relación con el uso de los certificados de firma electrónica o de sello electrónico, es si los mismos pueden utilizarse para que la

---

firma a un firmante y confirma su identidad", mientras que el artículo 11 de la propia LFE se refería al certificado reconocido como aquel expedido "por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten".

[247] Desde la perspectiva mercantil, (Ortega Díaz, 2008, pág. 178) ha indicado, con gran precisión, que "mediante el contrato de certificación electrónico, de carácter bilateral, oneroso, conmutativo y formalizado, comúnmente, mediante técnica de adhesión, una parte, el prestador de servicios de certificación, se obliga a realizar todas las conductas propias de su actividad, entre las que se encuentra fundamentalmente la expedición de un certificado, dirigidas a identificar, con niveles adecuados de seguridad, a la otra parte, a cambio de un precio cierto y determinado", identificando como causa del contrato, por tanto, la identificación del firmante, aunque admite que esta causa del contrato se ha expedido para recaer sobre las personas jurídicas y las cosas, como los sitios web (Ortega Díaz, 2008, pág. 179), lo que ha sido recogido en el actual Reglamento eIDAS. Como nota curiosa, el autor también se refiere a la certificación de imágenes u obras de carácter plástico o fotográfico, algo que podría ser reconducido al uso de atributos adicionales de certificados de autenticación de sitio web.

[248] Cfr. el epígrafe 4.1 de este trabajo.

persona física o jurídica identificada en el certificado pueda identificarse electrónicamente en un proceso que no exija la firma electrónica o el sello electrónico, como por ejemplo en el caso de acceso a una página web con contenidos informativos que requieran de la necesaria autenticación previa; es decir, si estos certificados sirven, además de para firmar o sellar, para autenticarse, normalmente en un proceso de control de acceso. O, dicho de otra forma, si los mismos se pueden emplear en un servicio de autenticación de entidad.

Se trata de una duda que el Reglamento eIDAS no resuelve de forma directa, porque el mismo no es aplicable, como veremos, a las decisiones que tomen los Estados miembros en procesos domésticos de autenticación –normalmente en el ámbito de la administración electrónica, aunque no de forma exclusiva–, por lo que esta posibilidad dependerá de lo que establezca al respecto el derecho nacional[249]; pero lo que sí es seguro es que un Estado podrá notificar el uso de certificados de firma o sello electrónico como sistema de identificación a efectos transfronterizos[250], en cuyo caso desde luego la respuesta será, desde luego, afirmativa.

A la vista de esta posibilidad, ciertamente parecería extraño que no se pudiera emplear un certificado cualificado de firma electrónica cualificada para cualquier otro proceso donde se requiera una identificación y autenticación electrónica, en su caso con base en la autonomía de la voluntad de las partes, sin perjuicio de la existencia de las excepciones legales que se encuentren debidamente justificadas[251].

Por otra parte, el Reglamento eIDAS no regula el uso de certificados electrónicos que no se puedan, al menos, emplear para validar firmas o sellos electrónicos, por lo que un certificado que se expida únicamente para identificarse –pero no para la creación de la firma o el sello electrónico– quedaría fuera de la regulación armonizada, pudiendo ser, como ya sabemos, objeto de regulación en sede nacional, o funcionar simplemente en base a la autonomía de la voluntad de las partes, como sucede con otros sistemas de identificación electrónica.

Un ejemplo de servicio de confianza de expedición de certificados empleado exclusivamente para la identificación electrónica lo encontramos en la normativa italiana, sin cualificación conforme al Reglamento eIDAS, pero con reconocimiento como tal servicio de confianza en sede nacional, y publicidad en la lista de confianza italiana. Se trata del certificado de autenticación (de entidad) que incorpora la tarjeta nacional de servicios (*Carta Nazionale dei Servizi*)[252], un documento emitido por las

---

[249] En relación con la normativa española a este respecto, cfr. los epígrafes 2.2.2 y 2.2.3 de este trabajo. Podemos avanzar que la respuesta es, en este caso, afirmativa.

[250] Sobre esta posibilidad, cfr. el epígrafe 3.1 de este trabajo.

[251] Ciertamente, resulta difícil pensar en alguna, dado el efecto jurídico del certificado cualificado de firma electrónica cualificada. Más fácil es pensar en restricciones en cuya virtud no se pueda realizar una identificación electrónica (a distancia), debiéndose realizar una identificación personal.

[252] Regulada por *Decreto del Presidente della Repubblica 2 marzo 2004, n. 117, Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3*; su definición legal actual se contiene en el artículo 1.1.d) del *Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (CAD)*, y el artículo 64.2-novies, incorporado por artículo 50.1.e) del Decreto Legislativo 26 agosto 2016, n. 179, autoriza el acceso mediante esta tarjeta a los servicios ofrecidos telemáticamente por las Administraciones Públicas, en pie de igualdad con la *carta d'identita' elettronica* y el novedoso sistema SPID. Anteriormente, pero esta posibilidad existía ya en la

Administraciones Públicas en soporte informático destinado a permitir el acceso telemático a los servicios prestados por las mismas –incluyendo la presentación de solicitudes y escritos[253]– con la particularidad de que dicho certificado es expedido por prestadores de servicios de confianza cualificados para la expedición de certificados electrónicos (públicos o privados), que ofrecen el servicio al ciudadano por cuenta de la Administración emisora de la tarjeta.

Es también común, en Estados donde no se ha regulado un servicio de confianza específico para la identificación, como hemos visto sucede en Italia, encontrar prestadores que expiden, a un mismo sujeto, certificados con clave segregadas por uso, de modo que entregan un certificado cualificado de firma o sello electrónico, y un certificado no cualificado de identificación electrónica. La principal diferencia con el caso italiano será, posiblemente, que dicho Estado no informará del servicio en su lista de confianza.

2.1.2 Los requisitos del servicio

Los servicios de confianza correspondientes a la expedición de certificados (de firma electrónica, de sello electrónico y de autenticación de sitio web) deben cumplir los requisitos establecidos en el Reglamento eIDAS y, en su caso, en la legislación nacional, en especial los correspondientes a la modalidad cualificada del servicio.

Los servicios de confianza de expedición de certificados (exclusivamente de identificación), al encontrarse fuera del ámbito de aplicación del Reglamento eIDAS, quedarán sólo sujetos a la normativa nacional, pudiéndose incluso regular completamente en base a acuerdos de derecho privado, y sin perjuicio de que dicha normativa pueda imponer la aplicación de las normas generales aplicables a los servicios de confianza, o incluso las normas específicas del servicio cualificado de expedición de certificados, como hemos visto que sucede en Italia, por ejemplo, y de forma fáctica también en España[254].

Los prestadores que ofrezcan este servicio deben cumplir, de una parte, las obligaciones generales que se imponen a todos los prestadores de servicios de confianza[255]; de otra, las obligaciones exigibles a los prestadores cualificados de servicios de confianza[256]; y, finalmente, las obligaciones correspondientes a los requisitos específicos del servicio.

Antes de entrar en el análisis de los principales requisitos específicos de este servicio[257],

---

redacción original del artículo 64. Por su parte, el artículo 66.2 del CAD remite a reglamento los aspectos relativos a las características y procesos asociados a dicha tarjeta, destacando que la misma puede servir como medio de autenticación para la realización de pago frente a sujetos públicos y privados. Cfr. también el *Decreto del Presidente del Consiglio dei Ministri 24 maggio 2010, Regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al D.P.R. n. 851 del 1967 rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 88, del decreto legislativo n. 82 del 2005*.

[253] Cfr. el artículo 65.1.b) del *CAD*, que ya previó esta posibilidad en su redacción inicial. En su redacción actual, se refiere también al SPID.

[254] Al menos, en el caso ya expuesto de la emisión de una pareja de certificados (firma + identificación) para un mismo sujeto.

[255] Cfr. el epígrafe 6.1 de este trabajo.

[256] Cfr. el epígrafe 6.2 de este trabajo.

[257] No es objeto de este trabajo realizar un análisis profundo de los requisitos del servicio de expedición de

conviene señalar la previsión legal contenida en los artículos 28.6, 38.6 y 45.2 del Reglamento eIDAS, en relación, respectivamente, con los certificados cualificados de firma electrónica, de sello electrónico y de autenticación de sitio web, y en cuya virtud, "la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados […]", de modo que "[s]e presumirá el cumplimiento de los requisitos establecidos […] cuando un certificado cualificado […] se ajuste a dichas normas", actos de ejecución que "se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2", como hemos ya presentado anteriormente[258].

Existen diversas normas técnicas candidatas a ser establecidas a estos efectos, pero de momento la Comisión no ha ejercido su competencia, algo que resulta algo sorprendente, dado el esfuerzo y coste dedicado a su desarrollo, bajo impulso por mandato de la propia Comisión –en especial, en virtud del importante mandato M/460–, durante los últimos dieciocho años[259]; así como su prestigio internacional, manifestado en su adopción generalizada fuera de la Unión Europea.

Resultado de estos esfuerzos son las normas técnicas ETSI EN 319 411, partes 1 y 2[260], relativa a los requisitos de procedimiento y de seguridad para la expedición de certificados, y EN 319 412, partes 1 a 5[261], que se dedica a los perfiles (o plantillas) de certificados.

Estas normas, junto a las de sistemas fiables[262] y a las de dispositivos de firma o sello[263], contienen los criterios que, incluso sin aprobación por la Comisión, se utilizan para la prestación del servicio, y que se emplean también para la evaluación de la conformidad

---

certificados, por no resultar necesario para el objeto del mismo, máxime dada la existencia de trabajos muy completos al respecto, como (Martínez Nadal, 1998) o (Martínez Nadal, 2009).

[258] Cfr. el epígrafe 1.4.2 de este trabajo.

[259] En efecto, ya en el año 1999 se pone en funcionamiento la *European Electronic Signature Standardization Initiative (EESSI)*, con un comité de dirección formado por prestadores de servicios de certificación, responsables de los organismos de normalización, funcionarios de la Comisión y otras partes interesadas, con el encargo de abordar la normalización necesaria para la correcta implementación de la DFE.

[260] En concreto, las versiones actualmente vigentes son ETSI EN 319 411-1 V1.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, y ETSI EN 319 411-2 V2.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

[261] En concreto, las versiones actualmente vigentes son ETSI EN 319 412-1 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures; ETSI EN 319 412-2 V2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; ETSI EN 319 412-3 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons; ETSI EN 319 412-4 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates; y ETSI EN 319 412-5 V2.2.1 (2017-11). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[262] Cfr. el epígrafe 6.2.5 de este trabajo.

[263] Cfr. el epígrafe 4.1.2 de este trabajo.

requerida legalmente, por lo que suplen en gran medida la necesidad de un desarrollo legal nacional específico, a pesar de lo cual las normas nacionales vendrán en concretar determinados aspectos del Reglamento eIDAS, como sucede, en España, en el caso del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

2.1.2.1 Los contenidos del certificado cualificado

Los certificados deben, al objeto de cumplir con su función de identificación, contener unas informaciones mínimas, que, en el caso del certificado cualificado, se encuentran legalmente determinadas, aunque la mayoría de ellas también deberán aparecer en los certificados sin cualificación.

El Reglamento eIDAS dedica a esta cuestión, de un lado, sus artículos 28.1[264] y 38.1, que refiere a los Anexos I y III, respectivamente en relación con los certificados de firma y de sello electrónico; y, de otro, su artículo 45.1, que refiere al Anexo IV, en relación a los certificados de autenticación de sitio web.

En los tres tipos de certificados se prevén algunas informaciones comunes[265], incluyendo las siguientes:

- Una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado (de firma[266], de sello o de autenticación de sitio web)[267], al objeto del necesario conocimiento que debe tener la parte usuaria de esta condición, a la que se asocian las garantías legales correspondientes.
- Los datos de identidad del prestador que expide el certificado[268], incluyendo su Estado de establecimiento[269].
- Los datos de identidad de la persona a la que se expide el certificado[270]; esto es, el nombre de la persona física o un seudónimo[271], o de la persona jurídica y, cuando proceda, el número de registro, tal como se recojan en los registros

[264] El artículo 28.1 del Reglamento eIDAS ha desplazado la aplicación de la LFE, que regulaba los contenidos mínimos del certificado de firma electrónica (de persona física y de persona jurídica) en su artículo 11.2. Sobre los contenidos de los certificados de firma electrónica en la LFE, cfr. (Martínez Nadal, 2009, págs. 210-227).

[265] La norma ETSI EN 319 412, partes 1 a 5, concreta estas cuestiones en el plano técnico de los certificados X.509.

[266] En sentido similar, cfr. el artículo 11.2.a) de la LFE y el numeral a) del Anexo I de la DFE.

[267] Cfr. los epígrafes 4.2.1 y 4.2.3 de la norma ETSI EN 319 412-5.

[268] En sentido similar, cfr. el artículo 11.2.c) de la LFE y el numeral b) del Anexo I de la DFE.

[269] Cfr. el epígrafe 4.2.3 de la norma ETSI EN 319 412-2, aplicable a los tres tipos de certificados.

[270] El artículo 11.2.e) de la LFE preveía que el certificado debía contener "[l]a identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal", ampliando lo previsto en el numeral c) del Anexo I de la DFE.

[271] Sobre el régimen de uso de seudónimos, que sólo aplica a certificados de firma electrónica, cfr. el epígrafe 6.1.1 de este trabajo.

oficiales[272].

Sólo en el caso del certificado de autenticación de sitio web, los datos de identidad se completan con elementos –atributos informativos, más correctamente– de la dirección física, incluida al menos la ciudad y el Estado, de la persona física o jurídica a quien se expida el certificado, y, cuando proceda, según figure en los registros oficiales; así como el nombre o los nombres de dominio, la dirección electrónica, explotados por la persona física o jurídica a la que se expida el certificado[273].

- Los datos de validación de la firma o sello electrónico[274], o, aunque el Reglamento no lo explicite, la clave pública del sitio web, que son precisos para la ejecución de las operaciones técnicas que sustentan la prueba electrónica correspondiente[275].
- Los datos relativos al inicio y final del período de validez del certificado[276], delimitando las fechas en que se pueden crear firmas o sellos –aunque la validación de las mismas podrá realizarse también transcurrido dicho periodo[277]–, o confiar en autenticaciones del sitio web; periodo que deberá establecerse conforme a lo que disponga el legislador nacional y, en todo caso, conforme a las normas criptográficas correspondientes[278].

  A este respecto, es preciso indicar que el artículo 4 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza establece, en su epígrafe 1, que "[l]os certificados electrónicos se extinguen por caducidad a la expiración de su período de vigencia"[279], para ordenar, en su epígrafe 2, que "[e]l período de vigencia de los certificados cualificados no será superior a 5 años", un máximo legal que no podrá ser superado pero que "se fijará en atención a las características y tecnología empleada para generar los datos de creación de firma o sello, o de autenticación de sitio web", en línea con la legislación anterior[280], remitiendo de nuevo a lo que establezca la normativa en materia de criptografía.

---

[272] Cfr. el epígrafe 4.2.4 de la norma ETSI EN 319 412-2, el epígrafe 4.2.1 de la norma ETSI EN 319 412-3 y el epígrafe 4.1 de la norma ETSI EN 319 412-4, que remite directamente a las normas del CA/Browser Forum.

[273] Cfr. el epígrafe 4.1 de la norma ETSI EN 319 412-4.

[274] Cfr. el artículo 11.e.f) de la LFE y el numeral e) del Anexo I de la DFE.

[275] Cfr. el epígrafe 4.2.5 de la norma ETSI EN 319 412-2, aplicable a los tres tipos de certificados.

[276] Cfr. el artículo 11.2.g) de la LFE y el numeral f) del Anexo I de la DFE.

[277] Sobre la revocación de los certificados, cfr. el epígrafe 2.1.2.3 de este trabajo. Sobre la validación de la firma o sello, cfr. el epígrafe 4.3.2 de este trabajo.

[278] Cfr. el epígrafe 6.2.6 de este trabajo.

[279] Cfr. el artículo 8.1.a) de la LFE, que se refiere a la expiración del período de validez que figura en el certificado con causa de extinción de la vigencia del certificado, sin emplear el término "caducidad".

[280] Cfr. el artículo 8.2 de la LFE, que estableció inicialmente el plazo de cuatro años, ampliado a cinco años por disposición adicional sexta de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Sobre esta cuestión en la LFE, cfr. (Martínez Nadal, 2009, págs. 166-172).

- El código de identidad del certificado[281], que debe ser único para el prestador cualificado de servicios de confianza, a los efectos de identificarlo unívocamente y diferenciarlo de cualquier otro certificado expedido por el mismo prestador.
- La firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor[282], a los efectos de que la misma proteja y autentique el certificado, y permita a la parte usuaria confiar en que sus contenidos no han sido modificados.
- El lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que nos acabamos de referir; esto es, la dirección de Internet en la que se puede recuperar el certificado expedido por la autoridad de certificación que, como vimos en la parte técnica, avala dicha firma o sello[283]. Se trata de una novedad importante del Reglamento eIDAS en relación con la DFE y la LFE, que se explica por la necesidad de que la parte usuaria tiene de acceder de forma efectiva a este certificado, a los efectos de poder verificar la correspondiente prueba electrónica.
- La localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado[284], de forma que la parte usuaria pueda determinar si puede confiar en las informaciones contenidas en el certificado. De nuevo, se trata de una importante novedad de Reglamento eIDAS respecto a la normativa anterior, que denota su importancia.
- Finalmente, aunque sólo en el caso de los certificados de firma o sello, cuando los datos de creación relacionados con los datos de validación se encuentren en un dispositivo cualificado de creación, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático[285]; lo cual permite diferenciar un certificado cualificado de firma o sello cualificado –que incorpora esta indicación–, de un certificado de firma o sello avanzado, que no la incorpora. También es innovación del Reglamento eIDAS.

Es interesante hacer notar que en el Reglamento eIDAS ya no se incluya, entre los contenidos de los certificados, los relativos a los límites relativos a su uso, sean los mismos materiales o relativos a la cuantía, que sí se encontraban contemplados, con carácter opcional, en la DFE y la LFE, seguramente por los problemas de interoperabilidad, en especial semántica y jurídica, que los mismos han generado[286].

El Reglamento eIDAS ordena taxativamente, en su artículo 28.2, que "[l]os certificados

---

[281] En el mismo sentido, cfr. el artículo 11.2.b) de la LFE y el numeral g) del Anexo I de la DFE.

[282] Cfr. el artículo 11.2.d) de la LFE, y el numeral h) del Anexo I de la DFE, que sólo se refería a la firma electrónica avanzada del prestador, dado que los sellos electrónicos no existían en dichas normas.

[283] Cfr. el Anexo A.2.3 de este trabajo.

[284] Cfr. los epígrafes 4.3.11 y 4.4.1 de la norma ETSI EN 319 412-2, aplicable a los tres tipos de certificados, y las normas del CA/Browser Forum.

[285] Cfr. el epígrafe 4.2.2 de la norma ETSI EN 319 412-5.

[286] Pero no sintáctica, porque las normas técnicas europeas establecieron desde un momento muy cercano a la aprobación de la DFE una sintaxis uniforme para estos campos, que hoy se contiene en la norma ETSI EN 319 412-5.

cualificados de firma electrónica no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo I", y de la misma forma hace con los certificados cualificados de sello electrónico, en el artículo 38.2, prohibición que no existe en el caso de los certificados de autenticación de sitio web, y que posiblemente responde a la necesidad de corregir la práctica de los Estados miembros de exigir contenidos concretos a los certificados, con independencia del lugar de expedición de los mismos, lo que había tenido el efecto de impedir su uso en operaciones transfronterizas.

En España, por ejemplo, la Orden HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria[287], establecía detalladas normas sobre el contenido del certificado, lo cual impedía que los certificados reconocidos expedidos en los restantes Estados miembros fueran admisibles para las relaciones tributarias[288].

Esta prohibición se justifica en el Considerando (54) del Reglamento eIDAS, que indica que "[l]a interoperabilidad y el reconocimiento transfronterizos de los certificados cualificados es un requisito previo para el reconocimiento transfronterizo de las firmas electrónicas cualificadas", por lo que "los certificados cualificados no deben estar sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el presente Reglamento", pero estableciendo, como excepción, que "no obstante, en el plano nacional debe permitirse la inclusión de atributos específicos, por ejemplo identificadores únicos, en los certificados cualificados, a condición de que tales atributos específicos no comprometan la interoperabilidad y el reconocimiento transfronterizos de los certificados y las firmas electrónicas cualificados".

Además, conforme a los artículos 28.3 y 38.3 del Reglamento eIDAS, respectivamente en relación con los certificados cualificados de firma y sello electrónico, se establece que "[l]os certificados cualificados […] podrán incluir atributos específicos adicionales no obligatorios", los cuales tampoco "afectarán a la interoperabilidad y el reconocimiento de las firmas electrónicas cualificadas".

La regla general, por tanto, relativa a la prohibición de que los Estados miembros establezcan exigencias adicionales a los certificados cualificados se excepciona para permitir la imposición, por la normativa nacional, de atributos específicos obligatorios; y además se autoriza la posibilidad de inclusión voluntaria de otros atributos.

Nótese que esta regulación va a permitir que una normativa nacional[289] pueda establecer prácticamente cualquier atributo adicional que se considere necesario en el marco de la

---

[287] Hoy derogada por Orden HAP/800/2014, de 9 de mayo, por la que se establecen normas específicas sobre sistemas de identificación y autenticación por medios electrónicos con la Agencia Estatal de Administración Tributaria.

[288] En concreto, la obligación de incluir dentro del certificado el Número de Identificación Fiscal implicaba que una empresa alemana, por ejemplo, debiera intentar obtener un certificado expedido en Alemania que contuviese en su interior el NIF español, algo evidentemente imposible.

[289] Por citar un ejemplo, la sección § 12 (1) de la Ley alemana de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017, prevé atributos relativos al poder de representación, relativos a datos oficinales, profesionales o de otro tipo relativos a la identidad del solicitante, y otras informaciones personales, en una dicción francamente amplia.

prestación de los servicios de confianza, pero siempre con el límite de que no se afecte a la citada interoperabilidad y reconocimiento mutuo. Este límite implica que no se dicten normas nacionales que menoscaben los contenidos armonizados –aunque podrán detallarlos más, en especial en el marco de las normas técnicas que garantizan dicha interoperabilidad– y que los contenidos adicionales no impidan a partes usuarias establecidas en otros Estados miembros el uso del certificado cualificado en base a los contenidos armonizados, ignorando los atributos adicionales[290].

En este modelo se podrán dar al menos tres situaciones diferenciadas. En primer lugar, un Estado miembro podrá obligar a los prestadores incorporar atributos adicionales obligatorios en relación con los tipos de certificados definidos en el Reglamento eIDAS –certificado de firma electrónica de persona física, certificado de sello electrónico de persona jurídica o certificado de autenticación de sitio web–, de modo que el prestador que incumpla no podrá expedir dichos certificados en ningún caso. Éste sería el caso de la obligación de incluir, por ejemplo, un identificador nacional de la persona física o jurídica en el certificado correspondiente. En segundo lugar, un Estado miembro podrá regular atributos voluntarios, que podrán o no aparecer en el certificado, pero estableciendo las reglas aplicables a los mismos cuando el prestador decida su empleo, incluyendo su sintaxis y semántica; así sucedería, por ejemplo, cuando nos referimos a la inclusión de un poder de representación dentro del certificado –en cuya virtud normalmente hablaremos de un subtipo de certificado, denominado "certificado de representante", por ejemplo–. Finalmente, cabe imaginar que los prestadores o sus colectivos de clientes definirán, en algunos casos, atributos adicionales voluntarios que puedan resultar útiles en diferentes ámbitos de actuación electrónica, sin necesidad de intervención del Estado miembro.

Por lo que respecta a España, y con carácter general para todos los tres tipos de certificados cualificados, el artículo 6.1 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza prevé, en línea con lo que anteriormente se establecía en la LFE, la obligación de incluir, en los certificados cualificados expedidos a dicha persona, el número de documento nacional de identidad –que podrá sustituirse por otro código o número identificativo cuando el firmante carezca de él, siempre que le identifique unívocamente–, y el número de identificación fiscal de la persona jurídica –que también podrá sustituirse por otro código identificativo que le identifique unívocamente, si dicha persona jurídica lo tuviera–.

Asimismo, el apartado 2 del mismo artículo 6 prevé la posibilidad de incluir el atributo de la representación de persona física o jurídica, que deberá considerar la "indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria, la inscripción de los datos registrales", una norma que resulta criticable dada la existencia de apoderamientos sustentados en documento privado, de amplio uso en determinados

[290] Esto se logra, desde una perspectiva técnica, marcando cualquier "extensión" del certificado; esto es, la información adicional para el uso del certificado, como "no crítica", lo que indica que el certificado se puede emplear incluso aunque dicha información no sea procesada. En otras ocasiones, los atributos se incluyen como componentes del nombre de la persona a la que se expide el certificado, por lo que dichos componentes pueden ser simplemente ignorados por el destinatario sin afectar al correcto funcionamiento del certificado.

entornos relacionales que no exigen tantas garantías[291], y que tampoco resuelve los problemas ya identificados por la práctica y la doctrina con ocasión de la LFE; a saber, la ausencia de sincronía entre los datos del certificado y del registro público[292], cuando el mismo exista; y la ausencia de normalización técnica de este atributo, que se traduce en problemas de interoperabilidad[293], a salvo de lo dispuesto sectorialmente para las relaciones con las entidades del sector público[294].

Asimismo, el artículo 7.5 del citado Anteproyecto de Ley autoriza indirectamente que el "certificado cualificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación", atributos también opcionales.

En todo caso, cualquier atributo –obligatorio o voluntario– que no haya sido objeto de armonización puede ser ignorado por la parte usuaria. Por ejemplo, en el caso de un certificado cualificado que incorpore el poder de representación del firmante, una parte usuaria podría adecuar su proceso de autenticación o de firma para hacer uso de dicha información, mientras que otra parte usuaria podría tratar el certificado como si el mismo no contuviera esta información. En ese ejemplo, para la primera parte usuaria el certificado es de persona física representante, y confía en el poder, y para la segunda parte usuaria el certificado es sólo de persona física, e ignora el poder.

Este régimen hace pensar que los atributos establecidos por la normativa nacional van a tener un reconocimiento limitado y preferentemente doméstico, debido a la falta de armonización de todos estos atributos en el nivel de la Unión Europea. Pero ello no significa que no puedan ser instrumentos útiles, como veremos sucede en el caso de los atributos extra previstos para las relaciones jurídico-administrativas.

Sin perjuicio de lo que se acaba de decir, y aunque el Reglamento no lo mencione, nada impide la aparición, en el nivel de la Unión Europea, de normativas que definan atributos que se impongan de forma obligatoria a determinadas personas, dado que el régimen contenida en los artículos 28.2 y 38.2 no afecta a las instituciones de la Unión, que lógicamente deberán actuar dentro de su ámbito de competencias.

Precisamente esto es lo que ha propuesto la Autoridad Bancaria Europea en relación con los prestadores de servicios de pago, en su proyecto de norma técnica de regulación, conforme a lo previsto en el artículo 98 de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE (en adelante, DSP2), a los efectos de establecer, entre otros, los requisitos para unos estándares de

---

[291] Como, por ejemplo, el procedimiento administrativo común, como se desprende de los artículos 5 y 6 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC).

[292] Cfr. (Martínez Nadal, 2009, pág. 221 y ss.).

[293] Dado que cada prestador de servicios de confianza que expide certificados define la sintaxis y la semántica de esta extensión, el coste de usar esta información de forma automatizada es tan elevado que en la práctica privada no se emplea.

[294] En estas relaciones se ha normalizado esta extensión, en virtud de lo establecido en el RDENI y su norma técnica de desarrollo.

comunicación abiertos comunes y seguros a efectos de identificación, autenticación, notificación e información, así como para la aplicación de medidas de seguridad entre los diferentes prestadores de servicios de pago.

El Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros[295] que adopta la norma técnica de regulación, aunque con diversas modificaciones, y que resulta de cumplimiento obligatorio para los prestadores, establece en su artículo 34.2 la obligación de los prestadores de servicios de pago de emplear, para su identificación, certificados cualificados de sello electrónico o de autenticación de sitio web –concretando que el número de registro que se debe contener en el certificado será el número de autorización del prestador, disponible en el registro público previsto en el artículo 14 de la DSP2– y, en lo que ahora nos interesa, dos atributos obligatorios[296], a los efectos de incorporar al certificado el rol del prestador de servicio de pago y la denominación de la autoridad competente para su supervisión (apartado 3 del artículo 34), atributos que, dice el apartado 4 del artículo 34, no podrán afectar a la interoperabilidad y el reconocimiento de estos certificados.

El primer atributo se orienta a la posibilidad de que se pueda determinar el rol en que actúa, en una comunicación segura, cada prestador de servicios de pago, mientras que el segundo, claramente, se dirige a la identificación del correspondiente supervisor, a los efectos oportunos, como la presentación de denuncias.

2.1.2.2 La verificación de la identidad de la persona identificada en el certificado y, en su caso, del solicitante del certificado

La verificación de la identidad de la persona a la que se expedirá el certificado y, por tanto, identificará en el certificado, es uno de los requisitos más importantes a considerar, que ya se manifestaba en la normativa anterior[297].

El Reglamento eIDAS contiene un novedoso régimen, en relación con la normativa anterior, en especial a la española, relativo a la verificación de la identidad de la persona a la que se expide certificados cualificados, que conviene reseñar.

En concreto, el artículo 24.1 del Reglamento eIDAS ordena, de forma genérica, que "al expedir un certificado cualificado para un servicio de confianza, un prestador cualificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el

[295] Conforme a lo establecido en el artículo 98.4 de la DSP2, la competencia para la adopción de estas normas técnicas de regulación corresponde a la Comisión, a partir del proyecto de la Autoridad Bancaria Europea, potestad que se deberá ejercer de conformidad con los artículos 10 a 14 del Reglamento (UE) Nº 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión Nº 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión.

[296] Ambos atributos han sido ya objeto normalización técnica en el Instituto Europeo de Normas de Telecomunicaciones, mediante la especificación técnica ETSI TS 119 495.

[297] (Martínez Nadal, 2009, pág. 231) recuerda que "la función central del certificado es vincular un dato de verificación de firma (una clave pública, en el caso de criptografía asimétrica) a una persona determinada", por lo que "es esencial la comprobación de la identidad del titular de tal elemento por parte del prestador de servicios de certificación".

Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado cualificado", obligación esencial dada la finalidad esencialmente identificativa del certificado, y cuya concreción se remite a lo que se establezca en el nivel nacional.

A pesar de ello, y seguramente para evitar excesivas diferencias en las exigencias relativas a esta actuación del prestador, que inevitablemente se traducirían en barreras al reconocimiento transfronterizo de los certificados cualificados y, por conexión, de las firmas o sellos respaldados por los mismos, y en un menor nivel de confianza en los sitios web, el mismo artículo dispone inmediatamente que "[l]a información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien por medio de un tercero de conformidad con el Derecho nacional" mediante alguna de las cuatro posibilidades que ofrece, y que constituyen una significativa novedad con respecto a la DFE[298].

Se trata de posibilidades que recogen, a buen seguro, prácticas que se han ido generando en las diferentes leyes nacionales, y que ahora se recogen para toda la Unión, pero no de forma plenamente armonizada, dada la remisión que en alguno de los casos se realiza a la normativa nacional correspondiente.

En primer lugar, conforme al numeral a) del artículo 24.1 del Reglamento eIDAS, la verificación se podrá realizar "en presencia de la persona física o de un representante autorizado de la persona jurídica", posibilidad que ya se encontraba prevista en la LFE, en el artículo 12.a) y 13.1, con carácter previo a la expedición del certificado[299], el cual indicaba que "[l]a identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho", norma que se mantiene idéntica en el artículo 7.1 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

Se trata de la regla que en las normas técnicas se ha venido denominando "presencia física directa", que supone una barrera bastante clara a la extensión de la prestación de servicios desde un Estado miembro a potenciales clientes en toda la Unión, claramente derivada del coste de crear una red europea de oficinas propias o de colaboradores para esta tarea de verificación de la identidad. Por este motivo, en las normas técnicas se promovió el

---

[298] Como ha indicado (Martínez Nadal, 2009, pág. 249), en la DFE no se exigía la personación física del solicitante, lo que permitía sostener la posibilidad de uso de servicios en línea de verificación de la identidad. La misma autora explica que de los "[…] distintos sistemas de verificación (personación física ante la autoridad de certificación o una autoridad de registro local delegada, envío de documentos acreditativos, suministro de información 'on-line') […] el único que ofrece seguridad (y no absoluta, pues aun así podrán darse supuestos de suplantación de personalidad no detectados y ni siquiera detectables por un proveedor diligente) es el de presencia física", posibilidad a la que "se refería expresamente la versión inicial del borrador no oficial de la propuesta de directiva […] y fue suprimida ya en la versión oficial […], no sabemos si en un intento de flexibilizar este requisito y adaptarse a las prácticas comerciales, que han generado unos sedicentes certificados en los que no existe verificación fiable de la identidad alguna, por lo que no cumplen su función ni son realmente tales certificados" (Martínez Nadal, 2009, pág. 137); crítica que desde luego no ha sido acogida en el Reglamento eIDAS, sino más bien al contrario.

[299] La dicción del artículo 24.1.a) del Reglamento eIDAS es ligeramente diferente a la de la LFE, que debe entenderse desplazada en este punto, al indicar que esta verificación se hará "al expedir", no antes de expedir, resultando más flexible por referirse a cualquier momento durante el procedimiento de expedición del certificado.

concepto de la "presencia física indirecta", a partir de lo establecido en algunas normativas nacionales[300], proceso que parece haber cristalizado en las restantes posibilidades previstas en el artículo 24.1 del Reglamento eIDAS, que veremos a continuación.

En efecto, la segunda posibilidad prevista en el numeral b) del artículo 24.1 es realizar dicha verificación "a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado cualificado, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto»", medios a los que nos referimos posteriormente[301], posibilidad que excluye el uso de estos medios de identificación cuando se hayan expedido sin la presencia personal de las citadas personas.

Se trata de un caso específico de uso de un medio de identificación para un uso privado, por previsión expresa del Reglamento eIDAS, que puede facilitar el desarrollo de la actividad de expedición de certificados en el Mercado Único Digital, al eliminar la necesidad de la presencia personal y autorizar al prestador a confiar en un subconjunto de los citados medios de identificación. Un ejemplo de esta posibilidad –seguramente el más relevante, y actualmente implementado por diversos prestadores españoles– es el uso del DNI electrónico o equivalente de otros Estados miembros, como la nPA alemana, que permitiría a un nacional alemán adquirir un certificado expedido en España, de convenirle, sin tener que desplazarse.

En tercer lugar, el numeral c) del mismo artículo 24.1 autoriza que la verificación se realice "por medio de un certificado de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con la letra a) o b)", en una norma que tiene una lógica similar a la del empleo de los medios de identificación electrónica anteriormente presentada, y que ya se encontraba, en cierto modo, prevista en el artículo 13.4.b) de la LFE, el cual permitía sustituir la presencia personal "[c]uando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años", norma que no se ha mantenido en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza[302].

Al contrario, el artículo 7.7 del Anteproyecto indica que "un certificado cualificado expedido de acuerdo con el artículo 24.1 c) del Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, no podrá ser utilizado para la obtención de un nuevo certificado cualificado", prohibición taxativa que podría considerarse contraria al Reglamento eIDAS, que armoniza este aspecto sin establecer

---

[300] En España, el artículo 13.4 de la LFE recogió esta tendencia, mientras que en otras normas nacionales sencillamente no se privilegió, como en España, la personación del solicitante.

[301] Sobre la definición de qué sean los medios de identificación electrónica, cfr. el epígrafe 1.2.1 de este trabajo; sobre los niveles de seguridad de estos medios, cfr. el epígrafe 3.1.3 de este trabajo.

[302] No deja de ser una lástima que se haya perdido esta posibilidad, menos rigorista que la previsión del artículo 24.1.c) del Reglamento eIDAS. El artículo 13.4.b) de la LFE permitía el uso del certificado para la identificación o para la firma electrónica avanzada, de forma alternativa o complementaria, mientras que el Reglamento eIDAS eleva la exigencia de forma muy significativa.

limitación alguna al respecto.

No quiere ello decir que el organismo de supervisión no pueda establecer pautas al respecto, dado que el riesgo de reutilizar una identificación para expedir una cadena de certificados aumenta con el tiempo[303], que ciertamente obligarán al prestador a justificar que se puede emplear dicho certificado, aunque haya transcurrido mucho tiempo desde la identificación inicial, pero cerrar legalmente esa posibilidad podría efectivamente infringir la normativa europea; aunque no es menos cierto que, en ausencia de la adopción de normas técnicas que presuman el cumplimiento del Reglamento, el legislador nacional tiene un amplísimo margen de actuación.

También en relación con esta posibilidad, implementada por diversos prestadores españoles, especialmente al objeto de reutilizar la identificación contenida en el certificado de firma electrónica de DNI-e, el borrador de Anteproyecto prevé la importante novedad de prever la inclusión, en el certificado, de información acerca de la forma en que se procedió a identificar a la persona física solicitante del certificado –a la fecha de expedición del certificado–, lo cual sin duda ayudará al cumplimiento de esta obligación. Alternativamente, la norma prevé el establecimiento de mecanismos de colaboración entre los prestadores al objeto de determinar el momento en que se produjo la última personación o medio equivalente a la misma.

El problema de esta propuesta normativa es, claramente, que no vincula ni puede exigirse a los prestadores no sujetos a la ley española, afectando negativamente a la competitividad en la prestación transfronteriza de servicios, muestra de la inconveniencia de establecer determinadas normas en el ámbito armonizado. En efecto, un prestador italiano no tendrá obligación de colaborar con un prestador español, por lo que éste último no podrá obtener esta información.

Finalmente, la cuarta posibilidad, y la más innovadora legalmente[304] –aunque no desde la perspectiva de las normas técnicas– se encuentra recogida en el numeral d) del artículo 24.1, conforme al cual la verificación se podrá realizar "utilizando otros métodos de identificación reconocidos a escala nacional que aporten una seguridad equivalente en términos de fiabilidad a la presencia física", seguridad equivalente que deberá ser "confirmada por un organismo de evaluación de la conformidad".

Se trata de una cláusula abierta, que permite introducir opciones alternativas, facilitando la adopción de innovaciones tecnológicas o de proceso, con la triple condición de que a) sean admitidos en el nivel nacional, b) que resulten equivalentes en fiabilidad, lo que se determina en atención a su seguridad, y c) que dicha seguridad haya sido objeto de la correspondiente evaluación[305].

La noción de reconocimiento a escala nacional implica, en algunos casos, la aparición de normativa específica al respecto, aunque no parece ser una exigencia impuesta por el Reglamento eIDAS, previsión que en algunos casos contiene una remisión a lo que se

---

[303] Dado que no se requiere la presencia personal, se incrementa el riesgo de una suplantación de identidad por parte de una persona que haya tenido acceso a la clave privada, quizá incluso con la autorización de su titular inicial.

[304] En los Estados miembros que adoptaron la regla general de la personación física, como España, pero no en los restantes.

[305] Sobre este procedimiento, cfr. el epígrafe 7.1.1 de este trabajo.

determine reglamentariamente, como sucede en Alemania[306], por ejemplo, y se ha propuesto en España[307], caso este último que sigue un enfoque exclusivamente reglamentista quizá basado en un exceso de prudencia.

Otros Estados, en cambio, tratan esta cuestión desde la perspectiva del *soft law* público, como uno de los criterios propuestos por el organismo de supervisión en relación con el procedimiento de cualificación, un enfoque mucho más flexible, plenamente alineado con el requerimiento previsto en el artículo 24.1.d) del Reglamento eIDAS de evaluación de conformidad en relación con el nivel de seguridad equivalente a la presencia física, que impulsa la adopción rápida de innovaciones, algo beneficioso para la competitividad de los prestadores establecidos en dichos Estados, como por ejemplo en el caso de Austria[308], de Francia[309] o de Italia[310].

Entre dichas innovaciones destaca, con gran fuerza, el uso de la identificación a través de la videoconferencia con la persona física, opción ya autorizada en Italia o Francia; o la posibilidad de reutilizar la identificación ya realizada por entidades sujetas a los procedimientos de verificación de la identidad previstos en la normativa de prevención del blanqueo de capitales, como en Italia o Austria.

Cabe, finalmente, preguntarse si resulta posible establecer, en sede nacional, exenciones a la personación que sean diferentes a los cuatro casos anteriores, como por ejemplo sucede en Derecho español con la previsión, ya contenida en el artículo 13.1 de la LFE[311],

---

[306] Cfr. la sección § 11 (1) de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017), pero con la posibilidad de obtener un reconocimiento provisional de métodos innovadores no regulados, en los términos dispuestos por el apartado (3) de la misma sección.

[307] En efecto, el artículo 7.2 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza prevé que "[p]or Resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital se podrán determinar las condiciones y requisitos aplicables a la verificación de la identidad y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado mediante otros medios de identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física".

[308] Cfr. la sección § 8 de la Ley Federal sobre Firmas Electrónicas y Servicios de Confianza para Transacciones Electrónicas – *Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)*, promulgada por artículo 1 de la Ley Federal de 8 de julio de 2016.

[309] Cfr. el artículo 6 del *Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique*, que no exige la personación física, y el *Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation* – dictado conforme a la previsión contenida en el artículo 7 del citado Decreto – que incorpora los criterios de la normativa técnica europea relativa a la prestación de servicios de certificación (ETSI TS 101 456 – referenciada como norma nacional AFNOR AC Z74-400 –, norma que actualmente corresponde a ETSI EN 319 411). Los criterios se contienen, actualmente, en la guía de evaluación de la conformidad publicada por el organismo de supervisión (ANSSI).

[310] Los criterios son establecidos de forma casuística por el organismo de supervisión (AgID), a petición de los prestadores.

[311] Para (Martínez Nadal, 2009, pág. 251), "la admisión de esta excepción nos plantea algunas dudas; de entre ellas, la inexistencia de plazo temporal máximo para la admisión de estas solicitudes basadas en la legitimación notarial de la firma del solicitante, de tal forma que podría darse la situación de que un

en cuya virtud "podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial" –sin que en este caso se exija formalmente la evaluación de la conformidad a efectos de la determinación de la equivalencia de seguridad–, y que se mantiene en el artículo 7.1, segundo párrafo, del borrador de Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

Parece que esta posibilidad debería rechazarse en una interpretación rigurosa del Reglamento eIDAS, dado que nos encontramos ante un aspecto armonizado, y que además puede afectar negativamente al reconocimiento transfronterizo de los certificados, al considerar otros Estados miembros, eventualmente, que dichos métodos alternativos no se pueden considerar equivalentes a la personación; problema que se puede solventar, en cualquier caso, mediante la reconducción del método en cuestión a la previsión del artículo 24.1.d) ya analizada, que esencialmente sólo implica sujetar todos los métodos alternativos a la evaluación de la conformidad. Ésta es la solución adoptada expresamente por la legislación alemana con respecto a los que denomina métodos innovadores de identificación, por ejemplo[312].

A la obligación de identificar a la persona a la que se expida el certificado, que incluye, como hemos visto, la obligación de identificar al solicitante del certificado de sello electrónico de persona jurídica, el artículo 9.3.a) segundo párrafo del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza añade la de registrar "también la información que permita determinar la identidad de la persona física a la que se hayan entregado los citados certificados, para su identificación en procedimientos judiciales o administrativos".

Cabe imaginar que esta obligación adicional sólo tendrá sentido cuando el certificado de sello electrónico se entregue a una persona diferente de la persona física solicitante, que como ya sabemos debe ser un representante autorizado de la persona jurídica a la cual se expide el certificado.

2.1.2.3 La gestión del ciclo de vida del certificado cualificado

El Reglamento eIDAS establece diversas obligaciones relativas a la gestión del ciclo de vida del certificado cualificado, que pueden ser objeto de complemento o ampliación por parte del legislador nacional, y que se orientan a la finalidad identificativa del certificado cualificado[313].

Así, el numeral k) del artículo 24.2 del Reglamento eIDAS ordena, en primer lugar, que "en caso de los prestadores cualificados de servicios de confianza que expidan

---

prestador de servicios de certificación admita una solicitud con legitimación notarial de firma, y sin realizar la preceptiva comprobación de identidad por personación física, pese a que la legitimación se produjo muchos años antes".

[312] Cfr. la sección § 11 de la Ley alemana de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017.

[313] Algunas de estas obligaciones son buena muestra de que el contrato de certificación debe mantenerse vigente incluso cuando el certificado ha perdido su vigencia, temporal o incluso definitiva, como ha puesto de manifiesto (Ortega Díaz, 2008, págs. 315-316), que excepciona de dicha posibilidad, por ejemplo, la muerte del firmante.

certificados cualificados, establecerán y mantendrán actualizada una base de datos de certificados", base de datos en la que deberán registrarse todos los eventos relativos al ciclo de vida del certificado[314], y que estará sustentada por el correspondiente sistema fiable, al que nos referimos posteriormente[315].

En particular, el Reglamento eIDAS prevé expresamente el registro, en esta base de datos, de la suspensión y de la revocación del certificado, a los efectos de la difusión de la información al público acerca del estado de los certificados; publicación que constituye condición de eficacia, frente a terceros, de estos cambios de estado.

Respecto a la suspensión de los certificados, en cuya virtud se produce una pérdida temporal de validez del certificado, el Reglamento eIDAS no la regula con carácter obligatorio[316], sino que remite a lo que establezca en este sentido la normativa nacional, de forma que nos encontramos ante un elemento de diversidad que podría influir en el funcionamiento del mercado único digital, en el sentido de que los prestadores obligados a ofrecer esta gestión tendrán un mayor coste operacional que sus competidores, aunque también es cierto que un cliente podría percibir la suspensión como una ventaja del servicio, en especial en términos de seguridad.

En todo caso, los artículos 28.5 y 38.5 del Reglamento eIDAS, referidos a los certificados de firma electrónica y sello electrónico, respectivamente, prevén dos reglas armonizadas, por lo que las mismas deberán recibir un tratamiento uniforme en todos los Estados miembros, en especial al efecto de la necesaria "transparencia cuando y donde esta práctica sea posible", en palabras del Considerando (53) del citado Reglamento eIDAS.

La primera regla, contenida en el numeral a) de los citados apartados, indica que "[s]i un certificado cualificado […] ha sido suspendido temporalmente, ese certificado perderá su validez durante el período de suspensión", determinando el efecto jurídico asociado a la suspensión, y sin perjuicio de otros efectos que se pudieren, en su caso, establecer en la legislación nacional; mientras que conforme a la segunda regla, contenida en el numeral b), "el período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado", a los efectos de que dicha condición sea conocida por las partes usuarias.

Como acabamos de ver, el Reglamento eIDAS sólo establece normas relativas a la suspensión de certificados de firma o sello electrónico, pero no de certificados de autenticación de sitio web, laguna que genera la duda acerca de si este aspecto puede también ser objeto de regulación por los Estados miembros o, por el contrario, si debe entenderse que no ha de ser legalmente posible suspender certificados cualificados de autenticación de sitio web. Se trata de una laguna que puede resolverse acudiendo a las normas técnicas, en especial si las mismas son adoptadas por la Comisión, dado que las mismas prohíben, en efecto, la suspensión de certificados de autenticación de sitio web[317].

---

[314] Pero no otras informaciones que debe conservar el prestador, conforme a lo establecido en el numeral h) del artículo 24.2. Cfr. el epígrafe 6.2.7 de este trabajo.

[315] Cfr. el epígrafe 6.2.5 de este trabajo.

[316] La suspensión no se encontraba prevista en la DFE, pero diversos Estados miembros la regularon, incluido el Estado español, que además imponía esta práctica con carácter obligatorio en la LFE.

[317] Cfr. el epígrafe 4.9.13 de (CA/Browser Forum, 2017b), especificación técnica a la que remite la norma

Por lo que se refiere a la revocación del certificado, conforme a los artículos 28.4 y 38.4 de Reglamento eIDAS, referidos a los certificados de firma electrónica y sello electrónico, respectivamente, "[s]i un certificado cualificado […] ha sido revocado después de su activación inicial, perderá su validez desde el momento de su revocación y no podrá en ninguna circunstancia recuperar su estado", lo que no significa que el mismo ya no pueda ser empleado para comprobar la identidad de la persona indicada en el mismo[318], sino que este uso queda limitado a las pruebas electrónicas respaldadas por dicho certificado que hayan sido creadas con anterioridad a la revocación, dado que las mismas pueden ser perfectamente válidas[319], en función de la causa que ha conducido a la revocación.

En efecto, si la revocación se ha producido como consecuencia de la libre voluntad del titular del certificado, sin que se haya puesto en riesgo la seguridad de la clave privada correspondiente a la clave pública contenida en el certificado, no tiene mucho sentido dejar de confiar en la identidad de esta persona que consta en las pruebas electrónicas que se hayan creado hasta el momento de la revocación, para lo que será preciso que la parte usuaria del certificado pueda determinar la causa de la revocación y su momento temporal preciso. De forma análoga sucede con la suspensión a que nos acabamos de referir.

A ello responden las reglas establecidas en los apartados 3 y 4 del artículo 24 del Reglamento eIDAS. El apartado 3 del artículo 24 ordena que "[c]uando los prestadores cualificados de servicios de confianza que expidan certificados cualificados decidan revocar un certificado, registrarán su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud", indicando además que "[l]a revocación será efectiva inmediatamente después de su publicación".

El Reglamento eIDAS armoniza una parte de la práctica profesional de los prestadores que expiden certificados, referida a uno de los aspectos de mayor relevancia, como es la obligación de registro y publicidad de la revocación, y del plazo correspondiente, que deberá ser el oportuno, y con un máximo de 24 horas en caso de que la misma responda a la solicitud de la persona titular. Nótese que la eficacia de la revocación se produce desde el momento de la publicidad[320], y no anteriormente, regla que claramente persigue afectar a la responsabilidad del prestador frente a las partes usuarias que hayan confiado en un certificado ya revocado, pero del que no se ha publicado la revocación.

En relación con esta publicación, el apartado 4 del artículo 24, que complementa al apartado 3 del mismo artículo, pero también los artículos 28.5.b) y 38.5.b) del

---

ETSI EN 319 411-1.

[318] A efectos de la validación de la firma o sello electrónico avanzado, o de una identificación electrónica de dicha persona.

[319] Por este motivo, resultaba muy correcto que el epígrafe 3 del artículo 10 de la LFE dijera que "[l]a extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos", previsión que no se ha incorporado al Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza. Para (Martínez Nadal, 2009, pág. 204), esta irretroactividad constituye una medida de protección a terceros y también del firmante.

[320] Por este motivo, (Martínez Nadal, 2009, pág. 187) se refiere a todas las causas de revocación y suspensión como "causas de eficacia diferida", por contraposición a la expiración del certificado, que sería la única causa de eficacia inmediata (y, cabe añadir, automática).

Reglamento eIDAS, ordena que "[l]los prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos", la cual "deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente"; previsión que supone una importante novedad con respecto a la LFE, cuyo artículo 10.4 exigía el mantenimiento de esta información sólo hasta la expiración del certificado, y que persigue facilitar la validación de las fuentes de prueba electrónica que se sustentan en dichos certificados, como las firmas electrónicas avanzadas o cualificadas[321].

Adicionalmente, el artículo 9.2 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza ordena que "[l]os prestadores de servicios que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público", en una previsión que extiende la obligación, ya establecida en el artículo 24.4 del Reglamento eIDAS en relación a los prestadores que expidan certificados cualificados, a los prestadores que expidan certificados no cualificados.

Nos encontramos, en este caso, ante normas que persiguen reforzar la función típica del certificado, que resultaría afectada negativamente si no resultara posible a la parte usuaria conocer el estado de validez del certificado, o si dicho acceso resultase muy gravoso; normas que resultan claramente novedosas con respecto a la DFE. Entre estas obligaciones destacan la imposición de que el mecanismo de información de estado funcione de forma automatizada[322] y, en segundo lugar, que dicha actuación sea gratuita, previsión legal que afecta contundentemente[323] a modelos de negocio como el de la

---

[321] Más en concreto, el objetivo de esta medida es poder determinar, sólo con la última lista de revocación de certificados expedida por el prestador, si un certificado ya expirado fue revocado. Aunque, como explica (Martínez Nadal, 2009, págs. 204-205), "parece razonable que un certificado inicialmente extinguido de manera anticipada por causas imprevistas pueda ser eliminado del servicio de consulta sobre la vigencia de certificados una vez que finaliza su periodo de validez inicialmente establecido, por cuanto esta caducidad se deduce del propio certificado, en el que los terceros no deberían confiar no ya por la propia revocación extraordinaria sino por la extinción ordinaria", lo cierto es que este enfoque impide verificar una firma electrónica cuando el certificado ha expirado, por lo que implementar un procedimiento de verificación de firma "en el pasado" obligaría a los verificadores todas las listas de revocación de certificados expedidas por el prestador.

[322] A los efectos de facilitar, en especial, el proceso de validación de la firma o sello electrónico avanzado. Cfr. el epígrafe 4.3.2.1 de este trabajo. En la DFE no existía esta obligación, al menos de forma explícita, ya que sólo se exigía disponer de un servicio rápido y seguro de guía de usuarios, que por tanto podía ser manual.

[323] (Valero Torrijos, 2013, pág. 168 y ss.) consideró que este modelo de negocio ya era incompatible con la legislación estatal y, más en concreto, con el artículo 21 de la LAE, si bien tal infracción lo sería sólo en relación con el uso de los certificados en el procedimiento administrativo. Más contundente resulta, en este sentido, la reflexión de (Ortega Díaz, 2008, pág. 257), en el sentido de considerar que la obligación del prestador de suministrar copias de los certificados expedidos, y la información de estado de vigencia de los mismos, "tiene una base legal (artículo 18.d LFE) y es que se trata de una prestación consustancial al tipo contractual. […] Y ello es así porque la obligación del certificador a conceder el acceso a los terceros, para que verifiquen el contenido del certificado electrónico, es una obligación al servicio de la certificación. De nada sirven todas las obligaciones si ésa no se cumple. La utilidad del servicio no se traslada al usuario del servicio (suscriptor) pues no se generará la confianza que hará posible la fiabilidad de la firma electrónica ante los ojos de los terceros".

FNMT-RCM, que ha venido cobrando por este servicio, tanto a entidades públicas cuanto a privadas[324].

Cualesquiera otros elementos relativos a la suspensión o la revocación quedan a lo que establezca el legislador nacional, como por ejemplo el establecimiento de causas legales de suspensión o revocación, algo que resulta conveniente en orden a establecer un correcto funcionamiento del mercado, expulsando del mismo los certificados potencialmente defectuosos, al tiempo que se protege a los prestadores que expiden los certificados frente a posibles reclamaciones de sus clientes asociadas a la toma de la decisión de suspensión o, en especial, de revocación[325].

En este sentido, el artículo 5 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza recoge el régimen legal español correspondiente, que analizaremos a continuación.

En su epígrafe 1, el citado artículo 5 establece la obligación –que no facultad– del prestador de servicios de certificación que expidió un certificado, cualificado o no cualificado, de proceder a la revocación del certificado en determinados supuestos, esencialmente alineados con la legislación anterior[326].

En primer lugar, procede la revocación en caso de "[s]olicitud formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web" (numeral a) del artículo 5.1 del artículo 5.1 del Anteproyecto[327]), que no tiene porqué justificarla en modo alguno[328], derecho que no puede ser limitado por el prestador de servicios de confianza que expidió el certificado, sin perjuicio de establecer condiciones para su ejercicio, como por ejemplo las relativas al horario y canal de atención a través del cual puede ejercer este derecho.

Se trata de una previsión que muestra el carácter puramente voluntario de la obtención del certificado de firma electrónica, sello electrónico o autenticación de sitio web, y que puede resultar conflictivo en aquellos escenarios en que se considere la imposición del uso de certificados electrónicos por parte de determinadas personas.

En efecto, cabría preguntarse si un empleado laboral o un funcionario público pueden ser

---

[324] En la dirección de Internet http://www.fnmt.es/documents/10179/35277/FNMT_Contrato-Tipo_VAL.OCSP_TRAMO.MAYORISTA_03.02.2011.pdf/ se contiene el modelo de contrato con las correspondientes tarifas, para el caso de prestación a privados. Desde julio de 2016, mantener este modelo de negocio implica que los certificados de este prestador ya no puedan continuar siendo reconocidos/cualificados, como en efecto ha supuesto en este caso, dado que la autoridad de certificación de Clase 2 de la FNMT-RCM ha perdido la cualificación con fecha 12 de septiembre de 2017.

[325] En relación con el régimen legal español de suspensión y revocación en la LFE, cfr. (Martínez Nadal, 2009, págs. 172-205) y (Ortega Díaz, 2008).

[326] Cfr. el artículo 8.1, epígrafes b) a h) de la LFE.

[327] El artículo 8.1.b) de la LFE se refería a la "revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica".

[328] (Martínez Nadal, 2009, pág. 173) se refiere a "la simple decisión voluntaria del titular del certificado de extinguir de forma anticipada un certificado […] de una decisión discrecional, sin necesidad de causa justificativa […] una revocación *ad nutum*". La autora también hace notar la incorrección de la LFE cuando se refiere a la revocación formulada por, cuando debería referirse a la solicitud de revocación, crítica que parece haber sido acogida en el Anteproyecto de Ley.

obligados a disponer de un certificado de firma electrónica, lo que implicaría la restricción de su derecho a solicitar la revocación de su certificado. Una interpretación muy estricta de la legislación conduciría a la conclusión de que no puede imponerse esta obligación a un empleado, lo cual supondría un claro desincentivo a la adopción de estos mecanismos, y ciertamente resultaría absurdo desde la perspectiva de la posibilidad, no discutida, de imponer el uso de sistemas de identificación y firma basados en contraseñas. Debe, por tanto, realizarse una interpretación integradora de esta norma en el ordenamiento jurídico y considerar la existencia de normas que pueden avalar la imposición del uso de los certificados por parte de los empleados[329].

De otro lado, debe también considerarse que otros sujetos diferentes del firmante o creador de sellos pueden solicitar la revocación, como son la persona física o jurídica representada[330] o cualquier otro tercero autorizado, como ya venía sucediendo en la LFE.

En segundo lugar, procede la revocación en caso de "[v]iolación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero" (numeral b) del artículo 5.1 del Anteproyecto[331]), previsión que recoge cuatro casos diferenciados que afectan con claridad a la confianza en el servicio. En efecto, difícilmente podrá producir el certificado electrónico su efecto típico[332] si no se tiene certeza acerca de la seguridad del más elemental elemento de seguridad que lo sustenta; esto es, la clave privada del par de claves del algoritmo asimétrico[333].

El primer caso cubierto por esta causa de revocación se refiere a la violación o puesta en peligro del secreto de los datos de creación de firma o de sello correspondientes a un certificado en concreto, sea o no cualificado, y conecta con el valor[334] de las pruebas electrónicas que constituyen la propia firma o sello y, por conexión, los documentos electrónicos a que ofrecen soporte; el segundo, a la violación o puesta en peligro del secreto de los datos de firma o sello del prestador empleados para la expedición del certificado; y el tercero, a la violación o puesta en peligro del secreto de los datos

---

[329] Así sucede, por ejemplo, en el caso de los empleados públicos, a los que posteriormente nos referiremos (cfr. el epígrafe 2.1.4.3 de este trabajo).

[330] (Martínez Nadal, 2009, págs. 173-174) indica que "sigue sin pronunciarse, en sede de extinción de certificados, la Ley de firma electrónica (como tampoco lo hacía el Real Decreto-ley) sobre si esta actuación para la que se legitima a las personas representadas es simplemente una facultad o es más bien una carga", aunque la misma autora reconoce que "esta cuestión sí es abordada de forma novedosa en el art. 23.2 de la ley que, en sede de responsabilidad de los prestadores de servicios de certificación, establece la obligación del representado de solicitar la revocación aunque matizando que 'sólo si tiene conocimiento de la existencia del certificado'".

[331] El artículo 8.1.c) de la LFE se refería a la "[v]iolación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero".

[332] Cfr. el epígrafe 2.1.3 de este trabajo.

[333] Cfr. el Anexo 0 de este trabajo.

[334] En opinión de (Martínez Nadal, 2009, pág. 176), "en el fondo de estas causas subyace una posible vulneración de uno de los principios básicos de funcionamiento del sistema de certificados, que es el control de la clave privada de firma por parte del titular de la misma", por lo que "la pérdida de tal control, que deja abiertas las puertas a usos indebidos por terceros, plantea importantes incógnitas en materia de responsabilidad".

correspondientes al certificado de autenticación de sitio web. Nótese que en los tres casos se incluye la efectiva violación de la seguridad, de un lado, y la puesta en peligro, o violación potencial, del secreto de dichos datos, de otro; debiendo el prestador, por tanto, actuar en cuanto tenga sospecha acerca de dicha puesta en peligro.

Normalmente, el prestador sólo podrá verificar estas circunstancias en relación con sus propios datos de firma o sello –empleados, como ya se ha dicho, para la expedición de certificados– o bien cuando gestione datos de creación de firma o sello por cuenta de terceros, ya que normalmente dispondrá de los correspondientes sistemas fiables[335] y de procedimientos de seguridad apropiados para ello. Más difícil será, sin embargo, que tenga noticia de la violación o puesta en peligro de los datos de creación de firma o sello, o de los datos para la autenticación de sitio web, en los casos en que no los gestione, por lo que cabe entender que sólo actuará en caso de notificación por parte de su titular o de un tercero, normalmente después de realizar las oportunas indagaciones y comprobaciones[336].

El cuarto caso se refiere a la utilización indebida de los datos anteriormente indicados por parte de un tercero, que será cualquier persona diferente del titular de los datos; esto es, la persona física firmante, la persona jurídica creadora de sellos, el prestador de servicios de confianza que expide certificados, o la persona física o jurídica titular del certificado de autenticación de sitio web. De nuevo, es evidente que el uso no autorizado de estos datos afecta a la finalidad de la prueba electrónica, por lo que establecer esta causa de revocación resulta plenamente razonable.

Aplicando una interpretación *a contrario sensu*, no procederá la revocación, sin embargo, cuando el uso por el tercero sea "debido", como ya sucedía en la LFE, en particular cuando se encuentre autorizado o incluso mandatado por el firmante, dicción legal que permite argumentar en favor de la posibilidad de que un firmante permita a cualquier tercero hacer uso controlado de sus datos de creación de firma, aunque no su generación ni gestión, ni mucho menos, posesión, como veremos posteriormente con mayor detalle[337].

En tercer lugar, procede la revocación en caso de "[r]esolución judicial o administrativa que lo ordene" (numeral c) del artículo 5.1 del Anteproyecto[338]), previsión que plantea el problema de dilucidar qué motivos pueden llevar a una autoridad judicial o administrativa a dictar dicha orden, al menos más allá de actuar en las competencias atribuidas por la propia legislación reguladora de los servicios de confianza[339], por ejemplo en el caso de que la orden se dicte como consecuencia de la previa constatación de un incumplimiento

---

[335] Sobre los sistemas fiables empleados por los prestadores de servicios de confianza cualificados, cfr. el epígrafe 6.2.5 de este trabajo.

[336] Dado el estricto modelo de responsabilidad civil del prestador cabe imaginar que, en caso de duda, el prestador optará preferentemente por la revocación del certificado de un cliente, en especial cuando el aviso proceda de un tercero cualificado, como una autoridad. Sin embargo, en el caso de la revocación de su propio certificado, dado que la misma invalida todos los certificados expedidos por el prestador, su preferencia será la contraria; es decir, revocar sólo en caso estrictamente necesario.

[337] Cfr. el epígrafe 4.1.2 de este trabajo.

[338] El artículo 8.1.d) de la LFE se refería también a la "[r]esolución judicial o administrativa que lo ordene".

[339] Cfr. el epígrafe 1.4.4 de este trabajo.

de la normativa jurídica por parte de prestador de servicios de confianza, o cuando se haya acreditado una incidencia que afecte a la fiabilidad del certificado.

Un ejemplo de esta posibilidad sería el caso de una resolución administrativa o judicial referida a la titularidad de un nombre de dominio en relación con el cual se haya expedido un certificado cualificado de autenticación de sitio web, que ordene la revocación de dicho certificado, y que eventualmente se dirija a la totalidad de prestadores de servicios incluidos en la Lista de Confianza[340].

En el derecho alemán, la sección § 14 de la Ley alemana de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017, autoriza la revocación por parte del organismo de supervisión en determinados casos tasados; a saber, cuando el prestador cese en su actividad y no transfiera los certificados a un tercer prestador, y cuando se produzcan hechos que justifiquen la presunción de que el certificado cualificado ha sido falsificado o ya no sea suficientemente resistente a falsificaciones, o cuando el dispositivo cualificado de creación de firma electrónica o selo electrónico tenga defectos de seguridad.

En cuarto lugar, procede la revocación en caso de "[f]allecimiento del firmante; incapacidad sobrevenida, total o parcial, del firmante; extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio de nombre de dominio en el supuesto de un certificado de autenticación de sitio web" (numeral d) del artículo 5.1 del Anteproyecto[341]), previsión que agrupa aquellas causas que afectan a elementos esenciales del certificado, como son los que afectan a la existencia de la persona física[342] o jurídica identificada en el certificado; a la capacidad de obrar de la persona física, incluso parcial, lo que supone

---

[340] Sobre el funcionamiento de este mecanismo de publicidad administrativa, cfr. el epígrafe 7.1.4.1 de este trabajo.

[341] El artículo 8.1.e) de la LFE se refería al "[f]allecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica".

[342] (Martínez Nadal, 2009, pág. 178) plantea la duda "de la persona que tiene la carga de solicitar la extinción anticipada (especialmente en el supuesto de muerte, y probablemente no tanto en el de incapacidad, en que cabe entender que entre las obligaciones de un tutor diligente se incluirá la de solicitar la extinción del certificado expedido a la persona ahora incapaz, siempre que el tutor tenga conocimiento de la existencia de tal certificado); pues no siempre la entidad certificadora tendrá noticia cierta y rápida de tales hechos […] (pudiendo darse la paradójica situación de que, tras la muerte del signatario, no sea revocado el certificado, y su clave de firma vaya a parar a manos de un tercero que la utilice ilegítimamente, con la consecuencia de la atribución *post mortem* de mensajes electrónicos al firmante)". Para (Ortega Díaz, 2008, págs. 317-318), la solución, en el caso del fallecimiento, variará en función si el firmante fallecido es o no el titular del certificado. A estos efectos, hay que hacer notar que, conforme al artículo 80.1.1ª de la Ley 20/2011, de 21 de julio, del Registro Civil, "[t]ambién se podrá tener conocimiento de los datos que constan en el Registro Civil mediante los procedimientos especiales que se acuerden por la Dirección General de los Registros y del Notariado, cuando la información […] sea precisa para comprobar por las entidades de certificación reguladas en la Ley 59/2003, de 19 de diciembre, de firma electrónica, que no se ha producido la extinción de los certificados electrónicos por las causas contempladas en el artículo 8, apartado 1, letra e), de dicha Ley", previsión que no ha sido desarrollada, dado que esta Ley no ha entrado en vigor.

que, como en la normativa anterior, sólo las personas con plena capacidad de obrar puedan disponer de un certificado para todas las funcionalidades de la firma[343]; y al cambio del nombre de dominio.

En quinto lugar, procede la revocación en caso de "[t]erminación de la representación en los certificados electrónicos con atributo de representante", en cuyo caso "tanto el representante como la persona o entidad representada están obligados a solicitar la revocación de la vigencia del certificado en cuanto se produzca la modificación o extinción de la citada relación de representación" (numeral e) del artículo 5.1 del Anteproyecto[344]), previsión que se refiere a otro elemento de gran importancia en el certificado[345], pero que ciertamente podría haber quedado absorbida en una causa más general, referida a cualquier otro atributo incluido en el certificado, como la que se encuentra en el numeral g) del mismo artículo 5.1, crítica que se podía realizar en la normativa anterior.

Nótese, sin embargo, que en el Anteproyecto dejan de ser causa explícita de revocación el fallecimiento o la extinción de la personalidad jurídica del representado, así como la incapacidad sobrevenida, total o parcial, del representado, y la disolución de la persona jurídica representada (todas ellas recogidas en el artículo 8.1.e) de la LFE), sin perjuicio de que dichas circunstancias puedan entenderse incluidas en la terminación de la representación.

En sexto lugar, procede la revocación en caso de "[c]ese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquél sea transferida a otro prestador de servicios de confianza" (numeral f) del artículo 5.1 del Anteproyecto[346]), previsión que ya existía en la LFE y que esencialmente se flexibiliza a efectos del consentimiento del interesado, como se analizará posteriormente[347].

En séptimo lugar, procede la revocación en caso de "[d]escubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo" (numeral g) del artículo 5.1 del Anteproyecto[348]), previsión

---

[343] Pero no implica, necesariamente, la extinción del contrato de certificación, ya que la firma electrónica se podría emplear para el ejercicio de otros derechos que el incapaz no tenga limitados, lo que se debería reflejar mediante el correspondiente atributo en el certificado, como ha defendido (Ortega Díaz, 2008, pág. 321 y ss.)

[344] El artículo 8.1.e) de la LFE se refería a la causa análoga.

[345] Parece, de todos modos, que el establecimiento de esta causa en un numeral específico da respuesta a la crítica que había realizado (Martínez Nadal, 2009, pág. 180) con respecto a la LFE, al observar "que no se resuelve la problemática generada por esta situación, por cuanto ni se resuelve ni se aborda siquiera la cuestión de cuáles son las personas que tiene la obligación, la carga o simplemente la legitimación para extinguir, o solicitar la extinción anticipada, del correspondiente certificado".

[346] El artículo 8.1.f) de la LFE se refería al "[c]ese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación".

[347] Cfr. el epígrafe 6.2.8 de este trabajo.

[348] El artículo 8.1.f) de la LFE se refería a la "[a]lteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la

sensiblemente diferente a la contenida anteriormente en la LFE, y que ahora se refiere al conocimiento posterior, a la expedición del certificado acerca de la falsedad o inexactitud de los datos que el solicitante entregó al prestador de servicios que expidió el certificado, mientras que en la LFE se refería a la alteración[349] de dichas informaciones.

Se mantiene, como es lógico, la causa legal de revocación referida a los cambios posteriores que sufran otras informaciones, en especial de los diferentes de los datos de identidad, que se incorporen como contenido del certificado, y que hubiera sido suficiente –como ya se avanzó– para exigir la revocación en el caso de la modificación o extinción de la representación.

En octavo, y último lugar, procede la revocación en caso de "[c]ualquier otra causa lícita prevista en la declaración de prácticas del servicio de confianza" (numeral h) del artículo 5.1 del Anteproyecto[350]), previsión que ya se encontraba prevista en la LFE y que encuentra su límite en la licitud de la causa que prevea el prestador. Como es evidente, la revocación del certificado no podrá producirse como sanción del prestador al cliente cuyos derechos como consumidor sean conculcados por el propio prestador, por ejemplo.

Entre dichas otras causas, se encuentran algunas previstas en la autorregulación, que deben ser adoptadas por los prestadores que se sujetan a la misma. En concreto, la norma ETSI EN 391 411-1 prevé la obligación de proceder a la revocación cuando el certificado ya no sea compatible con la política de certificación conforme a la que fue expedido, cuando el prestador de servicios sea consciente de cambios que afecten a la validez del certificado y cuando la criptografía empleada en el mismo deje de poder garantizar la vinculación entre el titular y la clave pública.

Asimismo, la especificación técnica del *CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates*, que resulta aplicable, como ya sabemos, a los certificados cualificados de autenticación de sitio web, prevé un completo elenco de quince causas de revocación, que resultan obligatorias para los prestadores que expiden este tipo de certificado.

En su epígrafe 2, el artículo 5 del Anteproyecto regula la posibilidad, que no obligación, de los prestadores de proceder a la suspensión de un certificado, pero sólo en los casos expresamente indicados. Nótese que lo que es opcional es suspender o no certificados, a diferencia de lo que sucedía en la LFE, en que era obligatorio, pero no las causas y las consecuencias, en caso de hacer uso de esta posibilidad, que entonces deben ser las legalmente previstas. El legislador español podría haber mantenido esta obligación[351], sin

---

realidad".

[349] (Martínez Nadal, 2009, págs. 182-183) diferencia, en la redacción de esta causa de revocación contenida en la LFE dos situaciones: "la manipulación voluntaria (normalmente por parte del solicitante) de los datos que se aportan para la obtención del certificado y en mismo momento o en momentos previos a la emisión" y "una alteración de dichos datos en un momento posterior a la emisión, no necesariamente de forma voluntaria y fraudulenta".

[350] El artículo 8.1.g) de la LFE se refería a "[c]ualquier otra causa lícita prevista en la declaración de prácticas de certificación", en sentido casi idéntico.

[351] Así ha sucedido, por ejemplo, en el caso del derecho austríaco. Cfr. la sección § 6 de la Ley Federal (austríaca) sobre Firmas Electrónicas y Servicios de Confianza para Transacciones Electrónicas – *Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)*, promulgada por artículo 1 de la Ley Federal de 8 de julio

infringir el Reglamento eIDAS, pero ha adoptado una posición más liberal, siempre en el marco de la responsabilidad del prestador de servicios, que por tanto tendrá un importante incentivo para limitar dicha responsabilidad, por ejemplo, adoptando la suspensión como mecanismo adicional a la revocación.

Hay que recordar que la suspensión tiene sentido como medida menos gravosa que la revocación en determinados casos, especialmente cuando existen dudas acerca de la concurrencia de causas que implicarían la revocación, por lo que será una práctica interesante especialmente en aquellos casos en que la revocación implicaría un coste de reposición elevado[352].

En primer lugar, procede la suspensión en caso de solicitud del titular del certificado, que no deberá ser objeto de justificación por parte del titular[353], sin perjuicio de que el prestador condicione el ejercicio del derecho a plazo, por ejemplo, debido a la inconveniencia que supone al prestador el mantener un certificado suspendido.

También debe procederse a la suspensión cuando lo ordene una resolución administrativa o judicial, o por cualquier causa lícita establecida por el prestador, en términos análogos a los anteriormente expuestos. Tomando uno de los ejemplos anteriormente indicados, en un juicio sobre la titularidad de un nombre de dominio o de marca registrada, se podría solicitar, como medida cautelar, la suspensión del certificado cualificado de autenticación de sitio web.

En segundo lugar, deberá procederse a la suspensión cuando exista duda[354] acerca de la violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero; o de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado; previsión que resulta razonable en atención a la finalidad de este mecanismo de suspensión.

En todo caso, conforme al mismo epígrafe 2 del artículo 5 del Anteproyecto, la opción que tome el prestador acerca de ofrecer o no la suspensión de certificados deberá constar en la correspondiente declaración de prácticas.

Finalmente, el epígrafe 3 del artículo 5 del Anteproyecto, parcialmente en línea con la LFE[355], debe informar al titular del certificado acerca de la revocación o, si la ofrece, la

---

de 2016.

[352] Como, por ejemplo, en el caso de un certificado en el que los datos de creación de firma electrónica o sello electrónico se encuentre en una tarjeta criptográfica en posesión del firmante o creador de sellos, en cuyo caso la revocación implica la sustitución de todos los elementos, lo que no sucedería en el caso de la suspensión temporal mientras se investiga un posible incidente.

[353] Para (Martínez Nadal, 2009, pág. 195), "cabe atribuir a estas solicitudes una cierta discrecionalidad, pero parece necesario también un fundamento de las mismas que justifique el recurso a la suspensión en lugar de la revocación definitiva".

[354] Nótese que la LFE exigía que las dudas fueran "fundadas", a diferencia del Anteproyecto de Ley.

[355] El artículo 10.2 de la LFE ordenaba que "[e]l prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del

suspensión, "de manera previa o simultánea a la indicación de la revocación o suspensión de un certificado electrónico cualificado en el servicio de consulta sobre el estado de validez o revocación de los certificados […] especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto".

Se trata de una previsión orientada, como en la LFE, a garantizar que el titular es consciente[356] del cambio de estado del certificado con anterioridad o, al menos, en el mismo momento de su eficacia frente a terceros, y tiene sentido, como es lógico, sólo en los casos en que la revocación o, en su caso, la suspensión haya sido realizada por una causa diferente a su solicitud, o sin su intervención o conocimiento previos.

Ha desaparecido, en relación con el régimen anterior, la obligación que informar al titular acerca de la duración máxima de la suspensión, si bien se mantiene la regla de que "la vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado".

No podemos acabar este análisis mencionando que, a pesar de lo que se acaba de exponer, ni el Reglamento eIDAS, ni el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza establecen las consecuencias concretas que implicará la pérdida de validez, temporal o definitiva, del certificado, sobre las firmas o sellos electrónicos creados empleando un certificado inválido, por lo que se deberá estar a la normativa aplicable al correspondiente acto jurídico a estos efectos[357].

2.1.3 Los efectos jurídicos del certificado electrónico

El Reglamento eIDAS no establece ningún efecto jurídico específico en relación con el uso del certificado electrónico, ni siquiera cuando el mismo es cualificado, seguramente por su carácter accesorio a los procesos a los que sirve de apoyo, y sin perjuicio de que, como hemos visto, de la propia definición del certificado se desprenda claramente que el certificado confirma la identidad de una persona, sea una persona física (un firmante), una persona jurídica (un creador de sellos), o una persona (física o jurídica) titular de un

---

certificado si transcurrido dicho plazo no se hubiera levantado la suspensión".

[356] (Martínez Nadal, 2009, pág. 203) considera que "esta obligación […] es especialmente relevante en aquellos casos en que la extinción o suspensión de vigencia ha sido a iniciativa de un tercero o de la propia autoridad de certificación, especialmente teniendo en cuenta que el titular tiene la obligación, o cuanto menos la carga, de no utilizar el certificado una vez se ha extinguido […] de forma que, a su vez, cabe entender que si el prestador incumple la obligación de notificación del artículo 10.2 no se beneficiará tampoco, en principio, de la exoneración de responsabilidad prevista […]".

[357] En el caso concreto de la actividad administrativa formalizada, (Valero Torrijos, 2013, págs. 174-175) se ha planteado la incidencia que tendría el uso de certificados revocados por parte de las autoridades administrativas, indicando que "[e]n principio, al no poder subsumirse en alguna de las causas de nulidad […] cabría pensar que se trata de un supuesto de anulabilidad que admitiría la convalidación siempre que el titular del certificado se ratificase en su actuación", pero añade que "el hecho de que el certificado ya no estuviera vigente no impide la declaración de voluntad, juicio, conocimiento o deseo en que consiste el acto administrativo reúna los requisitos generales exigibles sino que, simplemente, afecta a las condiciones de comprobación de la presunción legal en que se basa el uso de los certificados a los efectos de la imputación de la autoría del documento", consideración que de forma muy precisa se centra en el efecto jurídico del certificado, que no es otro que confirmar la identidad del firmante, por lo que concluye el autor que "la imposibilidad de llevar a cabo la comprobación […] no afectaría en sí misma a la validez sino, más bien, a su eficacia".

sitio web concreto.

Lo que no existe en el Reglamento eIDAS es, por tanto, una regla de equivalencia funcional con ninguna institución empleada para la prueba de la identidad en las relaciones presenciales o a distancia soportadas en papel.

Más en concreto, el Reglamento eIDAS no autoriza la sustitución de un mecanismo de identidad personal –como podría ser un documento nacional de identidad, en soporte físico– por un certificado electrónico, ni siquiera en el caso de la firma electrónica[358], por lo que el Derecho nacional se ve inalterado al respecto, siempre salvo la posibilidad de que una norma de la Unión establezca esta regla en algún caso concreto.

Por ello, será la normativa de la Unión o la normativa nacional[359] o, cuando resulte posible, la autonomía de la voluntad de las partes, la que permita habilitar, en su caso, esta posibilidad. Y, en su consecuencia, no podrá necesariamente asumirse, con carácter general, que "donde una ley ordene el uso de un documento de identidad, podrá emplearse un certificado de persona física o jurídica", que sería la plasmación a este caso de la regla del equivalente funcional.

Otra cosa será, sin embargo, que un Estado pueda reconocer un certificado como sistema de identificación conforme al Reglamento eIDAS, incluso con eficacia transfronteriza, como posteriormente veremos[360].

Como ejemplo de autorización sectorial, en el nivel de la Unión, relativo al uso de un certificado a efectos puramente identificativos podemos citar la propuesta de modificación de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. En virtud de la reforma, el artículo 13 de la Directiva, que establece las obligaciones de identificación del cliente, de forma previa o durante el establecimiento de una relación de negocios, autorizará de forma expresa el uso de "servicios de confianza relevantes" definidos en el Reglamento eIDAS o en la legislación nacional para dar cumplimiento de la obligación de identificación previa.

Otro ejemplo se encuentra, en este caso en el nivel nacional, en la autorización de uso de los certificados cualificados de firma electrónica y (hoy también) sello electrónico que se ha venido conteniendo en la legislación reguladora del procedimiento administrativo electrónico, a la que, por razones sistemáticas, nos referiremos algo más adelante[361].

Esta suerte de regla de equivalencia funcional, que ya hemos visto no existe en el Reglamento eIDAS, no tiene, además, sentido alguno en el caso del certificado de autenticación de sitio web.

Ciertamente, en el Reglamento eIDAS tampoco se establece presunción procesal alguna que apoye el uso de un certificado cualificado, algo que también podrá suceder, sin embargo, en la normativa nacional, si así lo considera necesario el legislador.

---

[358] Mucho menos en el caso del sello electrónico.

[359] El Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza no ha establecido esta regla de equivalencia, algo que posiblemente constituye una oportunidad perdida.

[360] Cfr. el epígrafe 3.1.1 de este trabajo.

[361] Cfr. los epígrafes 2.2.2 y 2.2.3 de este trabajo.

2.1.4 La regulación del certificado electrónico en el ámbito del sector público español

Nos interesa ahora ver la regulación de los certificados en el sector público español, que se refiere a diversos casos: en primer lugar, la utilización de certificados para la autenticación de las sedes electrónicas de las Administraciones Públicas, y para la identificación de las Administraciones, mediante certificado de sello electrónico; en segundo lugar, el establecimiento de atributos específicos para los certificados de las personas físicas vinculadas a las Administraciones Públicas, y para determinados certificados de los interesados en el procedimiento administrativo, que también despliegan su eficacia en relación con la identificación de todas estas personas.

En general, y sin perjuicio del análisis completo del origen y desarrollo de esta regulación, que realizamos, por razones sistemáticas, en el capítulo dedicado a la firma electrónica[362] (dado que se trata de una "regulación" aparecida en "desarrollo" de la misma), es preciso avanzar que todas estas normas referidas a "tipos" y contenidos concretos de los diferentes certificados forman parte de la Política de firma electrónica y de certificados de la Administración General de Estado, dictada al amparo de lo establecido en el artículo 24 del RDLAE y en el artículo 18 del RDENI, que también se dicta en desarrollo de la LAE, sin perjuicio de su ubicación actual dentro de la LRJSP.

En concreto, el artículo 24 del RDLAE, norma pocos meses anterior al RDENI, indica en su epígrafe 1 que "[l]a política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación", por lo que resulta aplicable, con carácter general, a los certificados empleados por la Administración General del Estado y sus entidades dependientes, lo que claramente incluye el uso de certificados para la función de identificación.

Asimismo, el epígrafe 2 del mismo artículo 24 del RDLAE prevé, entre los contenidos mínimos que debe incluir la política[363], "a) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos", lo que afecta potencialmente a los certificados expedidos a los interesados, y "b) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de certificación asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado recogidas en el presente real decreto", en una referencia que debe entenderse realizada a los certificados de sede electrónica, los certificados de sello electrónico para la actuación administrativa automatizada y los certificados de empleado público.

Por su parte, el artículo 18.1 del RDENI ordena que "[l]a Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación", sin perjuicio de que, como prevé el mismo epígrafe, "[d]icha política podrá ser utilizada como referencia por otras Administraciones

[362] En concreto, cfr. el epígrafe 5.2 de este trabajo.

[363] Además de las obligaciones que el artículo 23 del RDLAE impone a los prestadores que expiden dichos certificados, artículo que debe entenderse inaplicado por el Reglamento eIDAS, cuanto menos en parte.

públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales".

A su vez, el epígrafe 4 del mismo artículo 18 del RDENI especifica que "[l]os perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa", certificados que "serán los definidos en la Ley 11/2007, de 22 de junio, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sus desarrollos normativos", en una referencia a todos los tipos de certificados que se emplean en el procedimiento administrativo electrónico.

Como se puede ver, mientras que existe una fuerte redundancia entre el artículo 18.1 del RDENI y el artículo 24 del RDLAE, algo ciertamente criticable dado que en ambos casos se trata de normas aplicables sólo a la Administración General del Estado y sus entidades dependientes, en cambio no sucede lo mismo en el caso del artículo 18.4 del RDENI, que permitiría, al menos formalmente[364], a cada emisor de una política de firma electrónica proceder a establecer estos atributos de los certificados, resultando en una menor interoperabilidad que en caso de no establecerse los mismos, por lo que podemos imaginar que la voluntad del Gobierno ha sido la de armonizar[365] esta cuestión para todas las Administraciones y, por tanto, también para todos los prestadores, sean nacionales o extranjeros, aunque posiblemente operando dentro del espacio del Mercado Único Digital. Dado que ya conocemos el régimen legal relativo a la incorporación de atributos en los certificados, cabe preguntarse acerca de la compatibilidad de estas previsiones con el Reglamento eIDAS.

En todo caso, la política para la Administración General del Estado fue inicialmente aprobada por el grupo de trabajo CertiCA, en versión 1.8, el 11 de octubre de 2010, y posteriormente fue actualizada a la versión 1.9, aprobada por acuerdo de la Comisión Permanente de Consejo Superior de Administración Electrónica de 30 de mayo de 2012, el cual fue publicado por Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas. Precisamente el Anexo II de dicha Política describe los contenidos de los certificados[366], incluyendo diversos atributos que son obligatorios en relación a diversos tipos de certificados.

En concreto, el Anexo II de la Política de firma electrónica y de certificados de la Administración General del Estado prevé, para todos los certificados expedidos a favor de las Administraciones Públicas, la que denomina "identidad administrativa", consistente en una serie de atributos, adicionales a los previstos en el Reglamento

---

[364] A menos que se considere que el artículo 18.4 del RDENI se refiere a la Política de firma que defina la Administración General del Estado, claro, lo cual es más que discutible dada la extrema ambigüedad del artículo en cuestión.

[365] No se trata, de todos modos, de una verdadera armonización, como veremos, sin perjuicio de lo que han devenido una suerte de estándar adoptado por las restantes Administraciones Públicas, tanto para la función de identificación cuanto de firma o sellado.

[366] Este Anexo II ha sido actualizado para adecuarse al Reglamento eIDAS, siendo su versión vigente en la actualidad, la número 2.0.

eIDAS[367], que se especifican en función del tipo de certificado, y a los que nos referiremos posteriormente.

En este sentido, es preciso indicar que esta obligación no se refiere a los tipos previstos en el Reglamento eIDAS, sino a subtipos de dichos certificados; es decir, el Anexo II de la Política de firma electrónica de la Administración General del Estado no se refiere a atributos obligatorios para poder considerar que un certificado sea realmente de firma electrónica de persona física, por ejemplo, sino para considerar que además sea de empleado público, o de persona física representante.

Esto es importante porque supone que, como ya hemos avanzado anteriormente, la consecuencia del incumplimiento[368] de las normas que regulan esos atributos obligatorios –establecidas en el Anexo II de la citada Política– será que el certificado de empleado público, por seguir con el ejemplo anterior, sea considerado como un certificado de persona física, que, por supuesto, será legalmente válido para acreditar la actuación de dicha persona física, dado que los atributos serán ignorados, algo que eventualmente implicará que el certificado no es "admitido" o "reconocido" para un propósito concreto. De nuevo, en el ejemplo del certificado con atributo de representante que no cumple estas obligaciones, el mismo será admitido igual que cualquier otro certificado de persona física, y no se hará uso del atributo de representación.

Desde este punto de vista, hay que concluir que el enfoque es, en general, conforme con el derecho de la Unión, porque se trata de perfiles (por tanto, de atributos) de uso obligatorio, pero sólo para la admisión o adquisición de los certificados por parte de la Administración General del Estado, que actúa, en este sentido, en el marco de sus potestades de autoorganización. En efecto, nada en el Reglamento eIDAS impide a los diferentes colectivos de usuarios de certificados –para identificación, o para firma y sello– decidir que los certificados puedan tener otros contenidos adicionales, inclusive mediante la definición de un detallado perfil de certificado, en el que consten todas las informaciones que deben emplearse en el mismo; siempre que ello no afecte a la interoperabilidad ni al reconocimiento de dichos certificados.

El posible problema de ausencia de interoperabilidad y reconocimiento se podrá dar si la Administración General del Estado regulase el uso obligatorio de atributos (adicionales a los previstos en el Reglamento eIDAS) en los certificados de firma electrónica de persona física o de sello electrónico de persona jurídica porque ello impediría a los titulares de dichos certificados relacionarse con la Administración, en especial en operaciones transfronterizas. Mientras esto no suceda, no se incumple el Reglamento eIDAS.

Diferente es que la Administración General del Estado sólo admita certificados de sello electrónico para la actuación administrativa automatizada, o de empleado público expedidos por otras Administraciones cuando los mismos no sigan las especificaciones técnicas de su política, sino otras especificaciones establecidas por dichas Administraciones, como por ejemplo una Comunidad Autónoma, o una entidad local, algo que ya hemos visto pueden perfectamente hacer, con el marco legal actualmente

[367] Estas informaciones se incluyen en el campo SubjectAlternativeName, con excepción de los certificados de sede, que deben resultan conformes con las especificaciones del CA/Browser Forum.

[368] Por incumplimiento se puede entender, en este contexto, que el prestador emplee el atributo obligatorio de forma defectuosa (por ejemplo, empleando la sintaxis correcta pero una semántica incorrecta), pero también que un prestador incumpla completamente (por ejemplo, porque emplea una sintaxis definida por el prestador para definir el atributo en cuestión, con la misma semántica o con una semántica diferente).

vigente.

Esto es ciertamente problemático, porque en sentido estricto no supone una infracción del Reglamento eIDAS –ya que, como hemos dicho reiteradamente, las Administraciones no están obligadas a "entender" atributos adicionales contenidos en los certificados, ni a admitir el uso de más certificado que el armonizado en el Reglamento eIDAS, y no de forma absoluta–, pero puede producir el efecto de impedir la circulación de documentos públicos administrativos dentro del territorio nacional, porque aunque el certificado de empleado público sea "admisible" como certificado de persona física (al ignorarse los atributos), puede que no sea efectivamente "admitido" precisamente por no acreditar la condición de empleado público.

Y este es un problema que se puede dar, además, en ambos sentidos, porque igual que la Administración General del Estado puede negarse a admitir un certificado de empleado público que no cumpla con su política, también una Comunidad Autónoma podría negarse a admitir el certificado de empleado público expedido conforme a las especificaciones de la política de la Administración General del Estado. Este riesgo se ha visto parcialmente mitigado por varios motivos: en primer lugar, por el acuerdo tácito de las diferentes Administraciones Públicas de no "regular en contra" de estas especificaciones, dado que ello afectaría negativamente a los prestadores, que han venido solicitando de forma reiterada que las especificaciones fueran únicas para el territorio nacional; en segundo lugar, porque muchas Administraciones han venido empleado el servicio de validación de certificados operado por la Administración General del Estado, por lo que han adquirido certificados compatibles con dicho servicio, en una suerte de adhesión al estándar de la Administración General del Estado; finalmente, por la promoción, en la Norma Técnica de Interoperabilidad de Política de firma y sello electrónico publicada por Resolución de la Secretaría de Estado de Administraciones Públicas, de 27 de octubre de 2016[369], de la adhesión de todas las Administraciones a la Política de la Administración General del Estado frente a la aprobación de una política propia.

Para resolver definitivamente este problema potencial, y en el ya analizado marco del Reglamento eIDAS, se podrían convertir estas especificaciones de certificados electrónicos en simplemente obligatorias, mediante su traslado desde la Política de firma electrónica y de certificados de la Administración General del Estado –que aunque muy importante, no tiene competencias sobre las restantes Administraciones– e incorporación al Esquema Nacional de Interoperabilidad, que en definitiva es una norma reglamentaria, con una base legal más que suficiente y una justificación evidente en el interés general, apropiada para la regulación de estos atributos, con alcance para todas las Administraciones españolas, y sin que deba producir problema alguno que los mismos sean simple y llanamente obligatorios para estas tipologías de certificados.

Obviamente, la eficacia de estos atributos no vinculará a las entidades del sector público de los restantes Estados miembros de la Unión, pero ciertamente un marco legal armonizado facilitará la posible negociación al respecto, posiblemente en una tónica bilateral.

---

[369] Se trata de una novedad en relación con la primera versión de esta Norma Técnica de Interoperabilidad, contenida en la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.

2.1.4.1 El certificado de sede electrónica

Como es sabido[370], la LAE consagró el derecho de los ciudadanos, en el artículo 6.1, a "relacionarse con las Administraciones Públicas empleando medios electrónicos para el ejercicio de los derechos reconocidos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos"; derecho que posteriormente se perfiló en el artículo 6.2 y, en lo que ahora nos interesa, el epígrafe a) del mismo, que establecía que "[a]demás, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos: a) A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas […]".

Estos canales se definían en el anexo I de la LAE, epígrafe e), como "estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc)", en un enfoque ciertamente amplio; y eran también referidos en el artículo 8.1 de la misma ley, aplicable a todas las Administraciones Públicas, que ordenaba que "[l]as Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada", algo que ha dado lugar al denominado "principio de multicanalidad".

Concretaba el epígrafe 2 del propio artículo 8 de la LAE, sólo para la Administración General del Estado, los siguientes canales:

"a) Las oficinas de atención presencial que se determinen, las cuales pondrán a disposición de los ciudadanos de forma libre y gratuita los medios e instrumentos precisos para ejercer los derechos reconocidos en el artículo 6 de esta Ley, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.

b) Puntos de acceso electrónico, consistentes en sedes electrónicas creadas y gestionadas por los departamentos y organismos públicos y disponibles para los ciudadanos a través de redes de comunicación. En particular se creará un Punto de acceso general a través del cual los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles. Este Punto de acceso general contendrá la relación de servicios a disposición de los ciudadanos y el acceso a los mismos, debiendo mantenerse coordinado, al menos, con los restantes puntos de acceso electrónico de la Administración General del Estado y sus Organismos Públicos.

c) Servicios de atención telefónica que, en la medida en que los criterios de seguridad y las posibilidades técnicas lo permitan, faciliten a los ciudadanos el acceso a las informaciones y servicios electrónicos a los que se refieren los apartados anteriores".

[370] Cfr. (Cotino Hueso, 2010), *in toto*.

Nótese que los tres canales, en definitiva, sirven para el acceso remoto y a distancia por el ciudadano a la administración a través de medios electrónicos, acceso que se también podrá realizarse en oficinas de atención presencial o telefónicamente, en este último caso siempre que lo permitan criterios de seguridad.

En el modelo de la LAE, el acceso electrónico del ciudadano a los servicios públicos se debía producir necesariamente mediante la sede electrónica[371], que el artículo 10.1 de dicha ley definía como una "dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias", aclarando el epígrafe i) del Anexo I de la LAE que por dirección electrónica cabía entender el "identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones"[372].

Dado que el legislador nos decía que una sede electrónica era una dirección electrónica accesible por redes de telecomunicaciones –cabe entender que, principalmente, desde Internet–, no quedaba más remedio que identificar la sede electrónica con un espacio públicamente accesible a través de dicha dirección, que en Internet viene determinado por una URL del tipo protocolo://dirección, permitiendo el acceso a los servicios que se presten de acuerdo con dicho protocolo; y siendo el caso más habitual el del protocolo http:// que se emplea para servir páginas web, aunque nada impide el empleo de otros protocolos para la prestación de otros servicios, dado que la LAE viene –supuestamente– impregnada por el principio de neutralidad tecnológica[373]. En efecto, también será sede electrónica aquella accedida a través de ftp:// para el intercambio de ficheros, por ejemplo, en la medida en que corresponda al ejercicio de competencias de las Administraciones Públicas en el marco de procedimientos administrativos.

En este sentido, la sede electrónica es, con independencia del protocolo empleado, un espacio al que accede el ciudadano[374], en el sentido de que es el ciudadano quien se desplaza electrónicamente para iniciar y mantener un intercambio de mensajes, conforme al protocolo correspondiente.

Además, esta sede electrónica debía, conforme al epígrafe 3 del artículo 10 de la LAE, garantizar la identificación del titular de la misma y, por mandato del epígrafe 4 del mismo artículo 10, disponer de sistemas que permitiesen el establecimiento de comunicaciones seguras siempre que fueran necesarias; para lo cual debían utilizar "para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma

---

[371] Con acierto, (Valero Torrijos, 2010, pág. 346) indica que "la sede electrónica no es más que una prolongación virtual de las oficinas administrativas tradicionales". En el mismo sentido, en relación con la sede electrónica judicial, (Valero Torrijos, 2012, pág. 232). Por su parte, (Díaz-Romeral Gómez, 2011, pág. 393) se ha referido a la sede electrónica de la Administración "como su cuerpo electrónico, a modo de proyección en el espacio virtual de la actividad de su sede física". También (Martínez Gutiérrez, 2009) y (Martínez Gutiérrez, 2016a) o (Martín Delgado, 2010) equiparan sede con oficina administrativa.

[372] Sobre la sede, (Martínez Gutiérrez, 2009) considera que el concepto de sede se debería haber hecho equivalente al de concepto de "punto de acceso electrónico", para después indicar que la sede electrónica es la plataforma de la Administración ubicada en el sitio web, asimilando la sede electrónica a la oficina física como medio de relación con los ciudadanos.

[373] Sobre este principio, cfr. (Martínez Gutiérrez, 2009, pág. 375 y ss.) y (Boix Palop, 2010).

[374] Cfr. (Valero Torrijos, 2010, págs. 348-349) y (Valero Torrijos, 2012, págs. 234-235).

electrónica basados en certificados de dispositivo seguro o medio equivalente", según ordenaban los artículos 13.3.a) y 17 de la LAE.

De ello se desprende, necesariamente, que la dirección en qué consistía la sede electrónica hacía uso de un protocolo de comunicaciones seguro, que en el caso de los protocolos de Internet (como HTTP, FTP u otros) era el protocolo SSL o TLS, por lo que no tenía la consideración legal de sede electrónica la que no hiciera uso del mismo[375], al menos para la identificación de la dirección, mediante el correspondiente certificado de dispositivo seguro que, por cierto, no era un certificado de firma electrónica alguno, dado que no se encontraba regulado por la LFE.

En efecto, la LFE sólo se refería a los certificados de firma electrónica (de persona física o de persona jurídica), cuya utilidad se refería, por tanto, sólo a la atribución de la correspondiente actuación al firmante, y, por tanto, no a la función de identificación o autenticación. Tampoco se podía reconducir fácilmente –por no decir que era imposible hacerlo– el "certificado de dispositivo seguro" al que se refería la LAE al concepto de certificado contenido en la LFE, ni tampoco al concepto de dispositivo seguro de creación de firma también previsto en la LFE.

Y estupor causaba que el artículo 17 de la LAE autorizase, además, el uso de un "medio equivalente", referencia que resultaba ambigua, dado que la equivalencia podía predicarse en dos sentidos; esto es, podía entenderse que la LAE autorizaba el uso de un medio equivalente a un certificado de dispositivo seguro, pero también que autorizaba el uso de un certificado basado en un medio equivalente a un dispositivo seguro; y causaba estupor porque si la LFE no define un "dispositivo seguro" para un uso diferente al de la firma electrónica, ¿cómo se podía determinar si un medio diferente era equivalente o no? En cualquier caso, la segunda interpretación resultaría más correcta, a tenor del funcionamiento técnico de los protocolos de seguridad subyacentes a la sede electrónica, a los que nos acabamos de referir, y que exigen certificado en todo caso.

En todo caso, sólo partiendo de la consideración de la sede como espacio seguro se podía comprender que el epígrafe 2 del artículo 10 de la LAE ordenase que "el establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma".

Y nótese también que la LAE, aunque sólo en el ámbito de la Administración General del Estado, se refería al punto de acceso electrónico (y al punto de acceso general electrónico), como una sede electrónica[376], aunque no se indicase qué especialidad presentaba con respecto a cualquier otra sede, excepción hecha del punto de acceso general, que contenía la relación de servicios a disposición de los ciudadanos y el acceso a los mismos, debiendo mantenerse coordinado, al menos, con los restantes puntos de acceso electrónico de la Administración General del Estado y sus Organismos Públicos.

---

[375] Sin embargo, nada más alejado de la realidad, en que se han aprobado muchas sedes electrónicas que no hacían uso de estos protocolos, "falsas" sedes electrónicas que no cumplían con las garantías mínimas de seguridad legalmente exigibles.

[376] (Valero Torrijos, 2010, pág. 354) considera que "el punto de acceso electrónico puede consistir en una sede electrónica o, por el contrario, concebirse como una vía de acceso a las sedes electrónicas de múltiples Administraciones Públicas o, en su caso, departamentos de una misma entidad". Esta interpretación, que parece haber sido plenamente acogida y potenciada en la LRJSP, refuerza la noción de sede electrónica como "lugar".

El ya mencionado RDLAE desarrolló estas previsiones, en línea con la interpretación que hemos realizado de la LAE y, por tanto, partiendo de que en todo caso era obligatorio el uso de un certificado, fuera de dispositivo seguro o de medio equivalente a este dispositivo seguro.

En este sentido, el artículo 18.1 del RDLAE definió los contenidos del que denominó "certificado de sede electrónica", incluyendo la descripción del tipo de certificado, que debía incluir la denominación literal de "sede electrónica"; el nombre descriptivo de la sede electrónica; la denominación del nombre del dominio; el número de identificación fiscal de la entidad suscriptora; y la unidad administrativa suscriptora del certificado.

Por su parte, el epígrafe 2 del mismo artículo 18 del RDLAE limitó el uso de estos certificados exclusivamente a la "identificación de la sede, quedando excluida su aplicación para la firma electrónica de documentos y trámites", y finalmente el epígrafe 3 del propio artículo, remitió al Esquema Nacional de Seguridad –previsto en el artículo 42 de la LAE– para la determinación de "las características y requisitos que cumplirán los sistemas de firma electrónica, los certificados y los medios equivalentes que se establezcan en las sedes electrónicas para la identificación y garantía de una comunicación segura".

No fue, sin embargo, este Esquema[377], aprobado por Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica (en adelante, RDENS), el que regularía estas cuestiones. En efecto, aunque el artículo 38 del RDENS indica que "la seguridad de las sedes […], se regirán por lo establecido en el Esquema Nacional de Seguridad", en el mismo no se contiene norma alguna al respecto de estas características y condiciones[378].

En realidad, el contenido detallado de estos certificados fue establecido como parte de la anteriormente presentada Política de firma electrónica y de certificados de la Administración General del Estado, en concreto mediante su Anexo II.

Con la reforma del sector público este sistema ha sufrido leves retoques, refiriéndose la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP) a la sede electrónica en términos similares a la LAE. Su artículo 38.1 continúa caracterizando la misma como "aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias", manteniéndose los dos requisitos, anteriormente indicados, de identificación del órgano titular de la sede (epígrafe 3 del artículo 38) y del establecimiento de comunicaciones seguras (epígrafe 4 del artículo 38).

Como novedad significativa sobre el régimen de la LAE, el epígrafe 6 del artículo 38 se refiere, ciertamente con mayor corrección técnica, a la utilización imperativa de certificados cualificados de autenticación de sitio web o medio equivalente; los primeros

[377] Sobre esta norma, puede verse el completo análisis, especialmente interesante en cuanto a las normas e instrumentos para su desarrollo y aplicación, de (Fondevila Antolín, 2016, pág. 598 y ss.).

[378] Esto no significa que las restantes cuestiones de seguridad de la sede electrónica no se regulen en el RDENS, y en sus guías y normas de desarrollo. Al efecto, el epígrafe 7 del Anexo II del RDENS indica que "[l]a interpretación del presente anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas CCN-STIC correspondientes a la implementación y a diversos escenarios de aplicación tales como sedes electrónicas, […], atendiendo el espíritu y finalidad de aquellas".

se encuentran regulados en el artículo 45 y el anexo IV del Reglamento eIDAS, a que antes nos hemos referido; mientras que el medio equivalente se deberá intentar definir por analogía con los citados certificados cualificados de autenticación de sitio web, algo que en todo caso supone un incremento apreciable de la seguridad.

Por tanto, se puede apreciar cómo el legislador nacional ha procedido a alinearse con el Reglamento eIDAS que, como hemos visto, regula este mecanismo de forma uniforme, aunque desde luego parece criticable que se permita acudir a un medio equivalente.

2.1.4.2 El certificado de sello electrónico para las entidades del sector público

Una de las novedades importantes en la LAE fue la denominada "actuación administrativa automatizada" en el ejercicio de las competencias, que debía ser autenticada empleando alguno de los "sistemas de firma electrónica" previstos al efecto en el artículo 13.3.b) y 18 de la propia ley.

Entre dichos sistemas se encontraba el "[s]ello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica" (artículo 18.1.a) de la LAE), instrumento en cierto modo análogo a la firma electrónica prevista en la LFE, pero para su uso de forma completamente desatendida, como se desprendía de la propia definición de la actuación administrativa automatizada contenida en el Anexo de la LAE, en cuya virtud la misma era la "actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular".

En cuanto ahora nos interesa, como se puede ver, el artículo 18.1.a) de la LAE se remitía al uso de un certificado electrónico que reuniese los requisitos exigidos por la legislación de firma electrónica, en una referencia de difícil aplicación, dado que la LFE –como ya hemos visto en el caso de certificado para la sede electrónica– dicha norma no contenía ninguna prescripción directamente aplicable a este instrumento, algo que obligaba a realizar una interpretación forzada de los requisitos aplicables a los certificados de firma electrónica, pero con importantes dudas: ¿debían, por ejemplo, aplicarse analógicamente los requisitos de los certificados ordinarios o de los certificados reconocidos?; de otro lado, ¿dicha analogía se debía construir partiendo de los certificados de persona física o, por el contrario, de los certificados de persona jurídica?

El propio artículo 18.2 de la LAE ordenaba que estos certificados incluyeran "el número de identificación fiscal y la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos", en una dicción que hacía opcional la inclusión de los datos de identidad personal del titular de un órgano administrativo, lo cual se debía valorar de forma positiva, en especial porque un certificado de sello electrónico de órgano que no incluyese los datos del titular no debía ser revocado cuando se produjera un cambio de titularidad, algo razonable si nos estamos refiriendo a la identidad a efectos del ejercicio automatizado de la competencia; pero que alejaba enormemente este certificado de los previstos en la LFE, que en ambos casos exigían de forma imperativa la inclusión de los datos de identidad del firmante (en caso de certificado de persona física) o del custodio de los datos de creación de firma (en caso de certificado de persona jurídica).

El epígrafe 3 del mismo artículo 18 de la LAE también ordenaba que "[l]a relación de

sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos" y que "cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos", provisiones claramente necesarias por las insuficientes reglas de la LFE en este sentido.

Como ya hemos visto en el caso del certificado de sede electrónica, el RDLAE reguló, aunque sólo para el ámbito de la Administración General del Estado, los contenidos de los certificados de sello electrónico, indicando su artículo 19.2 que los mismos debían incluir la descripción del tipo de certificado, con la denominación "sello electrónico"; el nombre del suscriptor y el número de identificación fiscal del suscriptor", debiéndose entender por suscriptor a la entidad que adquiriese el certificado, que en su caso será el órgano administrativo en cuestión, lo cual generó alguna disfunción en algunos casos[379].

De nuevo, como sucedió en el caso del certificado de sede electrónica, también en el caso del certificado de sello electrónico estableció el artículo 19.3 del RDLAE que "[e]l modo de emitir los certificados electrónicos de sello electrónico se definirá en el Esquema Nacional de Seguridad", algo que no ha sucedido hasta la fecha.

Más interesante resulta la norma, aunque puramente auto-organizativa, contenida en el epígrafe 1 del mismo artículo 19 del RDLAE, relativa a la necesidad de que los sellos electrónicos sean creados "mediante resolución de la Subsecretaría del Ministerio o titular del organismo público competente, que se publicará en la sede electrónica correspondiente y en la que deberá constar:

a) Organismo u órgano titular del sello que será el responsable de su utilización, con indicación de su adscripción en la Administración General del Estado u organismo público dependiente de la misma.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y procedimientos en los que podrá ser utilizado".

Estas informaciones son precisas, de un lado, para poder emplear el "sistema de firma", dado que el mismo no se encuentra técnicamente normalizado –en especial, por la extraña referencia a la LFE–, pero también para determinar los usos para los que se encuentra autorizado este sistema; lo que justifica la ampliación de la publicidad prevista en la LAE. Y no es en absoluto desdeñable la norma que centraliza la toma de decisión sobre la creación de estos sellos, en un nivel de decisión ciertamente elevado, lo que permite evitar el descontrol que de otro modo podría darse en la creación de sellos electrónicos, que podría llegar al extremo de que cada órgano pudiera decidir si deseaba tener o no un sello electrónico.

Con la aparición de la LRJSP, el régimen expuesto se ha visto ligeramente afectado, sin

[379] En concreto, dada la exigencia de incluir este NIF, trasladada por extensión de los perfiles de CertiCA a que ya nos hemos referido, a todas las Administraciones Públicas, se planteaban problemas de emisión de certificados a órganos que no disponían de NIF, en algún caso por la negativa de la Administración tributaria a asignarles dicho número, por negarles la condición de órgano administrativo, como sucedió en diversos casos de secretarias municipales, situación que afortunadamente ha solventado la disposición adicional octava del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.

duda por influencia del Reglamento eIDAS, que ha conducido a la regulación separada de las funciones de identificación y "firma" del sello electrónico.

En primer lugar, el artículo 40.1 de la LRJSP autoriza que "[l]as Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica", en una dicción muy similar a la anteriormente contenida en la LAE, pero con la importante diferencia que, a la fecha de entrada en vigor de la LRJSP (el 2 de octubre de 2016) esa referencia debe entenderse realizada al Reglamento eIDAS, no a la LFE, dado que el Reglamento, como ya hemos visto, regula el certificado de sello electrónico. Además, a diferencia de la LAE, la LRJSP ordena que dicho certificado sea cualificado, algo que implica sujeción plena a las reglas del Reglamento eIDAS que, al menos en parte, ya conocemos.

Resulta llamativo que esta regulación del sello electrónico se contenga en un artículo titulado "sistemas de identificación de las Administraciones Públicas", dado que todos los certificados electrónicos tienen la función de identificar, y muy especialmente tienen esa función los certificados de sede electrónica a que nos acabamos de referir, y también la tienen los certificados que se expidan a las autoridades y empleados públicos que actúan en ejercicio las competencias y funciones que tienen atribuidas; función identificativa que, en el caso del sello, ha sido objeto de crítica por la doctrina[380].

Cabe entender, sin embargo, que el legislador ha querido explicitar un tipo de certificado que se puede emplear en aquellos casos en que una Administración debe identificarse frente a terceros –normalmente, estos terceros serán otras Administraciones– de forma automatizada o desatendida, como por ejemplo cuando solicita a otra Administración que le remita datos o documentos, al amparo de lo establecido en el artículo 28 de la LAC y del artículo 155 de la LRJSP[381], algo que encaja perfectamente en el uso típico del sello electrónico previsto por el Reglamento eIDAS.

El artículo 40.1 de la LRJSP mantiene, no obstante, las reglas originales de la LAE respecto a estos certificados, por lo que "[e]stos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos", texto que resulta ahora redundante en cuando al número de identificación fiscal y denominación (de la persona jurídica), por tratarse de datos de inclusión ya prevista en todo certificado de sello electrónico, pero no en cuanto a la identificación del órgano o de la persona titular del mismo, que serían atributos

[380] En concreto, (Bauzá Martorell, 2016, pág. 773) considera que "la Administración Pública no es directamente identificable en el tráfico jurídico, sino que su identificación viene derivada de manera indirecta por la propia del órgano administrativo que la representa y compromete", por lo que "puede apreciarse esta aparente disfunción en el propio contenido del precepto que, por un lado se refiere a la identificación de la Administración, y por otro alude expresamente al titular del órgano administrativo en los requisitos de contenido del sello electrónico", concluyendo que "la convivencia de ambos sistemas, el de la teoría del órgano en las comunicaciones físicas, y el de sello electrónico en la e-Administración, provocará por razones obvias problemas de seguridad jurídica, que pueden afectar a la validez y eficacia de los actos administrativos y de las solicitudes de los particulares" (Bauzá Martorell, 2016, pág. 775), queja que parece más aplicable al artículo 42 de la LRJSP, al que nos referimos más adelante (cfr. el epígrafe 5.2.3.1 de este trabajo).

[381] Es cierto que esta posibilidad se puede considerar como una actuación administrativa automatizada, lo que hace dudosa la necesidad de esta diferenciación.

adicionales de obligada inclusión en el certificado de sello electrónico. Nótese que, además, y a diferencia de la LAE, en la LRJSP parece obligatoria la inclusión de los datos de la persona titular, cuando el certificado se expida a un concreto órgano administrativo, al que en todo caso parece criticable, dado que dicha persona titular no actúa en ningún momento y porque en caso de cese de dicha persona se deberá revocar el certificado, algo absurdo a la luz de los automatismos en que se emplean estos certificados, que no dependen realmente de que el órgano tenga, en cierto momento, vacante la titularidad.

Asimismo, también conforme al artículo 40.1 de la LRJSP, "[l]a relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos", como se había ya previsto en la LAE, previsión que, de nuevo, ha quedado parcialmente obsoleta a la luz del Reglamento eIDAS, que ya viene a regular las características de los citados certificados y de los prestadores que los expiden; y "[a]demás, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos", previsión ésta última que podía tener sentido en la LAE pero desde luego no en la LRJSP, alineada con el Reglamento eIDAS que, como veremos posteriormente, ha regulado la validación de las firmas y los sellos electrónicos[382]. En este sentido, y como ha sucedido en otros ordenamientos que habían impuesto esta obligación, como el francés[383], se debería haber procedido a adecuar este aspecto.

Por su parte, el artículo 42.a) de la LRJSP se refiere, para el ejercicio de la competencia en actuación administrativa automatizada, al "[s]ello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica", en una referencia que debe entenderse realizada, de nuevo, al Reglamento eIDAS, y resultando aplicables los comentarios anteriormente realizados, dado que nos encontramos ante un mismo certificado que, como ya sabemos, respalda la realización de ambas funciones, identificación y "firma"[384].

---

[382] Cfr. el epígrafe 4.3.2 de este trabajo.

[383] En efecto, el artículo 10 de la *Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*, en cuya virtud se establecía que los certificados emitidos a las autoridades administrativas y sus agentes (entre los que se encontraba el agente automatizado, que disponía de sello electrónico) debían ser validados por el Estado en los términos establecidos por Decreto, ha sido derogado por el artículo 3 de la *Ordonnance n° 2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques*. Esta norma se dicta al amparo de la habilitación contenida en el artículo 86.II.2º de la *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*, al objeto de adaptarse al marco legal del Reglamento eIDAS, con la fundamentación de que esta validación no se emplea en la actualidad y ya no resulta necesaria tras la aprobación del Reglamento eIDAS, como indica el *Rapport au Président de la République relatif à l'ordonnance n° 2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques*.

[384] Resulta sorprendente que la LRJSP continúe refiriéndose al sello electrónico como "sistema de firma electrónica", confusión inexplicable después de la aprobación y entrada en vigor del Reglamento eIDAS. Cfr. al respecto, el epígrafe 4.1.1.2 de este trabajo.

2.1.4.3 El certificado de "empleado público"

Junto a los certificados para la sede electrónica y para el sello electrónico de actuación administrativa automatizada, la LAE previó también la posibilidad de que el personal al servicio de la Administración pudiera disponer de sistemas de firma electrónica, en los términos previstos en el artículo 19.

Dicho artículo autorizó, en su epígrafe 2, a las Administraciones a "proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios"[385], mientras que, en su epígrafe 3, indica que "[l]a firma electrónica basada en el Documento Nacional de Identidad podrá utilizarse a los efectos de este artículo".

Como ya hemos avanzado, entre dichos sistemas de firma electrónica se encontraban, lógicamente, aquellos respaldados por certificados –en su caso, reconocidos–, por lo que este personal podía, también, identificarse empleando el certificado, lo que de hecho podía suponer el aportar un nivel de garantía superior al disponible cuando se emplea el soporte papel[386].

Una de las dudas importantes que suscitaba este artículo venía dada por la expresión "personal al servicio de la Administración", que podía entenderse como estrictamente aplicable a dicho personal, con apoyo en la entonces recién aprobada Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público[387] (en adelante, LEBEP), cuyo título II precisamente se titulaba "clases de personal al servicio de las Administraciones Públicas", noción que se asimilaba inmediatamente en el artículo 8 de la LEBEP con las de "empleados públicos" y que englobaba a los funcionarios de carrera, los funcionarios interinos, el personal laboral, ya sea fijo, por tiempo indefinido o temporal y el personal eventual, sin perjuicio de las especificidades del personal directivo.

De admitirse esta interpretación, nos hubiéramos encontrado ante la no sujeción al artículo 19 de la LAE de las personas físicas sin dicha condición de empleado público, principalmente los titulares de los órganos administrativos unipersonales, o los miembros

---

[385] (Bauzá Martorell, 2016, págs. 785-786) opina que "carece de sentido articular un sistema de firma específico para el titular del órgano o cualquier empleado público cuando actúa en el ejercicio de una función pública, extremo que a nuestro juicio puede generar confusión y desde luego en nada simplifica, todo lo contrario, las comunicaciones públicas". Sin embargo, el autor no considera la problemática derivada de la imposición del uso, a las autoridades o empleados públicos, de su propio certificado para identificarse (o para firmar), que procede –entre otros factores– de la voluntariedad de obtención del citado certificado, incluso en el caso del DNI-e, como luego veremos (cfr. el epígrafe 2.2.1). Sobre la conveniencia de los certificados corporativos frente al uso del DNI-e, cfr. (Alamillo Domingo & Urios Aparisi, 2010, págs. 684-685), extrapolable a otros certificados estrictamente personales.

[386] Como ha indicado (Valero Torrijos, 2013, pág. 75), "si los certificados de firma electrónica que se utilizan permiten acreditar la condición subjetiva del titular del órgano o su permanencia en un determinado puesto de trabajo –ya sea a través de los denominados certificados de *atributos* o de sistemas dinámicos de gestión de identidad–, dicha circunstancia se incorporará al documento a través, en su caso, de la declaración de un tercero, esto es, el prestador de servicios de certificación; lo que no sucede si el mismo documento se genera en soporte papel, donde la condición subjetiva del autor la declara él mismo, salvo en los supuestos en que deba incorporarse el visto bueno de otro sujeto, como sucede singularmente con los acuerdos de los órgano colegiados".

[387] Norma que ha sido derogada por el hoy vigente Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

de los órganos colegiados. Ello no debía tener el efecto, sin embargo, de impedir la provisión de certificados electrónicos a dichas personas, sino únicamente la necesidad de hacerlo mediante la correspondiente disposición de carácter general[388], dada la potestad de auto-organización de que goza la Administración, con máxima intensidad en el caso de los órganos de gobierno, en especial los colegiados[389].

Por su parte, el RDLAE reguló en su artículo 22 las características de estos certificados, formalmente para el ámbito de la Administración General del Estado y de sus organismos públicos, aunque, como en los restantes casos, materialmente[390] se aplique a todas las Administraciones Públicas mediante su extensión a través del Anexo a la Política de firma electrónica.

Así, el epígrafe 3 de dicho artículo prevé los contenidos mínimos de estos certificados; a saber, "a) Descripción del tipo de certificado en el que deberá incluirse la denominación «certificado electrónico de empleado público».

b) Nombre y apellidos del titular del certificado.

c) Número del documento nacional de identidad o número de identificación de extranjero del titular del certificado.

d) Órgano u organismo público en el que presta servicios el titular del certificado.

e) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado".

Por su parte, el epígrafe 4 del mismo artículo, incorporado por el artículo único.Tres del Real Decreto 668/2015, de 17 de julio, dictado – en cuanto nos interesa ahora – para "permitir el certificado electrónico con garantías de seguridad para los empleados públicos al servicio de la Administración General del Estado y de sus organismos públicos vinculados o dependientes, cuando, por razón de competencia, utilicen información

---

[388] Véase, en este sentido, el excelente ejemplo de la Comunidad Autónoma de Cantabria, contenido en el Decreto 42/2017, de 22 de junio, por el que se regula el Régimen Jurídico de la Autorización y Uso de la firma electrónica de autoridades y empleados públicos de la Administración de la Comunidad Autónoma de Cantabria y su Sector Público, perfectamente alineado con el Decreto 31/2015, de 14 de mayo, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria. Se trata de una de las escasas normas que regulan de forma adecuada estas cuestiones – sin duda por el impulso que al mismo ha dado su principal autor, Jorge Fondevila, desde la asesoría jurídica de la Consejería, resultando ciertamente incomprensible el casi nulo interés de las restantes Administraciones Públicas en atención a la importancia de la cuestión, máxime a la vista del artículo 14.2.e) de la LPAC.

[389] La LRJSP no resulta aplicable a los órganos colegiados de gobierno, conforme indica su disposición adicional vigesimoprimera, por lo que habrá que estar a la normativa de cada Administración. Ello hace especialmente relevante la necesidad de proceder a modificar el Reglamento Orgánico Municipal, en el caso de las entidades que integran la Administración local, sin perjuicio de lo establecido por el artículo 3.2 del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional, que incide en el funcionamiento de los órganos colegiados por vía de regulación del cuerpo de habilitados nacionales, que ha sido objeto de crítica por (Campos Acuña, 2018) – versión electrónica.

[390] Se exceptúa de lo dicho el contenido del epígrafe 1 del citado artículo 22, que ordena que los "certificados facilitados específicamente a sus empleados por la Administración General del Estado o sus organismos públicos vinculados o dependientes sólo podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen o para relacionarse con las Administraciones públicas cuando éstas lo admitan", por tratarse de una previsión puramente auto-organizativa.

clasificada o estén afectos a la seguridad pública o a la defensa nacional", establece un régimen especial de contenidos en relación con "los certificados que se utilicen en aquellas actuaciones que realizadas por medios electrónicos afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización"[391].

Cuando se den las anteriormente indicadas circunstancias, "los prestadores de servicios de certificación podrán consignar en el certificado electrónico, a petición de la Administración solicitante, un seudónimo", por lo que "tendrán idéntico uso, capacidad y funcionalidad que el certificado electrónico de empleado público y al menos, el siguiente contenido:

a) Descripción del tipo de certificado en el que deberá incluirse la denominación «certificado electrónico de empleado público con seudónimo».

b) Seudónimo del titular del certificado, consistente en su número de identificación profesional u otro indicador proporcionado por la Administración correspondiente.

c) Órgano u organismo público en el que presta servicios el titular del certificado.

d) Número de identificación fiscal del órgano u organismo público en el que presta sus servicios el titular del certificado".

Como se puede ver, en este caso nos encontramos ante un certificado con la misma utilidad que el certificado de empleado público (por tanto, con la capacidad de sustentar su firma electrónica, lo que implica necesariamente su identificación), pero sin que aparezca la identidad personal "real", sino que la misma se oculta tras el seudónimo, que no es libre, sino que debe corresponder con un número asignado por la Administración, que normalmente se corresponderá con el número profesional.

Se trata de una norma que debe ser interpretada de forma restrictiva, a tenor de la propia justificación ofrecida por el regulador, dado que puede afectar al derecho del interesado "a identificar a las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos" reconocido en el artículo 53.1.b) de la LPAC.

Aunque es cierto que el inciso final del epígrafe 4 del artículo 22 del RDLAE prevé que "[l]os órganos judiciales y otros órganos y personas legitimadas podrán solicitar que se les revele la identidad de los firmantes con certificado electrónico de empleado público con seudónimo, en los casos previstos en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal", en cuyo caso "el prestador de servicios de certificación actuará de conformidad con lo previsto en la Ley 59/2003, de 19 de diciembre", lo cierto es que para la persona interesada supone una barrera a la necesaria transparencia en la instrucción del procedimiento administrativo, que pueden existir discrepancias acerca de su consideración como "persona legitimada" a estos

[391] Se trata de una disposición dictada partiendo de lo establecido en el artículo 4.4 de la LFE, que prevé que "[l]a utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica", aunque posteriormente no menciona dicha normativa, sino únicamente la posibilidad de uso de seudónimos. Sobre esta cuestión, cfr. el epígrafe 6.1.1 de este trabajo.

efectos, y que la referencia al artículo 11.2 de la LOPD puede ser claramente limitativa[392].

El Anexo II de la Política de firma electrónica de la Administración General del Estado, que contiene los perfiles de certificados, establece reglas específicas respecto a estos certificados, debiéndose incluir obligatoriamente la organización a la que pertenece el empleado, el atributo de seudónimo (que deberá incluir el número de identificación profesional correspondiente), y el nombre común (con un formato concreto que facilita la lectura de los datos correspondientes por parte de las personas que visualizan un certificado); y, opcionalmente, se podrá incluir el cargo correspondiente (como, por ejemplo, subinspector).

La aprobación de la LRJSP vino, de otro lado, a elevar a rango de ley formal esta última posibilidad de certificado de empleado público con seudónimo, al autorizar en su artículo 43.2 que "[p]or razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el número de identificación profesional del empleado público", en una dicción bastante más restrictiva que la prevista en el artículo 22.4 del RDLAE que acabamos de ver, y que podría suponer una futura reforma del mismo.

2.1.4.4 El certificado de persona física representante

Finalmente, y también en el marco del artículo 24 del RDLAE anteriormente indicado, el Anexo II de la Política de firma electrónica de la Administración General del Estado ha establecido perfiles y reglas de política específicas para dos certificados, correspondientes a la persona física representante de una persona jurídica y a la persona física representante de una entidad sin personalidad jurídica.

Como es fácil de intuir, la particularidad de estos certificados consiste en la acreditación de la representación que ostenta una persona, con base en la previsión legal expresa a la que anteriormente hemos tenido ocasión de referirnos[393], pero con determinadas especialidades. Y es que, aunque la legislación reguladora del servicio de expedición de certificados cualificados de firma electrónica permite la inclusión (voluntaria) de atributos que permiten indicar la representación, dicha normativa no define cómo debe procederse a dicha inclusión; esto es, se prevé la posibilidad de indicar que una persona física es representante de otra persona, pero no se desarrolla técnicamente cómo debe hacerse dicha indicación, por lo que diferentes prestadores pueden emplear diversas sintaxis para la representación de esta información.

Para evitar este problema, que por otra parte se podría resolver sin mayor dificultad mediante la intervención del organismo de supervisión –seguramente, promoviendo una norma técnica española, o incluso mediante instrucciones de cumplimiento obligatorio, a partir de la correspondiente previsión reglamentaria–, y en el marco de la desaparición de los certificados de persona jurídica previstos con anterioridad al Reglamento eIDAS, se regulan estos dos casos de representación para las relaciones, al menos, con las

[392] En efecto, en dicho epígrafe se enumeran los casos en que no será preciso el consentimiento para la cesión de los datos personales, de los cuales posiblemente sólo resulte aplicable precisamente que la cesión se encuentre prevista en una ley, algo que no siempre sucederá, en especial si se realiza una aplicación generosa de esta posibilidad.

[393] Cfr. el epígrafe 2.1.2.1 de este trabajo.

Administraciones Públicas españolas[394].

En primer lugar, los perfiles definen cómo debe incluirse, desde el punto de vista técnico, la información de la representación, incluyendo la identidad del representado y los datos acreditativos de la citada representación. En segundo lugar, es necesario hacer notar que ambos perfiles exigen que el representante disponga de poderes ilimitados para actuar en nombre del representado, restricción que se impone a los efectos de no tener que verificar el concreto apoderamiento, y que resulta razonable, dado que, en caso contrario, ya se podría realizar la actuación comprobando el apoderamiento mediante cualesquiera de los mecanismos previstos en la legislación vigente[395].

Estos dos casos no agotan, desde luego, todas las posibilidades de representación, y, en concreto, no se ha definido el caso de la persona física representante de otra persona física, algo que resulta criticable desde el punto de vista de estas personas, que también se deben relacionar con la Administración. Nos estamos refiriendo tanto a personas que no tienen capacidad de obrar, o la tienen limitada, como a personas que, teniendo capacidad de obrar, deciden conceder apoderamiento a terceros. Es cierto que, siguiendo la misma lógica que los restantes certificados de representante, debería tratarse de un representante ilimitado, algo que normalmente no sucederá, pero al menos en esos casos se debería admitir.

2.2 LOS SERVICIOS PÚBLICOS DE IDENTIFICACIÓN ELECTRÓNICA EN ESPAÑA

La identificación electrónica de las personas ha sido objeto de tratamiento jurídico en una variedad de instrumentos de derecho público, principalmente sustentados en la legislación de administración electrónica, con un enfoque limitado de uso en dicho sector, con la sola excepción del DNI electrónico, que constituye un sistema de identificación electrónica de carácter autónomo, y carácter universal.

En efecto, la identificación electrónica –y su correlato, que es la autenticación–, aparece mencionada en una importante cantidad de normas jurídicas españolas, generalmente al objeto de imponerla como requisito para la realización de una actuación, bien sea por parte del ciudadano cuanto de la Administración, permitiéndose el uso de diversos medios técnicos para ello, pero es más extraño, sin embargo, encontrar definiciones legales referidas a la identificación electrónica, en especial desde una óptica de aplicación general.

Quizá las definiciones de identificación y autenticación electrónicas de carácter más transversal que, hasta la aprobación del Reglamento eIDAS, hemos podido encontrar en el ordenamiento jurídico español sean las contenidas en la legislación de protección de datos de carácter personal, dado que las mismas son aplicables con carácter general, aunque las mismas se realicen a los efectos de la aplicación de las obligaciones de

[394] Nada impide a las entidades del sector público de otros Estados miembros de la Unión Europea el uso de estos certificados, ciertamente, siempre que decidan "comprender" el contenido adicional, definido en el perfil correspondiente.

[395] Entre dichos mecanismos, encontramos la remisión de copia electrónica auténtica del poder notarial, conforme a lo previsto en la legislación notarial, tras la reforma de la Ley 24/2001, de 27 de diciembre, o el registro electrónico de apoderamientos regulado en el artículo 6 de la LPAC.

seguridad referidas a los citados datos de carácter personal[396], y no en relación con las actuaciones de identificación realizadas frente a terceros, por lo que su utilidad es más bien escasa a los efectos que nos interesa.

Por ello, seguramente las definiciones de identificación y autenticación electrónicas contenidas en el Reglamento eIDAS, que ya conocemos[397], incorporadas directamente al ordenamiento jurídico español en virtud de la aplicación directa de dicha norma jurídica, vayan a ser las más relevantes, en especial por su efecto regulador indirecto[398].

Si dirigimos nuestra mirada al Estado español, parece innegable que el DNI electrónico viene siendo la principal estrategia española de identificación electrónica, estrategia que se ha complementado con otros medios, entre ellos el proyecto CERES de la FNMT-RCM, el recientemente aprobado Cl@ve, y otras iniciativas, en el ámbito autonómico y local, iniciativas que, como se ha avanzado, encuentran su base jurídica en la normativa de administración electrónica y en la normativa reguladora de los servicios de confianza, aunque sin limitarse en su uso exclusivamente a las relaciones con el sector público.

Esta segunda categoría de sistemas constituye una colección de verdaderos servicios públicos de identificación electrónica, que complementan los servicios (privados o públicos) de expedición de certificados de firma y sello electrónico, a que antes nos hemos referido detalladamente.

2.2.1 El Documento Nacional de Identidad electrónico

El DNI electrónico se definió inicialmente en el artículo 15.1 de la LFE, que estableció que "el documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos", definición que no se ha incorporado –acertadamente, en mi opinión– en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

Como se puede ver, en el caso del DNI electrónico se diferencia nítidamente entre la función de identificación electrónica y la de firma electrónica[399]; en este segundo caso, en virtud del artículo 16.1 de la propia LFE se impone a los órganos competentes para la expedición del DNI electrónico el cumplimiento de las obligaciones de los prestadores de

---

[396] Más en concreto, el artículo 5.2.h) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD), define la identificación como el "procedimiento de reconocimiento de la identidad de un usuario", mientras que la autenticación sería, de acuerdo con el mismo artículo 5.2.b), el "procedimiento de comprobación de la identidad de un usuario"; donde el usuario es el "sujeto o proceso autorizado para acceder a datos o recursos" (artículo 5.2.p) del RDLOPD).

[397] Cfr. el epígrafe 1.2.1 de este trabajo.

[398] Nótese que esta incorporación directa, sin embargo, lo es únicamente a los efectos del propio Reglamento eIDAS, al que nos referimos con detalle posteriormente, por lo que en diversos Estados miembros se han incorporado estas definiciones también en la Ley nacional.

[399] (Martínez Nadal, 2009, pág. 277) llama la atención sobre el hecho de que el DNI electrónico es algo más que el DNI tradicional, al incorporar la firma electrónica, por lo que "la transcendencia de la posesión y, en especial de la pérdida, de uno u otro documento identificativo no es la misma; de ahí la importancia de una custodia adecuada por parte del titular, que deberá ser instruido convenientemente por la administración al respecto".

servicios de certificación[400], algo que sólo tiene sentido, en efecto, porque se trata de dos instituciones diferenciadas, y con efectos jurídicos también diferentes.

El DNI electrónico es, pues, la versión electrónica del documento nacional de identidad, y se encuentra regulado en la actualidad en los artículos 8 y siguientes de la reciente Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (en adelante, "LOPSC/2015")[401], así como en el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica[402] y, finalmente, la Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior[403].

El artículo 8.1 de la LOPSC/2015 determina, en primer lugar, que "el Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a éstos otorgan las leyes, así como suficiente valor por sí solo para la acreditación de la identidad y los datos personales de su titular", estableciendo un régimen claramente público y monopolístico[404], reservado al Estado y, más en concreto, al Ministerio del Interior, que la ejerce a través de la Dirección General de la Policía[405]; monopolio derivado de la conexión entre el DNI y la función de seguridad pública, de la cual es un instrumento de implementación.

De acuerdo con el apartado 2 del artículo 8 de la LOPSC/2015, el Documento Nacional de Identidad se sustenta en una tarjeta soporte, que "incorporará las medidas de seguridad necesarias para la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación"[406].

El primer elemento diferenciador del DNI como sistema de identificación electrónica, es la obligación[407] de los nacionales españoles de obtenerlo a partir de los catorce años (artículo 9.1 de la LOPSC/2015), por lo que se trata del único sistema de identificación electrónica de carácter legalmente obligatorio para los citados nacionales; sin embargo, y

---

[400] Con la excepción de constituir la garantía económica de 3.000.000 euros prevista en el artículo 20.2 de la LFE; obligaciones que hoy deben entenderse referidas a las de los prestadores de servicios de confianza regulados en el Reglamento eIDAS.

[401] Que deroga la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, que regulaba el documento nacional de identidad en sus artículos 9 y siguientes.

[402] Modificado por Real Decreto 1586/2009, de 16 de octubre, por Real Decreto 869/2013, de 8 de noviembre y por Real Decreto 414/2015, de 29 de mayo.

[403] Modificada por Orden INT/665/2015, de 27 de marzo.

[404] No significa este monopolio que no puedan existir otros medios de identificación electrónica, ofrecidos por otras entidades públicas o privadas, inclusive al amparo de la normativa reguladora de los servicios de confianza, como posteriormente veremos.

[405] Cfr. los artículos 10 de la LOPSC/2015, y 12.1.A.a) de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. También el artículo 3 del Real Decreto 1553/2005.

[406] Incluyendo el empleo de impresión de imagen láser cambiante (CLI) sobre el soporte de policarbonato o la protección de los datos biométricos mediante zonas seguras protegidas criptográficamente, por ejemplo. Para un detalle completo de las tecnologías de seguridad del DNI electrónico, cfr. (Sarwat, 2010, pág. 121 y ss.)

[407] Para (Heichlinger & Gallego, 2010, p. 62), éste es uno de sus factores de éxito.

como se desprende del artículo 9.2 del Real Decreto 1553/2005, la funcionalidad de firma electrónica provista por el DNI electrónico es voluntaria para la persona física.

Por su parte, el artículo 8.3 de la misma LOPSC/2015 concreta, en relación con el artículo 15 de la LFE, que "el Documento Nacional de Identidad permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica"[408], limitando la posibilidad de estos usos electrónicos a los restantes titulares, como los menores de edad no emancipados o las personas con capacidad modificada judicialmente, que "podrán ejercer esas facultades cuando expresamente lo solicite el interesado y no precise, atendiendo a la resolución judicial que complemente su capacidad, de la representación o asistencia de una institución de protección y apoyo para obligarse o contratar".

A pesar de esta limitación amplia, de la lectura del segundo párrafo del artículo 8.3 de la LOPSC/2015 parece desprenderse que la citada limitación se refiere sólo a la firma electrónica, y no a la identificación electrónica. Dicho texto indica que "el prestador de servicios de certificación procederá a revocar el certificado de firma electrónica a instancia del Ministerio del Interior, tras recibir éste la comunicación del Encargado del Registro Civil de la inscripción de la resolución judicial que determine la necesidad del complemento de la capacidad para obligarse o contratar, del fallecimiento o de la declaración de ausencia o fallecimiento de una persona".

Como se puede ver, en ningún momento se prevé la revocación del certificado de identificación electrónica, por lo que cabe deducir que dichas personas también dispondrán del mismo en su DNI electrónico. Y en efecto, el segundo párrafo del artículo 1.4 del Real Decreto 1553/2005 especifica que "en el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado".

El segundo elemento de singularidad del DNI electrónico es la obligación de todas las personas físicas o jurídicas, públicas o privadas, de reconocer "la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos" (artículo 15.2 de la LFE), a pesar de lo cual no parece que se pueda defender la existencia de una obligación general de admitir su uso. Y que, además, no se ha incorporado al Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

En efecto, no parece existir un verdadero derecho de los ciudadanos a que, por ejemplo, en sus relaciones con las entidades financieras puedan exigir a las mismas que implementen el uso del DNI electrónico; mientras que, por el contrario, en determinados sectores sí se ha podido apreciar la existencia un verdadero derecho al uso del DNI electrónico, en especial en la administración electrónica.

Aún así, y aunque se han expedido 62.848.865 DNI electrónicos[409], no se puede decir que

[408] En sentido similar, cfr. artículo 1.4 del Real Decreto 1553/2005.

[409] Cfr. https://www.dnielectronico.es/PortalDNIe/ (última consulta: 12 de mayo de 2018).

el mismo haya sido un caso de éxito de uso abrumador en la administración electrónica[410], como se desprende de diversas fuentes: por ejemplo, de acuerdo con el Informe presentado al Consejo de Ministros de 10 de enero de 2014 sobre el grado de avance de la implantación de la administración electrónica en la Administración General del Estado[411], con datos referidos al ejercicio 2012, sólo el 2,41% de las validaciones de certificados de firma electrónica correspondía al DNI electrónico[412]; por el contrario, la Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares elaborada por el Instituto Nacional de Estadística (INE TIC-Hogares) referidas al 2013 reporta que el 14,9% de los usuarios que poseen DNI electrónico lo emplean para relacionarse con la administración electrónica, mientras que hasta un 4,9% lo usan para relaciones con el sector privado.

El DNI electrónico ha sufrido un proceso de transformación para convertirlo en un medio más adaptado a los entornos tecnológicos adoptados por los ciudadanos de forma masiva en los últimos años, en especial las tecnologías de movilidad[413]. En este sentido, una de las novedades del denominado DNI-e 3.0 es la incorporación de una interfaz inalámbrica para su uso, mediante el protocolo NFC, por lo que se elimina la necesidad de un lector para el empleo de este medio de identificación electrónica.

Asimismo, el Gobierno ha puesto en funcionamiento de una nueva modalidad del DNI-e, con claves almacenadas en la Nube[414], accesibles de forma ubicua bajo el control exclusivo de su titular, de acuerdo con las reglas del Reglamento eIDAS para la firma electrónica avanzada. Dicha posibilidad, incorporada al servicio Cl@ve, puede realmente ayudar a extender el uso de este sistema de forma decisiva, tanto para la identificación electrónica, como para la firma de documentos.

2.2.2 La identificación electrónica en la legislación común de acceso electrónico de los ciudadanos a los servicios públicos

La identificación electrónica, como servicio público, también ha encontrado una base jurídica en la legislación de administración electrónica, desde una doble óptica: en primer lugar, admitiendo y regulando el uso de sistemas basados en la legislación de firma electrónica[415] –en la medida en que los mismos identifican a sus titulares, como sucede en el caso de los certificados electrónicos cualificados, a los que ya nos hemos referido

---

[410] A pesar de las expectativas, como puede verse en (Heichlinger & Gallego, 2010, p. 63).

[411] Accesible en el Portal de Administración Electrónica, Observatorio de Administración Electrónica, en http://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Informes/pae_InformeAvanceAdmin/pae_InfDescarga.html.

[412] Hay que hacer notar que posteriormente a esta fecha se han dejado de publicar estadísticas de uso del DNI electrónico, por lo que no se puede apreciar si se ha producido algún aumento significativo. También la AEAT ha dejado, en dicha fecha, de publicar estadísticas en este sentido.

[413] (Fundación Telefónica, 2015, pág. 34 y ss.).

[414] Cfr. la información del proyecto publicada en la página web del servicio Cl@ve, accesible en http://clave.gob.es/clave_Home/dnin.html.

[415] Bajo la denotación de "firma electrónica", que en la LAE se refiere a aquellos que "sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos". Esta referencia debe entenderse realizada, hoy, al Reglamento eIDAS.

en términos generales–; y en segundo término, estableciendo una base jurídica, aunque ciertamente implícita, como veremos, para la expedición, por las Administraciones Públicas, de otros sistemas de identificación y firma electrónica, tanto para su uso por los ciudadanos cuanto por el personal a su servicio[416].

La LAE incluyó, por primera vez, en su catálogo de derechos, el de "obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública", que recoge el apartado g) del artículo 6.2 de la citada LAE.

Esta inclusión del "derecho a la identidad electrónica" debe relacionarse con la proyección a Internet de los derechos de la personalidad, de forma que se produce una extensión del clásico derecho al nombre, reconvirtiéndose en el derecho a la actuación por vía electrónica, como presupuesto del derecho a la relación electrónica de los ciudadanos con las Administraciones Públicas, que reconoce de forma plena el artículo 6.1 de la LAE.

El derecho a la identidad electrónica se relaciona, además, con el derecho a la igualdad en el acceso electrónico a los servicios públicos, indicado en el apartado c) del artículo 6.2 de la LAE, puesto que sólo las personas con identidad electrónica van a poder ejercitar de forma plena su derecho a la relación electrónica con las Administraciones Públicas, de modo que resulta exigible a dichas Administraciones Públicas el establecimiento de las políticas públicas adecuadas para el suministro de la identidad electrónica y de la firma electrónica a los ciudadanos, y prevenir posibles tratos discriminatorios derivados del sistema de firma electrónica empleado[417].

Uno de los ejes esenciales de este derecho a la obtención de la identidad ha sido, como ya hemos avanzado anteriormente, el suministro del DNI electrónico que, de hecho, es obligatorio en cuanto al soporte físico, pero voluntario en cuanto a los certificados que contiene. Sin embargo, al no cubrir el DNI electrónico a todos los ciudadanos[418], no ha podido constituir el único eje de la política pública de identidad electrónica, sino que ha debido completarse mediante el empleo de otros sistemas.

En concreto, se han admitido todos los sistemas de firma electrónica basados en certificados electrónicos reconocidos, dado que los mismos identifican a sus titulares y, además, el artículo 16.1 de la LAE establece que "las Administraciones Públicas podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos"; esto es, sistemas técnicos de identificación y autenticación electrónica. Nótese la referencia legal a estas técnicas como "otros sistemas de firma electrónica", dada la inexistencia de una definición legal de identificación electrónica a fecha de aprobación de la LAE, por lo que esta función queda absorbida por la definición de firma electrónica

[416] Sistemas que, además, se van a emplear también para la firma electrónica.

[417] Cfr. (Cotino Hueso, 2010, págs. 293-294).

[418] Dado que únicamente pueden obtener el DNI electrónico los nacionales españoles, pero no los extranjeros con residencia legal en España.

contenida en la LFE, a la que posteriormente nos referiremos con detalle.

Aunque habitualmente este artículo se ha interpretado, conjuntamente con el artículo 6.2.g) de la LAE, para entender que ofrece soporte normativo a la entrega por la Administración a los ciudadanos de sistemas de identificación electrónica diferentes de los certificados de firma electrónica avanzada o reconocida[419], también permite a la Administración la admisión de mecanismos de identidad expedidos por terceros, mediante la técnica de la "delegación de la autenticación"[420], en cuyo caso la Administración se acoge al uso de sistemas de identificación operados por terceros, incluidos prestadores privados.

Debido a las dificultades en el uso de los sistemas basados en certificados electrónicos[421], y en especial al amparo del régimen jurídico establecido por la LAE, diversas Administraciones Públicas españolas han desarrollado sistemas de identificación electrónica, diferentes de aquellos basados en los certificados electrónicos regulados en la LFE.

En un primer momento, estas experiencias se han limitado a la relación entre el ciudadano y la Administración en cuestión, pero con posterioridad han aparecido servicios orientados al uso por los ciudadanos frente a terceras Administraciones, por lo que su interés es mayor, en especial a la luz del Reglamento eIDAS.

El sistema Cl@ve – Identidad Electrónica para las Administraciones es un excelente ejemplo en ambos sentidos. Aprobado, en el marco del artículo 16 de la LAE, en su desarrollo por el RDLAE, por Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, publicado por Orden PRE/1838/2014, de 8 de octubre, Cl@ve se define inicialmente como la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

Cl@ve nace en el contexto de los trabajos de la Comisión para la Reforma de las

[419] A título de ejemplo podemos citar la Orden CUL/1132/2011, de 28 de abril, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en el Registro Electrónico del Ministerio de Cultura y se modifica la Orden CUL/3410/2009, de 14 de diciembre de 2009, que regula el Registro Electrónico del Ministerio de Cultura, o la Orden EHA/2219/2010, de 29 de julio, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en la sede electrónica de la Dirección General del Catastro, modificada por Orden HAP/2553/2015, de 25 de noviembre, entre otras.

[420] Asimismo, el empleo de mecanismos basados en federaciones de identidad y atributos puede también ser apropiado en muchos procedimientos administrativos donde realmente lo único que se requiere acreditar es un rol o atributo, sin que sean muy relevantes los datos de identidad raíz, ni mucho menos, imprescindible el empleo de un identificador universal, por lo que ofrecen una versatilidad inimaginable en el caso de los certificados reconocidos de firma electrónica, permitiendo una menor divulgación de datos personales de identidad. Por ejemplo, resulta perfectamente aceptable la simple acreditación del "rol" de vecino, para la actuación electrónica en el ámbito de los mecanismos y procesos participativos que los ayuntamientos deben desplegar: un consejo social de la ciudad de tipo consultivo, presupuestos participativos, mejores canales de comunicación con los ciudadanos aprovechando las TIC, una comisión de sugerencias y reclamaciones para la defensa de los vecinos o peticiones y consultas populares, entre otros.

[421] Se puede ver una buena muestra de ello en la experiencia de MiFirma.com, iniciativa que recoge firmas electrónicas en el ámbito de las iniciativas legislativas populares y en determinados procesos electorales (Peña & Alamillo Domingo, 2014, pág. 767 y ss.).

Administraciones Públicas (CORA) que, entre otros objetivos, tiene el de contribuir a crear un modelo de gestión común e integrada, facilitadora de las relaciones entre sociedad y Administración.

Al efecto, el Acuerdo del Consejo de Ministros considera "esencial habilitar un sistema simple, rápido y seguro de identificación, autenticación y firma de los ciudadanos en su relación electrónica con los prestadores de servicios del Sector Público Administrativo Estatal y, en la medida que así se acuerde, del resto del Sector Público Estatal, de las Administraciones Autonómicas y Entidades Locales", sistema que "debe permitir la expresión de la voluntad del usuario, cuando así lo requiera el servicio o trámite electrónico, por medio de los sistemas de firma electrónica válidos según la normativa vigente".

Cl@ve se justifica, en el citado Acuerdo, en elementos como la complejidad de los sistemas de firma electrónica basados en certificados, que "requieren, sin embargo, actualizaciones de software y reconfiguraciones frecuentes que añaden un componente de complejidad que puede resultar disuasorio y que no es siempre necesario, en virtud del principio de proporcionalidad, en aquellos trámites y procedimientos que no requieran tan alto nivel de seguridad"; así como en el hecho de que el uso de otros sistemas de firma electrónica, regulados en el artículo 13.2.c) de la LAE "no son interoperables entre sí, con el trastorno que ello supone para el ciudadano al tener que conocer y aplicar distintos sistemas según la Administración, el organismo o el servicio o trámite al que acceda".

Más notable aún, Cl@ve integra sistemas previamente existentes, de uso sectorial y desconectado en diversos órganos de la Administración General del Estado, para formar "un sistema colaborativo de identificación, autenticación y firma electrónica, llamado a resolver las limitaciones de los actuales, integrando los sistemas de claves concertadas de la Administración ya existentes en uno único, y abriendo su utilización a la totalidad del Sector Público Administrativo Estatal, y permitiendo también integrarse al resto de las Administraciones Públicas cuando esté disponible, habilitando de este modo la extensión práctica de los servicios de Administración Electrónica a la gran mayoría de los ciudadanos españoles, en aplicación de la Ley 11/2007, de 22 de junio".

Dado que el sistema Cl@ve se inscribe en el marco de las acciones clave números 3 y 16 de la Agenda Digital Europea, que sustentan el mandato de actuación de la Comisión Europea que culmina en el Reglamento eIDAS, parece que Cl@ve sería la segunda gran estrategia española de identificación electrónica[422].

Los sistemas previamente existentes que se integran en Cl@ve son el denominado PIN24H de la Agencia Estatal de Administración Tributaria, concebido para usuarios con acceso ocasional –que se denomina Cl@ve ocasional o Cl@ve PIN, y el sistema de usuario y contraseña de la Seguridad Social, orientado a usuarios con acceso frecuente– que se denomina Cl@ve Permanente.

A los mismos debe añadirse el denominado DNI-e en la Nube, ya disponible, y la interesante declaración de intención referida a que, en palabras del Acuerdo del Consejo de Ministros, "este sistema de identificación y firma electrónica podrá evolucionar en el futuro para admitir también la participación del sector privado en su provisión, o su combinación con otras soluciones tecnológicas ofrecidas por empresas especializadas".

[422] Como hemos visto, la primera estrategia sería el DNI electrónico.

El actual Cl@ve PIN fue inicialmente regulado por Resolución de 17 de noviembre de 2011, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Agencia Estatal de Administración Tributaria, que se refiere al mismo como sistema de firma con clave de acceso en un registro previo como usuario[423], aunque el mismo también era conocido como PIN24H[424].

Inicialmente puede sorprender el rango del instrumento "normativo" elegido para la creación de estos sistemas –resolución administrativa en el caso de Cl@ve PIN–, pudiéndose pensar que se requeriría una disposición de carácter general debido al establecimiento de derechos y obligaciones que en su caso proceda aplicar a los usuarios de estos sistemas, pero no hay que olvidar que es el artículo 11.1 del RDLAE el que prevé que "la admisión de otros sistemas de firma electrónica a la que se refiere el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberá aprobarse mediante orden ministerial, o resolución del titular en el caso de los organismos públicos, previo informe del Consejo Superior de Administración Electrónica", especificando en su epígrafe 3 que "el acto de aprobación contendrá la denominación y descripción general del sistema de identificación, órgano u organismo público responsable de su aplicación y garantías de su funcionamiento, y será publicado en las sedes electrónicas que sean de aplicación, donde se informará de las actuaciones en las que son admisibles estos medios de identificación y autenticación". Y lo hace dentro del marco de la propia LAE que, aunque de forma muy escasa, al menos regula las condiciones mínimas en que se configura el derecho a la admisión de este tipo de sistemas.

No parece, por tanto, que la determinación de las concretas condiciones aplicables a la expedición de medios de identificación electrónica, y su uso posterior para la autenticación o la firma electrónica, requieran de una disposición de carácter general, interpretación que también resulta reforzada por lo establecido en la norma reglamentaria que más va a influir en la determinación de dichas condiciones, que no es otra que el RDENS. Y en este sentido, basta recordar que la política de seguridad de la información –que, entre otros muchos aspectos, regula el uso de los identificadores y el proceso de autenticación, control de acceso y firma electrónica– se aprueba por el titular del órgano superior de la Administración Pública correspondiente, según dispone el artículo 11.1 del citado Real Decreto.

En cuanto al sistema Cl@ve PIN, el epígrafe 1 del Anexo III de la Resolución de 17 de noviembre de 2011 lo caracteriza en base a la inscripción del ciudadano en un registro de usuarios, mediante la cumplimentación del correspondiente formulario facilitado al efecto por la AEAT, si bien actualmente el proceso se inicia también desde la sede electrónica de Cl@ve.

El registro del ciudadano se puede realizar de tres formas diferentes, incluyendo un procedimiento a distancia sin certificado (la denominada Carta de Invitación), un procedimiento a distancia con certificados y un procedimiento presencial.

---

[423] La citada Resolución también regula otros dos sistemas adicionales de "firma", que son la clave o número de referencia, y la información conocida por ambas partes. Estos sistemas pueden combinarse, en su uso, entre si o con el de clave de acceso con registro previo como usuario.

[424] Básicamente, porque se remitía un número de identificación personal (PIN) que se podía emplear una o varias veces, durante el plazo máximo de 24 horas.

De los tres procedimientos de registro, el más novedoso es sin duda el primero, que funciona de la siguiente forma: en primer lugar, se solicita la Carta de Invitación, para lo cual se deben aportar el NIF, el primer apellido y determinados números del IBAN de una cuenta de la que se sea titular (eso sí, en entidades españolas), a efectos de que la AEAT pueda verificar que el solicitante es quien dice ser (obviamente, en cierto grado, puesto que ninguno de estos datos es de conocimiento reservado, y terceras personas los pueden poseer); en segundo término, la AEAT remite una Carta de Invitación mediante entrega postal al domicilio fiscal del solicitante que le consta a la AEAT, por lo que se puede suponer que será difícil que la pueda obtener un falso solicitante, en la que se contiene un código seguro de verificación de 16 caracteres, incluyendo letras y números; finalmente, el ciudadano puede completar el registro en la sede electrónica identificándose mediante la introducción de estos cuatro datos conjuntamente (NIF, primer apellido, código seguro de verificación y determinados números del IBAN), indicando un número de teléfono móvil de una operadora que preste servicios en España, un correo electrónico, y la fecha de expiración del DNI-NIE del titular, y aceptando las condiciones de uso del servicio.

El ciudadano registrado en Cl@ve, cuando necesite utilizar el sistema para autenticarse frente a un servicio, puede acceder al sistema –identificándose con su número de DNI-NIE y fecha de expiración–, elegir una clave de acceso personal (que introduce en el correspondiente campo) y solicitar la obtención del Cl@ve PIN, que será remitido al teléfono móvil registrado en el sistema, y que consiste en un código de un solo uso (OTP) y limitación temporal a los siguientes 10 minutos desde su recepción[425]. La autenticación frente al servicio se realizará mediante la introducción del número de DNI-NIE, de la clave de acceso personal y del PIN recibido en el teléfono móvil.

El procedimiento a distancia basado en el empleo de certificado elimina la necesidad de la Carta de Invitación, dado que la identidad del solicitante es acreditada precisamente mediante la autenticación basada en el citado certificado, y en el caso del procedimiento presencial, el solicitante deberá acudir en persona a una oficina de la AEAT o de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, al efecto de realizar el trámite.

Ya desde la perspectiva de la utilización de este sistema, la Orden HAP/2194/2013, de 22 de noviembre, por la que se regulan los procedimientos y las condiciones generales para la presentación de determinadas autoliquidaciones, declaraciones informativas, declaraciones censales, comunicaciones y solicitudes de devolución, de naturaleza tributaria[426], realiza una agresiva apuesta[427] al objeto de "reducir al máximo posible la

[425] Esta limitación a un verdadero código de un solo uso y con validez temporal limitada es una importante mejora con respecto al PIN24H.

[426] La denominación fue modificada por Orden HAP/2762/2015, de 15 de diciembre. Modificada, en lo que nos interesa, por Orden HAP/455/2014, de 20 de marzo; Orden HAP/1846/2014, de 8 de octubre, Orden HAP/365/2016, de 17 de marzo; y Orden HFP/255/2017, de 21 de marzo.

[427] Ampliada posteriormente por Orden HAP/2455/2013, de 27 de diciembre; Orden HAP/685/2014, de 29 de abril; Orden HAP/1136/2014, de 30 de junio; Orden HAP/2201/2014, de 21 de noviembre; Orden HAP/2178/2014, de 18 de noviembre; Orden HAP/2328/2014, de 11 de diciembre; Orden HAP/369/2015, de 27 de febrero; Orden HAP/1230/2015, de 17 de junio; Orden HAP/2118/2015, de 9 de octubre; Orden HAP/2762/2015, de 15 de diciembre; Orden HAP/2783/2015, de 21 de diciembre; Orden HAP/2835/2015, de 28 de diciembre; Orden HAP/296/2016, de 2 de marzo; Orden HAP/1349/2016, de 28 de julio; Orden

presentación en papel de las autoliquidaciones y declaraciones informativas mientras se potencian nuevas vías de presentación como son las basadas en los sistemas de firma electrónica no avanzada definidos en la Resolución de 17 de noviembre de 2011 de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Agencia Tributaria".

Para ello, su artículo 2 autoriza a los sujetos obligados[428] la presentación electrónica de diversas autoliquidaciones mediante la firma electrónica avanzada o un sistema de identificación y autenticación, en ambos casos utilizando un certificado electrónico reconocido emitido de acuerdo a las condiciones que establece la LFE que resulte admisible por la AEAT según la normativa vigente en cada momento; o alternativamente, y sólo en el caso de obligados persona física[429], también el sistema Cl@ve PIN.

En sentido esencialmente idéntico se manifiesta el artículo 12 de la propia Orden, respecto a la presentación de determinadas declaraciones informativas.

Estos artículos resultan llamativos por diversas cuestiones, seguramente llamadas a marcar el inicio de una tendencia para el resto de Administraciones Públicas.

En primer lugar, por la equiparación entre la firma electrónica avanzada basada en certificado electrónico reconocido, y la autenticación electrónica basada en el mismo certificado, dado que como indica la exposición de la Orden HAP/1846/2014, de 8 de octubre, "de acuerdo con los principios que fundamentaron la aprobación de la Orden HAP/2194/2013, de 22 de noviembre, y con la finalidad de facilitar y hacer más sencilla la presentación de declaraciones por vía electrónica a los obligados tributarios, se ha considerado conveniente introducir un nuevo sistema de presentación basado en el uso de

---

HAP/1695/2016, de 25 de octubre; Orden HFP/1922/2016, de 19 de diciembre; Orden HFP/1978/2016, de 28 de diciembre; Orden HFP/105/2017, de 6 de febrero; Orden HFP/550/2017, de 15 de junio; y Orden HFP/816/2017, de 28 de agosto; lo que trae cuenta de la importancia y extensión de estas políticas.

[428] En realidad, podríamos decir que en la gran mayoría de los casos lo impone taxativamente, dado que el artículo 3.1 de la misma Orden determina la obligación de realizar la presentación por Internet, y empleando necesariamente certificado reconocido, de "aquellos obligados tributarios que tengan el carácter de Administración Pública, o bien se encuentren inscritos en el Registro de Grandes Empresas regulado en el apartado 5 del artículo 3 del Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los Tributos, aprobado por el Real Decreto 1065/2007, de 27 de julio, bien estén adscritos a la Delegación Central de Grandes Contribuyentes o bien tengan la forma de sociedad anónima o sociedad de responsabilidad limitada", así como "en las autoliquidaciones del Impuesto sobre el Valor Añadido de aquellos obligados tributarios cuyo período de liquidación coincida con el mes natural, de acuerdo con lo establecido en los apartados 1.º, 2.º, 3.º y 4.º del artículo 71.3 del Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre, y en el supuesto del Modelo 430 "Impuesto sobre primas de seguros. Declaración-Liquidación", cualquiera que sea el obligado a su presentación". Asimismo, de acuerdo con el artículo 3.2 de la Orden, "también tendrá carácter obligatorio la presentación electrónica por Internet, […] en las presentaciones correspondientes al Impuesto sobre la Renta de las Personas Físicas y al Impuesto sobre el Patrimonio a realizar por las personas físicas que deban realizar la declaración del Impuesto sobre el Patrimonio", si bien en este caso podrán emplearse sistemas de firma avanzada o de identificación y autenticación basados en certificados electrónicos reconocidos, Cl@ve PIN o incluso número/s de referencia del borrador o de los datos fiscales previamente suministrados por la AEAT. De forma análoga, en el artículo 13 de la Orden, en relación con las declaraciones informativas.

[429] Pero únicamente cuando la misma no se encuentre obligada a la presentación con certificado, de acuerdo con lo establecido en el artículo 3.1 de la misma Orden.

certificados electrónicos reconocidos alternativo al de firma electrónica avanzada, eliminando con ello ciertas operaciones que en la práctica se ha puesto de manifiesto resultaban técnicamente complejas", por lo que "el ciudadano solo necesita disponer de un certificado electrónico reconocido que cumpla las condiciones que establece la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que resulte admisible por la Agencia Estatal de Administración Tributaria según la normativa vigente en cada momento".

Lo que sucede es que la identificación del ciudadano con su certificado se considera suficiente para las actuaciones de autoliquidación de los tributos, eliminándose la necesidad de firmar electrónicamente, y todos los elementos de complejidad que en efecto ello supone. No resulta particularmente arriesgado aventurar que esta norma es reflejo de los enormes problemas asociados al empleo de determinados componentes técnicos, como en especial determinados tipos de aplicación informática de firma electrónica empleados en los procedimientos web, como los *applets* de firma empleados en las sedes electrónicas. Ciertamente se trata de una orientación ya alineada con el Reglamento eIDAS al que anteriormente nos hemos referido, y supone una orientación alejada de la producción documental y su autenticación por el ciudadano: una innovación jurídica –impulsada por la tecnología– en la que la autenticación de entidad sustituye a la autenticación de los datos.

Y esto permite entender la segunda cuestión que llama la atención en los artículos 2 y 12 de la Orden HAP/2194/2013, que no es otra cosa que la plena equiparación de Cl@ve PIN al uso de un certificado electrónico reconocido, de modo que al menos en esta Orden se da por hecho que los dos medios de identificación se encuentran en un mismo nivel de seguridad. En efecto, ambos mecanismos son totalmente alternativos en el caso de las autoliquidaciones presentadas por personas físicas[430], y notablemente alternativos en el caso de las declaraciones informativas.

Como excepción, en el caso de la presentación de autoliquidaciones o de declaraciones informativas por representantes –legales, voluntarios o habilitados–, necesariamente se deberá emplear certificado electrónico reconocido, como disponen los artículos 6 y 16, respectivamente, de la Orden HAP/2194/2013.

También se establecen excepciones en favor de sistemas de inferior seguridad, como en el caso de las autoliquidaciones de los modelos 100 (IRPF) y 720 (Impuesto del patrimonio), en que también se autoriza "la consignación del Número de Identificación Fiscal (NIF) del obligado tributario u obligados tributarios y del número o números de referencia previamente solicitados a la Agencia Tributaria, según el procedimiento establecido en la Resolución de 17 de noviembre de 2011 de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la citada Agencia Tributaria, en el apartado primero.3.a) y desarrollado en el anexo I" (artículo 2.c) de la Orden[431]); o en el caso de las declaraciones informativas correspondientes a los modelos 390 (IVA anual), 347 (operaciones con terceros, anual) y 190 (retenciones e ingresos a cuenta IRPF, anual), en que también se autoriza "la presentación electrónica de la declaración también se podrá efectuar mediante

[430] Y si no lo son en el caso de las personas jurídicas o entidades sin personalidad jurídica, seguramente es porque Cl@ve PIN sólo se expide a personas físicas.

[431] En redacción dada por Orden HAP/365/2016, de 17 de marzo.

el envío de un mensaje SMS", si bien con fuertes restricciones[432] (artículo 12.b) de la Orden[433]).

Se trata de excepciones, éstas últimas, que se entienden bien en atención a la especialidad del procedimiento o del colectivo afectado, y que de hecho suavizan una norma que, en efecto, es altamente agresiva en esta apuesta de restringir al máximo el uso de papel, en especial por lo que respecta a ciudadanos con menores medios y capacidades en la tramitación electrónica.

Por su parte, el sistema actualmente conocido como Cl@ve Permanente fue regulado por Resolución de 4 de junio de 2014, del Instituto Nacional de la Seguridad Social, por la que se aprueban sistemas de identificación y autenticación de los ciudadanos para relacionarse electrónicamente con el Instituto Nacional de la Seguridad Social, y Resolución de 24 de julio de 2014, de la Tesorería General de la Seguridad Social, por la que se aprueba el sistema de identificación, autenticación y firma electrónica, para relacionarse electrónicamente con la Tesorería General de la Seguridad Social[434].

Dichas resoluciones, sustancialmente idénticas, prevén dos sistemas de identificación y autenticación electrónica distintos de la firma electrónica avanzada, que son el sistema de firma con contraseña personal, y el sistema de firma con contraseña personal y código de un solo uso y validez temporal (OTP), y que se diferencian entre sí en atención al número de factores de autenticación exigidos para el acceso a un servicio concreto.

Aunque en ambas Resoluciones se establece un procedimiento de registro basado exclusivamente en la presencia personal del solicitante, a efectos de comprobar su identidad y aportar un número de teléfono móvil, con la integración de ambos sistemas en Cl@ve se han unificado los procedimientos de registro, por lo que también se puede obtener Cl@ve Permanente a distancia, mediante certificado o carta de invitación.

En cualquier caso, el ciudadano registrado debe obtener un código de activación, remitido al teléfono móvil registrado, que le permitirá establecer su contraseña permanente[435], a cuyos efectos indica la Resolución de 4 de junio de 2014, del Instituto Nacional de la Seguridad Social, que se garantizará el cumplimiento de lo establecido en el RDENS para la gestión de contraseñas, en el nivel alto.

---

[432] Dado que esta posibilidad, en el caso de los modelos 347 y 190, sólo se aplica "a entidades a las que sea de aplicación la Ley 49/1960, de 21 de julio, sobre la propiedad horizontal, siempre que no exceda de 15 registros, que hayan sido obtenidas mediante la utilización del servicio desarrollado a estos efectos por la Agencia Estatal de Administración Tributaria en su Sede Electrónica" y nunca si las citadas entidades se encuentran sujetas a presentación obligatoria por Internet.

[433] En redacción dada por Orden HAP/1846/2014, de 8 de octubre.

[434] Como nota curiosa, esta Resolución no ha sido publicada en el BOE.

[435] Esta contraseña no podrá durar más de dos años, y deberá cumplir una serie de normas de seguridad, en cumplimiento del RDENS, que incluyen las siguientes: tener una longitud mínima de 8 caracteres; contener al menos un carácter de cada uno de los siguientes grupos: letras minúsculas, letras mayúsculas, dígitos y caracteres especiales; Las letras ñ y ç, así como las vocales con tilde se consideran letras permitidas. Como caracteres especiales se podrán utilizar alguno de los siguientes: ¡!$?%&#@/\()=¿?*[];,:._<>+-; si la contraseña tiene una longitud igual o superior a 16 caracteres no habrá restricciones en el tipo de caracteres a utilizar (esto permite utilizar una frase completa como contraseña); la contraseña no podrá contener el nombre, apellidos o DNI; y en la renovación de la contraseña no se podrá utilizar la contraseña anterior. Cfr. http://clave.gob.es/clave_Home/Clave-Permanente/Seguridad.html.

Para la autenticación empleando el sistema, el servicio solicitará la introducción de esta contraseña[436] y, caso que se estime oportuno en términos de seguridad del servicio, también del OTP[437] remitido por SMS al teléfono móvil registrado en el sistema.

La integración de estos sistemas al sistema común de la plataforma Cl@ve ha implicado una transformación organizativa relevante, ya que se nombra a la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado como órgano responsable del sistema, en desarrollo de las competencias para el impulso de la Administración digital, y del proceso de innovación de la Administración General del Estado y sus Organismos Públicos[438], como indica el epígrafe 1 del apartado segundo del Acuerdo del Consejo de Ministros, por lo que también se designa a dicha Dirección como responsable del correspondiente fichero de datos de carácter personal (epígrafe 3 del apartado segundo del Acuerdo), y la misma "establecerá, mediante resolución, las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve"[439] (apartado quinto del Acuerdo), que deberán referirse a "los elementos tecnológicos, procedimentales y organizativos necesarios para el desarrollo e implementación del sistema, y el aseguramiento de cada uno de los niveles de garantía de funcionamiento asociados a cada sistema de identificación de los previstos en este acuerdo; los procedimientos de registro de nuevos usuarios y los procedimientos para la incorporación de usuarios existentes en otros sistemas de firma ya operativos de los

[436] En el caso de la Tesorería General de la Seguridad Social, la Resolución de 24 de julio de 2014, por la que se determinan los servicios a los que se podrá acceder por los sistemas de identificación y autenticación, se podrá emplear la contraseña para la acreditación de la actividad agraria por cuenta propia, la consulta de autorizados RED que gestionan un NAF o una empresa, el duplicado de documento de afiliación, el informe de alta laboral a fecha determinada, el informe de bases de cotización, el informe de bases y cuotas ingresadas, el informe de datos identificativos y de domicilio, el informe de estar al corriente de las obligaciones de la Seguridad Social, el informe de situación actual del trabajador, el informe de situación de empresario individual, el informe de vida laboral, el informe de vida laboral acotado, la solicitud de rectificación de informe de bases de cotización y la solicitud de rectificación de informe de vida laboral.

[437] De nuevo, en el caso de la Tesorería General de la Seguridad Social, la Resolución de 24 de julio de 2014, por la que se determinan los servicios a los que se podrá acceder por los sistemas de identificación y autenticación, se podrá emplear la contraseña y el OTP para la solicitud de cambio de domicilio, la solicitud de alta en el RETA, la solicitud de baja en el RETA, la solicitud de domiciliación en cuenta, la solicitud de inscripción y asignación de CCC para empresario individual, la rescisión de CCC y NAFs asignados a un autorizado RED y la solicitud de cambio de base de cotización (de autónomos y en convenios especiales).

[438] Atribuidas de acuerdo con lo dispuesto en el Real Decreto 802/2014, de 19 de septiembre, por el que se modifican el Real Decreto 390/1998, de 13 de marzo, por el que se regulan las funciones y la estructura orgánica de las Delegaciones de Economía y Hacienda; el Real Decreto 1887/2011, de 30 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales; el Real Decreto 199/2012, de 23 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia; el Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas y el Real Decreto 696/2013, de 20 de septiembre, de modificación del anterior.

[439] Lo cual significa que deben considerarse anuladas previsiones como la contenida en la Resolución del 17 de noviembre de 2011, de la Presidencia de la Agencia Estatal de Administración Tributaria, anteriormente analizada, que establecía en el epígrafe II de su Anexo III que "la seguridad del sistema se ve reforzada por la limitación en cuanto a los trámites o actuaciones para las que puede ser utilizado, no siendo posible su uso fuera de dicho ámbito, ni permitiéndose el acceso o consulta de datos personales más allá de los propios del procedimiento e identificación del interesado al que va referido dicho trámite o actuación".

contemplados en el artículo 13.2 c) de la Ley 11/2007, de 22 de junio, previo consentimiento expreso de los mismos en los términos establecidos en la Ley 15/1999, de 13 de diciembre; las condiciones técnicas, económicas y organizativas para la incorporación de otras Administraciones Públicas al sistema Cl@ve; el sistema de identificación e imputación de costes de mantenimiento y explotación del sistema Cl@ve correspondientes a órganos y organismos del Sector Publico Administrativo Estatal; y en general, todas las cuestiones necesarias para asegurar el funcionamiento de Cl@ve y su interoperabilidad" (apartado quinto del Acuerdo).

Los anteriores órganos responsables pasan a ser, en este contexto, participantes en la construcción e implantación del sistema Cl@ve y, asimismo, serán garantes de su funcionamiento (epígrafe 2 del apartado segundo del Acuerdo), dado que se continúan encargando de la explotación de los correspondientes sistemas tecnológicos. Y en consonancia con ello, pasan a ser designados como encargados del tratamiento de los datos de carácter personal (epígrafe 3 del apartado segundo del Acuerdo), reforzándose la noción de base de datos única de identidades digitales de los ciudadanos inscritos en el sistema[440].

Finalmente, hay que reseñar la Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, que, como presentaremos posteriormente, ha incorporado el servicio de firma electrónica de documentos mediante certificados albergados en modo centralizado.

En la actualidad, y como se indica en el Centro de Transferencia de Tecnología[441], el diseño de Cl@ve está basado en un sistema de federación de identidades electrónicas, que integra los elementos que se muestran en la Ilustración 6 (Portal de Administración Electrónica del Ministerio de Hacienda y Función Pública).

Los actores de este sistema incluyen los proveedores de servicios de administración electrónica (SP), que son las entidades que proporcionan servicios electrónicos a los ciudadanos y utilizan la plataforma para la identificación y autenticación de los mismos; los proveedores de servicios de identificación y autenticación (IdP), que son las entidades que proporcionan mecanismos de identificación y autenticación de los ciudadanos para ser utilizados como medios comunes por otras entidades, y que, como hemos visto, son actualmente la AEAT y la Gerencia de Informática de la Seguridad Social[442]; la pasarela o Gestor de Identificación, que es el sistema intermediador que posibilita el acceso de los proveedores de servicios a los distintos mecanismos de identificación y la selección de éstos por parte del usuario y, adicionalmente, se podrá conectar con otros sistemas intermediadores, como @firma, en relación con los servicios de certificación y firma electrónica, y STORK, para la autenticación transfronteriza.

---

[440] Que, como se desprende de todo lo indicado anteriormente, serán nacionales españoles o extranjeros con residencia legal en España (esto es, con NIE).

[441] Cfr. http://administracionelectronica.gob.es/ctt/clave/infoadicional.

[442] Con la incorporación del DNI-e en Nube, también la Policía Nacional, como prestador de servicios de certificación, y pudiéndose integrar también otros prestadores públicos o privados.

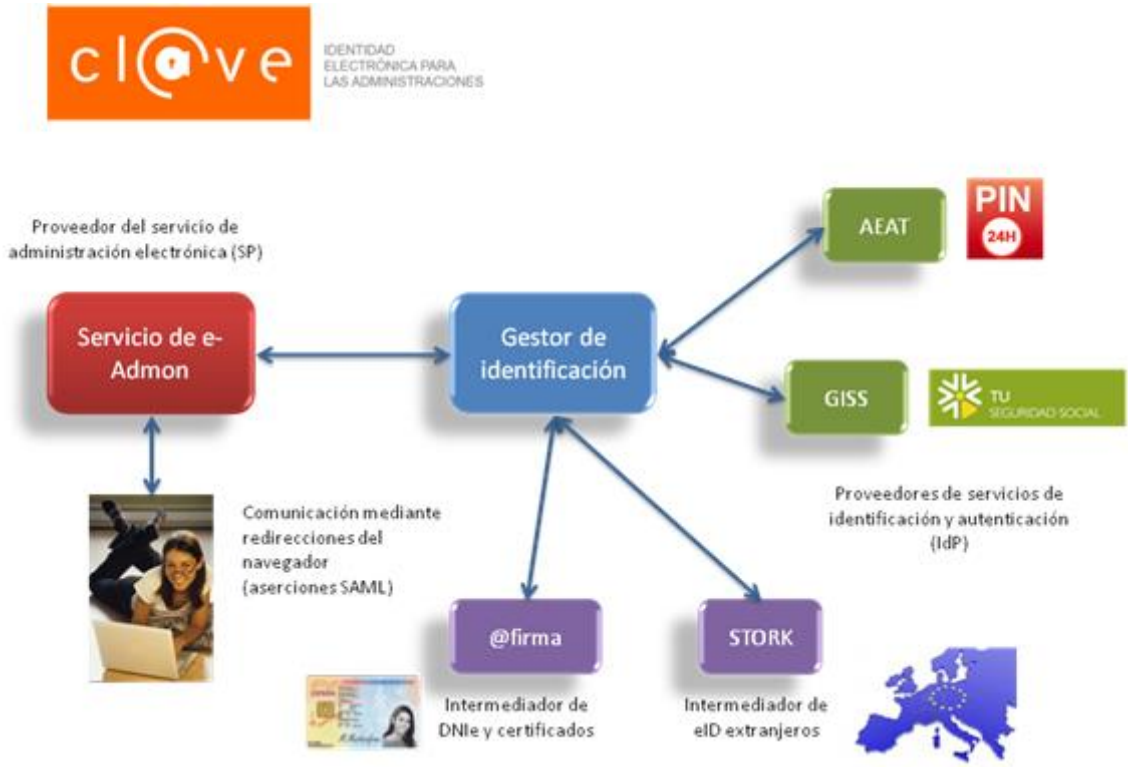


Ilustración 6. Participantes en Cl@ve (Portal de Administración Electrónica)

Hay que indicar que los dos sistemas de identificación electrónica, Cl@ve PIN y Cl@ve Permanente, se pueden también emplear, desde su integración en la plataforma común, en las relaciones entre los ciudadanos y otras Administraciones Públicas que lo consideren oportuno, mediante su adhesión "al sistema mediante convenio otras Administraciones Públicas en las condiciones técnicas, económicas y organizativas que se determinen en las prescripciones técnicas de desarrollo" por la Dirección de Tecnologías de la Información y las Comunicaciones de la AGE, de forma análoga a lo que se establezca para el propio ámbito interno de la AGE, adhesión que será plenamente voluntaria.

2.2.3 El tratamiento de la identificación electrónica de los interesados en la nueva legislación de procedimiento administrativo común

El régimen jurídico expuesto ha sido parcialmente alterado por la LPAC, dado que la misma procede a regular la identificación electrónica como institución jurídica claramente diferenciada de la firma electrónica[443], con efectos desde 2 de octubre de 2016.

En efecto, en la exposición de motivos de la LPAC se declara que el Título I, de los interesados en el procedimiento, "dedica parte de su articulado a una de las novedades más importantes de la Ley: la separación entre identificación y firma electrónica y la simplificación de los medios para acreditar una u otra, de modo que, con carácter general, sólo será necesaria la primera, y se exigirá la segunda cuando deba acreditarse la voluntad

[443] Pero téngase en cuenta que el legislador ha tenido a bien no modificar la LUTICAJ en el mismo sentido, lo cual generará, sin duda alguna, disfunciones notables.

y consentimiento del interesado", en un enfoque el que se va a conceder una fuerte preferencia a la identificación electrónica sobre la firma electrónica. Nos ocuparemos ahora del régimen relativo a la primera.

Continúa la exposición de motivos diciendo que "se establece, con carácter básico, un conjunto mínimo de categorías de medios de identificación y firma a utilizar por todas las Administraciones", de forma que "se admitirán como sistemas de identificación cualquiera de los sistemas de firma admitidos, así como sistemas de clave concertada y cualquier otro que establezcan las Administraciones Públicas", por lo que, en clave interna, no se establece una competencia exclusiva de identificación electrónica en favor de ninguna Administración, exceptuando el caso ya presentado del DNI electrónico, que por cierto no se cita de forma independiente en la LPAC.

Desde la perspectiva de la dimensión transfronteriza, la exposición de motivos de la LPAC indica que "tanto los sistemas de identificación como los de firma previstos en esta Ley son plenamente coherentes con lo dispuesto en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE", texto que parece prever la posibilidad de que se puedan notificar a la Comisión Europea diversos sistemas de identificación electrónica, incluyendo el DNI electrónico, y otros que establezcan las Administraciones Públicas.

Asimismo, la exposición de motivos de la LPAC recuerda también "la obligación de los Estados miembros de admitir los sistemas de identificación electrónica notificados a la Comisión Europea por el resto de Estados miembros […] en los términos que prevea dicha norma comunitaria", que como es lógico se proyecta sobre todas las Administraciones Públicas españolas, que deberán dotarse de los correspondientes mecanismos técnicos[444].

En primer lugar, hay que decir que el artículo 13.g) de la LPAC mantiene el derecho de las personas con capacidad de obrar ante las Administraciones Públicas a la obtención y utilización de los medios de identificación contemplados en la Ley, en una formulación formalmente más restrictiva a la considerada en la LAE, que venía referida a todos los ciudadanos, aunque seguramente sin constituir una limitación adicional al régimen anteriormente establecido.

Entrando en algo más de detalle, el artículo 9 de la LPAC se refiere de forma específica a los sistemas de identificación de los interesados en el procedimiento. Después de recordar, en su apartado 1, que "las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente", en el apartado 2 del mismo artículo determina, como regla general, que "los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad".

[444] O acudir a los que pueda ofrecer la Administración General del Estado, en su condición de autoridad pública del nodo de interoperabilidad de identificación electrónica; es decir, el PEPS de STORK o su sucesor.

Y el mismo epígrafe especifica que "en particular, serán admitidos, los sistemas siguientes:

a) Sistemas basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.

b) Sistemas basados en certificados electrónicos reconocidos o cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan".

Como se puede ver, se trata de una aproximación del carácter más amplio posible, algo que cabe considerar positivo en términos de neutralidad tecnológica, y que, con carácter general, contempla los certificados reconocidos o cualificados –lógico teniendo en cuenta que, como hemos visto, son medios especialmente idóneos para garantizar la identificación electrónica de su correspondiente titular[445]– y cualquier otro sistema técnico que una Administración Pública considere válido para ello, de acuerdo con lo que establezca al efecto.

Esta aproximación, en especial en lo que se refiere a esta segunda categoría, abierta, de sistemas de identificación electrónica no se encuentra exenta de problemas potenciales, porque la norma no concreta mínimo alguno con respecto al procedimiento de registro previo como usuario, ni acerca de cuánta garantía de la identidad resulta exigible para que dicho sistema resulte aceptable. Al contrario, ambas cuestiones quedan, en principio, al albur de cada Administración pública[446].

De hecho, no resulta ocioso notar que la dicción del artículo 9.2 permite admitir todos los sistemas de identificación, con independencia de si los mismos han sido expedidos por entidades públicas y privadas, por lo que estas cuestiones se proyectan en un doble plano, en función de si el registro previo lo ha realizado la misma Administración frente a la que se realiza la identificación, o si el mismo ha sido realizado por una entidad diferente, sea ésta pública o privada.

En el primer caso, será relativamente fácil establecer un conjunto de reglas y condiciones para la identificación electrónica, incluyendo la posterior autenticación, dado que dichas actuaciones se producen dentro del ámbito de la misma Administración, por lo que estas reglas y condiciones se podrán normativizar o consensuar considerando los riesgos asociados a los trámites y servicios públicos; pero en el segundo caso, puede resultar

---

[445] Cfr. el epígrafe 2.1 de este trabajo.

[446] La STC de 24 de mayo de 2018, indica en su fundamento jurídico 9º, que "[l]a Ley 39/2015 tampoco impone los sistemas de identificación electrónica en las relaciones del ciudadano con las Administraciones Públicas ni establece el régimen del registro previo ni fija requisitos mínimos de seguridad. Remite las decisiones en torno a los sistemas de identificación electrónica a cada una de las Administraciones Públicas (apartado 2) con los siguientes límites: la Administración que admita un sistema de claves concertadas o similares habrá de admitir necesariamente el uso de certificados de firma o sello, que proporcionan mayores niveles de seguridad (apartado 2, último párrafo)".

bastante más complejo, dado que la entidad usuaria de la identificación electrónica expedida por otra entidad precisará conocer y evaluar el sistema antes de admitirlo.

Podría ayudar a generar seguridad establecer criterios y requisitos referidos a los sistemas de identificación electrónica, mediante un desarrollo posterior de la LPAC[447], que quizá se podría sustanciar mediante una modificación del actualmente vigente Esquema Nacional de Seguridad, pero también se podrían aplicar directamente los requisitos que el Reglamento eIDAS impone a los sistemas de identificación para su notificación[448], algo que resultaría especialmente positivo para aquellos sistemas que efectivamente se desee notificar, para su uso de la autenticación transfronteriza[449].

Al respecto, la citada admisión corresponde, de acuerdo con el último párrafo del epígrafe 2 del artículo 9, a cada Administración Pública, que "podrá determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos, si bien la admisión de alguno de los sistemas de identificación previstos en la letra c) conllevará la admisión de todos los previstos en las letras a) y b) anteriores para ese trámite o procedimiento".

Como vimos en la LAE[450] –pero no en la LUTICAJ–, los certificados electrónicos reconocidos debían ser obligatoriamente admitidos por todas las Administraciones Públicas, por lo que constituía un derecho subjetivo del ciudadano; y, además, debían serlo para todos los trámites, por lo que el ciudadano podía decidir emplear su certificado como sistema único para la identificación electrónica (así como para la firma).

Este régimen no parece verse alterado –en cuanto a la identificación electrónica– por la nueva LPAC, ya que la Administración que admita un sistema diferente del certificado, también deberá obligatoriamente aceptar que el ciudadano pueda identificarse mediante el certificado reconocido o cualificado del que disponga. Como novedad sobre el régimen de la LAE y de la LUTICAJ, que también se puede emplear el certificado de sello electrónico previsto en el Reglamento eIDAS y que convive, en la LPAC, con el certificado de firma electrónica de persona jurídica y de entidad sin personalidad jurídica, que se mantiene en la dicción legal.

Esta convivencia va a ser, de todos modos, más formal que real, dado que cuando la LPAC inicie su periodo de vigencia, los certificados de firma electrónica de persona jurídica habrán desaparecido, al menos en su modalidad de certificado reconocido, por lo que nunca se llegará a poder ejercer este derecho.

Por tanto, parece que el régimen jurídico no ha cambiado, y que una Administración

---

[447] Que podría ser dictado por el Gobierno, en el ámbito de sus competencias, de acuerdo con lo establecido en la disposición final sexta de la LPAC; así como por cada Administración Pública usuaria de sistemas de identificación electrónica, en su propio ámbito de competencias (cfr. artículo 9.2 último párrafo, de la LPAC).

[448] Cfr. el epígrafe 3.1 de este trabajo.

[449] Y, por el motivo contrario, ser poco interesante, e incluso actuar como elemento de desincentivo, en el resto de casos. En efecto, puede ser precisa la expedición o admisión de determinados sistemas de identificación electrónica que no cumplen con los citados requisitos del Reglamento eIDAS, típicamente por ser de nivel inferior a los mismos, en cuyo caso no tiene mucho sentido acudir al Reglamento eIDAS como marco referencial.

[450] Después de su reforma por Ley 15/2014, de 16 de septiembre.

Pública puede decidir no admitir ningún sistema de identificación electrónica diferente de un certificado, algo que resultaría disfuncional con lo establecido en el Reglamento eIDAS, en cuya virtud, como veremos, se consagra el derecho de los ciudadanos (al menos, de los residentes en otros Estados de la Unión Europea) a la admisión de los sistemas de identificación electrónica de nivel sustancial o alto publicados por la Comisión Europea, los cuales no tienen por qué basarse en certificados electrónicos.

Este problema se resuelve mediante la norma establecida en el epígrafe 3 del artículo 9 de la LPAC, por la que "en todo caso, la aceptación de […] sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo", norma que residencia una suerte de competencia exclusiva del Estado referida a la admisión general de sistemas de identificación electrónica[451], con efectos en los restantes niveles de Administración, que entiendo ofrecería la cobertura legal para que el Estado pueda cumplir con las obligaciones que le impone el Reglamento eIDAS en cuanto al reconocimiento de los sistemas de identificación[452]; pero que también se extiende a otros sistemas de identificación electrónica que sólo se empleen en el territorio nacional, por lo que en último término es el Estado el que decide, con carácter general, la admisión de cualesquiera sistemas por todas las Administraciones y, por tanto, la extensión del derecho subjetivo de los ciudadanos al uso de estos sistemas para la tramitación[453], que podrán emplearlos para identificarse directamente frente a las citadas Administraciones.

Dichos sistemas no tienen por qué resultar idóneos para determinados trámites o servicios, por lo que las restantes Administraciones deben poder oponerse a su uso, posibilidad que, en mi opinión, encuentra acomodo en la referencia "salvo prueba en contrario" contenida en este epígrafe; prueba cuya carga corresponderá a la Administración, y que deberá ser suficientemente justificada, dado que la negativa a la admisión limita el derecho del ciudadano a la tramitación.

Asimismo, dado que la LPAC no impone ninguna obligación de gratuidad en el uso de los sistemas de identificación electrónica –a diferencia de la LAE y de la LUTICAJ–, nos podemos encontrar con prestadores privados de sistemas de identificación electrónica que

---

[451] La citada STC de 24 de mayo de 2018, también en su FJ 9, considera que "a la vez que dinamiza la autoorganización administrativa, la Ley garantiza un tratamiento común a todos los ciudadanos al atribuirles el derecho a utilizar ante cualquier Administración pública los sistemas de identificación electrónica que haya admitido la Administración General del Estado. Consecuentemente, la disciplina sobre la identidad electrónica de la Ley 39/2015, al tiempo que preserva amplios márgenes de autoorganización de las Administraciones Públicas, cumple una función típica de las normas de «procedimiento administrativo común»: «garantizar un tratamiento asimismo común de los administrados ante todas las Administraciones Públicas» (STC 227/1988, FJ 27)".

[452] De nuevo, la citada STC indica, también en su FJ 9, que "el art. 9.3 de la Ley 39/2015 permite cumplir el art. 6.1 del Reglamento eIDAS. Si el Reino de España reconoce un sistema de identificación electrónica de otro Estado miembro de la Unión Europea, el art. 9.3 de la Ley 39/2015 habilita su utilización ante cualquier Administración nacional, que es lo que exige el art. 6.1 del Reglamento eIDAS".

[453] Para el TC, "dejando a un lado consideraciones de oportunidad y técnica legislativa, que no nos corresponden, lo relevante es que la normativa efectivamente establecida y sometida a nuestro enjuiciamiento es un ejercicio de la libertad de configuración legislativa constitucionalmente garantizada que no desborda los límites del art. 149.1.18 CE y, por tanto, no invade las competencias autonómicas en materia de organización y procedimientos administrativos" (FJ 9).

pretendan cobrar una tarifa por su uso por parte de las Administraciones Públicas.

Cierto es que, como veremos con mayor detalle, el Reglamento eIDAS impone esta gratuidad en el caso de los medios de identificación electrónica por los organismos del sector público, pero sólo en relación con las operaciones de autenticación transfronteriza, por lo que se podría generar la duda acerca de la viabilidad jurídica del cobro en operaciones "domésticas".

En mi opinión, cuando nos encontremos ante el uso de un certificado cualificado para la identificación electrónica, deberemos acudir a la previsión contenida en el artículo 24.4 del Reglamento eIDAS[454], al que nos referiremos posteriormente, que aplica en todo caso, con independencia de si la operación es transfronteriza o no, lo que resolvería el problema potencial en este caso, pero no en el de los restantes medios de identificación que eventualmente pueda aceptar la Administración General del Estado, que por tanto no tienen la gratuidad legalmente impuesta, al menos por la LPAC.

No creo que exista base legal para que un acto unilateral de aceptación de un sistema de identificación electrónica por parte de una Administración pueda obligar a las restantes Administraciones Públicas a adquirir el sistema a cambio de un coste, dada la evidente infracción de las normas de contratación pública que ello supondría, por lo que cabe imaginar que el Estado únicamente hará uso de esta potestad en relación con sistemas de identificación electrónica que sean de uso gratuito.

Refuerza esta interpretación el artículo 7.f) del Reglamento eIDAS, al que nos referimos posteriormente, y que exige la gratuidad de la autenticación transfronteriza. En este sentido, y aunque el mismo no sería aplicable en operaciones dentro del territorio nacional, resultaría hacer de peor condición –económicamente hablando– estas operaciones domésticas que las transfronterizas.

En todo caso, y desde una perspectiva más operativa, para que esta potestad de la Administración General del Estado de admisión de sistemas de identificación de uso obligatorio por las restantes Administraciones Públicas sea realizable, se requiere de alguna plataforma técnica que permita a cualesquiera Administraciones el uso efectivo de los citados sistemas de identificación.

Esta plataforma será, con una elevada probabilidad, el sistema Cl@ve anteriormente presentado, por lo que habrá que estar atento al eventual establecimiento de las condiciones económicas de uso del sistema Cl@ve que se prevén en el epígrafe 3 del apartado quinto del Acuerdo del Consejo de Ministros que aprueba dicho sistema y en la Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, y sin perjuicio de que las Administraciones Públicas puedan establecer sus propias plataformas[455].

Se podría, de todos modos, realizar una interpretación diferente del artículo 9.3 de la LPAC, en el sentido de entender que el mismo es aplicable en los casos en que un

---

[454] En cuya virtud "los prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente".

[455] Sin que, en este caso, resulte aplicable lo previsto en la disposición adicional segunda de la LPAC.

interesado se debe identificar frente al punto general de acceso electrónico de la Administración General del Estado para acceder, desde allí, a un trámite de otra Administración Pública, como por ejemplo a los efectos de acceder a una notificación por comparecencia electrónica, una posibilidad que se encuentra implementada a efectos de la Ventanilla Única de la Directiva de Servicios.

En este caso se podría entender mejor el establecimiento de una norma de admisión general por parte de la Administración General del Estado de sistemas de identificación con eficacia frente a otras Administraciones, así como de una presunción *iuris tantum* al respecto de la misma, salvo prueba *en contrario*. Esta interpretación sería, en mi opinión, más respetuosa con el sistema y, al tiempo, más realista desde la perspectiva tecnológica.

Finalmente, cabe reseñar que, a tenor de lo establecido en el artículo 11.1 de la LPAC, "con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley", por lo que se restringe fuertemente la necesidad de proceder a la firma o sello electrónico para la autenticación de la actuación realizada, en una de las escasas muestras de innovación que pueden encontrarse en la norma, y a la que nos referiremos con detalle al tratar el régimen sectorial de uso de la firma en el ámbito de la administración pública[456].

[456] Cfr. el epígrafe 5.2.2.5 de este trabajo.

CAPÍTULO 3. EL USO DE LOS MEDIOS DE IDENTIFICACIÓN ELECTRÓNICA PERSONAL PARA LA AUTENTICACIÓN TRANSFRONTERIZA EN LA UE

Después de haber presentado el concepto de identificación electrónica y su marco regulatorio en la Unión Europea (Capítulo 1) y los medios de identificación electrónica válidos en España, en especial aquellos de titularidad pública (Capítulo 2), en este Capítulo nos vamos a ocupar del uso de los medios de identificación electrónica personal para la autenticación transfronteriza en la Unión Europea.

En efecto, constituye ahora objeto de interés conocer el régimen legal que permite extender el uso de los medios anteriormente estudiados, normalmente de alcance estrictamente nacional y por tanto limitados al territorio del correspondiente Estado miembro, de modo que los mismos puedan ser también empleados en las relaciones con elemento internacional donde sea precisa una autenticación personal, pero siempre que este elemento internacional se limite al ámbito territorial de alcance del Reglamento eIDAS.

El primer epígrafe de este Capítulo se ocupa de los requisitos que exige la normativa de la Unión para que se pueda materializar esta autenticación transfronteriza, requisitos que no constituyen un régimen jurídico de aplicación obligatoria a los sistemas de los Estados miembros, sino que sólo sirven para evaluar si dichos sistemas son apropiados, y en qué grado, para este uso transfronterizo. De este modo, nos encontramos ante una regulación que sólo resultará aplicable cuando un Estado miembro desee extender el uso de un sistema de identificación electrónica a relaciones jurídicas con terceros Estados.

El epígrafe segundo de este Capítulo se dedica al análisis detallado de los efectos jurídicos previstos en la normativa en caso de la ya mencionada extensión de uso de los sistemas domésticos de identificación electrónica a las relaciones transfronterizas, analizándose el efecto de autenticación para el acceso a los servicios públicos electrónico, expresamente previsto en el Reglamento eIDAS, y la posibilidad de que dichos sistemas también se puedan emplear en las relaciones jurídico-privadas, que el Reglamento no regula, limitándose a recomendar esta opción, pero que otras normas pueden habilitar, tanto en el nivel europeo como en el nacional.

3.1 LOS REQUISITOS PARA LA NOTIFICACIÓN DE SISTEMAS DE IDENTIFICACIÓN ELECTRÓNICA

3.1.1 Los sistemas de identificación electrónica susceptibles de notificación

En primer lugar, el artículo 7.a) del Reglamento eIDAS indica que los medios de identificación electrónica en virtud del sistema de identificación electrónica deben haber sido expedidos, alternativamente, por el Estado miembro que efectúa la notificación, por mandato del Estado miembro que efectúa la notificación, o independientemente del Estado miembro que efectúa la notificación y reconocidos por dicho Estado miembro.

Se trata, en mi opinión, de una muestra del carácter de servicio público de administración

electrónica[457] que impregna la regulación de la identificación electrónica en el Reglamento eIDAS[458], y que supone una nueva muestra de diversidad potencial entre los Estados miembros de la Unión Europea[459], puesto que, en efecto, el Reglamento eIDAS prevé hasta tres posibles regímenes jurídicos referidos a los medios identificación electrónica susceptibles de notificación[460], que tienen en común la necesaria intervención previa del Estado en cuestión para su reconocimiento transfronterizo.

La primera posibilidad es notificar un medio de identificación electrónica expedido por el propio Estado miembro; es decir, de su titularidad, como por ejemplo sucedería con sistemas como el DNI electrónico, el sistema Cl@ve en sus diversas modalidades, u otros expedidos por las Administraciones Públicas al amparo de la normativa de administración electrónica, u otra normativa diferente, incluída la normativa reguladora de los servicios de confianza de expedición de certificados.

La segunda posibilidad se refiere a la notificación de un medio de identificación electrónica expedido por una entidad diferente del Estado que realiza la notificación, pero bajo su mandato, de acuerdo con lo que se establezca en el Derecho nacional.

Finalmente, la tercera posibilidad se basa en el acto jurídico de previo reconocimiento, por el Estado, de un sistema de identificación electrónica diferente de los anteriores; esto es, expedido de forma independiente del Estado, categoría donde podemos englobar sistemas de identificación electrónica operados por entidades privadas[461], incluyendo entidades financieras, operadoras de servicios de comunicaciones electrónicas, o prestadores de servicios de la sociedad de la información, como portales de servicios de Internet, o de redes sociales, entre otros muchos.

Estos dos primeros casos de expedición de medios de identificación electrónica resultarían asimilables a verdaderos servicios públicos[462], cuanto menos en su noción más

---

[457] Cfr. el Considerando (14) del Reglamento eIDAS, cuando establece que "el principio de reconocimiento mutuo debe referirse únicamente a la autenticación a efectos de un servicio en línea. El acceso a estos servicios en línea y su prestación final al solicitante deben estar estrechamente vinculados al derecho a recibir dichos servicios en las condiciones fijadas por la legislación nacional", mostrando la conexión instrumental evidente entre los medios de identificación electrónica y el acceso a los servicios públicos de administración electrónica.

[458] En este sentido, la Propuesta de Reglamento eIDAS, indica en su epígrafe 3.2.a), en el que se justifica la prueba de necesidad a efectos del principio de subsidiariedad, que "la identificación electrónica no se puede abordar en la propuesta de Reglamento del mismo modo genérico que los demás servicios electrónicos de confianza, porque la expedición de medios de identificación constituye una prerrogativa nacional".

[459] Puede verse esta diversidad en la referencia a las diferentes credenciales a que se refiere (Merchán Murillo, 2016, pág. 49 y ss.).

[460] Como indica la Propuesta de Reglamento eIDAS, uno de los requisitos es que "los correspondientes medios de identificación electrónica sean expedidos por el Estado miembro que notifica un régimen, en su nombre o, al menos, bajo su responsabilidad".

[461] Así se indica en el documento de trabajo de los servicios de la Comisión correspondiente al Resumen de la evaluación de impacto que acompaña a la Propuesta de Reglamento eIDAS, cuando indica que "el concepto de identificación electrónica notificada no se limita a las expedidas por el sector público. Los Estados miembros podrían también notificar las eID expedidas por el sector privado que reconocen para sus propios servicios del sector público. Este enfoque es necesario, ya que no todas las autoridades de los Estados miembros expiden eID".

[462] Más concretamente, como ha puesto de manifiesto (Martínez Gutiérrez, 2009, págs. 225-232), la

amplia o imprecisa en Derecho español[463], que la identifica con la actividad administrativa en general, desde cuya perspectiva la principal diferencia entre ambos casos vendría dada por la modalidad de gestión de dicho servicio público, que sería directa en el primer caso, e indirecta en el segundo, resultando aplicables las reglas legales establecidas para la gestión de servicios, en función del tipo de Administración titular o mandante del servicio, así como las correspondientes normas para la contratación pública.

Sin embargo, dependiendo del caso, podemos defender también la expedición de medios de identificación electrónica como servicio público en sentido estricto, al concurrir las condiciones que la doctrina ha venido exigiendo para ello[464], como se pone de manifiesto en casos como el DNI-e, que se encuentra reservado al Estado. Esta consideración, referida al medio de identificación, es compatible con la noción amplia de servicio público electrónico sobre el sistema de identificación globalmente considerado[465], que permite la convivencia de estos medios monopolísticos con otros medios privados, como veremos a continuación.

Precisamente, este tercer caso resulta algo más complejo, porque en el mismo el Estado ni es titular del servicio público, ni el mismo se presta bajo su mandato, sino que podría ser simplemente un consumidor más de un sistema de identificación electrónica, que podría ser público[466] o privado.

---

legislación sobre administración electrónica, tanto española como de otros Estados de la Unión Europea, suele referirse al servicio público electrónico en este sentido amplio o e impreciso, referido a toda la actividad administrativa desarrollada a través de las tecnologías de la información y la comunicación, incluyendo aquella que se produce en la dimensión interna de la Administración y, también, en la dimensión externa o que se dirige a los ciudadanos. Este autor también diferencia, de forma acertada, entre el concepto de servicio público electrónico y el procedimiento administrativo electrónico; de modo que los servicios de identificación electrónica a los que nos estamos refiriendo encontraría acomodo en los denominado servicios públicos transaccionales, si bien el mismo autor se refiere a los sistemas de firma electrónica –que se han venido empleando para esta función de identificación– como instrumento para el acceso a los servicios públicos, enfatizando su carácter instrumental.

[463] Y no tanto en un sentido estricto, que no resulta reconocible en el del ordenamiento jurídico comunitario, que como explica (Miguez Macho, 2004) "no parece conocer ni mostrar el menor interés por la técnica del servicio público, a pesar de su importancia en muchos de los Estados miembros de la Comunidad y de que uno de los principios fundamentales del mercado común es el derecho de establecimiento y de libre prestación de servicios. […] De hecho, el Ordenamiento jurídico de la Comunidad europea se ha ocupado de los servicios públicos sobre todo cuando hace falta eliminar obstáculos a la libre competencia en los sectores económicos en los cuales se halla más avanzada la llamada armonización comunitaria, como el transporte, las telecomunicaciones o la energía eléctrica"; ello sin perjuicio de la innegable evolución que en esta materia se ha producido en la Unión Europea. En este sentido, cfr. la denominación de los servicios públicos en línea que se produce en relación con las actuaciones europeas referidas a la administración electrónica.

[464] Cfr. la discusión sobre las notas del servicio público y su evolución posterior, aplicada a las infraestructuras de Internet, en (Moles Plaza, 2004, págs. 50-63).

[465] Dado que el sistema de identificación electrónica se refiere también a los nodos de la arquitectura de interoperabilidad de identificación electrónica, encargados de ofrecer soporte a las operaciones de autenticación transfronteriza, también reservadas a las autoridades públicas; nodos que podrán procesar medios de identificación electrónica públicos o privados, indistintamente.

[466] Por ejemplo, en el caso de que, mediante una fórmula de colaboración, un Estado miembro haga uso de un sistema de identificación electrónica responsabilidad de otro Estado miembro, una posibilidad ciertamente extraña, al menos desde la óptica española.

Imaginemos, por ejemplo, que un Estado decide adquirir el derecho de uso de los medios de identificación electrónica suministrados a los ciudadanos por las entidades financieras para que los mismos puedan acceder a los servicios públicos[467], en lugar de expedirlos directamente. No resultaría conveniente que estos medios no pudieran ser empleados también para el acceso a los servicios públicos de organismos de terceros Estados miembros, por lo que este tercer caso se aleja de la noción de servicio público, y opera como mecanismo de extensión del servicio adquirido por dicho Estado al sector privado, frente a terceros Estados.

Como se puede intuir, es en esta tercera posibilidad donde podemos encontrar las soluciones más innovadoras y seguramente adecuadas a la naturaleza de la red Internet, fuertemente marcada por la intervención de múltiples intermediarios, y, por tanto, un nuevo elemento de fuerte diversidad entre los Estados miembros de la Unión.

Además, en los tres casos debemos considerar la posibilidad de que se decida emplear, como medio de identificación electrónica, un servicio de confianza que identifique a una persona; eso es, que se emita o reconozca un certificado, seguramente cualificado, de firma electrónica de persona física o de sello electrónico de persona jurídica.

Sea cual sea el caso, este acto de reconocimiento queda sujeto al Derecho nacional, y no se encuentra exento de retos jurídicos importantes.

En primer término, en la medida en que el acto de reconocimiento tiene aparejado el efecto jurídico de habilitar el medio de identificación electrónica para su uso en la autenticación transfronteriza, la forma en que se ejercite tendrá efectos claros en el mercado. Una posibilidad sería que el Estado reconozca a todos los proveedores privados que cumplan las condiciones para ello, aunque también podríamos encontrarnos ante el establecimiento de límites cuantitativos a los medios de identificación electrónica expedidos por prestadores privados, configurando una suerte de servicio público electrónico virtual[468].

En este caso, se deberían analizar cuidadosamente los efectos sobre la libre competencia derivados de, por ejemplo, reconocer a un único prestador privado (o a un grupo pequeño de prestadores), ya que podría suponer un efecto distorsionador de la misma, en el sentido de conceder una ventaja competitiva en relación con el uso de ese mismo sistema en operaciones *inter privatos*.

Por otra parte, como hemos visto, los sistemas de identificación electrónica se pueden

---

[467] Éste es el caso, por ejemplo, del sistema de identificación electrónica denominado BankID que opera en diversos Estados miembros, como Suecia, donde dispone de 6,5 millones de usuarios, sobre una población de aproximadamente 9,8 millones de personas. Dicho sistema se encuentra participado por las principales entidades financieras de Suecia, y se emplea en múltiples transacciones con el sector público sueco. BankID también existe en Noruega, de nuevo con la participación de las entidades financieras, donde dispone de 3,2 millones de usuarios, sobre una población de aproximadamente 5,15 millones de personas. Se trata de un sistema de firma digital basada en certificados con claves centralizadas. Cfr. (Gjøsteen, 2008).

[468] Esta posibilidad no podría darse si se reconocen los certificados cualificados como medios de identificación, ya que el Reglamento eIDAS no permite limitar el número de prestadores de servicios de confianza tipificados en el mismo; además, posiblemente resultaría también absurdo en el Reglamento eIDAS limitar los certificados cualificados de firma o sello para su uso como medio de identificación a efectos transfronterizos cuando el mismo Reglamento eIDAS obliga a los Estados miembros a aceptarlos cuando exijan una firma electrónica o un sello electrónico.

emplear perfectamente para la acreditación de la identidad en procesos de negocio electrónico –y, en función de la tecnología en que la misma se base, también de la integridad y de la autenticación del origen de los datos–, por lo que los mismos pueden actuar funcionalmente como la firma electrónica o sello electrónico, de modo que la posibilidad de su uso por partes privadas a cambio de un precio puede actuar como factor limitante al desarrollo de dicho mercado[469].

En este sentido, pues, entendemos que el Estado miembro que acuda a esta opción deberá ser diligente en la selección de los proveedores de identidad que reconozca, garantizando condiciones razonables en relación con esta actividad.

Y en este sentido, en segundo lugar debemos preguntarnos acerca de la selección del sistema de identificación electrónica privado a emplear por parte de la Administración, que entendemos debe regirse plenamente por el Derecho nacional y, más concretamente, asumiendo que la prestación del servicio no sea gratuita para la Administración, por las reglas de la contratación pública, actualmente contenidas, para España, en la reciente Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (en adelante, "LCSP/2017"), para lo cual entendemos deberá acudirse a la modalidad que resulte más apropiada en función de la organización del servicio.

Aunque ciertamente no se puede descartar de plano la posibilidad de que el prestador privado del sistema de identificación electrónica no cobre cantidad alguna al Estado que lo utiliza, esta posibilidad parece más bien remota, dados los costes evidentes que puede suponer este uso.

Por tanto, nos encontraremos ante un posible contrato de servicios[470], caso que la Administración adquiera para sí (y eventualmente, para terceros privados) el sistema de identificación electrónica, aunque también se podrá configurar como un contrato de concesión de servicios[471].

En resumen, conviene retener el dato de que, globalmente, el funcionamiento del sistema de identificación electrónica es configurado, en todo caso, como servicio público, con independencia de la consideración también como servicio público, servicio público virtual o servicio privado, de la expedición de los medios electrónicos de identificación dentro de ese mismo sistema.

---

[469] (Dumortier, Kelm, Nilsson, Skouma, & Van Eecke, 2003, pág. 149) indican que el establecimiento, por las Administraciones Públicas, de servicios de certificación para su uso exclusivo en los procedimientos administrativos resulta posible, pero que el uso de dichos servicios para otros usos resulta inadmisible en términos de competencia efectiva, constituyendo una barrera al mercado interior.

[470] Conforme al artículo 17 de la LCSP, "[s]on contratos de servicios aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o suministro, incluyendo aquellos en que el adjudicatario se obligue a ejecutar el servicio de forma sucesiva y por precio unitario".

[471] Conforme al artículo 15.1 de la LCSP, "[e]l contrato de concesión de servicios es aquel en cuya virtud uno o varios poderes adjudicadores encomiendan a título oneroso a una o varias personas, naturales o jurídicas, la gestión de un servicio cuya prestación sea de su titularidad o competencia, y cuya contrapartida venga constituida bien por el derecho a explotar los servicios objeto del contrato o bien por dicho derecho acompañado del de percibir un precio".

3.1.2 El uso de la identificación electrónica para el acceso a los servicios públicos electrónicos en el Estado miembro de expedición

En segundo lugar, el artículo 7.b) del Reglamento eIDAS exige que "los medios de identificación electrónica en virtud del sistema de identificación electrónica puedan usarse para acceder al menos a un servicio prestado por un organismo del sector público que exija la identificación electrónica en el Estado miembro que efectúa la notificación".

Se trata de una exigencia que conecta, como hemos avanzado anteriormente, con el carácter instrumental de la identificación electrónica con respecto al acceso a los servicios públicos, y su consecuencia jurídica principal es impedir la notificación de sistemas que no se empleen para ello.

Esta previsión se puede entender razonable, dado que como hemos visto la notificación de un sistema de identificación electrónica tiene por efecto imponer la obligación a los restantes Estados miembros de la Unión Europea de permitir el empleo de dicho sistema para el acceso transfronterizo a sus propios sistemas de administración electrónica; lógicamente resultaría absurdo que un sistema de identificación electrónica expedido en un Estado miembro y que no puede emplearse en dicho Estado miembro para el acceso a los servicios de administración electrónica sí pudiera, en cambio, emplearse en los restantes Estados miembro.

Sin embargo, no es menos cierto que este requisito deviene en un límite a la posibilidad de extender el uso de sistemas de identificación electrónica privados, ya que no podrá ser objeto de notificación un sistema privado para uso sólo privado, algo que tendría sentido al objeto de facilitar su reconocimiento mutuo, con base en la infraestructura técnica de nodos de interoperabilidad para la autenticación, y en su mapeo con los niveles de seguridad.

3.1.3 La alineación del sistema y los medios de identificación electrónica con un nivel de seguridad predeterminado

En tercer lugar, el artículo 7.c) del Reglamento eIDAS exige que "tanto el sistema de identificación electrónica como los medios de identificación electrónicos en su virtud expedidos cumplan los requisitos de al menos uno de los niveles de seguridad previstos en el acto de ejecución a que hace referencia el artículo 8, apartado 3" del propio Reglamento, de modo que aquellos que no cumplan dichos requisitos quedarían excluidos de esta posibilidad de reconocimiento mutuo[472].

La diferencia que se realiza entre sistema y medio de identificación trae cuenta del tipo de medidas de seguridad a considerar, algunas de las cuales recaen sobre la gestión del sistema, con un enfoque más intenso en los procedimientos, y otras en los medios, con mayor detalle en las correspondientes tecnologías.

En cualquier caso, hay que hacer notar que la obligación de reconocimiento sólo afecta a

[472] En sentido análogo, el epígrafe 1 del artículo del Reglamento eIDAS ordena que "un sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1, deberá especificar los niveles de seguridad bajo, sustancial y alto para los medios de identificación electrónica expedidos en virtud del mismo".

los sistemas de identificación electrónica de nivel sustancial o alto, mientras que, en el caso de sistemas de nivel bajo, dicho reconocimiento es potestativo y, por tanto, dependerá de los acuerdos a los que, en su caso, puedan llegar los Estados miembros.

El Reglamento eIDAS parte del hecho de que "la seguridad de los sistemas de identificación electrónica es esencial para la confianza en el reconocimiento transfronterizo recíproco de los medios de identificación electrónica" (Considerando 19), dado que los mismos "deben caracterizar el grado de confianza de un medio de identificación electrónica para establecer la identidad de una persona, garantizando así que la persona que afirma poseer una identidad determinada es de hecho la persona a quien se ha atribuido dicha identidad" (Considerando 16).

El enfoque del Reglamento eIDAS parte de la diversidad de medios de identificación, que ofrecen niveles de seguridad diferentes. Este nivel "depende del grado de confianza que aporte este medio de identificación electrónica sobre la identidad pretendida o declarada por una persona, teniendo en cuenta los procedimientos técnicos, (por ejemplo, prueba y verificación de la identidad, autenticación), las actividades de gestión (como la entidad que expide los medios de identificación electrónica, el procedimiento para expedir dichos medios) y los controles aplicados", por lo que "los requisitos que se establezcan deberán ser tecnológicamente neutros" y "ser posible cumplir los requisitos de seguridad necesarios mediante diversas tecnologías" (Considerando 16).

Además de esta referencia a los niveles de seguridad de los sistemas y medios de identificación electrónica, y la regulación correspondiente, que se encuentra en el artículo 8 del Reglamento eIDAS, el artículo 10 del mismo Reglamento establece algunas obligaciones en caso de violación de la seguridad.

La noción de nivel de seguridad de los sistemas de identificación electrónica no es, desde luego, original del Reglamento eIDAS, sino que más bien ha sido recibida por el mismo, a partir de la realidad preexistente[473].

En este sentido, el documento *Signposts* partía de esta diversidad, indicando que "aunque su identidad [la de los ciudadanos] debería ser suficientemente segura como para confirmar de forma inequívoca quienes son, la misma debería tomar diferentes formas de acuerdo con los deseos de los ciudadanos y tener en cuenta los diferentes niveles de autenticación que pueden ser requeridos para habilitar el acceso a servicios específicos"[474].

Esta noción fue recogida en el *Plan de acción sobre administración electrónica i2010*[475], que considera a la identificación y autenticación electrónicas como una de las herramientas clave en soporte de los servicios clave de gran impacto para ciudadanos y empresas, y prevé un enfoque pragmático, basado en la existencia de diferentes niveles

[473] En estudios realizados por la Comisión Europea se analiza esta diversidad en los Estados miembros, que incluye el uso de tarjetas físicas, certificados en software, contraseñas de uno o varios factores, contraseñas dinámicas, etc. como se puede ver, por ejemplo, en (Graux & Majava, 2007). También dentro del proyecto STORK se han realizado estudios completos sobre los sistemas de identificación desplegados por los diferentes Estados miembros; cfr. (Eertink, Hulsebosch, & Lenzini, 2008) y (Atzeni & Lioy, 2011).

[474] (European Commission, 2005, pág. 32). La traducción es mía.

[475] Comunicación de la Comisión, de 25 de abril de 2006, «Plan de acción sobre administración electrónica i2010: acelerar la administración electrónica en Europa en beneficio de todos» [COM (2006) 173 final].

de rigor en la implementación de la gestión de la identidad por los Estados miembros[476], en respuesta a necesidades de servicio, tradiciones culturales y preferencias nacionales en relación con la protección de los datos personales.

La *Hoja de ruta de la Comisión Europea para un marco de trabajo para la gestión de identidad pan-Europea*, aprobada en ejecución del *Plan de acción* anteriormente citado, también partió de la existencia de diversos niveles de seguridad en la autenticación, dedicando el bloque III de trabajos previstos en dicha *Hoja de ruta*, dedicados a la "definición de un conjunto de niveles de autenticación utilizando estándares concretos que describan diferentes niveles de seguridad, que puedan ser mapeados a los niveles de seguridad ya implementados por los Estados miembros, y que permitirían a los prestadores de servicios de administración electrónica elegir un nivel de seguridad apropiado"[477], para lo cual es preciso definir los niveles de autenticación en el nivel europeo, y sus correspondientes requisitos[478].

La existencia de múltiples niveles de seguridad en la autenticación también había sido identificada en el contexto de la interoperabilidad de los proyectos IDA (intercambio de datos entre administraciones) de la Comisión Europea y, más concretamente, en aplicación del artículo 7 de la Decisión 1720/1999/CE del Parlamento Europeo y del Consejo de 12 de julio de 1999 por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA), así como el acceso a las mismas[479], que obliga a la Comunidad a "a) definir, en cooperación con los Estados miembros, las prácticas jurídicas y de seguridad de referencia para el intercambio transeuropeo de datos entre administraciones y entre éstas y el sector privado, al objeto de facilitar la adopción de un enfoque común; […] d) establecer y analizar distintos niveles de seguridad, en función de la naturaleza y finalidad de las redes sectoriales; [y] e) elaborar orientaciones y proporcionar soluciones comunes, relativas a la elección y utilización de herramientas, componentes y sistemas destinados a mantener los niveles de seguridad previamente establecidos".

Como se puede ver en los programas de trabajo referidos a las medidas y acciones

---

[476] De hecho, el Plan de acción reconoce que "las tarjetas de identidad nacionales armonizadas podrían constituir una manera concreta de implementar la eIDM en los servicios públicos, pero se trata de algo que cada país debe decidir", y concreta que "las tarjetas de identidad nacionales biométricas y la eIDM para los servicios públicos son cosas claramente distintas: las tarjetas de identidad nacionales atienden a la seguridad pública, por ejemplo facilitando la gestión integrada de fronteras y la lucha contra el terrorismo, mientras que la identificación electrónica para los servicios públicos tiene por finalidad facilitar el acceso y ofrecer servicios personalizados y más inteligentes".

[477] La traducción es mía.

[478] (European Commission. Information Society and Media Directorate-General. eGovernment Unit, 2006, pág. 14).

[479] Modificada por Decisión n° 2045/2002/CE del Parlamento Europeo y del Consejo, de 21 de octubre de 2002, por Decisión n° 786/2004/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004 y por Reglamento (CE) n° 885/2004 del Consejo, de 26 de abril de 2004.

horizontales del programa IDA[480] para los años 2003 y 2004[481], se abordó para ello la definición de una política de autenticación de IDA, basada en las políticas de autenticación previamente existentes en los Estados miembros[482], para la evaluación y el establecimiento, por parte de los gestores de redes sectoriales y proyectos horizontales relativos a la seguridad, de mecanismos de autenticación apropiados para sus proyectos.

Dicha política de autenticación definió ya cuatro niveles de seguridad[483], tres de los cuales resultan nominalmente muy parecidos a los definidos en el Reglamento eIDAS, y posteriormente fue tomada como punto de partida de trabajos posteriores dentro del *programa IDABC* y, más en concreto, del proyecto *eID Interoperability for PEGS* (interoperabilidad de la identidad electrónica para los servicios pan-Europeos de administración electrónica)[484].

Dicho proyecto nace con el objetivo de analizar los requisitos de interoperabilidad de la identidad digital y de la autenticación surgidos de los pilotos de servicios pan-Europeos de administración electrónica, y aporta también una caracterización de niveles de seguridad[485], considerando los niveles previamente definidos en la política de autenticación de IDA[486], así como otras experiencias relevantes, notablemente las Guías del NIST referidas al proyecto *e-Authentication* del Gobierno Federal de los EEUU, y políticas de Estados miembros como Francia, Noruega, Reino Unido y Alemania.

En ambos marcos de trabajo el enfoque que sustenta la definición de los niveles de garantía de la autenticación es el mismo, y se basa en la severidad del impacto de los daños que se podrían producir en caso de amenaza al uso o apropiación indebidos de la identidad de una persona, enfoque que, a la luz del Considerando (16) del Reglamento eIDAS, ha sido acogido por la legislación.

En efecto, en la propuesta para un mecanismo de autenticación multinivel de IDABC, la

---

[480] Este programa comunitario, gestionado por la Dirección General de Informática de la Comisión, sería posteriormente denominado *IDABC – Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens* por Decisión 2004/387/CE de la Comisión de 28 de abril de 2004 - Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC).

[481] Disponibles ambos en http://ec.europa.eu/idabc/en/document/2548/3.html.

[482] En 2003, estas políticas nacionales se basan, con carácter general, en el uso de sistemas PKI de gestión de certificados digitales, por lo que esta acción se relaciona con los proyectos de PKI dentro de IDA, en especial el de crear una Autoridad de certificación puente (European Commission. Directorate-General for Informatics, 2003, pág. 33).

[483] Los niveles son: nivel 1 – garantía mínima; nivel 2 – garantía baja; nivel 3 – garantía sustancial; nivel 4 – garantía alta.

[484] Previsto en el programa de trabajo de IDABC para 2005-2009, disponible en http://ec.europa.eu/idabc/en/document/5101/3.html.

[485] Los niveles son: nivel 1 – garantía mínima; nivel 2 – garantía baja; nivel 3 – garantía sustancial; nivel 4 – garantía alta.

[486] La verdad es que ambos documentos son prácticamente idénticos en este sentido, por lo que parece que el objetivo haya sido reutilizar la política de autenticación IDA, que se enfoca al uso interno de los proyectos de administración electrónica de la propia Comisión, y sus relaciones con los Estados miembros, para ampliar su ámbito de aplicación también a las relaciones con los ciudadanos y las empresas.

garantía de la autenticación se basa en un nivel aceptable de confianza en una identidad de mundo real alegada y en una identidad electrónica presentada a un prestador de servicios a través de una credencial[487].

Más en concreto, la propuesta *IDABC* define un completo juego de amenazas a la autenticación[488], que en caso de ocurrir –con mayor o menor probabilidad[489]– pueden causar daños[490] con un determinado grado de gravedad[491], en un enfoque metodológico de riesgos similar al previsto en el RDENS español.

La noción es que, a mayor probabilidad y mayor impacto (un daño más grave), mayor es el riesgo asociado a una amenaza concreta, de forma que el prestador de un servicio puede valorar si es necesario ser más o menos exigente[492] con respecto a la acreditación de la identidad que se requiere, como se puede ver en la Ilustración 7.

		Impact of damages				
	Likelihood	Very High	High	Medium	Low	Negligible
Risk i	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1
(1): Not applicable to remote authentication over open networks.						

Ilustración 7. Matriz de medida del riesgo y niveles de garantía de identidad en IDABC (Comisión Europea, IDABC)

Por ejemplo, si en caso de una suplantación de la identidad de un ciudadano existe un impacto bajo en relación con la confidencialidad de sus datos personales (por ejemplo,

[487] (Graux & Majava, 2007, pág. 20).

[488] El documento citado se refiere a las mismas con la denominación de riesgos, y son los siguientes: la falsificación de una identidad del mundo real, la falsificación de las informaciones de una identidad, el robo de un elemento de acceso, el robo de una identidad del mundo real, la intercepción o revelación de la información secreta de autenticación, la retención de información secreta de autenticación en un terminal no autorizado, el uso no autorizado de un testimonio de acceso, el uso de una credencial comprometida, el uso de una credencial después de un cambio sustancial de las circunstancias, el uso de una credencial para un uso no intencionado, la retirada de una credencial sin una causa debida, el uso fraudulento de una credencial, el ataque de un hacker y el almacenamiento disperso de la información.

[489] La probabilidad de ocurrencia de la amenaza se define con una escala cualitativa de cinco niveles: rara, improbable, moderada, probable y casi segura. Obviamente, la probabilidad varía en función de las medidas de seguridad implantadas, así como de factores como la motivación de los atacantes.

[490] Referidos a la integridad, la disponibilidad o la confidencialidad de un servicio, a la seguridad personal o a pérdidas financieras.

[491] El grado de impacto se define con una escala cualitativa de cinco niveles: despreciable, bajo, medio, alto y muy alto.

[492] Pudiéndose llegar al extremo de no aceptar la autenticación remota para dicho servicio.

porque el servicio no contiene datos muy relevantes) y la probabilidad de que dicha suplantación pueda ocurrir es moderada, será suficiente con emplear un mecanismo que autenticación que ofrezca un nivel 2 o bajo de garantía. Sin embargo, si el daño causado fuera alto (porque los datos son sensibles), entonces sería preciso incrementar el nivel de garantía exigible al nivel 3 o sustancial.

A partir de los trabajos de IDABC indicados[493], nos debemos referir al proyecto STORK, donde se produce un avance importante en cuanto a la definición de los niveles de seguridad en la autenticación, a partir de la realización de pilotos reales, estableciéndose un enfoque basado en la calidad de las diferentes soluciones de autenticación, de forma que "cada nivel de garantía describe el grado de acuerdo con el que una parte en una transacción electrónica puede confiar en que la información de identidad que le es presentada por un proveedor de identidad realmente representa a la entidad referida en la misma"[494].

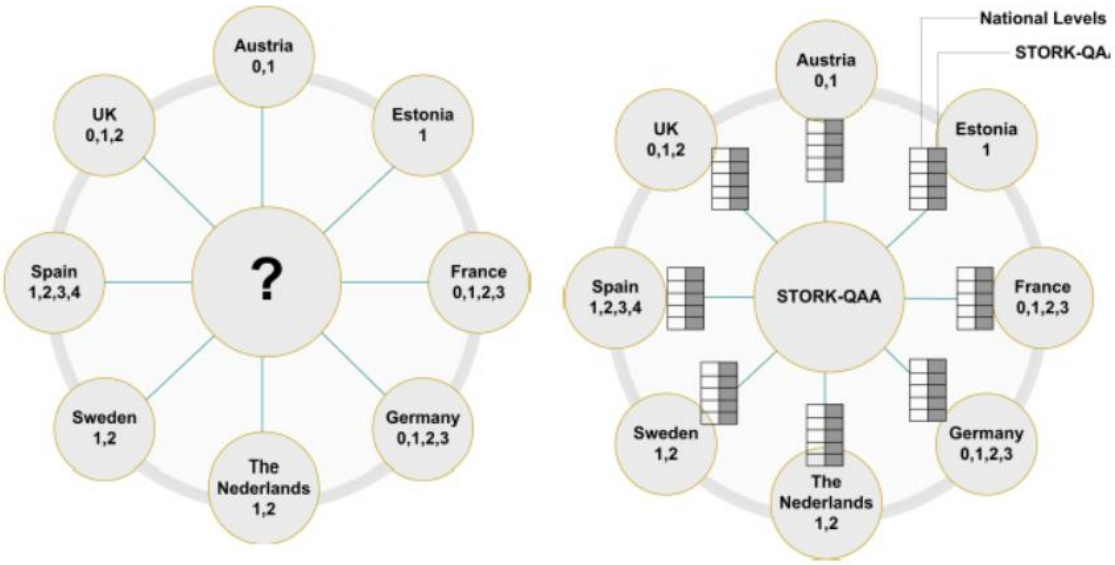


Ilustración 8. Mapeo de niveles de aseguramiento de autenticación en STORK (Consorcio STORK)

Los niveles de garantía de STORK se definen en el marco de trabajo de aseguramiento de la calidad de la autenticación (QAA), que se emplea para el mapeo entre el nivel de seguridad de los sistemas de identificación electrónica de los Estados miembros entre ellos. Los niveles se encuentran definidos en atención a los requisitos (típicamente, de un servicio) referidos a la identidad de un usuario[495], por lo que STORK no aborda otras modalidades de autenticación incorporadas a la definición del Reglamento eIDAS, centrándose en la autenticación de entidad o identificación en sentido estricto.

Por ejemplo, si en España se considera preciso –por ejemplo, en aplicación de los criterios contenidos en el ENS, por la sensibilidad de una información– exigir el nivel alto en un

[493] Aunque también de los trabajos del consorcio internacional Liberty Alliance, que tenía el objetivo de contribuir a la autorregulación de las federaciones de identidad digital.

[494] Cfr. (Eertink, Hulsebosch, & Lenzini, 2008, pág. 55).

[495] (Hulsebosch, Lenzini, & Eertink, 2009, pág. 7).

control de acceso, deberemos poder determinar qué sistemas cumplen con las exigencias del RDENS en este sentido. En lugar de comparar los requisitos de nivel alto del RDENS con todos los sistemas de identificación electrónica expedidos en los restantes Estados miembros de la Unión, algo seguramente inviable, lo que se hará es comparar las exigencias de este nivel alto del ENS con los requisitos del QAA de STORK para seleccionar el nivel de STORK aplicable; a partir de ahí, como cualquier sistema de identificación electrónica expedido en otro Estado miembro se encuentra clasificado en uno de los niveles de QAA de STORK, podemos reconocerlo como equivalente al nivel correspondiente del RDENS[496].

Por otra parte, los niveles de QAA de STORK se definen en términos de series de requisitos sobre factores de autenticación relevantes, y cada requisito define las propiedades funcionales y técnicas que se deben satisfacer por dicho factor de autenticación.

Estos factores se dividen en factores de tipo organizativo, referido a la fase de registro de la identidad, incluyendo los niveles de calidad del procedimiento de identificación (ID), de calidad del proceso de expedición de la credencial (IC), y de calidad de la entidad expedidora (IE); y de tipo técnico, referidos a la fase de autenticación electrónica, incluyendo los niveles de calidad del tipo y robustez de la credencial expedida (RC) y de calidad en la seguridad del mecanismo de autenticación (AM)[497]:

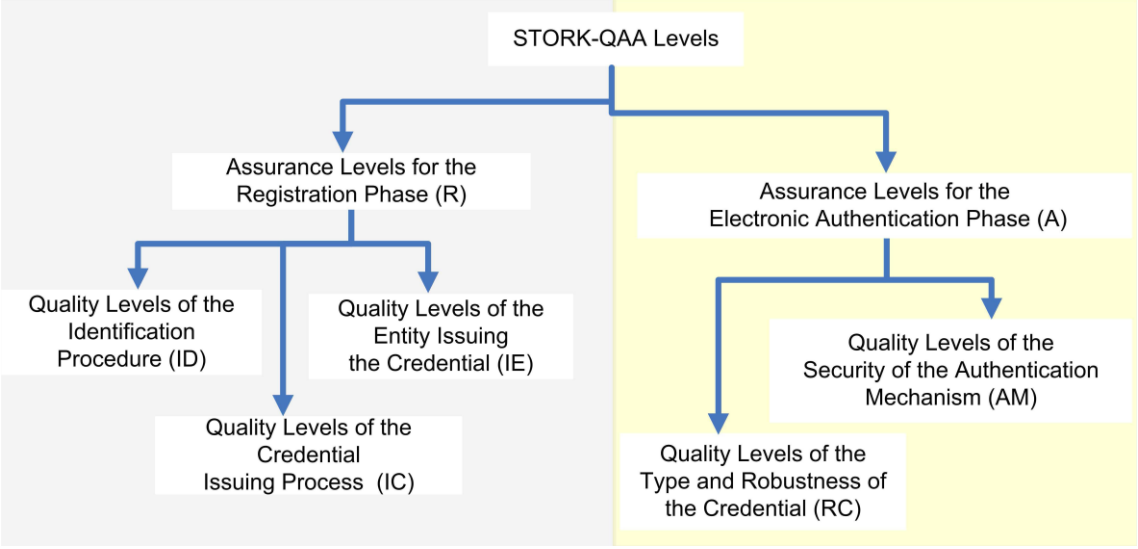


Ilustración 9. Factores que influyen en los niveles de QAA de STORK (Consorcio STORK)

La idea es que la calidad mínima de un sistema de identificación se corresponde con el nivel mínimo que alcance cada uno de esos cinco factores, por lo que el enfoque de STORK es abstracto, permitiendo la subsunción en el mismo de las concretas soluciones existentes en los Estados miembros[498] y su traducción a los niveles requeridos para el

[496] Este enfoque se muestra en (Hulsebosch, Lenzini, & Eertink, 2009, pág. 12).

[497] Cfr. (Hulsebosch, Lenzini, & Eertink, 2009, pág. 19).

[498] Esto no se encuentra exento de problemas prácticos, algunos de los cuales se han manifestado en el propio proyecto STORK. Por ejemplo, en algún Estado existen medios de identificación electrónica de

acceso a los servicios en los restantes Estados miembros, como se puede ver en la Ilustración 10[499].

Por ejemplo, España emplea un esquema de tres niveles de seguridad para la autenticación, de modo de los sistemas de nivel 1 en España mapean contra los niveles 1 y 2 de STORK; los de nivel 2 en España, contra nivel 3 de STORK; y finalmente, los de nivel 3 en España, contra nivel 4 de STORK. En un acceso a Austria, por ejemplo, donde se exige nivel 1 en el nivel nacional austriaco, dado que el mismo mapea contra nivel 4 de STORK, se exigirá el nivel 3 de España.

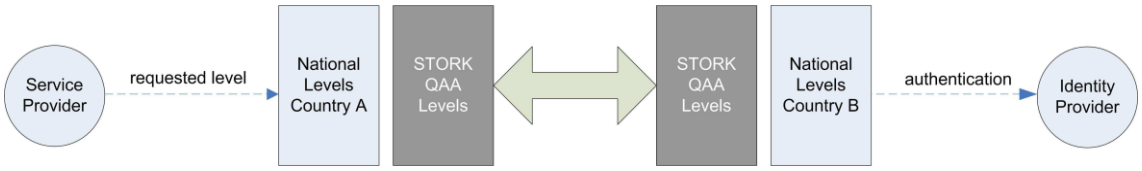


Ilustración 10. Aplicación del mapeo de niveles de seguridad en STORK (Consorcio STORK)

No resulta sorprendente, pues, que el Considerando (16) del Reglamento eIDAS reconozca de forma expresa que "como resultado de las actividades la normalización y las actividades internacionales de la financiación de la Unión de proyectos piloto a gran escala, existen varias definiciones y descripciones técnicas de niveles de seguridad", para añadir que "en particular, los proyectos piloto a gran escala STORK e ISO 29115[500] se refieren, entre otros, a los niveles 2, 3 y 4 que deben tenerse en cuenta en la máxima medida para establecer los requisitos técnicos mínimos, las normas y los procedimientos para los niveles de seguridad bajo, sustancial y alto entendidos en el sentido del presente Reglamento, garantizando al mismo tiempo la aplicación coherente del presente Reglamento, en particular con respecto al nivel de seguridad alto en relación con la acreditación de identidad para la expedición de certificados cualificados", referencia que tiene como efecto condicionar la posterior aplicación del Reglamento, que deberá alinearse con dichos referenciales[501].

Los niveles de seguridad se describen en el artículo 8.2 del Reglamento eIDAS, en forma de una serie de criterios –que son de alto nivel y en cierto modo abstractos– que sustentan un grado concreto de confianza en el medio de identificación emitido a la persona, descritos en dicho epígrafe, al tiempo que reducen o evitan el riesgo de uso indebido o alteración indebida de la identidad.

Sin perjuicio de entrar posteriormente en el análisis de los elementos referidos a cada uno de los niveles de seguridad, es preciso recordar que estos niveles se diferencian en función

---

niveles diferentes (en sede nacional) que en cambio mapean contra el mismo nivel de seguridad (en sede de interoperabilidad), por lo que resulta imposible para un tercer Estado miembro diferenciarlos en sus políticas de acceso; mientras que en otros casos se da la situación inversa (Hulsebosch, Lenzini, & Eertink, 2009, pág. 32).

[499] Cfr. (Hulsebosch, Lenzini, & Eertink, 2009, pág. 30).

[500] Norma internacional que se introduce en el Anexo A.3.6 de este trabajo.

[501] Como se puede ver, ambos referenciales son manifestaciones de la capacidad de autorregulación privada (especialmente en el caso de ISO/IEC 29115:2013), o público-privada (en el caso de STORK).

del riesgo de uso de la identificación electrónica en un servicio concreto; esto es, en función de la probabilidad de ocurrencia de una amenaza, con un impacto dañino cualitativa o cuantitativamente determinable[502], y que suelen corresponder a lo que en los estándares se denomina niveles de aseguramiento de autenticación, según hemos podido presentar anteriormente.

Los niveles de seguridad previstos se deben concretan posteriormente, según dispone el epígrafe 3 del propio artículo 8 en los siguientes términos: "a más tardar el 18 de septiembre de 2015, teniendo en cuenta las normas internacionales pertinentes, y en los términos del apartado 2, la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los cuales se especificarán los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica a efectos del apartado 1".

De esta forma, el legislador europeo busca la colaboración del ejecutivo comunitario para la concreción práctica de los citados niveles de seguridad, en un caso de reenvío indirecto, y que se sustancia mediante un acto de ejecución mediante el procedimiento de examen[503].

Sin embargo, el legislador europeo fija unos contenidos esenciales para las citadas especificaciones técnicas mínimas, normas y procedimientos, que a tenor del segundo párrafo del epígrafe 3 del artículo 8 del Reglamento eIDAS "se establecerán en referencia a la fiabilidad y la calidad de los siguientes elementos:

a) el procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los medios de identificación electrónica[504];

b) el procedimiento para expedir los medios de identificación electrónica solicitados[505];

c) el mecanismo de autenticación mediante el cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a una parte usuaria[506];

d) la entidad que expide los medios de identificación electrónica[507];

e) cualquier otro organismo que intervenga en la solicitud de expedición de los medios de identificación electrónica, y

f) las especificaciones técnicas y de seguridad de los medios de identificación electrónica[508]".

---

[502] De acuerdo con el enfoque descrito en (Graux & Majava, 2007, pág. 20).

[503] Previsto en el artículo 48.2 del Reglamento eIDAS, al que nos referiremos en otro lugar.

[504] Cfr. los criterios de calidad del procedimiento de identificación (ID) de los niveles de QAA de STORK (Hulsebosch, Lenzini, & Eertink, 2009, págs. 20-21).

[505] Cfr. los criterios de calidad del procedimiento de emisión (IC) de los niveles de QAA de STORK (Hulsebosch, Lenzini, & Eertink, 2009, págs. 21-22).

[506] Cfr. los criterios de tipos y robustez de la credencial de identidad (RC) de los niveles de QAA de STORK (Hulsebosch, Lenzini, & Eertink, 2009, págs. 25-26).

[507] Cfr. los criterios de calidad de la entidad que expide la credencial de identidad (IE) de los niveles de QAA de STORK (Hulsebosch, Lenzini, & Eertink, 2009, págs. 23-24).

[508] Cfr. los criterios de seguridad de los mecanismos de autenticación (AM) de los niveles de QAA de STORK (Hulsebosch, Lenzini, & Eertink, 2009, págs. 26-28).

Este acto de ejecución es el Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, "Reglamento de seguridad eIDAS").

De acuerdo con su Considerando (2), este Reglamento de Ejecución, "determina las especificaciones, las normas y los procedimientos técnicos mínimos es fundamental a fin de garantizar un entendimiento común en cuanto a los detalles de los niveles de seguridad, así como la interoperabilidad al correlacionar los niveles de seguridad nacionales de los sistemas de identificación electrónica notificados con los niveles de seguridad contemplados en el artículo 8, de conformidad con el artículo 12, apartado 4, letra b), del Reglamento (UE) Nº 910/2014", por lo que su finalidad es doble: por una parte, detallar los criterios de los niveles de seguridad para obtener una comprensión común de los mismos; por otra, facilitar el mapeo entre los niveles de las sistemas estatales con los niveles definidos en el Reglamento eIDAS.

Resulta interesante destacar, en primer lugar, que el Reglamento de seguridad eIDAS parte de lo establecido en la norma internacional ISO/IEC 29115:2013[509], aunque no referencia ningún contenido específico de la misma, debido a que el mismo "difiere de esa norma internacional, en particular por lo que se refiere a los requisitos de prueba y verificación de la identidad, así como a la forma en que se tienen en cuenta las diferencias entre las disposiciones de los Estados miembros en materia de identidad y las herramientas existentes en la UE para el mismo fin", a tenor de su Considerando (3). Asimismo, el Reglamento de seguridad eIDAS considera también los resultados del proyecto STORK anteriormente citado, en su Considerando (4).

En segundo lugar, el Reglamento de seguridad eIDAS establece, en su artículo 1, que "las especificaciones y los procedimientos establecidos en el anexo se utilizarán para especificar el nivel de seguridad de los medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica notificado por medio de la determinación de la fiabilidad y la calidad de los siguientes elementos:

a) inscripción, como se establece en la sección 2.1 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letra a), del Reglamento (UE) Nº 910/2014;

b) gestión de medios de identificación electrónica, como se establece en la sección 2.2 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letras b) y f), del Reglamento (UE) Nº 910/2014;

c) autenticación, como se establece en la sección 2.3 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letra c), del Reglamento (UE) Nº 910/2014;

d) gestión y organización, como se establece en la sección 2.4 del anexo del presente Reglamento, de conformidad con el artículo 8, apartado 3, letras d) y e), del Reglamento

[509] Esta norma, que se introduce en el Anexo A.3.6 de este trabajo, es resultado de la autorregulación privada en esta materia y es objeto de consideración necesaria a tenor de su mención específica en el Considerando (16) y el artículo 8.3 del Reglamento eIDAS, mandato que la Comisión (y los Estados) no puede desoír.

(UE) Nº 910/2014".

La noción es que el Reglamento que estamos analizando va a determinar, para cada uno de estos elementos[510], una o varias especificaciones y/o procedimientos, que contribuyen a que los Estados miembros puedan confiar en el medio de identificación electrónica, por lo que conviene presentarlos a continuación.

En primer lugar, el epígrafe 2.1 del Anexo del Reglamento de seguridad eIDAS se refiere a la inscripción en el sistema de identificación electrónica, en relación con la cual determina criterios para la solicitud y registro; la prueba y verificación de la identidad (de persona física, de persona jurídica); y la vinculación entre los medios de identificación electrónica de personas físicas y jurídicas.

Este apartado contiene los controles apropiados para el alta de un nuevo usuario en un sistema de identificación electrónica, frecuentemente también denominada "fase de registro", como en el marco de trabajo de QAA de STORK.

En segundo lugar, el epígrafe 2.2 del Anexo del Reglamento de seguridad eIDAS se refiere a la gestión de los medios de identificación electrónica, estableciendo criterios referidos a las características y diseño de los medios de identificación electrónica; a la expedición, entrega y activación de los mismos; a la suspensión, revocación y reactivación de los mismos; y a la renovación y sustitución de estos mismos medios.

Se adopta, en este caso, un enfoque de procesos de gestión organizados alrededor del ciclo de vida de los medios de identificación electrónica, o credenciales, que requerirá las correspondientes adecuaciones a cada tecnología.

En tercer lugar, el epígrafe 2.3 del Anexo del Reglamento de seguridad eIDAS se refiere a la autenticación, en relación con la que esencialmente establece requisitos referidos al mecanismo de autenticación, a través del cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a la parte usuaria.

Esto es, en esta fase es donde la persona emplea su credencial para alegar su identidad ante el servicio al que pretende acceder, mediante el uso del protocolo técnico correspondiente, debiéndose hacer notar que este proceso únicamente permite confiar en los datos de identificación de la persona, y no predica nada acerca de la idoneidad de dichos datos a los efectos del servicio al que se accede[511].

Finalmente, el epígrafe 2.4 del Anexo del Reglamento de seguridad eIDAS se refiere a la gestión y organización de los participantes que presten un servicio relacionado con la identificación electrónica en un contexto transfronterizo, a los que denomina proveedores, medidas que incluyen determinadas disposiciones generales; avisos publicados e información del usuario; gestión de la seguridad de la información; conservación de la información; instalaciones y personal; controles técnicos y cumplimiento y auditorías.

Concretando los niveles de seguridad, el artículo 8.2.a) del Reglamento eIDAS establece que "el nivel de seguridad bajo se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en

[510] Bastante alineados con los previstos en la sección 8 de la norma internacional ISO/IEC 29115:2013, que establece las fases del marco de trabajo de la autenticación de entidad.

[511] Cfr. sección 8.3 de la norma internacional ISO/IEC 29115:2013.

referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad"; definición que parece corresponder al nivel 2 o bajo del STORK QAA, que se define como "el nivel empleado por aquellos servicios donde el daño causado por una apropiación indebida de una identidad del mundo real tiene un impacto bajo", por lo que aunque no se exige la presencial personal del solicitante durante el registro, una entidad sujeta a un acuerdo específico con el Gobierno debe validar su identidad del mundo real y expedirle una credencial, que debe ser entregada con garantías de precisión y seguridad, y se deben emplear protocolos de autenticación suficientemente seguros durante la fase de autenticación[512].

En segundo lugar, el artículo 8.2.b) del Reglamento eIDAS establece que "el nivel de seguridad sustancial se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad"; definición que parece corresponder al nivel 3 o sustancial del STORK QAA, que se define como "el nivel empleado por los servicios que pueden sufrir daños sustanciales en caso de un mal uso de la identidad", por lo que el registro de una identidad se procesa con métodos que identifican al solicitante de forma no ambigua y con un alto nivel de certeza; los proveedores de identidad son supervisados o acreditados por el Gobierno; las credenciales libradas son al menos certificados en software; y los mecanismos de autenticación empleados son robustos[513].

Finalmente, En tercer y último lugar, el artículo 8.2.c) del Reglamento eIDAS establece que "el nivel de seguridad alto se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es evitar el uso indebido o alteración de la identidad"; definición que parece corresponder al nivel 4 o alto del STORK QAA, que se caracteriza como "el nivel más alto de aseguramiento, dirigido a los servicios donde el daño causado por un mal uso de la identidad podría tener un gran impacto", por lo que el registro requiere al menos una vez la presencia personal del solicitante o un encuentro personal con el mismo o, alternativamente, la validación de su identidad mediante una firma electrónica confiable, como por ejemplo mediante el empleo de un certificado electrónico reconocido basado en dispositivo seguro de creación de firma, todo ello expedido por un prestador cualificado[514].

---

[512] (Hulsebosch, Lenzini, & Eertink, 2009, pág. 17).

[513] (Hulsebosch, Lenzini, & Eertink, 2009, pág. 18).

[514] (Hulsebosch, Lenzini, & Eertink, 2009, pág. 18). Por su parte, (Buchmann, Rathgeb, Baier, & Busch, 2014, pág. 173 y ss.) presentan las características de seguridad y el funcionamiento del eIDAS Token, que consideran el futuro estándar de los documentos nacionales de identidad.

3.1.4 La atribución exclusiva de los datos y medios de identificación electrónica

En cuarto lugar, y como especificación del requisito de alineación con un nivel de seguridad predeterminado, los numerales d) y e) del artículo 7 del Reglamento eIDAS exigen la garantía de atribución exclusiva de los datos y los medios de identificación electrónica a la persona en cuestión.

En el primer caso, se exige que "el Estado miembro que efectúa la notificación garantice que los datos de identificación de la persona que representan en exclusiva a la persona en cuestión se atribuyen de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecido en el acto de ejecución a que se refiere el artículo 8, apartado 3, a la persona física o jurídica a la que se refiere el artículo 3, punto 1, en el momento de expedición de los medios de identificación electrónica previstos en este sistema".

Como se recordará, los datos de identificación son aquellos que permiten la identificación de la persona, como por ejemplo en el caso de un certificado electrónico, o de una ficha de identidad contenida en una base de datos.

Dicha garantía debe ofrecerse en los términos del acto de ejecución[515] que define los niveles de seguridad, y en el momento en el que se expiden los medios de identificación; se trata, como veremos, por tanto de un requisito de lo que se conoce como "registro" del usuario, y resulta muy significativo que esta obligación se imponga sobre el Estado –y con la correspondiente responsabilidad[516]–, y no sobre la entidad que expide los medios de identificación, algo que trae cuenta de la importancia fundamental de la identidad digital.

En el segundo caso, en cambio, se exige que "la parte que expide los medios de identificación electrónica previstos en este sistema garantice que los medios de identificación electrónica se atribuyan a la persona a que se refiere la letra d) del presente artículo de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecidos en el acto de ejecución a que se refiere el artículo 8, apartado 3", al que posteriormente nos referiremos.

En este caso, es la parte que expida los medios de identificación quien debe ofrecer esta garantía –y asumir la correspondiente responsabilidad[517]– algo que resulta comprensible dado que es la entidad que se hace cargo de la operación del sistema, debiendo realizarlo con las medidas mínimas de seguridad.

---

[515] Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

[516] Cfr. el artículo 11.1 del Reglamento eIDAS.

[517] Cfr. artículo 11.2 del Reglamento eIDAS.

3.1.5 La disponibilidad de un mecanismo de autenticación en línea

En quinto lugar, el artículo 7.f) del Reglamento eIDAS requiere que "el Estado miembro que efectúa la notificación garantiza la disponibilidad de la autenticación en línea de manera que cualquier parte usuaria establecida en el territorio de otro Estado miembro pueda confirmar los datos de identificación de la persona recibidos en formato electrónico" cuando dicha persona precisa del acceso a un servicio ofrecido en línea por dicha parte usuaria.

En mi opinión, esta obligación es esencial para el funcionamiento del sistema de identificación electrónica, ya que la parte usuaria frente a la que la persona se va a identificar necesita poder comprobar que efectivamente la persona es quien dice ser[518], de acuerdo con el sistema tecnológico en cuestión y por tanto se proyecta sobre el proveedor de identidad correspondiente, al que el Estado deberá trasladar esta obligación.

Sin embargo, la obligación prevista en este epígrafe también se debe entender referida a la necesidad de que el Estado establezca y garantice el funcionamiento global del sistema de identificación electrónica, así como de uno o varios nodos de la arquitectura de interoperabilidad de identificación electrónica[519], todo ello sujeto a un régimen de servicio público electrónico reservado a la autoridad pública competente en cada Estado miembro[520].

De nuevo se trata de un servicio público electrónico, con un marcado carácter instrumental, facilitador de la prestación de otros servicios públicos finalistas o de la realización de procedimientos administrativos electrónicos, en especial desde la perspectiva de relación con el ciudadano; pero también en soporte de la realización de operaciones *inter privatos*, por lo que eventualmente puede superar los mimbres de la denominada administración electrónica.

Y es que la parte usuaria precisa acceder en línea a este proceso de autenticación transfronteriza, de forma que, si el mismo no se encuentra disponible, el acceso al servicio ofrecido por la parte usuaria queda simplemente interrumpido. Por consiguiente, se configura como un servicio de prestación obligatoria, y que como hemos visto se ubica en mano pública, con independencia de la titularidad del medio de identificación electrónica expedido –y del correspondiente proceso de autenticación–, o de la también titularidad del servicio al que se accede mediante la citada autenticación.

De acuerdo con el segundo párrafo de este numeral f), "la autenticación transfronteriza deberá ser gratuita cuando se realice en relación con un servicio en línea prestado por un

---

[518] O, en su caso, el origen y/o la integridad de los datos.

[519] Cfr. la definición contenida en el artículo 2 del Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

[520] Cfr. sección 2.4.1 del Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

organismo del sector público", exigencia que acertadamente persigue evitar el complejo y problemático debate de la facturación por el consumo del servicio entre los diferentes Estados miembros de la Unión Europea, y de la cual podemos, además, inferir *a contrario sensu* que se podrá establecer una tarifa por el uso de este servicio en otros casos –como en el mismo párrafo se viene a dar a entender, mediante la indicación de que "para las partes usuarias distintas de los organismos del sector público, el Estado miembro que efectúa la notificación podrá definir las condiciones de acceso a esa autenticación"–; cuestión que trataremos posteriormente con mayor profundidad.

Que el proceso de autenticación transfronteriza sea gratuito cuando se emplee para el acceso a los servicios públicos electrónicos implica, por otra parte, que también deba ser gratuito el uso del medio de identificación electrónica para dicha autenticación; es decir, que tanto el uso del medio de identificación electrónica (como por ejemplo, el DNI electrónico, o un certificado cualificado, o una contraseña) como de la plataforma técnica que implementa el proceso de autenticación han de ser gratuitos. Y ello con independencia de la titularidad del medio de identificación electrónica por lo que, si la misma es privada, la gratuidad será una condición exigible para el reconocimiento. Y ello con independencia de la titularidad del medio de identificación electrónica por lo que, si la misma es privada, la gratuidad será una condición exigible para el reconocimiento.

En la experiencia española referida al operador de referencia en certificados electrónicos de firma electrónica, la FNMT-RCM[521] precisamente había establecido un modelo de pago donde son los prestadores públicos de servicios electrónicos (en cumplimiento de la legislación de administración electrónica) que se adhieren a su servicio los que sustentan la totalidad de costes asociados a la expedición y posterior gestión de los certificados, de obtención gratuita por los ciudadanos[522], certificados que desde luego se pueden emplear para la identificación electrónica; mientras que el uso del servicio de validación de certificados[523] por los prestadores privados de servicios ha venido exigiendo el abono de las tarifas aprobadas por dicha entidad[524].

Por lo que se refiere a los organismos del sector público, el modelo de negocio de la FNMT-RCM tiene una lógica que hay que reconocer razonable, al menos desde el punto de vista del servicio público al ciudadano, y dentro del contexto del derecho de acceso

---

[521] Con más de 4,5 millones de certificados, es indudablemente el prestador de referencia en certificados software en España.

[522] Nótese, de todos modos, que en el caso de que el medio de identificación electrónica sea un certificado cualificado de firma o sello electrónico, nos encontraremos ante una situación verdaderamente peculiar, dado que – como veremos con mayor detalle al estudiar este tipo de certificado – el Reglamento eIDAS obliga, en su artículo 24.4, al prestador que lo expida a proporcionar "a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos", información que "deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente". Ciertamente, si la validación del certificado se debe poder realizar sin abonar coste adicional alguno al prestador, parecerá difícil establecer un precio por el uso del mismo certificado para la identificación electrónica; aunque no necesariamente por el uso del servicio público electrónico que sustenta el proceso de autenticación electrónica transfronteriza.

[523] Servicio que permite confiar en la autenticación del usuario.

[524] Cfr. el Contrato para la prestación de servicios de consulta del estado de vigencia de certificados electrónicos de la FNMT-RCM, a que antes nos hemos referido.

electrónico a los servicios públicos (electrónicos o no)[525]. En efecto, cobrar una tarifa al ciudadano por el medio de identificación electrónica supone establecer una barrera de entrada que ciertamente penaliza la adopción de la administración electrónica[526]. Dado que el ciudadano no asume el coste, sólo existen dos posibilidades para la financiación del sistema de identificación electrónica; a saber, financiarlo a cargo de los presupuestos generales del Estado, o instaurar un modelo de reparto del coste entre los diferentes organismos del sector público que voluntariamente decidan adherirse a este sistema.

En el caso de la FNMT-RCM, se ha optado por la segunda opción, y además mediante un método de repercusión de costes calculado sobre la población correspondiente al ámbito territorial de actuación de cada Administración Pública, y que se formaliza mediante la firma del correspondiente convenio de colaboración interadministrativa[527], por lo que nos encontramos ante un sistema de membresía.

Sucede, sin embargo, que, en este modelo, los organismos públicos que no se adhieran al convenio no tienen, en principio, derecho al uso de los certificados, algo que entra en contradicción clara con lo establecido en el Reglamento eIDAS, lo que ha obligado a la modificación de este modelo de negocio.

Nada obstaba a mantener el sistema actual de convenios con las entidades del sector público, en la medida en que se puede considerar que a las mismas es a las que interesa financiar la expedición de certificados por la FNMT-RCM, pero si las entidades del sector público que no contribuyen al sostenimiento del sistema tienen derecho a su uso de forma gratuita, situándose en una posición de consumidores libres de cargas o *free riders*, algo que perfectamente pueden hacer porque la AEAT expide certificados en todo el territorio nacional, lo más probable es que se produjera un abandono progresivo del sistema de cofinanciación, en especial en el actual contexto de fuertes restricciones presupuestarias, y que el sistema acabase financiado en exclusiva por la Administración General del Estado.

Como es lógico, si el uso del servicio de identificación electrónica ha de resultar gratuito para las entidades del sector público, ello obliga a decidir si el sistema continúa siendo gratuito o establecer una contraprestación por su obtención por los ciudadanos, mediante la oportuna tasa o precio público, modelo que ya se aplica al DNI-e y que, por tanto, sitúa a ambos organismos en condiciones de competencia, aunque sólo para las personas físicas de nacionalidad española, y no en relación con las personas jurídicas o sus representantes.

Nótese que este reto lo afrontan también los restantes proveedores públicos de identidad, como el Consorci Administració Oberta de Catalunya, que expide certificados idCAT y presta servicios de identificación basados en contraseñas de un solo uso entregadas por SMS, todo ello de forma gratuita a los ciudadanos. En el caso de la FNMT-RCM, se ha

---

[525] Aunque no tanto desde la perspectiva de la libre competencia, cuando dichos sistemas pueden también emplearse para transacciones privadas, como posteriormente analizaremos.

[526] Sin embargo, el DNI-e es un medio de identificación electrónica y de firma electrónica cualificada que se financia mediante la correspondiente tasa asociada al dispositivo físico que lo sustenta, la cual se ha incrementado en el coste extra correspondiente. Y hay que recordar que es de obtención obligatoria por parte de los ciudadanos de nacionalidad española mayores de 14 años.

[527] Bien es cierto que, con algunos factores correctores, como por ejemplo la posibilidad de que un nivel de administración pueda asumir el coste de los niveles inferiores, como en el caso de los convenios con entidades locales supramunicipales, o con las autonomías; factores que buscaban evitar la doble y hasta triple "facturación" de la FNMT-RCM por un mismo ciudadano beneficiario del servicio.

procedido al abandono del modelo de suministro gratuito del servicio a los ciudadanos, y se ha establecido una tarifa por la obtención del certificado de firma electrónica, pero sólo en relación con los de representante de persona jurídica o entidad sin personalidad jurídica, manteniéndose la gratuidad en la expedición de los certificados de persona física.

Finalmente, el segundo párrafo de este numeral exige que "los Estados miembros no impondrán requisitos técnicos específicos desproporcionados a las partes usuarias que tengan intención de llevar a cabo tal autenticación, cuando esos requisitos impidan u obstaculicen significativamente la interoperabilidad de los sistemas de identificación electrónica notificados", al objeto de maximizar el uso potencial de los medios de identificación electrónica en la autenticación transfronteriza en línea.

Esta previsión se refiere a las partes usuarias del sistema; esto es, principalmente los organismos del sector público de los Estados miembros diferentes de aquel en cuyo territorio se ha expedido el medio de identificación electrónica, pero en el fondo protege a los ciudadanos dotados de los citados medios, que son los interesados en poder autenticarse frente a los servicios de administración electrónica, o de otro tipo, en el territorio de otro Estado miembro.

Qué se deba considerar como un requisito técnico desproporcionado, y en qué circunstancias el mismo impide u obstaculiza de forma significativa la interoperabilidad, es una cuestión fáctica que se deberá resolver caso por caso, si bien la imposición de requisitos de instalación o empleo de software por los ciudadanos es un buen candidato[528], pero desde luego nos estamos refiriendo a condiciones técnicas adicionales y diferentes a las que formen parte del marco de interoperabilidad[529] previsto en el propio Reglamento, y deben ser formalmente compatibles con el mismo.

Cierto es que la propia existencia del marco de interoperabilidad, y su aplicación posterior por los Estados miembros, puede aportar elementos que ayuden a objetivar estas circunstancias, lo que refuerza su relevancia como instrumento de *soft law* público.

3.1.6 La notificación previa del sistema

En sexto lugar, el artículo 7.g) del Reglamento eIDAS exige al Estado miembro que desee notificar a la Comisión Europea un sistema de identificación electrónica, que de forma previa –con al menos seis meses de antelación– a dicha notificación presente a los demás Estados miembros una descripción del sistema.

La finalidad de esta actuación es informar a los restantes Estados miembros de la Unión Europea acerca del sistema que se prevé notificar, a efectos de la cooperación entre los mismos prevista en el Reglamento, y que se orienta a la interoperabilidad y seguridad del

[528] En este sentido, el Considerando (19) del Reglamento eIDAS también establece que "toda vez que los sistemas de identificación electrónica puedan requerir el empleo de equipos o programas informáticos específicos por las partes usuarias a escala nacional, la interoperabilidad transfronteriza exige que los Estados miembros no impongan tales requisitos y los costes asociados a las partes usuarias establecidas fuera de su territorio. En tal caso, se deben debatir y desarrollar soluciones adecuadas dentro del ámbito de aplicación del marco de interoperabilidad. Sin embargo, resultan inevitables los requisitos técnicos derivados de las especificaciones intrínsecas de los medios de identificación electrónica nacionales (por ejemplo, tarjetas inteligentes), que pueden afectar a los titulares de esos medios electrónicos".

[529] Así como a los detalles técnicos descritos en las especificaciones dimanantes de los proyectos STORK y STORK 2.0, a que nos referiremos en el epígrafe 3.1.7.2 de este trabajo.

sistema de identificación electrónica objeto de la notificación.

El Reglamento eIDAS no define con precisión el contenido de esta descripción del sistema, pero podemos entender que se tratará de la misma descripción prevista en el artículo 9.1.a) del mismo, como parte de los contenidos de la notificación a remitir a la Comisión Europea.

Así se desprende de lo establecido en el artículo 13 de la Decisión de Ejecución (UE) 2015/296 de la Comisión, de 24 de febrero de 2015[530], que obliga al Estado miembro que vaya a realizar la notificación a remitir a la Red de Cooperación del proyecto de formulario de notificación con los contenidos previstos en el artículo 9.1.a) del Reglamento eIDAS[531].

3.1.7 La garantía de interoperabilidad de identificación electrónica

Por último, el artículo 7.h) del Reglamento eIDAS exige que, para poder ser notificado, un sistema de identificación electrónica debe cumplir obligatoriamente con lo previsto en el marco de interoperabilidad previsto en el artículo 12.8 del mismo Reglamento[532], aprobado por Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015 (en adelante, Reglamento de interoperabilidad eIDAS)[533], del que nos ocupamos a continuación.

3.1.7.1 El marco de interoperabilidad para la identificación electrónica

La interoperabilidad es, como hemos avanzado en el Capítulo 1[534], uno de los elementos clave del enfoque regulatorio de la identificación electrónica, y en este sentido se plasma en el artículo 12.1 del Reglamento eIDAS, que determina que "los sistemas nacionales de

---

[530] Por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al artículo 12, apartado 7, del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

[531] Sin embargo, se debe tener en cuenta que el Considerando (6) de esta misma Decisión de Ejecución (UE) 2015/296 establece, al respecto del procedimiento de revisión por pares, que el mismo "obliga a los Estados miembros notificantes a facilitar suficiente información sobre sus sistemas de identificación electrónica. No obstante, debe tenerse también en cuenta la necesidad de que los Estados miembros preserven la confidencialidad de determinada información, cuando sea fundamental para la seguridad".

[532] Que establece que "a más tardar el 18 de septiembre de 2015, a efectos de establecer condiciones uniformes para la ejecución de los requisitos del apartado 1, la Comisión, sin perjuicio de los criterios establecidos en el apartado 3 y teniendo en cuenta los resultados de la cooperación entre Estados miembros, adoptará actos de ejecución sobre el marco de interoperabilidad tal como se establece en el apartado 4".

[533] El Considerando (6) de este Reglamento reconoce que "el proyecto piloto a gran escala STORK, incluidas las especificaciones que desarrolle, y los principios y los conceptos del marco europeo de interoperabilidad para los servicios públicos europeos se han tenido en cuenta en la mayor medida posible al establecer las disposiciones del marco de interoperabilidad previsto en el presente Reglamento"; mientras que, por su parte, el Considerando (7) del mismo Reglamento indica que "los resultados de la cooperación entre los Estados miembros se han tenido en cuenta en la mayor medida posible". El Reglamento de interoperabilidad eIDAS se ajusta al dictamen del Comité del artículo 48 del Reglamento eIDAS.

[534] Cfr. el epígrafe 1.1.3 de este trabajo.

identificación electrónica notificados de conformidad con el artículo 9, apartado 1, serán interoperables" entre sí, obligación en relación con la cual en el epígrafe 2 del artículo 12 se prevé que "se establecerá un marco de interoperabilidad" (para la identificación electrónica).

El marco de interoperabilidad de la identificación electrónica, de corte sectorial, debe cumplir, a tenor del epígrafe 3 del artículo 12 del Reglamento eIDAS, los siguientes criterios: "a) aspirar a ser neutro desde un punto de vista tecnológico y no discriminar entre soluciones técnicas nacionales específicas para la identificación electrónica dentro del Estado miembro; b) ajustarse a las normas internacionales y europeas, siempre que sea posible; c) facilitar la aplicación del principio de privacidad desde el diseño, y d) garantizar que los datos personales se procesen con arreglo a la Directiva 95/46/CE".

El primer criterio informador del marco de interoperabilidad se refiere a su necesaria neutralidad tecnológica, de modo que no impida la utilización de las diversas soluciones técnicas para la identificación electrónica que se aplican en los Estados miembros, tanto respecto de los medios de identificación existentes como de los procesos de autenticación en que se emplean[535].

Nos encontramos, pues, ante un marco de interoperabilidad que no debe forzar al Estado miembro a modificar sus opciones tecnológicas domésticas –por lo que el ciudadano debe poder continuar empleando el sistema de identificación del que ya disponga–, sino que debe limitarse a la adopción de la tecnología estrictamente necesaria para extender el uso de ese sistema a las actuaciones transfronterizas, y siempre con las mínimas restricciones sobre el ciudadano, en particular en la necesidad de emplear aplicaciones de *software*[536]. Nótese, sin embargo, que se trata de un criterio informador, y de que el mismo se refiere sólo a que el sistema aspire a ser neutro, sin que legalmente deba en todo caso serlo, siendo más una directriz que una verdadera regla jurídica.

El segundo criterio informador apuesta porque el marco de interoperabilidad se base, en la medida que resulte posible, en normas internacionales y europeas[537], en lugar de ser

---

[535] Recuérdese la rica variedad de sistemas y medios existente en los diferentes Estados, que hemos ido reseñando, y cómo el empleo de estándares como el protocolo SAML ayuda a que los mismos sean interoperables en su funcionamiento.

[536] En este sentido, el Considerando (3) del Reglamento de interoperabilidad eIDAS indica que "cuando un Estado miembro o la Comisión proporcionan software para habilitar la autenticación en un nodo explotado en otro Estado miembro, la parte que suministra y actualiza el software utilizado para el mecanismo de autenticación puede acordar con la parte que aloja el software cómo se gestionará el funcionamiento del mecanismo de autenticación. Un acuerdo de este tipo no debe imponer requisitos técnicos o costes desproporcionados (incluidos la asistencia, las responsabilidades, el alojamiento y otros costes) a la parte que realiza el alojamiento", considerando que seguramente se refiere principalmente al *middleware* y al *software* intermediador de inicialmente creado en los proyectos STORK, a que posteriormente nos referiremos, y que actualmente se encuentra incorporado en el acervo de bloques de construcción del Mecanismo Conectar Europa, como componente eID.

[537] Y en este sentido, como hemos presentado anteriormente, el componente eID se basa en estándares internacionalmente aceptados como SAML, que sin embargo no goza de la consideración legal de norma técnica internacional ni europea, sino de especificación técnica de las TIC, porque la misma no ha sido aprobada ni por un organismo internacional de normalización, ni por una organización europea de normalización (cfr. el Reglamento (UE) Nº 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la

creado *ad hoc*, aproximación que también facilita la interoperabilidad, dado que existe un acervo tecnológico creado y adoptado por la industria que se puede reutilizar, reduciendo los costes y tiempos de implementación.

El tercer criterio informador tiene como propósito impulsar que el marco de interoperabilidad aplique el importante principio de "privacidad por el diseño", en línea con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en cuya virtud, y especialmente en este caso, "[e]l responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento" (artículo 25.2), sin perjuicio de otras medidas.

Finalmente, el cuarto criterio informador viene a exigir que los datos personales sean tratados conforme a la normativa reguladora. No nos encontraríamos en este caso ante un principio, sino ante una verdadera obligación jurídica, también recogida en el artículo 5 del Reglamento eIDAS, que ordena que "el tratamiento de los datos personales será conforme a lo dispuesto en la Directiva 95/46/CE", referencia que, en la actualidad, debe entenderse realizada al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, sin perjuicio de que resulte también de aplicación la legislación correspondiente aprobada en el nivel nacional.

Estas dos obligaciones denotan la enorme importancia que presenta la protección de los datos de carácter personal en la identificación electrónica, especialmente dada su estructura de nodos en una red[538]. En efecto, si se instala una red de puntos únicos (en cada Estado) por el que se intermedian todas las autenticaciones transfronterizas por parte de la Administración, resulta evidente el riesgo de seguimiento de la actividad de los ciudadanos y la creación de perfiles de comportamiento, intereses, etc., mediante la exigencia de registro de metadatos acerca de las operaciones[539] o la inspección de la mensajería de las mismas, un riesgo que puede resultar inaceptable desde un punto de vista social[540], en especial a tenor de los debates suscitados al hilo de diferentes programas de vigilancia –secreta y sin control judicial– de ciudadanos por parte de algunos Gobiernos. Para reducir este riesgo, un marco de interoperabilidad de identificación electrónica debe adoptar un enfoque lo más restrictivo posible respecto al tratamiento de los datos personales.

Decisión 87/95/CEE del Consejo y la Decisión Nº 1673/2006/CE del Parlamento Europeo y del Consejo).

[538] En efecto, la arquitectura de interoperabilidad de identificación electrónica es buen ejemplo de una arquitectura de control a la que se refiere (Moles Plaza, 2004), que podría permitir al Estado la obtención de informaciones personales valiosas de los ciudadanos.

[539] Por ejemplo, imagínese que el operador de esta infraestructura registra las autenticaciones de los usuarios a efectos de determinar sus opciones de participación política, mediante los metadatos de las plataformas a las que accede.

[540] Resulta, en este sentido, muy ilustrativo el análisis de (Martin, van Brakel, & Bernhard, 2009, p. 217) relativo al sistema de identidad nacional del Reino Unido.

Asimismo, este marco de interoperabilidad consistirá en lo siguiente, según ordena el epígrafe 4 del artículo 12 del Reglamento eIDAS: "a) una referencia a los requisitos técnicos mínimos relativos a los niveles de seguridad contemplados en el artículo 8; b) una correlación entre los niveles de seguridad nacionales de los sistemas de identificación electrónica y los niveles de seguridad contemplados en el artículo 8; c) una referencia a los requisitos técnicos mínimos para la interoperabilidad; d) una referencia a un conjunto mínimo de datos de identificación de la persona que representan de manera única a una persona física o jurídica, y que está disponible en los sistemas de identificación electrónica; e) reglas de procedimiento; f) acuerdos para la resolución de litigios, y g) normas comunes de seguridad operativa".

El artículo 1 del Reglamento de interoperabilidad eIDAS indica que "el presente Reglamento establece los requisitos técnicos y de funcionamiento del marco de interoperabilidad con el fin de garantizar la interoperabilidad de los sistemas de identificación electrónica que los Estados miembros notifiquen a la Comisión".

Respecto al ámbito subjetivo, el artículo 2.1) del Reglamento de interoperabilidad eIDAS define al nodo como el "punto de conexión que forma parte de la arquitectura de interoperabilidad de identificación electrónica, que participa en la autenticación transfronteriza de las personas y que tiene la capacidad de reconocer y procesar o reenviar transmisiones a otros nodos permitiendo a la infraestructura de identificación electrónica nacional de un Estado miembro interaccionar con las infraestructuras de identificación electrónica nacionales de otros Estados miembros", a los efectos de establecer las correspondientes obligaciones de interoperabilidad entre los mismos.

Este nodo se corresponde, como en breve veremos[541], con uno de los componentes principales del sistema que facilita la autenticación transfronteriza, que en el caso de STORK es el Pan European Proxy Server o PEPS, actualmente en forma de componente eID.

Entrando en el contenido normativo del Reglamento de interoperabilidad eIDAS, en primer lugar se contienen dos referencias a los niveles de seguridad de los su artículo 3 establece que "los requisitos técnicos mínimos relacionados con los niveles de seguridad serán los establecidos en el Reglamento de Ejecución (UE) 2015/1502 de la Comisión" (el Reglamento de seguridad eIDAS, al que luego nos referiremos), en un pretendido desarrollo de la previsión contenida en el artículo 12.4.a) del Reglamento eIDAS, de acuerdo con la cual el marco de interoperabilidad deberá contener "una referencia a los requisitos técnicos mínimos relativos a los niveles de seguridad contemplados en el artículo 8"; desarrollo que no se va a realizar en este Reglamento sino en el de medidas de seguridad, algo que desde luego resulta criticable en términos de técnica legislativa.

En segundo lugar, y también en relación con la seguridad, el artículo 4 del Reglamento de interoperabilidad eIDAS establece que "la correlación de los niveles de seguridad nacionales de los sistemas de identificación electrónica notificados se ajustará a los requisitos establecidos en el Reglamento de Ejecución (UE) 2015/1502 de la Comisión" (Decisión de listas de confianza eIDAS), previsión que supuestamente da cumplimiento a la exigencia contenida en el artículo 14.2.b) del Reglamento eIDAS, en cuya virtud el marco de interoperabilidad debe contener "una correlación entre los niveles de seguridad nacionales de los sistemas de identificación electrónica y los niveles de seguridad

[541] Cfr. el epígrafe 3.1.7.2 de este trabajo.

contemplados en el artículo 8"; esto es, un mapeo entre el nivel de seguridad de un sistema en un Estado y en el Reglamento eIDAS.

Pues bien, y como se puede ver, el artículo 4 del Reglamento de interoperabilidad eIDAS de nuevo reenvía esta cuestión íntegramente a lo que se determine en el Reglamento de seguridad eIDAS[542].

Mayor interés reviste la segunda frase del artículo 4 del Reglamento de interoperabilidad eIDAS, que prevé que "los resultados de la correlación se notificarán a la Comisión mediante la plantilla de notificación establecida en la Decisión de Ejecución (UE) 2015/1505 (2) de la Comisión".

Esta Decisión, que regula las listas de confianza que analizaremos posteriormente en mayor detalle, establece en su Anexo II un formulario para la notificación de la información sobre el organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales, y de los detalles relativos al lugar en que se publican dichas listas, los certificados utilizados para firmar o sellar las listas de confianza y cualquier modificación de los mismos (artículo 4.1 de la Decisión, que da cumplimiento al artículo 22.3 del Reglamento eIDAS).

Esta notificación se emplea, en los servicios de confianza, para la publicación, por la Comisión, de una lista compilada con las anteriores informaciones, de forma que resulte sencillo localizar la lista de servicios de confianza de un supervisor concreto. Pero su uso para la notificación de la correlación de los niveles de seguridad de los sistemas de identificación electrónica resulta bastante difícil de comprender, a menos que la voluntad del ejecutivo europeo haya sido establecer que los resultados de esta correlación se contengan, en efecto, en una lista de confianza[543], pero referida exclusivamente a sistemas de identificación.

Si este es el caso, en mi opinión se deberá adaptar el contenido de dicha lista de confianza, con base en los estándares europeos en la materia[544], dado que el contenido previsto en el anexo I de la Decisión de listas de confianza eIDAS no resulta en absoluto apropiado para dicha correlación, por no disponer de una sintaxis ni de una semántica que permitan representar el "resultado de" la correlación citada. El caso contrario sería incluso peor, ya que obligaría a definir desde cero el documento con la correlación, y de forma desalineada de las listas de confianza, algo que aún haría más difícil de comprender este enfoque.

La norma tampoco aclara quién debe realizar esta correlación, ni notificar la misma a la Comisión Europea, pero cabe imaginar que será el Estado miembro notificante, a tenor de lo establecido en los artículos 7 y 9 del Reglamento eIDAS, y del análisis que la

---

[542] El Considerando (2) de este Reglamento indica que "determinar las especificaciones, las normas y los procedimientos técnicos mínimos es fundamental a fin de garantizar un entendimiento común en cuanto a los detalles de los niveles de seguridad, así como la interoperabilidad al correlacionar los niveles de seguridad nacionales de los sistemas de identificación electrónica notificados con los niveles de seguridad contemplados en el artículo 8, de conformidad con el artículo 12, apartado 4, letra b), del Reglamento (UE) Nº 910/2014".

[543] Esta conclusión deriva del hecho que los contenidos de esta plantilla de notificación son poco más que la identificación del órgano responsable de la lista de confianza, del Estado correspondiente, los lugares donde se publica la lista de confianza y sus fechas.

[544] En particular, ETSI TS 119 612, a la que nos referiremos con mayor detalle en el epígrafe 7.1.4.1 de este trabajo.

Decisión de cooperación eIDAS anteriormente realizado.

En segundo lugar, el Reglamento de interoperabilidad eIDAS dedica dos artículos dedicados al establecimiento de requisitos técnicos mínimos de interoperabilidad, tomando esta noción en sentido estricto, que vienen referidos a los nodos de la arquitectura de interoperabilidad de identificación electrónica y al formato de los mensajes para la comunicación.

Respecto a los nodos, el artículo 5 del Reglamento de interoperabilidad eIDAS se limita a indicar que los mismos deberán poder conectarse a los restantes nodos (epígrafe 1); que los nodos deberán poder distinguir entre los organismos del sector público y otras partes usuarias por medios técnicos (epígrafe 2); y que la aplicación por parte de un Estado miembro de los requisitos técnicos establecidos en el presente Reglamento no impondrá requisitos técnicos y costes desproporcionados a los demás Estados miembros con el fin de que puedan interoperar con la aplicación adoptada por el primer Estado miembro (epígrafe 3), regla a la que ya nos hemos referido anteriormente.

Se trata de una normativa extremadamente parca, que desde luego sólo facilita la interoperabilidad desde una perspectiva de muy alto nivel, por lo que su concreción se deberá producir mediante ulteriores especificaciones técnicas.

Por su parte, en relación con el formato de los mensajes para la comunicación –esto es, para la comunicación entre los nodos a efectos de la autenticación transfronteriza–, el artículo 8 del Reglamento de interoperabilidad eIDAS exige que "los nodos utilizarán para la sintaxis formatos de mensaje comunes basados en las normas que ya se hayan implantado más de una vez entre los Estados miembros y que hayan demostrado funcionar en un entorno operativo", regla que conduce casi de forma inexorable, en mi opinión, a la aplicación exclusiva de STORK como marco de interoperabilidad, y a la necesidad de que, para su sustitución por otro marco, el mismo se deba antes implementar y probar de forma reiterada y exitosa en diversos Estados miembros.

En cualquier caso, el Reglamento de interoperabilidad eIDAS establece reglas referidas a la sintaxis que se deberá emplear, en el sentido de que la misma "permitirá: a) el correcto tratamiento del conjunto mínimo de datos de identificación de la persona que representen de manera exclusiva a una persona física o jurídica; b) el correcto tratamiento del nivel de seguridad de los medios de identificación electrónica; c) la distinción entre los organismos del sector público y otras partes usuarias; d) la flexibilidad para satisfacer las necesidades de atributos adicionales relacionados con la identificación", requisitos que de nuevo se refieren fuertemente a la base protocolaria técnica, sintáctica y semántica de STORK, que es SAML 2.0[545].

En tercer lugar, el Reglamento de interoperabilidad eIDAS determina el conjunto mínimo de datos de identificación de personas que representan de manera exclusiva a una persona física o jurídica. En este sentido, su artículo 11 autoriza el uso de diversos atributos para la representación, en un medio de identificación empleado en un contexto transfronterizo, de la identidad de una persona física o jurídica (epígrafe 1), o de una persona física que representa a una persona jurídica (epígrafe 2), especificando que "los datos se transmitirán según el alfabeto original y, en su caso, también se transliterarán al alfabeto latino" (epígrafe 3).

[545] Eso sí, perfilado y ampliado en los proyectos STORK.

La finalidad de esta norma no es otra que acordar los contenidos mínimos obligatorios que se emplearán para la descripción de una persona física o jurídica, en el contexto transfronterizo. Dado que los diferentes números o códigos de identidad asignados por las autoridades de los Estados miembros – que serán empleados por los proveedores de identidad de dichos Estados – pueden resultar incomprensibles para los prestadores de servicios en otros Estados miembros, o pueden existir dificultades jurídicas para el uso transfronterizo de un código de identidad, por ser el mismo de uso exclusivo dentro del Estado miembro, resulta necesario establecer reglas de asignación de identificadores específicos para la autenticación transfronteriza, o de uso de identificadores de uso autorizado en transacciones transfronterizas.

En este sentido, el epígrafe 1 del anexo del Reglamento de interoperabilidad eIDAS impone la obligación de emplear los siguientes atributos para la identificación de una persona física: a) apellido o apellidos actuales; b) nombre o nombres actuales; c) fecha de nacimiento y d) un identificador único confeccionado por el Estado miembro expedidor de conformidad con las especificaciones técnicas para los fines de identificación transfronteriza y que sea tan constante como sea posible a lo largo del tiempo.

Asimismo, se autoriza el uso de los siguientes atributos adicionales: a) nombre o nombres y apellido o apellidos de nacimiento; b) lugar de nacimiento; c) dirección actual y d) sexo; debiéndose entender que siempre que se cuente con el necesario consentimiento previo, excepto en aquellos casos donde la normativa lo excepcione.

Por su parte, el epígrafe 2 del anexo del Reglamento de interoperabilidad eIDAS impone la obligación de emplear los siguientes atributos para la identificación de una persona jurídica: a) nombre jurídico actual y b) un identificador único confeccionado por el Estado miembro expedidor de conformidad con las especificaciones técnicas para los fines de identificación transfronteriza y que sea tan constante como sea posible a lo largo del tiempo.

Asimismo, se autoriza el uso de los siguientes atributos adicionales: a) dirección actual; b) número de registro de IVA; c) número de referencia fiscal; d) el identificador relacionado con el artículo 3, apartado 1, de la Directiva 2009/101/CE del Parlamento Europeo y del Consejo; e) el identificador de entidades jurídicas (LEI) al que se refiere el Reglamento de Ejecución (UE) Nº 1247/2012 de la Comisión; f) el número de registro e identificación de operadores económicos (número EORI) al que se refiere el Reglamento de Ejecución (UE) Nº 1352/2013 de la Comisión; o g) número de impuestos especiales indicado en el artículo 2, punto 12, del Reglamento (UE) Nº 389/2012 del Consejo.

Puede llamar la atención de que, tanto para persona física como para persona jurídica, se prevea la necesidad de emplear un identificador único, que deberá ser conforme a las especificaciones técnicas para los fines de identificación transfronterizas, siendo opcionales los restantes identificadores personales, y que se podrán emplear en función de las necesidades y, en especial, del contexto jurídico aplicable. Asimismo, este identificador deberá ser lo más constante como sea posible a lo largo del tiempo, lo cual facilita múltiples operaciones transfronterizas, pero también permitirá un mayor grado de trazabilidad potencial del ciudadano.

STORK ha establecido especificaciones técnicas para fines de identificación transfronteriza, partiendo de una serie de principios que tratan de conciliar las diversas sensibilidades jurídicas de los Estados miembros con respecto al uso de identificadores.

En cuarto lugar, el Reglamento de interoperabilidad eIDAS establece normas de seguridad operativa comunes, referidas a la privacidad y confidencialidad de datos; a la integridad y autenticidad de los datos para la comunicación entre los nodos; a la gestión de los metadatos y la información de seguridad; y, finalmente, a la seguridad de la información y las normas de seguridad; mientras que, en quinto lugar, el Reglamento de interoperabilidad eIDAS contiene disposiciones para la solución de litigios.

3.1.7.2 Los procesos de interoperabilidad en la identificación electrónica de STORK

Ayuda bastante a la comprensión práctica del concepto de identificación electrónica, formado por elementos legalmente expresados de forma bastante abstracta, conocer con mayor detalle el funcionamiento de estos sistemas de identificación electrónica, para lo cual nos podemos referir a los Anexos A.3.4 y A.3.5 de este trabajo, pero también a los trabajos de los proyectos STORK[546] y STORK 2.0, alrededor de los cuales se ha construido la autenticación transfronteriza en la Unión Europea[547], base del actual Servicio Público Digital de identificación electrónica del Mecanismo Conectar Europa (MCE o CEF, en su acrónimo inglés), conocido como componente eID.

STORK, desarrollado entre los años 2008 y 2011, es un Piloto de Gran Escala financiado dentro del Programa de Competitividad e Innovación de la Comisión Europea[548], liderado por un consorcio formado por 35 miembros, en el que participaron diversas administraciones públicas, universidades, organizaciones privadas y asociaciones sin ánimo de lucro, pertenecientes a 18 países europeos[549]; por su parte, STORK 2.0 es la continuación del proyecto anterior, financiado dentro del mismo Programa[550], entre los años 2012 y 2015, e incluye hasta 58 socios de 19 Estados miembros y asociados.

Ambos proyectos se pueden ver, en el fondo, como iniciativas de autorregulación público-privada orientada a facilitar la interoperabilidad de la identificación electrónica, si bien siempre con un mayor protagonismo de los participantes públicos[551], y han permitido la

---

[546] Para (Leitold, Lioy, & Ribeiro, 2014), se asume que STORK está llamado a convertirse en la base técnica que soporte el Reglamento eIDAS. Y, en efecto, de la lectura del Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, parece ser de esta forma.

[547] En el Derecho comparado, también existen experiencias interesantes en este sentido, como el programa de autenticación electrónica del gobierno federal de Estados Unidos, que hace uso de las identidades provistas, entre otros, por proveedores de servicios de Internet, red social y servicios Cloud para el acceso a determinados procedimientos administrativos, en función del nivel de seguridad y confianza de la credencial. Se puede acceder a más información en la página web gubernamental http://www.idmanagement.gov/pages.cfm/page/ICAM.

[548] El coste del proyecto STORK ha sido aproximadamente de 26 millones de euros, contando con una financiación europea del 50%.

[549] Por cierto, con un liderazgo notable del Estado español, a través del (hoy) Ministerio de Hacienda y Administraciones Públicas, en relación con la definición de los flujos de autenticación transfronteriza y de las especificaciones técnicas comunes que sustentan el marco de interoperabilidad.

[550] Con un coste aproximado de 18,65 millones de euros, con una contribución de la Unión Europea algo inferior al 50%.

[551] De hecho, todos los Estados miembros de la Unión Europea fueron consultados en relación con las

creación de una verdadera infraestructura pan-Europea en sustento de la identificación electrónica transfronteriza.

En ambos proyectos la forma de colaboración entre los participantes ha adoptado un enfoque pragmático antes que teórico; partiendo del análisis de los sistemas de identificación electrónica previamente existentes en los Estados participantes, en STORK se desarrolló un marco de interoperabilidad y se probó en seis pilotos reales[552], referidos al acceso transfronterizo a servicios públicos electrónicos[553], al uso seguro de medios de comunicación electrónica transfronterizos por niños y jóvenes[554], al acceso transfronterizo a servicios académicos[555], a la notificación electrónica transfronteriza[556], al cambio transfronterizo de dirección[557] y, finalmente, el acceso a los servicios de la propia Comisión Europea[558].

A título de ejemplo[559], el piloto de acceso transfronterizo a servicios públicos electrónicos definió[560], entre otros casos de uso, la funcionalidad que permitía a un ciudadano residente en Cataluña el acceso a un servicio electrónico de un tercer Estado miembro (Limosa, en Bélgica, un servicio para el registro de trabajadores desplazados), empleando un certificado electrónico reconocido, incluyendo el contenido en el DNI electrónico y el certificado idCAT expedido por la Agència Catalana de Certificació[561], así como, a la inversa, la posibilidad de que un ciudadano europeo pudiera acceder al portal de trámites de la Generalitat de Catalunya empleando su certificado expedido en su Estado de residencia, en ambos casos empleando la infraestructura de intermediación[562] ofrecida por el Estado español, a través del Ministerio responsable de la administración electrónica (Ministerio de la Presidencia, Ministerio de Administraciones Públicas, y actualmente,

---

especificaciones técnicas comunes de STORK, con independencia de su participación en el consorcio (STORK-eID Consortium, 2011).

[552] Cfr. (Leitold, 2010, pág. 145) y (STORK-eID Consortium, 2011), *in toto*.

[553] Cross-border Authentication Platform for Electronic Services Pilot, disponible en https://www.eid-stork.eu/pilots/pilot1.htm.

[554] Safer Chat Pilot, disponible en https://www.eid-stork.eu/pilots/pilot2.htm.

[555] Student Mobility Pilot, disponible en https://www.eid-stork.eu/pilots/pilot3.htm.

[556] Electronic Delivery Pilot, disponible en https://www.eid-stork.eu/pilots/pilot4.htm.

[557] Change of Address Pilot, disponible en https://www.eid-stork.eu/pilots/pilot5.htm.

[558] ECAS Integration Pilot, disponible en https://www.eid-stork.eu/pilots/pilot6.htm.

[559] Aunque finalmente no se completó el piloto español, lo cierto es que coadyuvó a la generación de las especificaciones comunes de interoperabilidad de los medios de identificación electrónica, y resulta muestra de una madurez temprana de nuestro país en estas cuestiones, por lo que sin duda resulta de cita obligada.

[560] Cfr. (Purves, 2009, págs. 46-49) y (Heppe, 2010, págs. 43-48).

[561] Hoy, el Consorci Administració Oberta de Catalunya.

[562] Denominada en STORK, y otros proyectos de administración electrónica, como Pan European Proxy Servers o, en forma de acrónimo, PEPS. El Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, se refiere a los PEPS como “nodos” de una arquitectura de interoperabilidad de identificación electrónica.

Ministerio de Hacienda y Administraciones Públicas).

Por lo que respecta a STORK 2.0, en el mismo se han extendido las funcionalidades existentes en STORK, con un enfoque claramente dirigido a la representación y los poderes de actuación de las personas jurídicas, también mediante cuatro pilotos reales, referidos a las cualificaciones académicas y la enseñanza electrónica a distancia[563]; la banca electrónica[564]; los servicios públicos para empresas[565] y la sanidad en línea[566].

Los proyectos STORK han producido una importante cantidad de resultados, entre los cuales un completo marco de interoperabilidad, pero también una infraestructura común operativa que sustenta los procesos de autenticación transfronteriza, y aplicaciones de referencia para facilitar su adopción por los Estados[567].

Los proyectos STORK –de forma conjunta con otros proyectos piloto a gran escala entre los Estados miembros y cofinanciados por el Programa de Innovación y Competitividad[568], como PEPPOL, epSOS, eCODEX o SPOC– se citan en el Reglamento (UE) Nº 283/2014 del Parlamento Europeo y del Consejo, de 11 de marzo de 2014, relativo a unas orientaciones para las redes transeuropeas en el sector de las infraestructuras de telecomunicaciones y por el que se deroga la Decisión Nº 1336/97/CE como "servicios digitales transfronterizos clave en el mercado interior, sobre la base de unos componentes elementales comunes", componentes que "deben tener prioridad frente a otras infraestructuras de servicios digitales, ya que los primeros son condición previa para las segundas".

En este sentido, este Reglamento prioriza[569], entre los proyectos de interés común referidos a infraestructuras de servicios digitales, aquellos servicios que permiten el reconocimiento y la validación transfronterizos de la identificación electrónica y la firma electrónica[570], para su financiación, siempre que –entre otras condiciones previstas en el artículo 6.1 del Reglamento en cuestión –se ajusten a las normas internacionales o europeas o a las especificaciones y orientaciones abiertas acordadas en materia de

---

[563] eLearning and Academic Qualifications Pilot, disponible en https://www.eid-stork2.eu/pilots/elearning/index.php/en/.

[564] eBanking Pilot, disponible en https://www.eid-stork2.eu/pilots/ebanking/index.php/en/.

[565] Public Services for Business Pilot, disponible en https://www.eid-stork2.eu/pilots/public_services/index.php/en/.

[566] eHealth Pilot, disponible en https://www.eid-stork2.eu/pilots/ehealth/index.php/en/.

[567] Con financiación a cargo del Mecanismo "Conectar Europa", previsto en el Reglamento (UE) Nº 1316/2013, del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013 por el que se crea el Mecanismo Conectar Europa, por el que se modifica el Reglamento (UE) Nº 913/2010 y por el que se derogan los Reglamentos (CE) Nº 680/2007 y (CE) Nº 67/2010

[568] Decisión Nº 1639/2006/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 2006, por la que se establece un programa marco para la innovación y la competitividad (2007 a 2013).

[569] El artículo 6.3 del Reglamento indica que "deberá concederse prioridad absoluta a la financiación de los componentes elementales esenciales para el desarrollo, despliegue y explotación de otras infraestructuras de servicios digitales que se enumeran en la sección 1, punto 1, del anexo, y con perspectivas demostrables de ser utilizados en ellas".

[570] Junto a los servicios de entrega electrónica de documentos, también regulados en el Reglamento eIDAS, dentro de los denominados servicios de confianza.

interoperabilidad, tales como el marco europeo de interoperabilidad, y aprovechen las soluciones existentes, por lo que la conexión con STORK es evidente.

En STORK se han definido, por tanto, los flujos de proceso que sustentan la autenticación transfronteriza[571], en hasta cuatro escenarios de implementación técnica, de los que describiremos[572] sólo uno, para mantener la simplicidad en la exposición del funcionamiento del sistema, pero que muestra los diferentes roles donde intervienen los participantes en este tipo de servicios.

En este sentido, en la Ilustración 11 podemos ver un diagrama[573] donde se muestra un proceso de autenticación transfronteriza[574], en la que un ciudadano residente en un Estado A accede a un servicio público prestado por un Estado B.

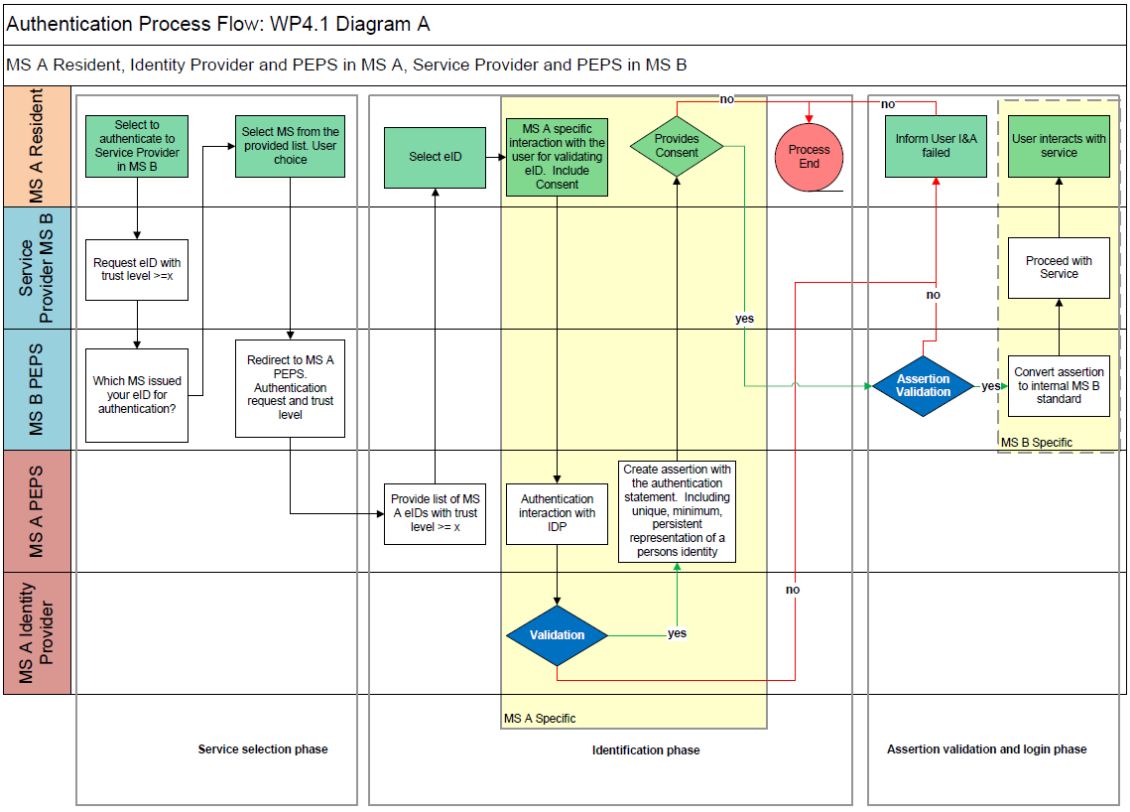


Ilustración 11. Proceso de autenticación transfronteriza con STORK (Consorcio STORK)

[571] Así se puede ver, con carácter general, en (Clowes & Brathwait, 2009) y (Heppe, 2010).

[572] Para una visión más completa de la arquitectura de STORK, cfr. (Leitold & Zwatterndorfer, 2010).

[573] En este tipo de diagrama, aparece una fila para cada interviniente en el proceso que realiza una actuación: así, en la primera fila encontramos al ciudadano del Estado A; en la segunda fila, al prestador del servicio público del Estado B; en la tercera fila, al servicio de intermediación o PEPS del Estado B; en la cuarta, al PEPS del Estado A; y finalmente, en la quinta, el proveedor de identidad del Estado A.

[574] Nótese que las diferentes actuaciones se agrupan en tres fases, incluyendo la fase de selección del servicio, la fase se identificación y la fase de validación de aserciones y acceso.

Veamos dichas actuaciones con detalle[575]:

1. El proceso de autenticación se inicia cuando el ciudadano del Estado A selecciona autenticarse frente a un servicio de un prestador establecido en el Estado B.
2. El prestador del servicio del Estado B envía la petición de autenticación y la información sobre el nivel de seguridad requerido para el acceso a dicho servicio al PEPS del Estado B, al objeto de proceder a la autenticación del ciudadano del Estado A. Por ejemplo, podría tratarse un servicio que requiere nivel sustancial de seguridad.
3. El PEPS del Estado B pregunta al ciudadano qué Estado ha expedido el medio de identificación electrónica que quiere emplear para autenticarse, en forma de un listado de Estados.
4. El usuario selecciona de esta lista el Estado en cuestión.
5. El PEPS del Estado B solicita al PEPS del Estado A la autenticación del ciudadano, de acuerdo con el nivel de seguridad requerido, reenviando al ciudadano a este PEPS.
6. El PEPS del Estado A ofrece al ciudadano el listado de medios de identificación electrónica (en el Estado A) que resultan apropiados para proceder a su autenticación, de acuerdo con el nivel de seguridad requerido. Por ejemplo, podría hacer uso de un certificado reconocido en software, pero no de una contraseña estática.
7. El ciudadano selecciona el medio de identificación electrónica que quiere emplear para autenticarse, en su caso interactuando con el proveedor de identidad del Estado A (en función del protocolo técnico aplicable). Por ejemplo, en el caso del certificado, el propio PEPS del Estado A puede realizar la autenticación, mediante una firma digital que se valide con la clave pública certificada, y posteriormente verificar la corrección del certificado, y que el mismo no ha sido revocado, mediante OCSP; sin embargo, en el caso de una contraseña, la autenticación deberá realizarla directamente el proveedor de identidad del Estado A, por lo que se deberá reenviar al ciudadano a la correspondiente interfaz de servicio.
8. Una vez validada con éxito la autenticación[576], el PEPS del Estado A crea una aserción[577] que indica que la autenticación ha tenido éxito y que incluye la información personal del ciudadano imprescindible para su reconocimiento por el prestador del servicio del Estado B; asimismo, solicita el consentimiento del ciudadano para la entrega de esta aserción al PEPS del Estado B (y al prestador del servicio del Estado B), debido a que esta operación se considera un tratamiento de datos de carácter personal.

---

[575] Cfr. (Heppe, 2010, págs. 25-26). Para un detalle completo de las funcionalidades referidas a la autenticación, cfr. (Heppe, y otros, 2011, pág. 54 y ss.)

[576] Si la autenticación no se puede validar con éxito, el proceso fracasa y devuelve un mensaje de error.

[577] Una aserción de autenticación es un documento electrónico que contiene un conjunto de datos de identidad que se devuelven a una parte que confía (en este caso, el organismo del sector público) durante un proceso de autenticación.

9. En caso de haber consentido el ciudadano[578], se remite la aserción al PEPS del Estado B, que la valida y, en su caso, transforma al estándar técnico apropiado, para entregarla al prestador del servicio del Estado B.
10. El prestador de servicio del Estado B autentica al ciudadano, mediante la información de la aserción, y le permite el acceso.

Como se puede ver, se trata de un sistema complejo que involucra diversos actores, y que presupone la existencia de servicios de administración electrónica especializados en esta materia, para su funcionamiento.

Con independencia de la titularidad del medio de identificación electrónica y de la titularidad del servicio al que se accede en virtud de la autenticación, en todo caso resulta precisa la existencia de estos PEPS o nodos de la arquitectura de interoperabilidad de identificación electrónica y, como veremos, los mismos se configurarán legalmente como servicios de necesaria titularidad pública[579].

El objeto de los trabajos de STORK, sin embargo, tiene un alcance mayor que la definición estricta del flujo de autenticación, dado que parte de una noción de identidad amplia, que incluye los atributos que identifican a la persona, como el nombre, la fecha de nacimiento, el lugar de nacimiento, el sexo y otros análogos (también conocidos frecuentemente como "datos de filiación"); así como también otros atributos que puede ser necesario intercambiar en un proceso de identificación[580], como por ejemplo cualificaciones académicas, poderes y mandatos, etc.

En la Ilustración 12 podemos ver un diagrama[581] donde se muestra un proceso de intercambio transfronterizo de atributos de identidad, entre un ciudadano residente en un Estado A y un prestador de un servicio público en el Estado B.

[578] Si el ciudadano no consiente, el proceso fracasa y devuelve un mensaje de error.

[579] Debe, sin embargo, advertirse que en STORK también se pueden realizar las operaciones de autenticación (así como las restantes que veremos a continuación) sin emplear estos PEPS o nodos de interoperabilidad, ya que la arquitectura contempla la posibilidad de instalar un software intermedio tanto en el sistema del ciudadano – por ejemplo, asociado a su tarjeta nacional de identidad –, como en el sistema del prestador del servicio. STORK también define escenarios mixtos, donde interviene sólo uno de los PEPS o nodos, sea el del ciudadano o el del prestador del servicio. Como han indicado (Leitold, Lioy, & Ribeiro, 2014, pág. 3), la decisión de emplear cada tipo de escenario por un Estado suele depender de la infraestructura de identificación electrónica existente, del modelo de responsabilidad por la prestación del servicio o de consideraciones asociadas a la normativa de protección de datos de carácter personal.

[580] Proceso que se muestra en la Ilustración 12 (Clowes & Brathwait, 2009) y (Heppe, 2010).

[581] Como en el caso anterior, tenemos una fila para cada interviniente en el proceso que realiza una actuación: así, en la primera fila encontramos al ciudadano del Estado A; en la segunda fila, al prestador del servicio público del Estado B; en la tercera fila, al servicio de intermediación o PEPS del Estado B; en la cuarta, al PEPS del Estado A; y finalmente, en la quinta, el proveedor de identidad y atributos del Estado A.

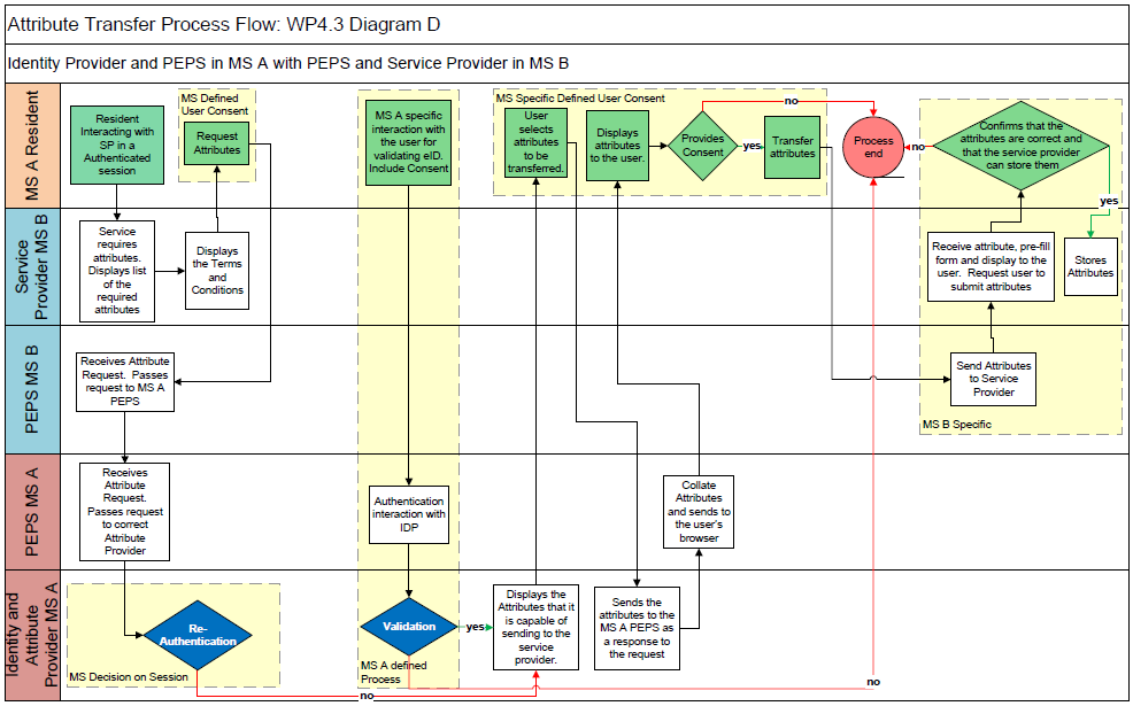


Ilustración 12. Proceso de intercambio transfronterizo de atributos con STORK (Consorcio STORK)

Veamos dichas actuaciones con detalle[582]:

1. El proceso de transferencia de atributos se inicia una vez que el ciudadano del Estado A se ha autenticado frente a un servicio de un prestador establecido en el Estado B.
2. El prestador del servicio del Estado B presenta al ciudadano una solicitud para que el mismo le transmita uno o varios atributos. En dicha solicitud, le informa acerca de los atributos requeridos, de su política de tratamiento de los mismos, conforme a la legislación de protección de datos de carácter personal, y de los derechos que le asisten.
3. El ciudadano manifiesta su consentimiento, y remite la solicitud, a través del PEPS del Estado B y del Estado A, hasta el proveedor de identidad y atributos del Estado A.
4. El proveedor de identidad y atributos del Estado A, muestra los atributos solicitados, siempre que disponga de ellos.
5. El ciudadano selecciona los atributos a transferir y manifiesta su consentimiento para el intercambio.
6. El proveedor de identidad y atributos del Estado A remite los atributos al ciudadano, a través del PEPS del Estado A.
7. El ciudadano entrega los atributos al prestador del servicio del Estado B, a través del PEPS del Estado B.

[582] Cfr. (Heppe, 2010, págs. 21-22). Para un detalle completo de las funcionalidades referidas a la autenticación, cfr. (Heppe, y otros, 2011, pág. 76 y ss.)

8. El prestador del servicio del Estado B muestra los atributos recibidos al ciudadano del Estado A, que confirma su validez.

Este flujo de proceso, muy basado en los estándares autorregulados por la industria, a los que nos hemos referido anteriormente[583], permite al ciudadano decidir qué atributos se intercambian entre el proveedor de identidad y atributos, y el prestador del servicio que los precisa, una característica que se viene denominando "usuario-centrismo".

Uno de los casos de uso relevantes que se puede implementar extendiendo este flujo de trabajo de intercambio transfronterizo de atributos es la denominada autenticación en nombre de tercero; otro caso de uso, la validación del poder para firmar en nombre de tercero; finalmente, la obtención de otras informaciones personales relevantes, como las capacidades profesionales, la colegiación, etc.; flujos de proceso que han sido tratados en STORK 2.0.

Una de las limitaciones al alcance del primer proyecto STORK fue su enfoque a la autenticación de personas físicas; sin embargo, habiéndose detectado que muchas de las operaciones transfronterizas son realizadas por personas jurídicas y representantes profesionales de las mismas, en STORK 2.0 se aborda esta problemática, en particular en su piloto de servicios públicos para empresas[584].

El proceso definido se muestra[585] en la Ilustración 13[586], en la que podemos ver un diagrama[587] donde se muestra un proceso de autenticación transfronteriza en nombre de tercero, entre un ciudadano residente en un Estado A y un prestador de un servicio público en el Estado B, y que apoyaría la aplicación, anteriormente analizada, de identificación electrónica en el Reglamento eIDAS, en lo referido a las personas físicas que representan a las personas jurídicas.

Veamos dichas actuaciones con detalle[588]:

1. El proceso de autenticación en nombre de tercero se inicia cuando el ciudadano del Estado A desea acceder, con su credencial STORK, a un servicio personalizado ofrecido por un prestador establecido en el Estado B.
2. El prestador del servicio del Estado B solicita al ciudadano que seleccione su Estado, redirigiéndole al mismo.
3. El PEPS del Estado del ciudadano le autentica, y le solicita que indique a la

[583] Cfr. el Anexo A.3.4 de este trabajo.

[584] Cfr. (Leitold, Lioy, & Ribeiro, 2014).

[585] Como en los casos anteriores, se ha escogido sólo uno de los escenarios técnicos posibles, a efectos ilustrativos. Se trata del escenario donde intervienen los PEPS de los Estados involucrados en la operación.

[586] Cfr. (STORK 2.0. D4.8 Final version of process flows, 2015, págs. 9-15).

[587] De nuevo, tenemos una fila para cada interviniente en el proceso que realiza una actuación: así, en la primera fila encontramos al ciudadano; en la segunda fila, al PEPS del Estado del ciudadano (C-PEPS); en la tercera, al PEPS del Estado del prestador del servicio (S-PEPS); y, finalmente, en la cuarta, al prestador del servicio.

[588] Cfr. (STORK 2.0. D4.8 Final version of process flows, 2015, págs. 11-12). Para un detalle completo de las funcionalidades referidas a la autenticación transfronteriza en nombre de tercero, cfr. (STORK 2.0. D4.2 First version of Functional Design, 2013, pág. 97 y ss.)

persona representada y dónde se pueden obtener los poderes de representación.

4. El PEPS del Estado del ciudadano recupera la información correspondiente de los registros nacionales, y la remite al prestador del servicio en el Estado B.

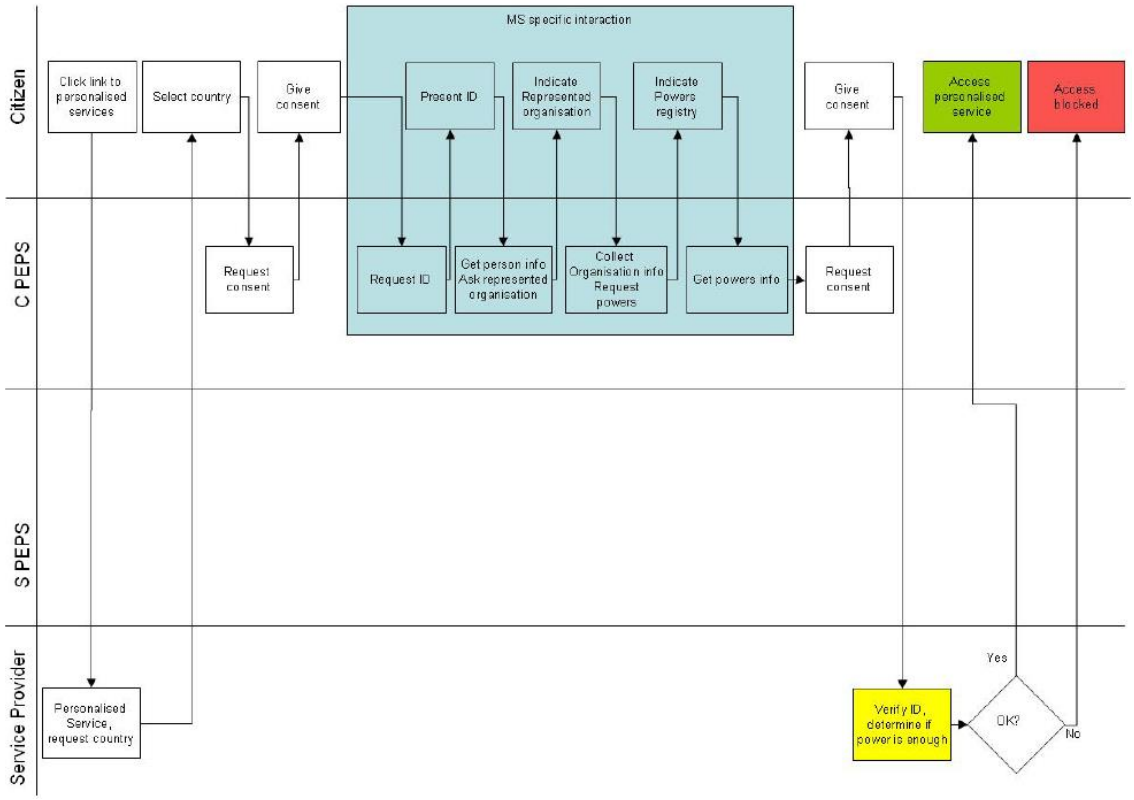


Ilustración 13. Proceso de autenticación transfronteriza en nombre de tercero con STORK 2.0 (Consorcio STORK)

De este flujo de trabajo interesa hacer notar que es el menos automatizable de todos los que hemos visto hasta este momento, debido a la dificultad semántica del tratamiento de los diferentes tipos de poderes y facultades de actuación, que normalmente va a exigir la intervención de una persona que los valide o declare bastantes; actuación que, además, se deberá realizar de acuerdo con el derecho nacional aplicable.

A pesar de lo que se acaba de decir, y por lo que respecta al Estado español, es preciso reseñar la conexión clara entre este proceso y el registro electrónico de apoderamientos[589] previsto en el artículo 6 de la LPAC, ya que el mismo será, muy probablemente, la fuente de datos a emplear.

En efecto, dado que el citado registro prevé la posibilidad de registrar apoderamientos generales, así como otorgarlos *apud acta* electrónicamente, también con carácter general, resultaría perfectamente viable consumir en este tipo de actuación transfronteriza.

[589] Sobre esta institución, cfr. el detallado estudio de (Martínez Gutiérrez, 2016a, págs. 147-154).

3.2 LOS EFECTOS JURÍDICOS DE LOS SISTEMAS DE IDENTIFICACIÓN ELECTRÓNICA NOTIFICADOS CONFORME AL REGLAMENTO EIDAS

3.2.1 El efecto jurídico principal: el reconocimiento mutuo en el ámbito del sector público

Desde la perspectiva de los efectos jurídicos sustantivos de los sistemas de identificación electrónica[590] a los que nos acabamos de referir, en el Reglamento eIDAS se centran precisamente en su reconocimiento mutuo dentro del ámbito territorial de aplicación de la norma, de forma que se extiende el derecho de uso de dichos sistemas al resto de Estados de la Unión Europea. Así se deriva del artículo 6.1 del Reglamento eIDAS, cuando establece que "cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro" que cumpla los requisitos y condiciones previstos en el Reglamento, y sus actos de desarrollo.

Dicho reconocimiento no se produce de forma inmediata, sino diferida en el tiempo, y más en concreto, en el plazo máximo de un año[591] desde la publicación de la lista de sistemas de identificación a la que posteriormente nos referiremos, por parte de la Comisión Europea[592].

Por su parte, el artículo 6.2 del Reglamento determina también que los sistemas de identificación electrónica que no cumplan dichos requisitos y condiciones puedan ser objeto también de reconocimiento por otros Estados, si bien de forma plenamente voluntaria.

Este efecto jurídico de reconocimiento transfronterizo de la identificación electrónica se garantiza sólo en las relaciones entre las personas y los organismos del sector público[593],

---

[590] Aunque nuestro interés se centra en la dimensión jurídica de estos medios, su relevancia es mayor, dado que la identificación electrónica se considera uno de los elementos fundamentales de la "soberanía digital", que se puede definir como "tener conocimiento completo y control individual o social acerca de quién puede acceder a qué datos y a dónde se transfieren dichos datos" (Posch, 2017, p. 77), que opina que la identificación electrónica debe ser la base para el acceso remoto a los datos en *Cloud*.

[591] Nada impide, desde luego, que el citado reconocimiento se produzca con anterioridad, lo cual dependerá de factores tecnológicos, presupuestarios o simplemente políticos.

[592] Para los sistemas notificados antes de la primera publicación de la lista de sistemas de identificación, según prevé el artículo 9.2 del Reglamento eIDAS, dado que los sistemas notificados posteriormente serán publicados en el plazo de dos meses después de la notificación, según dispone el apartado 3 del mismo artículo.

[593] Como ha puesto de manifiesto (Dumortier, 2016, p. 11), "el resultado perseguido por el Reglamento eIDAS, si se logra algún día, se encuentra limitado al reconocimiento de una identidad", por lo que "[p]ermite a un prestador de un servicio público en el Estado miembro A controlar si la identidad de usuario extranjero es conocida o no en el Estado miembro B", añadiendo que "[e]n la práctica, sin embargo, el prestador del servicio público necesita mucha más información antes de que pueda conceder acceso al

que de acuerdo con el artículo 3.7 del Reglamento eIDAS, se definen como "las autoridades estatales, regionales o locales, los organismos de Derecho público y las asociaciones formadas por una o varias de estas autoridades o uno o varios de estos organismos de Derecho público, o las entidades privadas mandatarias de al menos una de estas autoridades, organismos o asociaciones para prestar servicios públicos actuando en esa calidad"; en una muestra evidente de la conexión de esta institución con las políticas de la Unión Europea en la administración electrónica de los Estados miembros.

En segundo lugar, es preciso señalar la posibilidad de que la ley nacional establezca efectos jurídicos sustantivos propios en relación con uno o diversos sistemas de identificación electrónica. Y entre dichos efectos se puede perfectamente incluir el de la equiparación plena de un sistema de identificación electrónica con la firma escrita. Aunque seguramente se trate de una posibilidad poco justificada, dado que entraría en colisión con la firma o sello electrónico cualificado, tampoco puede descartarse[594].

Para ello posiblemente deba tratarse de un sistema que haga uso de medios de identificación que permitan la autenticación del origen de los datos y la integridad de los datos, además de la autenticación de entidad, como por ejemplo en el caso de un instrumento como el DNI electrónico.

Sucederá, sin embargo, que este efecto jurídico de equivalencia no gozará de reconocimiento transfronterizo, a diferencia de lo que sucede con la figura de la firma electrónica cualificada prevista en el Reglamento eIDAS, por lo que –como hemos avanzado anteriormente– seguramente dicho tipo de medio de identificación quedará sujeto a ambas normativas.

Como se acaba de indicar, para que se produzca este efecto jurídico de reconocimiento transfronterizo con respecto a los sistemas de identificación electrónica, deben concurrir simultáneamente las tres condiciones legalmente previstas en el artículo 6.1 del Reglamento eIDAS.

En primer lugar, el medio de identificación electrónica debe haber sido expedido en virtud de un sistema de identificación electrónica incluido en una lista publicada por la Comisión, de acuerdo con lo establecido en el artículo 9 del propio Reglamento eIDAS, para lo cual debe haber sido previamente notificado por el Estado miembro[595].

En segundo lugar, el nivel de seguridad de este medio de identificación electrónica debe corresponder a un nivel de seguridad igual o superior al nivel de seguridad requerido por

---

servicio", citando atributos como la condición de profesional, de apoderado o de estudiante, por lo que concluye que "el Reglamento eIDAS establece la base inicial para la futura prestación de servicios públicos transfronterizos", base que considera necesaria, pero siendo "necesarios muchos más esfuerzos en el futuro para producir resultados prácticos a gran escala" (la traducción es mía). Se trata de una crítica que sólo en parte resulta, en mi opinión, acertada porque olvida las restantes políticas de la Unión en orden al intercambio de documentos, significativamente en el marco del Sistema de Información del Mercado Interior y en la reciente iniciativa de Portal Digital Único.

[594] Por ejemplo, para no tener que sujetar el medio de identificación electrónica a las condiciones previstas en la sección del Reglamento eIDAS dedicada a la regulación de los servicios de confianza, o, más probablemente, cuando el medio de identificación electrónica no se base en el uso de certificados cualificados, en cuyo caso simplemente no puede cumplir las condiciones de la firma o sello cualificados, muestra de la evidente infracción del principio de neutralidad tecnológica por esta norma.

[595] En relación con los requisitos para la notificación, cfr. el epígrafe 3.1 de este trabajo.

el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto[596].

En tercer lugar, el organismo público en cuestión debe utilizar un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea, previsión que sorprendentemente excluye la posibilidad de que una persona dotada de un sistema mejor que el requerido lo pueda emplear, como por ejemplo sucederá con un ciudadano español que pretenda emplear su DNI electrónico para el acceso a un servicio en otro Estado miembro que sólo requiera contraseña (y de baja calidad), por la escasa sensibilidad del servicio.

Se trata de una restricción contraria a la lógica –parece que debería aplicar el principio de que "quien puede lo más, puede lo menos"– y que sólo puede entenderse, en mi opinión, desde el punto de vista presupuestario; es decir, para no obligar a ese Estado miembro a incorporar ninguna autenticación transfronteriza a ese servicio[597].

3.2.2 El uso de los sistemas de identificación electrónica para las relaciones jurídico-privadas como efecto jurídico secundario

Aunque su objetivo principal es facilitar el acceso transfronterizo a los servicios públicos, lo cierto es que el Reglamento eIDAS también fomenta el uso de los sistemas de identificación electrónica por parte de los usuarios privados, para las operaciones de autenticación transfronteriza en el acceso a sus servicios; esto es, para la autenticación frente a empresas y otras organizaciones privadas, en relación con usos completamente privados[598].

En este sentido, el Considerando 17 del Reglamento indica que "los Estados miembros deben fomentar que el sector privado utilice voluntariamente los medios de identificación electrónica amparados en un sistema notificado a efectos de identificación cuando sea necesario para servicios en línea o transacciones electrónicas", dado que "la posibilidad de utilizar estos medios de identificación electrónica permitiría al sector privado recurrir a una identificación y autenticación electrónicas ampliamente utilizadas ya en muchos Estados miembros, al menos para los servicios públicos, y facilitar el acceso de las empresas y los ciudadanos a sus servicios en línea a través de las fronteras".

La posibilidad de uso de los sistemas de identificación electrónica para las relaciones jurídico-privadas tiene un indudable atractivo[599] y, como ya hemos visto, así viene

---

[596] Los niveles de seguridad se presentan en el epígrafe 3.1.3 de este trabajo.

[597] Puesto que, como se ha dicho anteriormente, no es obligatorio el reconocimiento de los sistemas de identificación de nivel bajo.

[598] Este impulso no resulta especialmente novedoso, ya que la Hoja de ruta de la Comisión Europea para un marco de trabajo para la gestión de identidad pan-Europea ya prevé esta posibilidad, curiosamente desde la perspectiva del retorno de la inversión (European Commission. Information Society and Media Directorate-General. eGovernment Unit, 2006, pág. 5).

[599] Así se indica en el documento de trabajo de los servicios de la Comisión Resumen de la evaluación de impacto que acompaña a la Propuesta de Reglamento eIDAS, cuando indica que "el enfoque intersectorial de la legislación permitiría al sector privado integrar el uso de identificaciones electrónicas notificadas en

sucediendo en España, como en el caso del DNI electrónico español o de los certificados cualificados expedido por los prestadores públicos inicialmente para facilitar el acceso de los ciudadanos a los servicios públicos, que aunque en la actualidad se sujetan principalmente al régimen establecido en el Reglamento eIDAS para los servicios de confianza[600], resultan perfectamente encuadrables también dentro del concepto de identificación electrónica contenido en el Reglamento eIDAS, para este uso.

En efecto, disponer de acceso a una gran cantidad de personas ya identificadas facilitaría la actuación de las partes usuarias privadas, a las que por cierto cada vez se imponen mayores requisitos de identificación con respecto a sus clientes, en especial en función del sector. Por ello, resulta cada vez más importante poder determinar la identidad real de las personas con las que se relacionan, sin incurrir en costes excesivos, en especial cuanta mayor sea la distancia geográfica entre las partes.

El primer ejemplo de uso, por entidades del sector privado, de los medios de identificación electrónica lo encontramos –cabe recordar que así lo vimos en su momento[601]– en la posibilidad de emplearlos para la verificación de la identidad de la persona a la que se debe expedir un certificado cualificado.

Sin ánimo de exhaustividad, en la normativa de la Unión Europea podemos encontrar buenos ejemplos del uso potencial de la identificación electrónica en el ámbito privado, como por ejemplo en la Recomendación 2014/478/UE de la Comisión, de 14 de julio de 2014, relativa a principios para la protección de los consumidores y los usuarios de servicios de juego en línea y la prevención del juego en línea entre los menores, cuyo epígrafe 20, siguiendo la solicitud realizada por el Parlamento Europeo, mediante Resolución de 10 de septiembre de 2013 sobre el juego en línea en el mercado interior, de introducir controles obligatorios de identificación de terceros, anima a los Estados miembros a que adopten sistemas de identificación electrónica en el proceso de registro.

Asimismo, podemos citar la Propuesta de modificación de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. En virtud de la reforma, el artículo 13 de la Directiva, que establece las obligaciones de identificación del cliente, de forma previa o durante el establecimiento de una relación de negocios, autorizará de forma expresa el uso de "medios de identificación electrónica" definidos en el Reglamento eIDAS para dar cumplimiento de la obligación de identificación previa[602].

Para completar esta visión no exhaustiva, resulta finalmente necesario referirse al Reglamento (UE) 2017/1128 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, relativo a la portabilidad transfronteriza de los servicios de contenidos en línea en el mercado interior, cuyo artículo 5 autoriza expresamente la posibilidad de uso de un medio de identificación electrónica para la comprobación del Estado de residencia de un abonado a un servicio de contenidos en línea, en el momento de la celebración o

---

los servicios electrónicos cuando se necesite una identificación segura".

[600] Cfr. el epígrafe 2.1 de este trabajo.

[601] Cfr. el epígrafe 2.1.2.2 de este trabajo.

[602] Juntamente a servicios de confianza relevantes, definidos en el Reglamento eIDAS o en la legislación nacional. Cfr. el epígrafe 2.1.3 de este trabajo.

renovación del contrato, aunque siempre que el citado medio ofrezca dicha información, que es opcional[603].

También en el ámbito de la legislación española tenemos interesantes ejemplos, como la obligación de identificación establecida por el artículo 98.9[604] del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, en relación con la formalización de contratos a distancia, cuando ordena que "el empresario deberá adoptar las medidas adecuadas y eficaces que le permitan identificar inequívocamente al consumidor y usuario con el que celebra el contrato", algo que difícilmente podrá realizar de forma eficaz sin disponer de acceso al uso de los medios de identificación de los que previamente disponga el consumidor o usuario.

Otro ejemplo de indudable interés lo encontramos en los artículos 3 y siguientes de la vigente Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo[605], aplicable a un importante número de sujetos[606], que

---

[603] Así lo hemos visto con ocasión del análisis del Reglamento de interoperabilidad eIDAS. Cfr. el epígrafe 3.1.7 de este trabajo.

[604] En su redacción dada por el artículo único.28 de la Ley 3/2014, de 27 de marzo, dictada con el fin de transponer al derecho interno la Directiva 2011/83/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo.

[605] Modificada por Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

[606] Entre los cuales, las entidades de crédito; las entidades aseguradoras autorizadas para operar en el ramo de vida y los corredores de seguros cuando actúen en relación con seguros de vida u otros servicios relacionados con inversiones; las empresas de servicios de inversión; las sociedades gestoras de instituciones de inversión colectiva y las sociedades de inversión cuya gestión no esté encomendada a una sociedad gestora; las entidades gestoras de fondos de pensiones; las sociedades gestoras de entidades de capital-riesgo y las sociedades de capital-riesgo cuya gestión no esté encomendada a una sociedad gestora; las sociedades de garantía recíproca; las entidades de pago y las entidades de dinero electrónico; las personas que ejerzan profesionalmente actividades de cambio de moneda; los servicios postales respecto de las actividades de giro o transferencia; las personas dedicadas profesionalmente a la intermediación en la concesión de préstamos o créditos, así como las personas que, sin haber obtenido autorización como establecimientos financieros de crédito, desarrollen profesionalmente alguna de las actividades a que se refiere la Disposición adicional primera de la Ley 3/1994, de 14 de abril, por la que se adapta la legislación española en materia de Entidades de Crédito a la Segunda Directiva de Coordinación Bancaria y se introducen otras modificaciones relativas al Sistema Financiero; los promotores inmobiliarios y quienes ejerzan profesionalmente actividades de agencia, comisión o intermediación en la compraventa de bienes inmuebles; los auditores de cuentas, contables externos o asesores fiscales; los notarios y los registradores de la propiedad, mercantiles y de bienes muebles; los abogados, procuradores u otros profesionales independientes cuando participen en la concepción, realización o asesoramiento de operaciones por cuenta de clientes relativas a la compraventa de bienes inmuebles o entidades comerciales, la gestión de fondos, valores u otros activos, la apertura o gestión de cuentas corrientes, cuentas de ahorros o cuentas de valores, la organización de las aportaciones necesarias para la creación, el funcionamiento o la gestión de empresas o la creación, el funcionamiento o la gestión de fideicomisos («trusts»), sociedades o estructuras análogas, o cuando actúen por cuenta de clientes en cualquier operación financiera o inmobiliaria; las personas que con carácter profesional y con arreglo a la normativa específica que en cada caso sea aplicable presten los siguientes servicios a terceros: constituir sociedades u otras personas jurídicas; ejercer funciones de dirección o secretaría de una sociedad, socio de una asociación o funciones similares en relación con otras

establece obligaciones de identificación formal de los titulares reales de las operaciones sujetos a la ley, de forma que el artículo 3.1, segundo párrafo, impone que "en ningún caso los sujetos obligados mantendrán relaciones de negocio o realizarán operaciones con personas físicas o jurídicas que no hayan sido debidamente identificadas".

Para la identificación de los intervinientes el caso de operaciones sujetas a esta Ley se deberán emplear documentos fehacientes, según se determine reglamentariamente, a cuyos efectos determina el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, qué documentos reciben dicha consideración. Así, el artículo 6 del RD 304/2014 se refiere de forma expresa al DNI, para las personas físicas de nacionalidad española, debiendo entenderse que se refiere a la tarjeta soporte del mismo.

Algo más dudosa resulta la posibilidad de empleo del DNI electrónico, y en especial de otros sistemas de identificación electrónica, para la identificación formal, excepto en los siguientes casos: en primer lugar, en el caso previsto en el artículo 12.1 de la Ley 10/2010, así como en el artículo 231 del Real Decreto 304/2014, referido a las relaciones de negocio y operaciones no presenciales, en cuya virtud "los sujetos obligados podrán establecer relaciones de negocio o ejecutar operaciones a través de medios telefónicos, electrónicos o telemáticos con clientes que no se encuentren físicamente presentes, siempre que […] a) La identidad del cliente quede acreditada de conformidad con lo dispuesto en la normativa aplicable sobre firma electrónica"[607]; en segundo término, "cuando no concurran dudas respecto de la identidad del interviniente, quede acreditada su participación en la operación mediante su firma manuscrita o electrónica y dicha comprobación se hubiera practicado previamente en el establecimiento de la relación de negocios", según determina el tercer párrafo del artículo 4.1 del Real Decreto 304/2014, que permitiría el empleo de sistemas de identificación como el DNI electrónico, y también

---

personas jurídicas o disponer que otra persona ejerza dichas funciones; facilitar un domicilio social o una dirección comercial, postal, administrativa y otros servicios afines a una sociedad, una asociación o cualquier otro instrumento o persona jurídicos; ejercer funciones de fideicomisario en un fideicomiso («trust») expreso o instrumento jurídico similar o disponer que otra persona ejerza dichas funciones; o ejercer funciones de accionista por cuenta de otra persona, exceptuando las sociedades que coticen en un mercado regulado y estén sujetas a requisitos de información conformes con el derecho comunitario o a normas internacionales equivalentes, o disponer que otra persona ejerza dichas funciones; los casinos de juego; las personas que comercien profesionalmente con joyas, piedras o metales preciosos; las personas que comercien profesionalmente con objetos de arte o antigüedades; las personas que ejerzan profesionalmente las actividades a que se refiere el artículo 1 de la Ley 43/2007, de 13 de diciembre, de protección de los consumidores en la contratación de bienes con oferta de restitución del precio; las personas que ejerzan actividades de depósito, custodia o transporte profesional de fondos o medios de pago; las personas responsables de la gestión, explotación y comercialización de loterías u otros juegos de azar respecto de las operaciones de pago de premios; las personas físicas que realicen movimientos de medios de pago; las personas que comercien profesionalmente con bienes; las fundaciones y asociaciones; y los gestores de sistemas de pago y de compensación y liquidación de valores y productos financieros derivados, así como los gestores de tarjetas de crédito o débito emitidas por otras entidades.

[607] Previsión claramente oscura e insuficiente, a mi juicio, dado que no todos los tipos de firma electrónica necesariamente aportan una verdadera identidad, en especial con la nueva definición de la firma electrónica prevista en el Reglamento eIDAS, como estudiaremos más adelante en este trabajo. Seguramente sólo la firma electrónica avanzada basada en un certificado electrónico cualificado y la firma electrónica cualificada sean aceptables en este contexto, dada la condición de nuevo cliente de la persona, que precisamente exige su identificación.

de los sistemas de firma electrónica cualificada, en operaciones presenciales. Nótese que esta regulación se va a ver indudablemente afectada por la reforma de la Directiva (UE) 2015/849 anteriormente referida.

En España, el Anteproyecto de Ley por la que se modifica la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, de noviembre de 2017, procede a la modificación del artículo 12.1.a) anteriormente mencionado, exigiendo que "[l]a identidad del cliente quede acreditada mediante la firma electrónica cualificada regulada en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE", propuesta que, a mi juicio, no resulta conforme a la nueva redacción propuesta para el artículo 13 por la ya mencionada Propuesta de modificación de la Directiva (UE) 2015/849, por cuanto no prevé el uso de medios de identificación electrónica notificados conforme al Reglamento eIDAS.

Más correcto resulta, en este sentido, el artículo 19.1[608] del *Decreto legislativo 21 novembre 2007, n. 231, Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione*, autoriza el uso de sistemas de identificación sin presencia física personal, incluyendo los certificados cualificados, siempre que los mismos cumplan con la normativa nacional –prevista en el artículo 64 del *Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale–*, o que hayan sido notificados al amparo del artículo 9 del Reglamento eIDAS, exigiéndose el nivel de seguridad alto, o que el certificado corresponda a una firma digital asociada a un documento informático, conforme al artículo 24 del *Codice dell'amministrazione digitale*.

Como se puede fácilmente constatar, en todos estos casos resultaría coherente el uso de algunos de los sistemas de identificación electrónica ofrecidos o reconocidos por los Estados miembros al amparo del Reglamento eIDAS para ello, al menos en el caso de sistemas de nivel de seguridad sustancial o alto.

El punto clave lo encontramos cuando se dice que "para facilitar el uso por parte del sector privado de tales medios de identificación electrónica a través de las fronteras, debe estar disponible la posibilidad de autenticación ofrecida por cualquier Estado miembro para las partes usuarias del sector privado establecidas fuera del territorio de dicho Estado miembro en las mismas condiciones aplicadas a las partes usuarias del sector privado establecidas dentro de dicho Estado miembro"; es decir, que "por lo que respecta a las partes usuarias del sector privado, el Estado miembro que efectúa la notificación podrá definir condiciones de acceso a los medios de autenticación", entre las cuales "informar de si en un momento dado los medios de autenticación relacionados con el sistema notificado están disponibles para las partes usuarias del sector privado".

Como hemos visto anteriormente, el artículo 7.f) del Reglamento eIDAS establece que

---

[608] En redacción dada por artículo 2 del *Decreto legislativo 25 maggio 2017, n. 90, Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006*.

"para las partes usuarias distintas de los organismos del sector público, el Estado miembro que efectúa la notificación podrá definir las condiciones de acceso a esa autenticación", previsión que se refiere, como hemos visto anteriormente, al uso de la infraestructura que aporta el Estado para habilitar el proceso de autenticación; esto es, los nodos de interoperabilidad de identificación electrónica[609].

En este sentido, debemos plantearnos qué tipo de condiciones se pueden establecer por el Estado miembro, dado que las mismas deben ser conforme con los principios informadores del Derecho de la Unión. Y, en este sentido, hay que entender que cualquier condición a establecer deberá ser, cuanto menos, objetiva, razonable y no discriminatoria.

Una de estas condiciones viene referida a la posibilidad de establecer tarifas en relación con el servicio[610], dado que es evidente que el Reglamento eIDAS no se opone a ello, al exigir la gratuidad únicamente en relación con los procesos de autenticación con los organismos del sector público, decisión de corte netamente político y que responde, una vez más, a la existencia de diversos modelos de financiación de los servicios de identificación electrónica en los Estados miembros de la Unión Europea[611], así como a las dudas que se han suscitado en los proyectos STORK acerca de la sostenibilidad de la autenticación transfronteriza.

Esta cuestión del coste no sólo puede referirse al derecho de uso de la identificación electrónica; esto es, del medio empleado para dicha identificación, sino que también debe contribuir al sostenimiento de la infraestructura ofrecida por cada Estado para el proceso de autenticación, que incluye, entre otros, los costes de funcionamiento de los nodos de interoperabilidad de identificación electrónica, de la acreditación de los componente de servicio en sede nacional, de las actividades de márquetin y, finalmente, de explotación de los servicios centrales de la red[612].

Esta heterogeneidad dificulta la definición de un modelo común de precios para las

---

[609] Que típicamente se corresponderán con los puntos de acceso (denominados PEPS) de STORK o sus sucesores.

[610] (Gobert, 2015, p. 14).

[611] En este sentido, (Brugger & Fraefel, 2013) han estudiado con un alto nivel de detalle el estado actual, y los planes futuros de desarrollo nacional y transfronterizo, de las infraestructuras de identificación electrónica existentes en 16 Estados participantes en STORK (Austria, República Checa, Estonia, Francia, Islandia, Italia, Lituania, Luxemburgo, Países Bajos, Eslovaquia, Eslovenia, España, Suecia, Suiza, Turquía y Reino Unido), incluyendo los costes de uso para los prestadores de servicios, así como para las personas que adquieren los medios de identificación electrónica, tanto físicas como jurídicas. De este estudio se desprende que los modelos de coste y las estrategias de precios existentes en el nivel nacional son heterogéneas; aunque en la mayoría de casos analizados no se establece un precio en relación con el uso de la identificación electrónica para los prestadores privados de servicios, al menos en República Checa, Estonia, Luxemburgo, Suecia y Turquía se cobra por dicho servicio, y en Reino Unido esta posibilidad se encuentra en estudio. Por lo que respecta a España, en el estudio se indica que el uso de la identificación electrónica es gratuito para los prestadores de servicios, pero con la anotación de que esta información sólo se refiere al DNI-e, existiendo otras soluciones, públicas y privadas, sobre las que no se informa. El propio estudio indica que se encuentra limitado en cuanto a su alcance al medio de identificación electrónica principal de cada Estado, por lo que en el caso de España se analiza el DNI-e. Debido a la complejidad de las políticas públicas referidas a la identificación electrónica de los ciudadanos en España, que como veremos, es claramente multinivel y con una diversidad de modelos de negocio, sería deseable ampliar el alcance de este tipo de trabajos, por su indudable interés.

[612] (Brugger, y otros, 2014, pág. 66).

transacciones transfronterizas, en especial por haberse planteado la existencia de modelos de coste diferenciados en relación con los prestadores de servicio radicados en territorio nacional o en otros Estados; en este caso, se podría dar la situación de que se cobrase sólo a los prestadores de servicio extranjeros, algo que penalizaría de forma importante a las transacciones transfronterizas[613], levantando una barrera a la adopción de estos servicios, que podría considerarse ilícita en los términos de la Directiva de Servicios.

En definitiva, dado que el Reglamento eIDAS ha optado por no restringir la libertad de los Estados miembros de establecer tarifas en relación con el uso de los servicios de autenticación transfronteriza por los prestadores privados, seguramente dicha posibilidad se acabará desarrollando, en función de las políticas públicas que impulse cada Estado, pudiéndose optar por modelos basados en la membresía en el sistema o el consumo de transacciones en el mismo[614].

[613] (Brugger, y otros, 2014, pág. 67).

[614] (Brugger, y otros, 2014, pág. 68).

CAPÍTULO 4. LA FIRMA ELECTRÓNICA, EL SELLO ELECTRÓNICO, Y LOS SERVICIOS DE CONFIANZA QUE LOS SUSTENTAN

En este cuarto Capítulo procede abordar el estudio de las instituciones jurídicas creadas a partir de las tecnologías de seguridad que permiten la atribución de la actuación electrónica a las personas físicas o jurídicas; esto es, la firma electrónica, que ya tiene una relativamente larga historia, y el novedoso sello electrónico. Instituciones que realmente se basan en las mismas tecnologías subyacentes, diferenciándose nítidamente, al menos en la normativa de la Unión, desde la perspectiva de su utilidad y efecto jurídico.

En relación con estas instituciones, el epígrafe primero de este Capítulo se dedica a su caracterización legal, que exige referirse a los diversos niveles que los mismos presentan atendiendo en lo establecido en el Reglamento eIDAS. Ello nos lleva a presentar la firma electrónica o sello electrónico, en general, un concepto más amplio que la firma electrónica avanzada o sello electrónico avanzado, y finalmente el concepto, aún más restringido, de firma electrónica cualificada o sello electrónico cualificado.

Con ocasión del análisis de estas tipologías, se estudian los diferentes elementos integradores de cada tipo de firma electrónica y sello electrónico, lo que justifica el análisis de los datos y dispositivos de creación de firma electrónica y sello electrónico, con especial atención a su fiabilidad, cuestión imprescindible en orden a la efectiva atribución de los documentos y mensajes electrónicos a las personas físicas y jurídicas. En ese momento tendremos ocasión de detenernos en el sistema público de garantía de la necesaria seguridad de estos productos, alineada con la normativa de seguridad industrial. No será, sin embargo, necesario referirnos a los certificados electrónicos que sustentan tales firmas electrónicas y sellos electrónicos, dado que ya se han estudiado en el Capítulo 2.

El segundo epígrafe de este Capítulo se dedica a los efectos jurídicos de estas dos instituciones, incluyendo el análisis de la validez de los diferentes tipos de firma electrónica y sello electrónico, así como de su diversa eficacia, tanto desde la perspectiva sustantiva cuanto desde la procesal.

Finalmente, el tercer epígrafe del Capítulo se dedica al estudio de los servicios de confianza que ofrecen soporte a algunos tipos de firma electrónica o de sello electrónico, como son la creación, la validación y la conservación de estas fuentes de prueba electrónica, análisis que deberá ser complementado con el más general de todos los servicios de confianza, contenido en el Capítulo 6.

4.1 CARACTERIZACIÓN DE LA FIRMA Y EL SELLO ELECTRÓNICOS

El Reglamento eIDAS, como anteriormente ya hicieran la DFE y la LFE, institucionaliza jurídicamente la firma electrónica, en un concepto que el Reglamento eIDAS reserva en exclusiva a la actuación de las personas físicas, así como el sello electrónico, destinado a

la "actuación" de las personas jurídicas[615].

Como veremos, una de las principales diferencias entre ambas instituciones (firma y sello) va a ser precisamente el tipo de entidad usuaria de la misma –persona física para la firma, persona jurídica para el sello–; motivo por el cual procederemos a su estudio conjunto, sin perjuicio de ir anotando las diferencias relevantes entre ambas, que desde luego no son pocas.

El Reglamento eIDAS, siguiendo el mismo enfoque que anteriormente la DFE y la LFE, diferencia diversos tipos de firma/sello electrónico, cuyo estudio abordamos a continuación.

Como se verá, la firma/sello electrónico es un artefacto técnico que va a ser reconocido jurídicamente en función de una serie de propiedades que lo hacen relevante como fuente de prueba electrónica, al objeto de atribuir un documento a una persona y, en su caso, también identificar a dicha persona. Y, en este sentido, también hay que recordar que la firma/sello electrónico no es un servicio de confianza, sino que es una institución que hace uso de los mismos, en algunos casos, como elemento de respaldo.

4.1.1 La firma y sello electrónicos, en general

4.1.1.1 El concepto de firma: de la autenticación de datos a la finalidad de firmar

El artículo 3.10 del Reglamento eIDAS define la firma electrónica como los "datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar", en una definición ligeramente diferente a la contenida originalmente en la DFE y en la LFE, que refuerza el aspecto funcionalista de la definición, ya que lo importante será que los citados datos sean empleados precisamente para esta función de firmar, mientras que en la regulación anterior se hacía hincapié en el aspecto funcional de la firma como sistema de identificación/autenticación electrónica.

En efecto, de acuerdo con el artículo 2.1 de la DFE, la firma electrónica se definió como "los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación", mientras que el artículo 3.1 de la LFE la definió como el "conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante"[616]; es decir, una suerte de credencial que sustentaba la identificación y

[615] En la LFE, el artículo 7 reguló los certificados electrónicos de personas jurídicas, que han quedado desplazados por el nuevo concepto de sello electrónico del Reglamento eIDAS, con el que se consideran incompatibles. Sobre estos certificados, cfr. (Martínez Nadal, 2009, pág. 145 y ss.).

[616] Anteriormente, el artículo 2.a) del RDLFE definía la firma electrónica como "el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge", mientras que la firma electrónica avanzada se definía, en el numeral b) de mismo epígrafe, como "la firma electrónica que permite la identificación del signatario […]", lo que había suscitado la crítica de la doctrina, como en el caso de (Alonso Ureba & Alcover Garau, 2000, pág. 192), que consideraban la diferencia entre la identificación formal y la identificación potencialmente peligrosa, dado que "parece que en la identificación hay grados y es claro que no debería haberlos, sino que se identifica o no se identifica, de forma que la

autenticación por vía electrónica, pero debiéndose indicar que sólo constituían firma electrónica las tecnologías de autenticación que se referían a los datos electrónicos[617], y sólo a éstos, no a los datos en soporte papel[618], no siéndolo aquellas que sólo se referían a la autenticación de entidades[619].

Resultaba ciertamente criticable que la LFE hubiera empleado exclusivamente la expresión "identificación del firmante", dado que suponía una confusión clara con respecto a la autenticación de los datos a los que se refiere la DFE, que es un servicio de seguridad diferente[620]; a pesar de lo que cual las definiciones de firma electrónica de la DFE y de la LFE podían considerarse esencialmente equivalentes y de amplio alcance. Las mismas calificaban como firma electrónica (sin mayor adjetivo) cualquier producto resultante de la aplicación de tecnología de autenticación de origen de datos, y de hecho, lo hacían con independencia de su idoneidad como instrumento de declaración volitiva, dado que de lo que se trataba es de autenticar a una persona en relación con unos datos, por lo que debía entenderse que sólo las tecnologías que ofrecían al menos esta capacidad de autenticación podían ser incluidas en el concepto legal de "firma electrónica" contenido en dichas normas.

Se corresponde esta definición de firma de la DFE y LFE, en términos generales, con la función más básica que se puede predicar de una firma escrita, que es sencillamente indicar a qué persona se puede atribuir una comunicación o un documento autenticado por la misma.

El problema de este enfoque es que, ontológicamente, la identificación/autenticación constituye elemento esencial para que se pueda hablar de "firma electrónica", y como ni la DFE ni la LFE aclaraban qué significa "identificación" ni "autenticación", nos encontrábamos ante una noción que podía generar interpretaciones radicalmente enfrentadas.

Y esto presentaba una gran importancia práctica, dado que de ello dependía que se pudiera emplear, o no, un mecanismo técnico concreto para generar una firma electrónica; a título de ejemplo, nos podíamos plantear la duda de si se podía firmar un contrato con un

---

firma o sirve para identificar o no es firma".

[617] Para (Martínez Nadal, 2009, págs. 73-74), "una firma electrónica sería simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita", definición absolutamente acertada que, sin embargo, excede con mucho la letra de la ley, al menos en relación con la caracterización que hace la LFE de la firma no avanzada. Este enfoque se encuentra más alineado con la definición de firma electrónica del Reglamento eIDAS. Algún otro autor ha notado que "el significado de la firma electrónica no determina que se trate de una auténtica firma, sino más bien se puede hablar de un sello por ejemplo, lo que ocurre que se utiliza la misma tecnología quizá por ser más expresiva, y como comparación con la firma manuscrita" (García Mas F. , 2010, pág. 1124).

[618] Así lo hace notar, agudamente, (Illescas Ortíz, 2001, pág. 91), que se refiere a esta cuestión como un límite absoluto de la firma electrónica, que aparece casi de forma oculta o solapada. Aunque su observación se refiere al RDLFE, resulta plenamente aplicable también a la definición del Reglamento eIDAS.

[619] Cfr. COM (2010) 120 final, página 4.

[620] En favor de la noción de identificación, sin embargo, se manifiesta (Rodríguez Adrados, 2000, pág. 384), porque "[e]n la contratación informática, la indicación es precisa porque naturalmente es una contratación entre ausentes, a distancia, en que las partes ni se conocen ni se ven, por lo que no se pueden identificar", opinión que parece partir de una interpretación del término "autenticación" diferente al que pretendía el legislador comunitario.

consumidor con el que no se había interactuado jamás, empleando una simple dirección IP de Internet. Para responder afirmativamente conforme a la LFE, debíamos aceptar que una IP de una persona a la que no conocíamos era un mecanismo que identificaba/autenticaba a dicha persona.

El Diccionario de la Real Academia de la Lengua española se refiere a la identificación como "la acción y efecto de identificar o identificarse", mientras que para el verbo identificar ofrece dos acepciones relevantes; a saber, "reconocer si una persona o cosa es la misma que se supone o busca", y "dar los datos personales para ser reconocido".

Asimismo, el Diccionario se refiere a la autenticación como "la acción y efecto de autenticar", mientras que para el verbo autenticar ofrece sólo como acepción relevante la que lo considera sinónimo de "acreditar", verbo para el cual resultan apropiadas las siguientes acepciones: "hacer digno de crédito algo, probar su certeza o realidad", y "dar seguridad de que alguien o algo es lo que representa o parece".

Desde esta perspectiva, parecía lógico que en la LFE se optara por el término "identificación" en lugar del de "autenticación" contenido en la DFE, aunque como ya se ha indicado resultaba criticable porque alejaba el concepto legal español del previsto en la normativa comunitaria, enfocando erróneamente el núcleo de dicho concepto en la autenticación de entidades, y no en la autenticación de origen de datos; y en cualquier caso, era igualmente necesario entender su significado legal exacto.

Para ello, podíamos acudir a la autorregulación de la industria, en forma de normas técnicas, que como ya sabemos[621] ofrece un enfoque bastante amplio al efecto, por lo que debíamos estar al caso concreto para determinar si nos encontrábamos, o no, ante una firma electrónica en el sentido de la DFE o de la LFE. Por ejemplo, cuando una entidad financiera habilita la banca electrónica para un usuario, debe previamente identificarlo, procedimiento durante el cual le entregará una tarjeta de coordenadas[622] que el cliente podrá posteriormente emplear para autenticarse a distancia en relación a una operación en concreto; o cuando se registra el trazo o la voz de la persona para posteriormente reconocer a dicha persona, también se la debe previamente identificar[623].

En todos estos casos parece más que razonable entender que existe un nivel más o menos adecuado de comprobación previa de la identidad y de la posterior autenticación de la citada persona, por lo que no parece existir dificultad ninguna en admitir dichos sistemas en el concepto legal de la firma electrónica de la LFE[624], siempre y cuando funcionen conjuntamente con un mecanismo que también garantice la autenticación de los datos.

---

[621] Cfr. el Anexo A.1 de este trabajo.

[622] Se trata de una tarjeta de plástico en la que consta una serie de números de identificación personal (por ejemplo, 40), que se deben introducir a requerimiento de la entidad financiera, generalmente para autorizar (esto es, firmar) una operación determinada.

[623] Pero no si lo que se desea es sencillamente obtener la firma a efectos contractuales, ya que siempre se podrá practicar, igual que en soporte papel, una prueba pericial caligráfica en relación con los datos del trazo capturado electrónicamente.

[624] Otra cosa es cuánta garantía de autenticación se precisa, aspecto que en mi opinión depende de otros factores y, muy en especial, de la legislación aplicable a cada transacción concreta, dado que no aplica el mismo rigor el legislador a unas operaciones que a otras. Ciertamente, se exige mayor control en el sector financiero, sujeto a estrictas obligaciones de identificación para luchar contra el blanqueo de capitales, que para vender bienes de consumo a distancia por lo que se deberá aplicar el principio de proporcionalidad.

La cuestión –al menos en relación con la interpretación estricta del concepto de firma electrónica en la LFE que parte de la necesaria identificación del firmante, y no de la autenticación de los datos– es qué sucede con el uso de sistemas donde no existe este proceso previo de verificación de la identidad, o donde el mismo es laxo, o no ofrece determinadas garantías: ¿podíamos aceptar como sistema de firma electrónica la identidad alegada de un consumidor del que únicamente tenemos como elemento de autenticación su dirección IP de Internet?; ¿podíamos aceptar como sistema de firma el trazo manuscrito capturado en una tableta digitalizadora y remitido a distancia por una persona a la que jamás hemos visto?; finalmente, ¿podíamos aceptar un perfil de red social como mecanismo de identificación/autenticación?

En primer lugar, parece razonable descartar la consideración, como sistema de firma electrónica, al menos en la definición contenida en la LFE, aunque no en la DFE, de aquellos sistemas en los que resulte imposible la identificación del firmante. Así sucedería, por ejemplo, en aquellos casos donde el "firmante" emplee mecanismos de autenticación anónima[625] o de firma digital anónima[626]. Aquí es donde se visualiza el diferente concepto de firma electrónica de ambas normas, por cuanto estos mecanismos entran perfectamente en la definición de firma electrónica de la DFE, pero no de la LFE, contradicción que sólo se puede salvar aplicando el principio de interpretación conforme del derecho nacional al europeo.

Sin embargo, ya no parecía tan razonable descartar aquellos mecanismos en los que la comprobación de la identificación/autenticación se pueda realizar *a posteriori*, por ejemplo. En estos casos, aun no existiendo registro previo de la identidad, sí que se podría practicar prueba para determinar la identidad de firmante, algo que ya sucede con la firma manuscrita en los contratos celebrados por correspondencia, y nadie duda de que los mismos hayan sido firmados[627].

Entre este tipo de mecanismos podríamos ubicar a la firma manuscrita capturada electrónicamente[628] ("digitalizada"), sin duda alguna[629]. Más dudas podrían existir acerca de la posibilidad de verificar la dirección IP de Internet de una persona que alegue no haber generado la firma[630], aunque desde luego resulta defendible –en el plano formal,

---

[625] La norma internacional ISO/IEC 20009, partes 1 a 4, describe diversos mecanismos de autenticación anónima de entidad.

[626] La norma internacional ISO/IEC 20008, partes 1 y 2, describe el uso de mecanismos de firma anónima de grupo y de claves públicas múltiples.

[627] Cosa diferente será que la firma manuscrita sea falsa, un hecho que se podrá discutir en una eventual impugnación.

[628] (Gruber, Hook, Kempf, Scharfenberg, & Sick, 2006) muestran un sistema de bolígrafo digitalizador capaz de verificar la autenticidad de una firma manuscrita, que puede cualificar perfectamente como sistema de firma electrónica. Cfr. también (Bashir & Kempf, 2009).

[629] Puede verse un análisis completo de las implicaciones jurídicas de esta tecnología en (Anguiano Jiménez, 2015), que el autor considera claramente subsumible dentro del concepto de firma electrónica. En contra de esta posición, (Cámara Largo, 2013, pág. 92) opina que la firma manuscrita capturada electrónicamente no casa con la definición de firma electrónica, por lo que no cabe considerarla como tal.

[630] Dadas las restricciones de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que limita la cesión de los datos de tráfico a los "fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales". Cfr. también el artículo 42 de la Ley 9/2014, de 9 de mayo,

que no de la eficacia probatoria– que la IP identifica a la persona, después de la jurisprudencia de los Tribunales que así lo ha afirmado[631].

Aún menos razonable parecía descartar los mecanismos de identificación basados en perfiles de redes sociales, dada la calidad de algunos de ellos, en especial debido al cada vez mayor rigor que aplican en forma de políticas de veracidad en los datos del perfil. Nos encontraríamos en este caso ante un caso de firma electrónica con autenticación delegada a una tercera parte, en la que la fiabilidad de la identificación/autenticación dependerá de sus políticas y prácticas; esto es, de forma similar a cuando la comprobación previa de la identidad es realizada por la parte que desea contratar con la otra parte.

Y algo parecido sucedería con los sistemas de identificación "agregada", donde se suman determinados datos de identidad como, por ejemplo, una cuenta de correo electrónico alegada (pero verificada técnicamente como existente) más una tarjeta de pago también verificada, o incluso fotografías de documentos oficiales; suma de elementos que permiten, sin verificación presencial previa de la identidad, confiar en que la misma es suficientemente cierta para determinadas transacciones[632].

En definitiva, todos estos mecanismos debían ser considerados como sistemas de firma electrónica de acuerdo con la DFE y, en aplicación del principio de interpretación conforme de la ley nacional con el Derecho comunitario, también de acuerdo con la LFE. Podemos concluir, pues, que con carácter general la DFE y la LFE han venido permitiendo el empleo, como sistema de firma electrónica, de cualesquiera mecanismos de autenticación del origen de los datos, siempre que los mismos resulten apropiados para el contexto de la operación de que se trate.

Sin embargo, la nueva definición europea, que como hemos avanzado se centra en que dichas tecnologías persigan la finalidad de "firmar", prescinde completamente del requisito de la identificación/autenticación –tanto de la entidad como de los datos–, sin perjuicio de que evidentemente sea necesario poder identificar de forma efectiva al firmante[633], de forma previa o *a posteriori*, para poder beneficiarse del valor probatorio de una firma electrónica[634].

General de Telecomunicaciones.

631 El Tribunal Supremo, en su Sentencia de 3 de octubre de 2014 (caso PROMUSICAE), ha indicado que "no cabe duda que, a partir de la dirección IP puede identificarse directa o indirectamente la identidad del interesado, ya que los proveedores de acceso a internet tienen constancia de los nombres, teléfono y otros datos identificativos de los usuarios a los que han asignado las particulares direcciones IP", aunque es claramente un mecanismo que sólo aproximadamente identifica a una persona física.

632 Resulta muy interesante comprobar el sistema de verificación de identidad de comercios electrónicos como AirBnB, en este sentido, de excelente calidad y resultados prácticos, en especial comparado con otros mecanismos "oficiales".

633 Aunque esto es cierto con carácter general, la definición de la firma/sello electrónico avanzado sí que exige –igual que sucedía en la DFE y la LFE– la identificación/autenticación de la entidad.

634 En este sentido, para (Merchán Murillo, 2016, pág. 32), "la determinación de la identidad del signatario es uno de los requisitos para crear una firma electrónica válida. Se trata de establecer como rasgo esencial de la firma electrónica su capacidad para identificar al firmante y mostrar su capacidad respecto del mensaje", aunque añade, y esto es muy relevante en mi opinión, que "[e]sta aprobación no debe entenderse en sentido estricto; es decir, no respecto a la emisión del consentimiento para quedar jurídicamente obligado; pues de lo contrario, estaríamos hablando de la autenticación de la transacción", concluyendo que "[p]or ello, lo que se pretende es establecer un nexo de unión entre la información del mensaje de datos y

Por este motivo, con el nuevo concepto de firma electrónica, cualquier mecanismo técnico formado por datos asociados a otros datos que se emplee "para firmar" será admisible, incluso aunque el mismo no identifique/autentique de forma previa a la persona física, y sin perjuicio de que no todos éstos resultarán probatoriamente útiles.

Al menos en una lectura superficial, se trata de una definición que parece tener implícita la noción de la utilización de algún tipo de clave para firmar, algo que no resulta especialmente neutral en términos tecnológicos, y que resulta algo extraña cuando se emplean ciertas tecnologías, como la ya aludida firma manuscrita capturada electrónicamente, en la que no existe clave ninguna a emplear. En este caso, los datos en formato electrónico que el firmante utiliza para firmar incluyen aquellos que representan la dinámica de la firma manuscrita (una modalidad de biometría basada en el comportamiento), como la velocidad, la presión, o la inclinación, por lo que dichos datos constituyen una firma electrónica sólo cuando los utiliza el firmante para firmar, y no en otros casos[635].

De otro lado, respecto a qué signifique la expresión "para firmar"[636], se trata de una cuestión que se debe analizar conforme al derecho nacional, dado que el Reglamento eIDAS nada dice al respecto[637].

En este sentido, resulta claro que la firma manuscrita cumple diversas funciones sociales típicas[638], que normalmente han sido institucionalizadas jurídicamente por la legislación

---

la persona que lo emite, con independencia de que se produzcan o no, consecuencias jurídicas concretas". Sin embargo, como ya hemos visto, aunque toda firma deba enlazar con una identificación concreta, no siempre la identificación se produce en conexión con una firma, dado que son funciones plenamente diferenciadas.

[635] Como, por ejemplo, para autenticar a una persona, utilidad que también permite esta tecnología.

[636] De gran interés resultan, en este sentido, las aportaciones de la historia, la antropología y la diplomática. (Fraenkel, 1992, p. 7) dijo, con gran autoridad, que "la firma es el vestigio de un verdadero sistema de signos de identidad, del que se desgaja en el siglo XVI, y que, desde entonces, persiste sólo, como un signo aislado. Además, pertenece a los llamados signos de «validación», cuya función es transformar cualquier documento escrito en un acto legal. Debemos, por tanto, insertar este signo dentro de un universo de signos y de prácticas, si queremos darle su dimensión real" (la traducción, del francés, es mía), que abarcan los siglos VI a XVI, incluyendo armaduras, nombres propios, firmas, signos, sellos e insignias, con un gran dominio formal de la imagen. La misma autora analiza cómo el abandono progresivo de signos, en beneficio de la firma personal, deriva de un lento cambio de mentalidad, paralelo a la progresiva importancia de la singularidad del sujeto, explicando que "[e]l período que nos interesa termina precisamente en el siglo XVI, cuando la firma encontró su forma canónica: la aposición autógrafa del nombre propio, y donde la misma se convierte en obligatoria. Este triunfo de la firma, durante mucho tiempo un modesto y auxiliar de prestigiosos sellos y señas, tiene su parte de austeridad. El universo de signos de identidad es reducido y disciplinado. Considerada como la culminación de este período de diez siglos, indica, a la inversa, de entre estos numerosos signos y de estas prácticas múltiples, lo que mejor cumple con los requisitos de la identidad moderna. La firma los incluye a ambos: el nombre propio y la escritura. Lo que es significativo, incluso más que este signo y esta práctica, es el modo de inscripción mediante el cual se actualizan: la autografía. Lo que es nuevo en la selección de la autografía es la extensión de este principio a todo el dominio legal y su carácter obligatorio, sepa uno escribir o no" (Fraenkel, 1992, pp. 9-10).

[637] Esto significa, como han puesto de manifiesto (Dumortier & Vandezande, 2012a, p. 5), que incluso en el caso de la firma electrónica cualificada, que recibe el efecto jurídico de equivalencia con la firma manuscrita, este efecto jurídico podría ser diferente el cada uno de los Estados miembros, algo que les lleva a considerar excesivo el uso de un reglamento que no ofrece mayor armonización que la directiva.

[638] Desde una perspectiva muy amplia, y desde luego, más general que la jurídica, (Chou, 2015, p. 84) refiere, entre las funciones de la firma manuscrita, la de conferir carácter, compromiso y cumplimiento, por

o la jurisprudencia, por lo que cualquier tecnología que permita dicho cumplimiento deberá ser considerada como firma electrónica, sin perjuicio de la conveniencia de modificar ligeramente la definición de esta institución en el sentido de hacerla más neutral, por ejemplo, en línea del derecho inglés, quizá el mejor ejemplo en este sentido[639].

Desde este punto de vista, sucede que, como ya hemos visto al analizar el concepto de firma electrónica en la DFE y en LFE, una de las funciones de la firma electrónica puede ser simplemente la atribución del mensaje a una persona identificada, pero sin que de la misma se desprenda la realización de declaración de voluntad alguna –así sucedería, por ejemplo, con la firma de una postal remitida a un familiar–; mientras que otra función socialmente típica será la prestación del consentimiento contractual[640], para la que se requerirán condiciones específicas a este respecto[641].

A diferencia de otros ordenamientos jurídicos, como el francés[642], en Derecho español no

---

tratarse de una potente representación de uno mismo; pero también enfatiza el valor simbólico de las firmas de artistas y celebridades, y que la firma manuscrita actúa como un comportamiento altamente expresivo que distingue la identidad del firmante, de otros.

639 En este sentido, el artículo 7(2) de la *Electronic Communications Act 2000*, en redacción dada por la *Electronic Identification and Trust Services for Electronic Transactions Regulations 2016*, que dispone que "a los propósitos de esta sección una firma electrónica es cualquier cosa en forma electrónica que — (a) sea incorporada a o lógicamente asociada con una comunicación electrónica o datos electrónicos; y (b) pretende ser utilizada por el individuo que la crea para firmar" (la traducción es mía, y debe notarse, en especial, la dificultad de uso de la intraducible expresión inglesa "an electronic signature is so much of anything in electronic form".

640 (Illescas Ortíz, 2001, págs. 78-79) había hecho notar, a este respecto, que "no plantea dificultad grave afirmar que la FE es un medio –o datos– electrónico para atribuir origen personal cierto a un MD y establecer o atribuir la conformidad de la persona firmante con el contenido de lo firmado", tratándose "al igual que la firma manuscrita, de un instrumento cierto de atribución de paternidad a una declaración de voluntad o ciencia"; si bien apunta otras funciones que, a su juicio, puede satisfacer el medio o método electrónico de firma: "(ii) función de privacidad –cifrado del mensaje y del nombre del firmante– y (iii) función de seguridad e integridad –evidencia de la apertura o alteración del mensaje entre el momento de su emisión firmada y el de su llegada a su destinatario–". En mi opinión, esta al menos hoy, caracterización de funciones es propia, no tanto de la institución de la firma electrónica como de determinados servicios de confianza, en concreto del servicio de entrega electrónica certificada, que sustenta el no rechazo.

641 (Couto Calviño, 2007, págs. 7-8) estimó, a la luz de la LFE, inviable el paragón entre firma manuscrita y firma electrónica, en rigor, denunciando que "entre las manifestaciones de esta inadecuada comparativa podemos referirnos al hecho de asociarse la firma electrónica indefectiblemente […] una función autenticadora, junto a la función identificativa que indudablemente tiene. La doctrina más general o consagrada viene estimando que función identificativa y declarativa o de autenticación van pareja en la firma electrónica, en el sentido de que el uso de la misma siempre se vincula de forma esencial a una declaración de voluntad, sin que queda abstraer dicho uso de un mensaje con contenido negocial", añadiendo que "una concepción netamente autónoma y singular de la firma electrónica, no presupondría en modo alguno la existencia de aquella función de autenticación, que sí nos vemos obligados a asumir y a estimarla inherente a la firma electrónica, si partimos del esquema comparativo con la firma manuscrita". A mi juicio, este autor acierta al indicar que pueden existir firmas electrónicas sin una función autenticadora de una declaración de voluntad, pero ello no deriva de que la firma manuscrita sí la tenga, porque lo cierto es que no tiene porqué ser así, existiendo firmas manuscritas que ninguna voluntad expresan, como la firma en una postal. Con la definición del Reglamento eIDAS, ha quedado resuelta la posible identificación de la firma electrónica sólo como equivalente de las firmas manuscritas que tienen función autenticadora, aunque al precio de remitir a cada Derecho nacional la determinación de las funciones de la firma manuscrita.

642 El artículo 1316-4 del Código Civil francés, incorporado por artículo 4 de la *Loi nº 2000-230 du 13 mars*

existe una definición de los requisitos que debería cumplir una firma manuscrita para la prestación del consentimiento contractual, pero la jurisprudencia ha concretado algunas de estas características.

Así, la Sentencia del Tribunal Supremo de 3 de noviembre de 1997 indica que "la firma es el trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse con lo que en ellos se dice. Aunque la firma puede quedar reducida, sólo, a la rúbrica o consistir, exclusivamente, incluso, en otro trazado gráfico, o en iniciales, o en grafismos ilegibles, lo que la distingue es su habitualidad, como elemento vinculante de esa grafía o signo de su autor. Y, en general, su autografía u ologrāfía, como vehículo que une a la persona firmante con lo consignado en el documento, debe ser manuscrita o de puño y letra del suscribiente, como muestra de la inmediatez y de la voluntariedad de la acción y del otorgamiento".

De esta Sentencia del Tribunal Supremo se pueden, de hecho, obtener los tres elementos que debe cumplir una tecnología para "servir para firmar" desde la óptica del Derecho; a saber, la identificación del firmante en condición de autor del documento, la voluntad de obligarse y la vinculación con el texto contenido en el documento, que presupone que el autor ha tenido acceso directo al mismo[643].

De ello se desprende que cualesquiera de las funciones sociales típicas de la firma manuscrita sólo tienen sentido en relación con un documento escrito[644] –en particular, la función social típica jurídicamente más importante se produce cuando el documento incorpora una declaración de voluntad u otra, que produce efecto jurídico–, por lo que cualquier firma electrónica también se deberá proyectar sobre un soporte electrónico duradero que incorpore dicho escrito.

Asimismo, es preciso recordar que una cosa es que la función social típica más importante de la firma (manuscrita y, por tanto, electrónica) sea vincular una declaración a una persona, normalmente a los efectos de la declaración de voluntad, pero que de ello no se deriva una obligación de estampar la firma en todo soporte (papel o electrónico duradero) en el que se contenga un régimen jurídico-privado (un clausulado) que vincule a las partes, dado que en efecto existen casos en que un simple soporte duradero será suficiente,

---

2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique –actualmente, artículo 1367 del Código Civil francés, tras la reforma realizada por artículo 4 de la *Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations*–, dice que la firma necesaria para la perfección de un acto jurídico identifica a su autor, y que expresa su consentimiento a las obligaciones derivadas de dicho acto. Por ello, en Derecho francés una tecnología que no garantice estas dos propiedades simplemente no se podrá considerar como una firma electrónica a los efectos de la perfección de actos jurídicos, aunque ciertamente lo podría ser a otros efectos. Adicionalmente, dicha norma (también mantenida tras la reforma del Código Civil mencionada) indica que cuando la firma sea electrónica, la misma consiste en un proceso de identificación fiable que garantice su vinculación con el acto a que se adjunte.

643 Cfr. el análisis de esta sentencia en (Anguiano Jiménez, 2015).

644 Para (Fraenkel, 2008, p. 23), "los actos de escritura pertenecen a una categoría distinta de los actos orales y el caso de la firma puede considerarse como un caso prototípico de esta categoría. Esta primera hipótesis conduce a una segunda: las prácticas de escritura implican siempre la realización de escritos, los cuales implican actos que de ninguna manera son actos lingüísticos pero que participan completamente en la producción de documentos". Cfr. también (Fraenkel & Pontille, 2006), en relación con la firma electrónica.

sin que deba incorporar firma alguna[645].

Será ésta, por tanto, una cuestión que quedará en el ámbito de los requisitos de forma que, en su caso, pueda imponer el derecho nacional, como ha confirmado el TJUE en su Sentencia de 9 de noviembre de 2006, dictada en el asunto C-42/15, Home Credit Slovakia, en el que declara que "[e]l artículo 10, apartados 1 y 2, de la Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo, en relación con el artículo 3, letra m), de esta Directiva, debe interpretarse en el sentido de que: […] – no se opone a que el Estado miembro disponga en su normativa nacional, por un lado, que el contrato de crédito que esté comprendido en el ámbito de aplicación de la Directiva 2008/48 y establecido en papel deba ser firmado por las partes, y, por otro, que este requisito de firma sea aplicable respecto de todos los datos del contrato enumerados en el artículo 10, apartado 2, de la Directiva".

Esto es, precisamente, lo que sucede en nuestro Derecho, nada más y nada menos que en la contratación mediante condiciones generales de la contratación, después de la reforma de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación (LCGC) operada por Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, que procede a la derogación del artículo 5.4 de la LCGC[646], que exoneraba del uso de la firma convencional en los casos de contratación electrónica o telefónica, por considerarlo incompatible con el enfoque de armonización máxima de la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo, que la citada Ley traspone, con el efecto potencial de considerar no incorporadas al contrato las condiciones generales correspondientes, en los términos establecidos por el artículo 7 de la LCGC.

Por tanto, en ausencia de un requisito de forma, simplemente no resultará exigible el uso de firma electrónica[647] de tipo alguno, sin perjuicio que las partes puedan decidir

---

[645] Particularmente claro resulta (Madrid Parra, 2001, págs. 187-188), cuando explica que "[n]uestro Código Civil (CC) no exige la firma para la perfección de los contratos. Entre otros requisitos, exige el consentimiento, pero no la firma. Sin embargo, la práctica ha hecho que la firma sea el medio más frecuente y habitual de expresar el consentimiento. Se ha evolucionado desde las formas rituales y verbales de expresión de la voluntad a las escritas en un documento en papel", siendo lo jurídicamente relevante que "[s]e utiliza la firma como medio para manifestar la propia voluntad o el conocimiento que se tiene de algo. Hecha una declaración, contenida en un documento, se establece un nexo jurídico entre el contenido de la misma y una persona, sujeto de derechos y obligaciones, que actúa en representación propia o ajena". Nótese que esta concepción de la "voluntariedad" de la firma encuentra sus límites en las normas imperativas que exijan, en su caso, imponer la firma.

[646] Sobre el contenido y origen parlamentario de este artículo, puede verse (Feliú Rey, 1999, pág. 54 y ss.), que resulta muy crítico con su redacción, que contiene referencias específicamente aplicables a los consumidores, algo que considera improcedente en una normativa que también aplica a las relaciones entre profesionales.

[647] En este sentido, (De Miguel Asensio, 2015, pág. 1000) explica que "[e]n la medida en que en materia contractual un ordenamiento jurídico proclama como principio de base –sin perjuicio de la existencia de

emplearla, como posteriormente veremos[648], o sustituirla por otra fuente de prueba electrónica[649], como podría ser un registro electrónico de la actuación generado por un tercero interpuesto, a modo de "caja negra de avión".

Y por supuesto, será también posible obtener una declaración de voluntad de una persona sin que exista un soporte escrito electrónico duradero, como sucedería en una contratación verbal registrada electrónicamente –siempre que la misma, como acabamos de ver, no venga sustanciada mediante el uso de condiciones generales de la contratación–, pero en este caso no tendría sentido acudir a ninguna firma electrónica, igual que en el contrato verbal no se firma documento alguno en papel.

4.1.1.2 La aparición del concepto de sello electrónico de persona jurídica

Como novedad relevante en relación con la DFE y la LFE, el artículo 3.25) del Reglamento eIDAS define el sello electrónico como los "datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de los datos de estos últimos"[650].

Se trata de un mecanismo en cierto modo parecido a la firma electrónica, pero para su uso[651] por personas jurídicas, como se deduce del Considerado 59 del Reglamento eIDAS, el cual indica que "los sellos electrónicos deben servir como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento"; mientras que, de acuerdo con el Considerando 65, "además de autenticar el documento expedido por la persona jurídica, los sellos

---

importantes excepciones– la libertad de forma, una consecuencia admitida de manera generalizada, como quedó ya reseñado, es la posibilidad de celebrar los contratos mediante el intercambio de mensajes electrónicos, sin especiales requisitos en cuanto a su formalidad y, por lo tanto, sin necesidad de acudir al empleo de firmas electrónicas", y añade que "el significado práctico de la firma electrónica se ve afectado por la tendencia a considerar la contratación hecha por escrito cuando tiene lugar mediante cualquier transmisión efectuada por medios electrónicos que proporcione un registro duradero del acuerdo", por lo que "[c]uando estas normas resultan de aplicación, tienen como consecuencia que la exigencia legal de forma escrita pueda satisfacerse en el comercio electrónico a través del intercambio de mensajes de correo electrónico o de información en un sitio de Internet, sin necesidad de incorporar mecanismos especiales de firma electrónica". Aunque esto es formalmente correcto, alerta (De Urbano Castrillo, 2009, págs. 63-64) que "el documento privado generado informáticamente plantea problemas de autenticidad e integridad, especialmente peliagudos en un ámbito de tan evidente inseguridad", añadiendo que "si la ley no permite concluir siquiera que un documento con firma electrónica reconocida hace prueba plena, pues cabe su impugnación, un documento informático no firmado entra dentro de aquéllos que deben ganarse su reconocimiento con alegaciones contundentes y el concurso de otros medios probatorios".

[648] Cfr. el epígrafe 5.1 de este trabajo.

[649] Desde este punto de vista, quizá debamos plantearnos, siguiendo a (Dumortier, 2004, p. 281) que, dado que progresivamente las nuevas leyes dejan de exigir el requisito de la firma, es posible que en el futuro también la firma electrónica –en especial, la firma electrónica cualificada– simplemente desaparezca.

[650] A diferencia de lo que sucede con la definición de firma electrónica, que en último término resulta dependiente del derecho nacional, en este caso nos encontramos ante un concepto autónomo, que no se verá afectado en el nivel doméstico.

[651] De forma relativamente temprana, apostaba (Muñoz Soro, 2003, pág. 134) por la existencia de "firmas de máquinas con efectos jurídicos", más apropiadas para "el entorno en que surge esta tecnología, que es el de la automatización […] que […] precisamente, consiste en que la intervención humana sea substituida por la de las máquinas".

electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores".

Mientras que, en el caso de firma electrónica, el firmante es "una persona física que crea una firma electrónica" (artículo 3.9) del Reglamento eIDAS), en el caso del sello electrónico, el creador del sello es "una persona jurídica que crea un sello electrónico" (artículo 3.24) del Reglamento eIDAS), mientras que, en la DFE, por firmante se entendía "la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa" (artículo 2.3 de la DFE) –y de la misma forma sucedió con el artículo 6.2 de la LFE, que estableció que "[e]l firmante es la persona que utiliza un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa"–, lo que dejaba espacio para la interpretación de entender que el firmante podía ser, indistintamente, una persona física o jurídica[652].

La definición legal del sello electrónico se refiere, conforme al artículo 3.25) del Reglamento eIDAS, a los "datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos", por lo que su utilidad viene dada por estos dos elementos, que vienen referidos a los servicios de seguridad informática de autenticación del origen de los datos y de la integridad de los datos, presentados anteriormente.

Como se puede apreciar, una diferencia muy relevante entre ambos conceptos es que el de firma electrónica se construye por relación a la firma escrita, por lo que deberá poderse emplear una firma electrónica donde la legislación venga referida a una firma escrita[653] –por lo que la firma electrónica se considera equivalente de la firma escrita– pero en el caso del sello electrónico no se aplica este enfoque, sino que se define para qué sirve el mismo, en lugar de referenciarse contra el empleo del "sello físico", del que muchas personas jurídicas disponen, y cuyo uso se encuentra regulado en gran cantidad de casos[654]; por lo que quizá se hubiera podido emplear también la técnica del equivalente

---

[652] Para (Martínez Nadal, 2009, págs. 141-142), "[…] en principio, y en apariencia, una primera lectura de este precepto parece conducirnos a pensar que el legislador comunitario parece inclinarse por la tesis de la vinculación de personas jurídicas a través de la firma de personas físicas con poder de representación suficiente; en especial si entendemos la exigencia de posesión como posesión física, material e inmediata. No obstante, y, tras una lectura más pausada, obsérvese que, quizá de forma deliberada, no se cierra totalmente la polémica cuestión de la capacidad de la firma de la persona jurídica, pues se habla simplemente del firmante como persona, sin especificar si física o jurídica". La misma autora recuerda, además, que el RDLFE sí exigía que el firmante fuera una persona física, exigencia que no se incorporó a la LFE.

[653] O a la ausencia de la misma.

[654] Por poner algunos ejemplos, el artículo 44.2 del Real Decreto 1829/1999, de 3 de diciembre, por el que se aprueba el Reglamento por el que se regula la prestación de los servicios postales prevé que "la entrega de notificaciones a las personas jurídicas se realizará al representante de éstas, o bien, a un empleado de la misma, haciendo constar en la documentación del empleado del operador postal y, en su caso, en el aviso de recibo que acompañe a la notificación, su identidad, firma y fecha de la notificación, estampando, asimismo, el sello de la empresa"; por su parte, el Anexo de la Ley 32/2006, de 18 de octubre, reguladora de la subcontratación en el Sector de la Construcción, referido al libro de subcontratación de llevanza obligatoria exige el sello de la empresa; o el Anexo II del Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención, referido a la notificación sobre concurrencia de condiciones que no hacen necesario recurrir a la auditoría del sistema de prevención de la empresa, también exige el sello de la empresa; o el Real Decreto 919/2006, de 28 de julio, por el que se aprueba el Reglamento

funcional para la conceptualización jurídica de este mecanismo de seguridad informática.

En todo caso, se trata de una innovación importante en términos del derecho europeo, pero que resulta sólo parcialmente novedosa en relación al ordenamiento jurídico español, en que ya se habían regulado algunos casos aparentemente similares. En este sentido, el artículo 7 de la LFE reguló el certificado de firma electrónica de persona jurídica, que cumplía una función similar a los sellos electrónicos del Reglamento eIDAS[655], pero con la limitación de que "los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario"[656]. Por su parte, la LAE reguló, para el ámbito del procedimiento administrativo electrónico, el sello de Administración, órgano o entidad de derecho público, que actúa como sistema de firma electrónica en actuaciones automatizadas, sin intervención humana[657]; instrumento que también se mantiene como instrumento para el funcionamiento electrónico del sector público[658] en la LRJSP. De forma muy similar, la LUTICAJ ha regulado, para el ámbito del procedimiento judicial, el sello de la oficina judicial, que actúa como sistema de firma electrónica en actuaciones judiciales automatizadas, sin intervención humana[659]. Finalmente, la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público (BOE núm. 311, de 28/12/2013), autoriza el uso del sello electrónico avanzado basado en certificado reconocido, el cual define como "el conjunto de datos en forma electrónica, consignados o asociados con facturas electrónicas, que pueden ser utilizados por personas jurídicas y entidades sin personalidad jurídica para garantizar el origen y la integridad de su contenido"[660], figura que ya parece haberse inspirado en la definición contenida en la propuesta del Reglamento eIDAS, que ya se encontraba en tramitación parlamentaria.

La aprobación del Reglamento eIDAS permitía prever que estos casos podían quedar absorbidos dentro del concepto de sello electrónico, cuyo régimen jurídico general se unifica tanto para el sector público como para el privado, y en ese sentido, hay que entender –como han confirmado la Comisión Europea y el supervisor español– que el concepto de firma electrónica de persona jurídica de la LFE es incompatible con el Reglamento eIDAS y, por tanto, se ha debido dejar de expedir certificados de este tipo a

---

técnico de distribución y utilización de combustibles gaseosos y sus instrucciones técnicas complementarias ICG 01 a 11, que exige en los certificados e informes que regula el uso del sello de la empresa.

[655] Nótese que el Considerando 60 del Reglamento eIDAS establece que "los prestadores de servicios de confianza que expidan certificados cualificados de sello electrónico deben instaurar las medidas necesarias para poder determinar la identidad de la persona física que representa a la persona jurídica a la que se entregue el certificado cualificado de sello electrónico, cuando se requiera tal identificación a nivel nacional en el contexto de procedimientos judiciales o administrativos".

[656] En relación con el régimen jurídico de estos certificados, hoy desaparecidos, cfr. (Martínez Nadal, 2009, págs. 145-162).

[657] Cfr. los artículos 18, 39 y el anexo, epígrafe a).

[658] Cfr. los artículos 40 y 42.a).

[659] Cfr. los artículos 19, 20, 42 y el anexo.

[660] Cfr. el artículo 5.2.

partir de la entrada en aplicación de la norma europea[661].

Asimismo, los sellos definidos en las tres leyes mencionadas han debido necesariamente alinearse con el Reglamento eIDAS, sin perjuicio de incorporar las particularidades que se contemplan en tales normas, a los que posteriormente nos referiremos.

En definitiva, el concepto legal de firma electrónica se restringe absolutamente a las personas físicas, y el de sello electrónico, a las personas jurídicas, a cuyo efecto hay que recordar, de acuerdo con el Considerando 68 del Reglamento eIDAS, que "de conformidad con las disposiciones del Tratado en materia de establecimiento, el concepto de "personas jurídicas" permite a los operadores elegir libremente la forma jurídica que consideren adecuada para la realización de sus actividades. Por tanto, las "personas jurídicas" en el sentido del Tratado incluyen todas las entidades constituidas en virtud de la legislación de un Estado miembro, o que se rigen por la misma, independientemente de su forma jurídica", por lo que deben también entenderse incluidas en este concepto a las entidades sin personalidad jurídica, lo que supone una mejora sustancial sobre la LFE[662].

4.1.2 La firma y sello electrónicos avanzados

El artículo 3.11) del Reglamento eIDAS define la firma electrónica avanzada como "la firma electrónica que cumple los requisitos contemplados en el artículo 26"; a saber: "a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable".

Por su parte, el artículo 3.2 de la LFE había definido inicialmente la firma electrónica avanzada como "la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a los que se refiere y que ha sido creada por medios que el firmante

---

661 Http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Documents/nota-web-certifs-pers-juridica.pdf. No deja de llamar la atención que se acuda a una nota de prensa para dar cuenta de semejante interpretación, aunque en el caso de la Comisión Europea se ha acudido a un instrumento no menos llamativo, como son unas "Preguntas Más Frecuentes", disponibles en https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas

662 La LFE había previsto, en su disposición adicional tercera, que "podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 33 de la Ley General Tributaria a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministro de Hacienda", posibilidad que fue objeto de regulación por Orden EHA/3256/2004, de 30 de septiembre, por la que se establecen los términos en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 35.4 de la Ley General Tributaria; y que fue objeto de ampliación al resto de procedimientos administrativos, mediante la previsión contenida en el artículo 15.3 de la LAE ("los certificados electrónicos expedidos a Entidades sin personalidad jurídica, previstos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica podrán ser admitidos por las Administraciones Públicas en los términos que estas determinen"), así como a los procedimientos judiciales, de acuerdo con el artículo 15 de la LUTICAJ ("las personas jurídicas y entidades sin personalidad jurídica podrán utilizar sistemas de firma electrónica de persona jurídica o de entidades sin personalidad jurídica para todos aquellos procedimientos y actuaciones ante la Administración de Justicia en los términos establecidos en las leyes procesales").

puede mantener bajo su exclusivo control", hasta su modificación por Ley 25/2015, de 28 de julio, que la definió como "la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control", adelantándose a la entrada en aplicación de la definición del Reglamento eIDAS.

Como se puede ver de su definición, la firma electrónica avanzada es técnicamente idónea para cumplir el fin social típico de la firma escrita a los que antes nos hemos referido, incluyendo la identificación del firmante en condición de autor del documento, la voluntad de obligarse y la vinculación con el texto contenido en el documento[663], lo cual veremos que se basa en el uso de determinadas tecnologías.

De forma análoga, aunque no idéntica[664], a la firma electrónica avanzada, el artículo 3.26) del Reglamento eIDAS define el sello electrónico avanzado como "un sello electrónico que cumple los requisitos contemplados en el artículo 36", que son los siguientes: "a) estar vinculado al creador del sello de manera única; b) permitir la identificación del creador del sello; c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control, y d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable".

Como se puede ver de ambas definiciones, para la creación de la firma y sello electrónico avanzado se requiere del uso de unos datos de creación, que deberán ser objeto de diverso grado de control por parte de su titular, dado que de ello depende la vinculación de la firma o sello con su titular[665].

Los datos de creación de firma electrónica son, de acuerdo con el artículo 3.13) del Reglamento eIDAS, "los datos únicos que utiliza el firmante para crear una firma electrónica", y a los mismos se refería ya el artículo 24.1 de la LFE como "los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica", diferenciándose ambas definiciones en el enfoque más neutral que adopta el Reglamento.

El Reglamento eIDAS se refiere también a los datos de creación de sello electrónico como "los datos únicos que utiliza el creador del sello electrónico para crearlo", en su artículo 3.28).

En ambos casos, se trata del aspecto de mayor criticidad del sistema, ya que la posesión o el acceso a los datos de creación de firma permite suplantar al firmante o creador del

---

[663] En opinión de (Martínez Nadal, 2009, pág. 76), las exigencias de la firma electrónica avanzada se pretende garantizar la autenticación del autor y evitar el rechazo en origen de los mensajes electrónico, pudiendo determinar su autoría y que el autor no pueda negarla.

[664] Como curiosidad, en el artículo 36.c) de la versión en lengua española del Reglamento eIDAS se hacía mención al "control exclusivo", error que se corrigió el 1 de noviembre de 2016, más de dos años tras la aprobación del Reglamento.

[665] Para (Mason, 2017, p. 152), y en relación con la vinculación única con el firmante, "[n]inguna forma de firma electrónica puede resultar conforme con esta parte del requisito. Por ejemplo, un usuario pierde en control sobre su firma digitalizada una vez ha misma ha sido enviada. Una firma digital no es encuentra vinculada a la persona que la crea: el vínculo único se realiza con la clave privada, no con el usuario. Nadie es capaz de retener una clave privada en su memoria, porque es excesivamente complicado".

sello, respectivamente, motivo por el que los datos de creación de firma o sello han de poder ser protegidos contra la utilización indebida por terceros, algo que tradicionalmente se había interpretado en el sentido de la exclusiva posesión de la clave únicamente por el firmante, si bien el Reglamento eIDAS considera un enfoque más amplio para adaptarse a nuevas opciones tecnológicas, incluso autorizando la gestión, por terceros, de los datos de creación, en determinadas condiciones; enfoque que ya había sido incorporado a la LFE, mediante Ley 25/2015, de 28 de julio, antes mencionada.

En este sentido, también es preciso aclarar que la creación de la firma o sello electrónico avanzado se produce empleando un dispositivo. El mismo se define en el artículo 3.22) del Reglamento eIDAS, en sentido similar al artículo 24.2 de la LFE[666], como "un equipo o programa informático configurado que se utiliza para crear una firma electrónica", mientras que el artículo 3.31) del Reglamento eIDAS define el dispositivo de creación de sello electrónico como "un equipo o programa informático configurado que se utiliza para crear un sello electrónico".

Estas definiciones conectan la creación de la firma o sello electrónico con la aplicación (es decir, el uso) de los datos de creación de firma, de forma que el poseedor del dispositivo es realmente la persona que controla el proceso de creación de la firma o del sello, sea o no el suscriptor del certificado correspondiente.

Por este motivo, la firma o sello será imputable al firmante o creador del sello en la medida en que una persona no autorizada no pueda utilizar los datos de creación correspondientes, lo que justifica la necesidad de disponer del control del uso de los datos de activación de la firma o sello electrónico, al objeto de poder hacer esta atribución, algo que como hemos visto está previsto en la propia definición de firma o sello electrónico avanzado, aunque con la diferencia de que ese control deberá ser exclusivo en el caso de firma electrónica, y no en el caso del sello electrónico[667].

Las aplicaciones informáticas (*software*) de servicios criptográficos[668] se han convertido en los dispositivos más genéricos de creación de firma electrónica, y aunque progresivamente ofrecen un mayor grado de seguridad, difícilmente pueden ser calificados como dispositivos seguros o cualificados de creación de firma[669], a los que nos referiremos posteriormente, empleándose en el contexto de la firma o sello electrónicos avanzados a los que anteriormente nos hemos referido.

La especificación técnica CEN CWA 14170:2004 estableció un conjunto de medidas de

---

[666] Hay que notar que, de acuerdo con el artículo 4.2 del Reglamento eIDAS, "se permitirá la libre circulación en el mercado interior de los productos y servicios de confianza que se ajusten al presente Reglamento", lo que resulta de gran importancia para los fabricantes o importadores, así como para los prestadores de servicios de confianza que empleen dichos productos.

[667] Cfr. también el epígrafe 4.3.1 de este trabajo.

[668] Se trata de aplicaciones o software de amplio uso instalado en los sistemas operativos más habituales, de acuerdo con dos especificaciones técnicas de programación (CSP en entorno Microsoft y PKCS11 en todos los entornos).

[669] Aunque algunas aplicaciones así los consideran: en concreto, la Agencia Estatal de Administración Tributaria ha reconocido que, a los efectos de sus procedimientos administrativos, se considera que los proveedores de servicios criptográficos son dispositivos seguros, algo que nos parece absolutamente criticable, por generar una cierta confusión en el mercado.

seguridad funcional aplicables a las aplicaciones y programas de firma electrónica[670], para garantizar un nivel apropiado de seguridad; especificación técnica que ha sido recientemente actualizada en el TC 224 de CEN, grupo de trabajo 17, para su conversión en norma europea[671].

Asimismo, hay que considerar también la existencia de otras normas europeas, en especial relativas a los procedimientos de firma electrónica, entre las cuales resulta relevante la norma ETSI EN 319 102-1 V1.1.1 (2016-05), que detalla el proceso de creación de una firma o sello electrónico avanzado (y también cualificado).

Resulta también preciso referirse al artículo 3.40) del Reglamento eIDAS, que se refiere a los datos de validación de firma o sello electrónico, que define como "los datos utilizados para validar una firma electrónica o un sello electrónico" (por parte de los terceros destinatarios de comunicaciones y documentos firmados), en lugar de "verificación", que era el término empleado por el Anexo IV de la DFE o el artículo 25 de la LFE, cambio que no tiene efecto práctico ninguno, pero que en ambos casos apunta al empleo de tecnologías de doble clave, como la firma digital[672].

Esta segunda definición de firma y sello electrónico, incremental en requisitos sobre la más general de simple firma y sello electrónico, exige que la tecnología permita identificar y atribuir unos datos a la persona que utiliza los mecanismos para producir la firma o sello[673], y a diferencia de la firma manuscrita, la tecnología calificable como firma y sello electrónico avanzado debe garantizar la integridad del documento, de modo que las modificaciones posteriores del mismo sean detectables[674].

Como ya se ha avanzado, la definición se corresponde con las funciones tradicionalmente asignadas a la firma manuscrita, de modo que la firma electrónica avanzada resulta, con carácter general, un sistema más idóneo para que las personas físicas procedan a utilizar dicha tecnología en sustitución de la firma escrita.

De nuevo, se trata de una orientación que pretende resultar neutral desde una perspectiva técnica, permitiendo que diversas tecnologías reciban la calificación jurídica de firma y

---

[670] Que, en su caso, funcionan conjuntamente con dispositivos cualificados de creación de firma.

[671] Cfr. las normas EN 419 111-1 – Protection profiles for signature creation and verification application - Part 1: Introduction; EN 419 111-2 - Protection profiles for signature creation and verification application - Signature creation application - Part 2: Core PP; y EN 419 111-3 – Protection profiles for signature creation and verification application - Signature creation application - Part 3: Possible extensions

[672] Cfr. la sección A.1.1.3 de este trabajo.

[673] Como veremos más adelante, el Reglamento eIDAS prevé de forma expresa la posibilidad de que los datos de creación de firma sean gestionados por un tercero, posibilidad que en nuestra LFE también ha sido acogida tras la reforma operada por Ley 25/2015, de 28 de julio, con limitaciones importantes respecto a la legislación europea.

[674] En este sentido, (Elías Baturones, 2008, pág. 49) ha señalado, precisamente, las diferencias con la firma manuscrita, indicando que "la cuestión es que, en una firma tradicional, aparece el nombre y apellidos de su autor junto con la rúbrica, que sirve de impronta a la hora de vincular a la persona que firma el documento con su contenido, mientras que, en la firma electrónica, se acentúa más la identidad entre el autor con el contenido, resumiendo una parte esencial del mismo, cifrándolo posteriormente, con la fecha y hora de la emisión, por lo que la menor variación del algoritmo, así obtenido, supondría una prueba de manipulación externa que derivaría a la existencia de un tercero no querido, y posiblemente malintencionado, entre las partes en cuestión".

sello electrónico avanzado, a pesar de que claramente el legislador comunitario regula con una determinada tecnología en mente[675], que no es otra que la firma digital basada en criptografía de clave asimétrica basada en certificado electrónico; esto es, la denominada PKI o infraestructura de clave pública[676]. En este sentido, la neutralidad se encuentra más orientada a las diversas tecnologías de firma digital[677] que a otras tecnologías diferentes[678].

En efecto, resulta más que evidente la equivalencia entre la clave privada (concepto técnico) y el dato de creación de firma o sello (concepto jurídico), así como entre la clave pública (concepto técnico) y el dato de validación de firma o sello (concepto jurídico), apoyando la equivalencia entre la firma digital (concepto técnico) y la firma electrónica avanzada o el sello electrónico avanzado (concepto jurídico), si bien ello exige del empleo de determinada sintaxis técnica[679].

En todo caso, y al menos desde una perspectiva puramente teórica, la firma y sello electrónico avanzado puede, sin embargo, corresponderse con una firma digital, o no hacerlo, y en el primer caso, basarse en certificado, o no hacerlo, sin que ello afecte a su valor jurídico, pero siempre que se emplee una tecnología que permita el cumplimiento de todos los requisitos de la firma o sello electrónico avanzado, algo que no siempre es fácil.

Sucede además que, en el ámbito de la Administración electrónica, como veremos posteriormente con mayor detalle[680], se ha venido admitiendo con carácter general la firma electrónica de los ciudadanos siempre que la misma se base en certificado cualificado admitido por la Administración; es decir, se ha configurado como un derecho del ciudadano en sus relaciones con la Administración[681], y sin perjuicio de que se hayan habilitado otros mecanismos de firma y sello electrónico[682]; por lo que ciertamente se ha

---

[675] Cfr. COM (2006) 120 final, página 4.

[676] En relación con el RDLFE y la DFE, aunque plenamente aplicable al Reglamento eIDAS, (Madrid Parra, 2001, págs. 202-203) explica que "a la hora de elaborar normas jurídicas resulta difícil abstraerse sobre la realidad existente y proyectar los supuestos de hecho a futuras realidades venideras. Las nuevas realidades conocidas y no reguladas son las que demandan seguridad jurídica. Por eso las normas que se elaboran ponen de manifiesto su dependencia y servidumbre en relación con los supuestos de hecho que se tienen presentes al elaborar las normas", admitiendo que esto es lo que sucede con las disposiciones que regulan la firma electrónica, dado que "[c]omo planteamiento de principio se proclama una pretendida neutralidad en relación con las posibles tecnologías aplicables. Pero de hecho la estructura y el contenido de las normas reguladoras de la denominada firma electrónica siguen el esquema de la conocida como infraestructura de clave pública".

[677] Como hemos visto en el Anexo A.1.1.3 de este trabajo, existen diversos algoritmos diferentes de firma digital.

[678] En contra de esta opinión, cfr. (Sorge, 2014, p. 135), que opina que se podrían emplear firmas basadas en identidad, por ejemplo.

[679] Al respecto, se puede consultar el Anexo B de este trabajo.

[680] Cfr. el epígrafe 5.2 de este trabajo.

[681] Hasta la aprobación de la LPAC que, como veremos en el epígrafe 5.2.2.5 de este trabajo, modifica sustancialmente este régimen legal.

[682] La AEAT utiliza, además de los sistemas de firma electrónica avanzada basada en certificado reconocido, y de sistemas de firma electrónica reconocida, sistemas de firma electrónica ordinaria, incluso sin empleo de mecanismos criptográficos para la práctica totalidad de sus procedimientos tributarios.

producido una fuerte promoción de una de las tecnologías de firma electrónica avanzada.

4.1.3 La firma y sello electrónicos cualificados

Contiene, finalmente, el artículo 3.12) del Reglamento eIDAS una tercera definición de firma electrónica, a la que denomina como cualificada[683], y que conceptúa como "una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica".

La LFE también contenía una suerte de tercera definición de firma electrónica, en su artículo 3.3, en virtud de la que se consideraba firma electrónica reconocida a "la firma electrónica avanzada basada en un certificado reconocido y que ha sido producida mediante un dispositivo seguro de creación de firma electrónica", categoría cuyo "reconocimiento" se refería a una idoneidad que la cualifica especialmente como equivalente a la firma manuscrita, y sin que ello deba implicar la discriminación de los restante tipos de firma electrónica. Esta definición no se contenía en la DFE, aunque se podía considerar implícita en la misma[684], ni tampoco se encontraba en el RDLFE[685].

Se trata, de nuevo, de una definición incremental en cuanto a los requisitos, que incorpora dos elementos adicionales a la firma electrónica avanzada –el dispositivo cualificado de creación de firmas electrónicas y el certificado cualificado de firma electrónica, a los que nos referiremos posteriormente en detalle–, en orden a garantizar que la tecnología de firma electrónica reconocida o cualificada produzca su efecto típico; es decir, que sea idónea y adecuada para que una persona física se identifique y firme.

Nótese que tanto el dispositivo de firma como el certificado[686] de firma deben ser cualificados, como medida de control previo que garantiza su idoneidad y, por tanto, que la firma electrónica cualificada efectivamente lo es.

De esta forma, el concepto de firma electrónica cualificada va a servir para denotar un subconjunto de tecnologías de firma electrónica como institución jurídica, a la que se asociarán efectos jurídicos específicos, "proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión", en palabras del Considerando (2) del Reglamento eIDAS anteriormente

---

683 El Reglamento eIDAS traduce el término inglés "qualified" como "cualificada", en lugar del término "reconocida" empleado en nuestra LFE, que ha generado gran confusión.

684 Cfr. COM (2006) 120 final, página 4.

685 En opinión de (Martínez Nadal, 2009, pág. 86), "la firma electrónica reconocida más que un nuevo concepto de firma basado en el establecimiento de nuevas exigencias inherentes a la propia firma es un término en el que, a efectos simplificadores, se agregan los distintos requisitos extrínsecos a la propia firma electrónica reconocida ya existente para que éste tenga validez y eficacia", entendiendo que "las diferencias con la firma electrónica avanzada son más formales que reales", hasta el punto de considerar que "la firma electrónica reconocida, más que un nuevo concepto técnico o jurídico de firma electrónica, con requisitos propios, podría ser un concepto comercial, un producto de firma electrónica". Aún estado de acuerdo con la autora en que una firma electrónica cualificada es una firma electrónica avanzada que cumple ciertas condiciones, entiendo que existe como institución jurídica diferenciada en requisitos y en efectos jurídicos de la firma electrónica avanzada, de la que se puede ver como una subclase.

686 Cfr. el epígrafe 2.1.1 de este trabajo.

introducido[687].

Debe quedar claro, de todos modos, que no se debe considerar que una firma electrónica cualificada sea mejor ni más segura que otros tipos de firma, al menos técnicamente hablando[688]. En realidad, lo que sucede es que se ha realizado una cierta apuesta, en cierto modo infringiendo el principio de neutralidad tecnológica, en favor de unas tecnologías concretas[689], lo cual sólo es aceptable porque la Ley sigue permitiendo, en régimen de no discriminación, otras tecnologías.

Sólo de esta forma se explica que el sector privado haga un uso comparativamente mínimo de los sistemas de firma electrónica cualificada (como, por ejemplo, el DNI electrónico) en favor de otros mecanismos, como las contraseñas u, más recientemente, las firmas manuscritas capturadas electrónicamente[690], sin que se incrementen los niveles de fraude efectivo.

La firma electrónica cualificada y, en concreto, la que se encuentra sustentada en el DNI electrónico, constituye una línea de identificación y firma electrónica ofrecida por el Estado perfectamente razonable y defendible[691], y de la que las compañías privadas pueden hacer uso, pero sin renunciar a otras tecnologías idóneas en escenarios diversos, porque la realidad es que la base tecnológica que requiere el DNI electrónico (igual que otros sistemas de firma electrónica reconocida o cualificada) no se encuentra disponible en todos los escenarios, principalmente por cuestiones de interoperabilidad técnica[692].

Igualmente, la firma electrónica cualificada ha planteado problemas de usabilidad y de rechazo social en determinados procesos[693], por lo que el mercado sigue innovando y produciendo tecnologías seguras que, aun no gozando de una ventaja jurídica especial, resultan tanto o más seguras que la firma electrónica cualificada.

De esta conceptualización jurídica cabe criticar que la cualificación deba venir referida necesariamente estos dos elementos, porque supone una apuesta tecnológica que infringe el principio de neutralidad tecnológica; al contrario, la cualificación debería ser abstracta, porque de otro modo se discrimina la innovación; y ello sucede en la mayoría de servicios de confianza.

---

[687] Este Considerando (2) se refiere a todos los servicios o productos de confianza cualificados.

[688] En efecto, existen sistemas más seguros, como los que emplean múltiples factores de autenticación biométrica, que no utilizan certificados de clave pública.

[689] Aunque, quizá irónicamente, el Considerando (27) del Reglamento eIDAS afirma que "el presente Reglamento debe ser neutral en lo que se refiere a la tecnología", así como que "los efectos jurídicos que otorga deben poder lograrse por cualquier medio técnico, siempre que se cumplan los requisitos que en él se estipulan". Sólo desde una óptica de formalismo puro se puede considerar neutral un concepto de firma electrónica cualificada que exige la certificación de una clave pública, incluso aunque se pueda acudir a tecnologías "diferentes" para dicha actuación de certificación.

[690] Frecuentemente empleando tecnologías "biométricas", como el registro de la presión y la dinámica de la firma.

[691] Cfr. el epígrafe 2.2 de este trabajo. En cualquier caso, se trata de un sistema que no ha tenido éxito en su adopción.

[692] No sólo es el sector privado el que se encuentra con dificultades graves para el empleo de instrumentos como en DNI electrónico, sino también la Administración, algo que se trata de corregir precisamente con el Reglamento eIDAS y las iniciativas de interoperabilidad a las que ya nos hemos referido.

[693] Véase la crítica, por ejemplo, de (Roβnagel, 2006).

Por su parte, y de nuevo en una analogía clara con la firma electrónica cualificada, el artículo 3.27 del Reglamento eIDAS define el sello electrónico cualificado como "un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico"; de nuevo resultando aplicables las consideraciones realizadas en relación con la firma electrónica cualificada, pero para su uso por personas jurídicas.

Como hemos avanzado, uno de los elementos requeridos para obtener una firma o sello electrónicos cualificados –que como ya hemos visto es directamente equivalente a la firma escrita de la persona física, o directamente atribuible a la persona jurídica que lo genera, respectivamente– es el dispositivo cualificado de creación de dicha firma o sello, que procede analizar con detalle.

Dicho dispositivo se define en el artículo 3.23) del Reglamento eIDAS, en relación con la firma electrónica, como "un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II", mientras que el artículo 3.32) del mismo Reglamento se refiere, en relación con el sello electrónico, a "un dispositivo de creación de sellos electrónicos que cumple *mutatis mutandis* los requisitos enumerados en el anexo II". De forma manifiestamente reiterativa, dispone el artículo 29.1 del Reglamento eIDAS, "[l]os dispositivos cualificados de creación de firmas electrónicas cumplirán los requisitos establecidos en el anexo II", previsión aplicable *mutatis mutandis* a los dispositivos cualificados de creación de sello electrónico en virtud de lo establecido en el artículo 39.1 del mismo Reglamento eIDAS.

En este sentido, por lo que respecta los dispositivos cualificados de firma electrónica, el Considerando (56) del Reglamento eIDAS indica que "en el presente Reglamento se establecen requisitos aplicables a los dispositivos cualificados de creación de firmas electrónicas, a fin de garantizar la funcionalidad de las firmas electrónicas avanzadas", dando buena cuenta de la finalidad y orientación de dichos requisitos.

El Anexo II del Reglamento eIDAS, aplicable por tanto a dispositivos de creación de firma cualificados como a dispositivos de creación de sello cualificados, es el que realmente establece los requisitos que deben cumplir dichos productos, que en gran medida se refieren a los datos de creación de firma o sello, en diversas previsiones relevantes[694].

En primer lugar, el apartado 1.a) del Anexo II del Reglamento eIDAS exige que "esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica [o sello electrónico] utilizados para la creación de firmas electrónicas [o sellos electrónicos]", mientras que el artículo 24.3.a) de la LFE determinaba que los dispositivos seguros de creación de firma electrónica han de garantizar "que asegura razonablemente su [de los datos de creación de firma] secreto".

Se trata de una previsión completamente lógica, ya que, si estos datos de creación de firma o sello son conocidos por terceros, entonces dichos terceros pueden emplearlos para producir firmas en lugar de los legítimos firmantes.

En segundo lugar, el Anexo II del Reglamento eIDAS determina en su apartado 1.b) que

[694] Hay que notar que estos requisitos se exigen únicamente en relación con los datos de creación de firma y sello electrónicos cualificados, sin perjuicio de la conveniencia de aplicarlos también a la generación de claves de firma y sello electrónicos avanzados, al objeto de reforzar su eficacia, si bien claramente con un nivel inferior de exigencia.

los dispositivos cualificados han de garantizar que "los datos de creación de la firma electrónica [o sello electrónico] utilizados para la creación de una firma electrónica [o sello electrónico] solo puedan aparecer una vez en la práctica"; mientras que el artículo 24.3.a) de la LFE determinaba que los dispositivos seguros de creación de firma electrónica han de garantizar "que los datos utilizados para la generación de firma pueden producirse sólo una vez".

Nótese la diferente formulación de ambas normas, que en el caso del Reglamento eIDAS es bastante más realista que en la LFE, reconociendo la imposibilidad de ofrecer esta garantía de forma absoluta; en efecto, la garantía de unicidad del dato de creación se puede obtener de forma lo más aleatoria posible a partir de espacios numéricos muy grandes, pero incluso en este caso es difícil asegurar que dicho dato sea único, en especial cuando diversos prestadores generan datos de creación empleando mecanismos diversos.

En tercer lugar, el Anexo II del Reglamento eIDAS, aplicable tanto a la firma como al sello electrónico, determina en su apartado 1.c) que los dispositivos cualificados han de garantizar que "exista la seguridad razonable de que los datos de creación de firma electrónica [o sello electrónico] utilizados para la creación de una firma electrónica [o sello electrónico] no pueden ser hallados por deducción"; mientras que el artículo 24.3.b) de la LFE determinaba que los dispositivos seguros de creación de firma electrónica han de garantizar "que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma".

Como se puede ver, la legislación no exige una seguridad absoluta o total, que difícilmente se podría garantizar, sin perjuicio de que el término "razonable" deba interpretarse a la luz de los potentes efectos jurídicos asociados a la firma o sello electrónicos cualificados, en especial a su efecto de equivalencia plena con la firma escrita o a su presunción de autenticidad, cuando se establezca.

Además, por su importancia, y como hemos avanzado, el dato de creación de firma y sello ha de ser convenientemente protegido por el firmante o creador del sello, habitualmente mediante el propio dispositivo de firma o sello electrónico, que por ello debe tener la consideración de cualificado, de acuerdo con el Reglamento eIDAS, o seguro, como lo denominaba la LFE.

En cuarto lugar, se contiene una referencia explícita a la protección de los datos de creación en el Anexo II del Reglamento eIDAS, aplicable tanto a dispositivos de creación de firma cualificados, como a dispositivos de creación de sello cualificados, cuando su apartado 1.d) dispone que los dispositivos deben garantizar que "los datos de creación de la firma electrónica utilizados para la creación de una firma electrónica puedan ser protegidos por el firmante [o creador del sello] legítimo de forma fiable frente a su utilización por otros"; así como en el artículo 24.3.c) de la LFE, que indicaba "que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros"; formulaciones muy similares donde sólo cabe destacar la adición, en el Reglamento eIDAS, del adjetivo "legítimo" como calificador del firmante o creador del sello.

A la protección de la clave hace referencia la propia definición de la firma/sello electrónico avanzado, cuando indica que ésta ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo (artículos 26.c) y 36.c) del Reglamento eIDAS). Nótese la diferente dicción del artículo 3.2 de la LFE, que

se refería al uso de medios que el firmante puede mantener bajo su exclusivo control, una redacción mucho más objetiva que se había interpretado en el sentido de impedir toda forma de cesión de dichos datos de creación de firma a terceros.

La formulación del Reglamento eIDAS es, como se puede comprobar, bastante más flexible que la contenida en la LFE, principalmente porque la referencia a la utilización de los medios de creación de firma –que no del sello– bajo control exclusivo se debe hacer con un alto nivel de confianza y, por tanto, no se exige un nivel absoluto o total de control, como se podía interpretar del texto de la LFE. También resulta más acertado el uso del verbo "utilizar" que "mantener", referido a dichos medios, puesto que denota mejor la relación entre los medios de creación de firma/sello y la propia firma/sello, que es precisamente que los medios son el instrumento para la creación de la firma/sello, empleando los datos de creación.

Además, debe también hacerse notar que el Reglamento eIDAS no establece ninguna obligación al firmante o creador de sellos a hacer un uso exclusivamente personal de los datos de creación de los mismos, como hubiera sido el caso si el legislador hubiera empleado el verbo "deber", lo cual permite defender la tesis de la posible cesión del uso de los datos (y medios) de creación de firma y sello a cualquier tercero[695].

En este sentido, hay que mencionar los datos de activación de la creación de la firma y sello electrónico, que son los aquéllos que se utilizan para iniciar el proceso de creación. Aunque los mismos no aparecen definidos en la LFE, ni tampoco en el Reglamento eIDAS, su existencia y necesidad conecta con la protección de los datos de creación de firma y sello electrónicos, ya que con los datos de activación –que son conocidos únicamente por el firmante o el creador de sellos electrónicos, o por las personas en quien "delegue" la creación de la firma o del sello[696]– se puede autorizar el uso de los datos de creación de firma o sello y "activar" el procedimiento de generación de la firma o del sello.

Generalmente, estos datos de activación representan verdaderamente el mecanismo de control –en el caso de la firma, exclusivo– del uso de los datos de creación de firma o sello, con independencia del dispositivo en el que los mismos se encuentren[697].

Precisamente este dato de activación de la creación de la firma o sello electrónico es el mecanismo de protección más habitual de los datos de creación de firma electrónica al que se hace referencia en el artículo 24.3.c) de la LFE y Anexo II, apartado 1.d) del Reglamento eIDAS; generalmente es un dato alfanumérico, que puede tener una longitud variable, y que debería tener como mínimo ocho caracteres, aunque muchas veces coincide con un Número de Identificación Personal de cuatro dígitos.

---

[695] Nótese que tampoco la LFE estableció dicha restricción. Sobre este punto profundizamos en el epígrafe 4.3.1.1 de este trabajo.

[696] Obviamente, dicha delegación sólo producirá efectos internos, dado que la firma o sello se imputará al firmante o creador del sello aparente, en especial en aquellos sistemas que empleen certificados electrónicos reconocidos o cualificados, en los que conste la identidad de la persona correspondiente.

[697] En efecto, tanto si la clave privada (el dato de creación de firma o sello electrónico avanzado de uso más habitual) se encuentra en un repositorio de software, como el registro de Windows o un fichero PKCS#12, en una tarjeta con microprocesador o en un hardware de acceso remoto, el control exclusivo sobre dicha clave suele implementarse mediante mecanismos de autenticación que emplean datos de activación.

Otra posibilidad, menos frecuente, es que se empleen sistemas de autenticación de un solo uso (OTPs) o incluso biometría (por ejemplo, la comprobación de la huella digital) para la activación de la firma electrónica, posibilidades prometedoras en el contexto de las firmas a distancia[698].

Debido a este especial efecto de equivalencia, las especificaciones técnicas europeas desarrolladas para concretar los requisitos de los dispositivos seguros (o, ahora, cualificados) de creación de firma han adoptado una interpretación estricta del concepto de seguridad, que habitualmente conecta con el uso de un elemento de maquinaria o hardware, como por ejemplo un microchip criptográfico[699], para poder considerar el sistema como dispositivo cualificado de creación de firma electrónica.

En concreto, la especificación técnica CEN CWA 14169:2004[700] ofrecía un perfil de protección, escrito de acuerdo con la norma ISO 15408, que determina criterios comunes para la evaluación de la seguridad de las tecnologías de la información, para dispositivos seguros o cualificados de creación de firma electrónica; es decir, contenía el conjunto de medidas de seguridad que deben cumplir estos dispositivos de firma electrónica reconocida, de forma que permitía la comprobación de que uno de estos dispositivos era realmente seguro, en una interpretación de la DFE, consensuada por la industria.

La especificación técnica CEN CWA 14169:2004 ha sido periódicamente actualizada en el TC 224 de CEN, grupo de trabajo 17, para su conversión en norma europea. El resultado de dicha actualización es la norma europea CEN EN 419 211, partes 1 a 6[701], referida a los dispositivos cualificados de creación de firma y sello, conforme al Reglamento eIDAS, y que permite la certificación de los mismos, a la que posteriormente nos referiremos. Asimismo, y como complemento de las anteriores normas, se aprobó la norma EN 14890:2008, partes 1 y 2, que ha sido recientemente actualizada en el TC 224 de CEN, grupo de trabajo 16, para su conversión en norma europea. El resultado de dicha actualización[702] es la norma europea CEN EN 419 212, partes 1 a 2[703].

---

[698] Cfr. la especificación técnica CEN/TS 419 241:2014.

[699] Frecuentemente este chip se ha venido distribuyendo en forma de tarjeta ISO 7816, aunque también se han realizado implementaciones en forma de SD o microSD, para su uso en terminales de telefonía inteligente (*Smartphone*).

[700] Publicada en España por AENOR como UNE-CEN/CWA 14169:2005.

[701] En concreto, las normas son CEN EN 419 211-1:2014 – Protection profiles for secure signature creation device - Part 1: Overview; CEN EN 419 211-2:2013 – Protection profiles for secure signature creation device - Part 2: Device with key generation; CEN EN 419 211-3:2013 – Protection profiles for secure signature creation device - Part 3: Device with key import; CEN EN 419 211-4:2013 – Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application; CEN EN 419 211-5:2013 – Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application; y CEN EN 419 211-6:2014 – Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application.

[702] Se han previsto otras partes de esta norma, dedicadas a la autenticación, la privacidad, así como una parte introductoria.

[703] En concreto, las normas son CEN EN 419 212-1:2014 – Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services: y CEN EN 419 212-2:2014 – Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services.

En general, sólo los microchips criptográficos han implementado los controles previstos en estas normas europeas, por lo que, al objeto de mantener la neutralidad tecnológica y atender a las nuevas demandas del mercado, se ha desarrollado una nueva norma técnica europea, identificada como CEN EN 419 241, partes 1 y 2[704], que se orientan, de forma específica, al establecimiento de los requisitos de seguridad de los dispositivos cualificados que soportan la firma en servidor, con claves generadas y/o gestionadas por un prestador de servicios de confianza, tanto para la generación de firma o sello electrónico avanzado como para la firma o sello electrónico cualificado, así como del sistema fiable que los gestiona.

En concreto, la especificación técnica define una aplicación de creación de firma o sello en servidor que emplea un módulo físico de seguridad criptográfica conectado a una red (normalmente conocido como *networked* HSM) que permite a uno o más firmantes o creadores de sellos crear firmas o sellos de forma remota empleando claves centralizadas utilizadas bajo el control del firmante o creador de sellos, en los términos a los que, como novedad, se refiere el Reglamento eIDAS, que analizamos posteriormente[705].

En otro orden de cosas, y hasta la aprobación del Reglamento eIDAS, en relación con la acreditación del cumplimiento de los requisitos aplicables a los dispositivos seguros de creación de firma electrónica, la LFE había previsto que los fabricantes o importadores pudieran utilizar el mecanismo de la certificación de productos de firma electrónica previsto en su artículo 27; certificación que debía ser realizada por parte de un organismo designado por el Estado español[706], siempre que el mismo cumpliera lo establecido en la Decisión de la Comisión 2000/709/CE, de 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica[707].

Hay que iniciar este análisis recordando que en el marco legal anterior al Reglamento eIDAS la certificación de producto de firma electrónica era un mecanismo considerado puramente opcional, dado que ni la DFE ni la LFE habían impuesto la obligación de

---

[704] En concreto, las normas son CEN EN 419241-1:2018 – Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements y CEN EN 419241-2:2018 – Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.

[705] Cfr. el epígrafe 4.3.1 de este trabajo.

[706] En España, se trata de una unidad del Centro Criptológico Nacional – accesible en la página web https://www.oc.ccn.cni.es –, que se encuentra al frente del esquema nacional de evaluación y certificación de la seguridad de productos, y opera de acuerdo con lo establecido en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, y la Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Asimismo, se encuentra acreditado por ENAC para la certificación de productos, conforme a UNE-EN ISO/IEC 17065.

[707] El artículo 30.4 del Reglamento eIDAS también prevé que "[l]a Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 47, en lo que respecta al establecimiento de criterios específicos que deben satisfacer los organismos designados a que se refiere el apartado 1 del presente artículo", potestad de la que no ha hecho aún uso, seguramente por la existencia de la ya citada Decisión 2000/709/CE.

proceder a la certificación[708], ni habían establecido infracción alguna que sancionase el empleo o la comercialización de dispositivos seguros de creación de firma electrónica sin certificación, por lo que la calificación legal de un sistema como "firma electrónica reconocida" no podía depender en ningún caso[709] de la certificación del producto, que únicamente aliviaba la carga de la prueba cuando fuera preciso.

Al contrario, para que la certificación fuera obligatoria, se debería haber previsto en la Ley o, cuanto menos, dictar el correspondiente reglamento de seguridad, de acuerdo con lo que dispone el artículo 12 de la vigente Ley 21/1992, de 16 de julio, de industria[710].

En este sentido, la relevancia de esta certificación era básicamente comercial[711], en el sentido de que el fabricante o importador que hubiera obtenido la correspondiente certificación aparecía en el mercado con una apariencia de mayor calidad, pudiendo servir para dar una orientación y una mayor seguridad a los usuarios a la hora de elegir su producto de firma electrónica.

Opinión a la que hay que añadir el indudable valor que aportaba esta certificación en las relaciones con el supervisor, que es competente para el control del cumplimiento de las obligaciones del prestador[712], incluyendo, por supuesto, que los dispositivos que éste suministre como seguros lo fueran en realidad; así como en caso de controversia judicial, donde –como hemos visto anteriormente– la carga de la prueba referida a que una firma era reconocida incumbía al que la aportaba, que por tanto debía demostrar que el dispositivo cumplía con los requisitos legales.

Dicho artículo 27 de la LFE disponía, en su apartado 1, que "la certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma", mientras que, de acuerdo con su apartado 3, "en los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el Diario Oficial de la Unión Europea y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología[713] que se publicarán en la dirección de Internet de este Ministerio".

---

[708] El artículo 3.4 de la DFE decía que "[l]a conformidad de los dispositivos seguros de creación de firma con los requisitos fijados en el anexo III será determinada por los organismos públicos o privados pertinentes, designados por los Estados miembros". El uso del verbo "determinar", en lugar de "certificar", creó dudas acerca del alcance de dicha obligación, y más aún, acerca de la posibilidad de imponer una certificación.

[709] En este sentido, hay que notar que la propia "definición" de la firma electrónica reconocida se refiera a un dispositivo seguro de creación de firma electrónica, y no a un dispositivo seguro de creación de firma electrónica certificado, a diferencia de lo que sucedía en el Real decreto-Ley 14/1999, que sujetaba la presunción de eficacia de la firma electrónica avanzada a la certificación del dispositivo (cfr. artículos 3 y 21).

[710] Un dispositivo de creación de firma es, a los efectos de la Ley de industria, un producto industrial, debido a la amplia definición que del mismo realiza su artículo 8.1: "Producto industrial: Cualquier manufactura o producto transformado o semitransformado de carácter mueble aun cuando esté incorporado a otro bien mueble o a uno inmueble, y toda la parte que lo constituya, como materias primas, sustancias, componentes y productos semiacabados".

[711] (Martínez Nadal, 2009, pág. 494), por ejemplo.

[712] Cfr. artículo 29.1 de la LFE.

[713] Hoy, esta referencia debe entenderse realizada al Ministerio de Economía y Empresa.

Por su parte, el artículo 28.1 de la LFE también determinaba que "se presumirá que los productos de firma electrónica aludidos en el párrafo d) del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el Diario Oficial de la Unión Europea", en cumplimento de lo establecido en el artículo 3.5) de la DFE.

En la Decisión de la Comisión 2003/511/CE, de 14 de julio de 2003, relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, dictada al amparo de lo establecido en el artículo 3.5 de la DFE, se referenció exclusivamente la especificación técnica CEN CWA 14169, a la que ya nos hemos referido anteriormente, por lo que la certificación de los dispositivos seguros podía realizarse conforme a dicha norma.

Ello no significaba que en sede nacional no se pudieran aprobar otras especificaciones para la certificación de los dispositivos seguros de creación de firma. Aunque la LFE lo configurase con carácter excepcional, en Estados como Austria se fomentó dicha técnica con carácter general, en igualdad de condiciones que la certificación conforme a la especificación referenciada por la Comisión Europea.

Nótese que el artículo 28.2 de la LFE establecía que "se reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo", provisión[714] que perseguía facilitar la libre circulación de estos productos, por lo que se debían considerar como seguros los dispositivos certificados conforme a dichas normas nacional.

No fue así en todos los casos[715], seguramente debido a la desconfianza que en muchos casos tenían los Estados entre sí; es más, dado que la especificación técnica CEN CWA 14169 imponía requisitos de seguridad funcional que superaban el nivel máximo[716] amparado por el Acuerdo de Reconocimiento Mutuo de Certificados de Criterios Comunes de Seguridad de las Tecnologías de la Información (CCRA)[717], algunos Estados miembros consideraban que, aunque el producto fuera, en principio, seguro conforme a la DFE, se podía exigir una certificación adicional referida a las medidas de seguridad no cubiertas por el CCRA. Esta interpretación podía obligar a realizar una certificación complementaria en cada Estado donde se desease comercializar el producto, situación que defraudaba el objetivo de la legislación europea, al impedir la libre circulación de estos productos.

---

[714] Dictada para dar cumplimiento al mandato contenido en el artículo 3.4 de la DFE, en cuya virtud "[l]a conformidad con los requisitos del anexo III establecida por dichos organismos será reconocida por todos los Estados miembros".

[715] Se puede ver un análisis muy detallado de las diferentes problemáticas en el reconocimiento transfronterizo de los dispositivos de creación de firma en (Delos, Lacroix, & Graux, 2010).

[716] En la versión actual del CCRA, este nivel es EAL4 y ALC_FLR para perfiles de protección colaborativos desarrollados y mantenidos, de acuerdo con lo establecido en el anexo K del CCRA, por un Comité Técnico Internacional admitido por el Comité de Dirección del CCRA.

[717]

http://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf.

Para lograr que los certificados de seguridad expedidos a los correspondientes productos fueran reconocidos en Estados miembro diferentes al de su expedición sin necesidad a proceder a certificaciones adicionales en los mismos, la especificación CEN CWA 14169, y sus versiones posteriores, fueron objeto de inclusión en el acuerdo de reconocimiento mutuo del SOG-IS[718].

A estos efectos, en la página web del Portal de Criterios Comunes[719] se pueden ver los dispositivos certificados como seguros por cualquier organismo de certificación de Criterios Comunes establecido en el Espacio Económico Europeo[720], lo cual facilita la verificación por el firmante del cumplimiento de la legislación de firma electrónica por parte del prestador que suministre dichos dispositivos[721].

En resumen, es claro que el mecanismo que mayor seguridad jurídica aportaba, en el marco de la LFE, en cuanto a la garantía de cumplimiento de un dispositivo seguro de creación de firma electrónica era la certificación prevista en el artículo 27 de dicha Ley, que necesariamente debía ser realizada por un organismo designado, en el marco del acuerdo de reconocimiento mutuo del SOG-IS y empleando exclusivamente la norma prevista al respecto (CEN CWA 14169, y sus versiones posteriores, CEN EN 419 211, partes 1 a 6).

En este caso, se aplicaba la presunción de conformidad establecida en el artículo 28 de la LFE y, por tanto, se invertía la carga de la prueba, debiendo el supervisor o la otra parte en juicio demostrar que el dispositivo no cumplía los requisitos establecidos en el artículo 24.3 de la LFE, y además se eliminaba toda duda acerca de la posibilidad de comercializar el producto en toda la Unión.

Cabe, ahora, preguntarse si el prestador podía acudir, en el marco de la LFE, a otras fórmulas para demostrar que un dispositivo era seguro y, más en particular, si era posible realizar dicha demostración conforme a una norma o especificación técnica diferente a CEN CWA 14169 o sus versiones posteriores, o a las normas correspondientes adoptadas en un Estado miembro concreto. En concreto, esta situación se podía dar en el caso de empleo de tarjetas con microprocesador certificadas contra otras normas o especificaciones técnicas, como por ejemplo un perfil de protección diferente al contenido en CEN CWA 14169 o sus versiones posteriores, o a las normas correspondientes adoptadas en un Estado miembro concreto, o también caso de empleo de un producto (software y HSM), conforme a la especificación técnica CEN/TS 419 241:2014, que como hemos visto anteriormente, define los requisitos aplicables al uso de un sistema fiable para la gestión centralizada de los datos de creación de firma o sello electrónico empleando un dispositivo cualificado gestionado por un tercero, manteniéndose el control exclusivo del firmante o creador de sellos.

En ambos casos, y dada la inexistencia en la LFE de obligación legal de proceder a la certificación del producto a la que nos hemos referido anteriormente, el prestador[722]

---

[718] http://sogis.org/documents/mra/20100107-sogis-v3.pdf.

[719] Common Criteria Portal, accesible en http://www.commoncriteriaportal.org/products/.

[720] Dentro del acuerdo SOG-IS, como hemos indicado anteriormente.

[721] Habitualmente será el prestador de servicios de certificación el que asuma esta verificación, dado que adquiere para el firmante el dispositivo, lo personaliza y lo entrega debidamente operativo.

[722] O el fabricante, el importador o, incluso, el usuario final, que también puede ser el adquirente final de

podía, bajo su responsabilidad, declarar que el dispositivo era conforme con los requisitos legal y que, por tanto, permitía la generación de firmas electrónicas reconocidas, pudiendo aportar, como prueba de ello, cualquiera de las previstas en la legislación industrial y, en concreto, una certificación técnica.

Sucedía que, evidentemente, si dicha certificación de producto se realizaba contra una norma o especificación técnica diferente de las previstas en el artículo 27.3 de la LFE –que, como ya hemos visto, era sólo CEN CWA 14169 y sus versiones posteriores[723]–, no podía legalmente considerarse a dicha certificación como una certificación de dispositivo seguro de creación de firma electrónica, por lo que tampoco gozaba de la presunción contenida en el artículo 28 de la LFE. Esta certificación, sin embargo, se situaba a caballo entre la simple auto-declaración por parte del fabricante y la certificación contra las normas "oficiales" de la Comisión o de Estado miembro correspondiente, reforzando la posición del prestador frente a una posible discusión con el supervisor (o en sede judicial) respecto al cumplimiento de los requisitos contenidos en el artículo 24.3 de la LFE.

La consecuencia jurídica de todo ello era que la firma electrónica generada mediante este sistema podía ser perfectamente denominada como "firma electrónica reconocida", porque para ello no se exigía ninguna certificación en concreto, pero que no gozaba de la presunción procesal de autenticidad; más en concreto, podía ser objeto de controversia judicial que la firma fuera verdaderamente reconocida, porque la parte que desease impugnar la firma electrónica reconocida podía alegar que la otra parte no había demostrado que el dispositivo cumplía los requisitos del artículo 24.3 de la LFE, alegando que la certificación técnica se había realizado contra una norma que no era idónea para ello; inconveniente que se podía reproducir en la relación jurídico-administrativa con el supervisor, que tenía la potestad de controlar el cumplimiento de las obligaciones de los prestadores, incluyendo el suministro de dispositivos seguros: así como con otros supervisores, en caso de comercialización del producto en otros Estados miembros.

Sin embargo, en este punto el Reglamento eIDAS ha supuesto un cambio de orientación radical con respecto a la LFE, ya que su artículo 30.1 establece que "la conformidad de los dispositivos cualificados de creación de firmas electrónicas con los requisitos que figuran en el anexo II será certificada por los organismos públicos o privados adecuados designados por los Estados miembros", convirtiendo esta certificación, que como hemos visto era opcional, en obligatoria.

Se trata de una norma que hay que poner en relación directa con el artículo 29.2 del Reglamento eIDAS, que indica que "[l]a Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los dispositivos cualificados de creación de firmas electrónicas", con el efecto jurídico de que "[s]e presumirá el cumplimiento de los requisitos establecidos en el anexo II cuando un dispositivo cualificado de creación de firmas electrónicas se ajuste a dichas normas"; actos que "se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2"; artículo que resulta también aplicable a los dispositivos cualificados de creación de sello en virtud de lo establecido en el artículo 39.1 del Reglamento eIDAS.

---

este tipo de tecnologías, aunque no será lo habitual.

[723] Dado que en España no se hizo uso de la competencia de establecer normas nacionales, quizá por su caracterización como "excepcional" en la LFE.

La consecuencia jurídica de esta modificación es que, desde el 1 de julio de 2016, fecha de inicio de aplicación del artículo 30.1[724], no se puede comercializar un dispositivo como cualificado sin proceder a su previa certificación; la cual, según indica el apartado 3 del artículo 30 del Reglamento eIDAS, "se basará en los elementos siguientes: - un proceso de evaluación de la seguridad llevado a cabo de conformidad con las normas para la evaluación de la seguridad de los productos de tecnología de la información incluidos en la lista que se establecerá de conformidad con el párrafo segundo, o - un proceso distinto del proceso contemplado en la letra a), con tal de que ese proceso haga uso de niveles de seguridad equivalentes y que los organismos públicos o privados a los que se refiere el apartado 1 notifiquen ese proceso a la Comisión. Podrá recurrirse a ese proceso únicamente a falta de las normas a que se refiere la letra a) o cuando esté en curso el proceso de evaluación de la seguridad a que se refiere la letra a)", previsión que se completa con el mandato de que "[l]a Comisión establecerá, por medio de actos de ejecución, la lista de las normas para la evaluación de la seguridad de los productos de tecnología de la información a que se refiere la letra a). Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2".

Este artículo ofrece dos opciones: una más estricta, que es la preferible para el legislador europeo, y que consiste en el empleo, como hasta ahora, de metodologías específicas de seguridad funcional de productos, principalmente Criterios Comunes, para las que se van generando estándares europeos, como hemos mostrado anteriormente; y otra más flexible, que autoriza la certificación empleando otras metodologías, incluso *ad hoc*, pero que sólo se puede emplear en ausencia de normas europeas conforme al primer guion, o mientras un producto se encuentre en el proceso de evaluación conforme a dichas normas, todo ello de acuerdo con la reciente Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior[725].

Por lo que respecta a los contenidos de la ya citada Decisión 2016/650, es preciso hacer notar que la misma se dicta al amparo de los artículo 30.3 y 39.2 del Reglamento eIDAS, sin que se realice mención alguna a los artículos 29.2 y 39.1 del Reglamento; y ello a pesar de que en la misma se referencian tanto "normas para la evaluación de la seguridad de los productos de tecnología de la información" cuanto "normas relativas a los dispositivos cualificados de creación de firmas electrónicas" (aplicables *mutatis mutandis* a los dispositivos cualificados de creación de sellos electrónicos).

Entre las primeras, que en efecto serían las propias de los artículos 30.3 y 39.3, encontramos las referencias a los Criterios de evaluación para la seguridad de la TI[726] y a

---

[724] En virtud de lo dispuesto en el artículo 52.2.a) del Reglamento eIDAS.

[725] Que ha derogado la Decisión de la Comisión 2003/511/CE, de 14 de julio de 2003, relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica.

[726] En concreto, ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. (Tecnología de la información — Técnicas de seguridad — Criterios de evaluación para la seguridad de la TI. Parte 1). ISO, 2009; ISO/IEC 15408-2:2008 — Information

la Metodología para la evaluación de la seguridad de la TI[727].

Sin embargo, entre las segundas encontramos la norma CEN EN 419 211, partes 1 a 5, que es, como ya hemos dicho, la sucesora de CEN CWA 14169, que fue referenciada en la Decisión 2003/511 precisamente como una norma que goza de reconocimiento general para productos de firma electrónica, gozando del efecto de presunción de cumplimiento. Lo lógico es que esta norma se hubiera referenciado, por tanto, no con la base legal de los artículos 30.3 y 39.2 del Reglamento eIDAS, como se ha hecho, sino a los efectos de los artículos 29.2 y 39.1 del Reglamento, dado que se podría dar el caso de que se llegue a considerar que un producto cualificado que haya obtenido la correspondiente certificación no se considere protegido por la presunción legal de cumplimiento de los requisitos legales establecidos en el Anexo II del Reglamento eIDAS.

En segundo lugar, la Decisión 2016/650 hace uso de las dos posibilidades previstas en el artículo 30.3 del Reglamento eIDAS, al establecer, de un lado, "normas para la evaluación de la seguridad de productos de tecnología de la información que se aplican a la certificación de dispositivos cualificados de creación de firma electrónica o dispositivos cualificados de creación de sello electrónico de conformidad con el artículo 30, apartado 3, letra a), o con el artículo 39, apartado 2, del Reglamento (UE) Nº910/2014, cuando los datos de creación de firma electrónica o los datos de creación de sello electrónico se conservan íntegramente, aunque no necesariamente de forma exclusiva, en un entorno gestionado por el usuario", y, de otro, autorizar la certificación de los dispositivos cualificados de creación de firmas electrónicas o dispositivos cualificados de creación de sellos electrónicos, cuando un prestador cualificado de servicios de confianza gestione los datos de creación de firma electrónica o los datos de creación del sello electrónico en nombre de un firmante o de un creador de un sello, que "se basará en un proceso que, de conformidad con el artículo 30, apartado 3, letra b), haga uso de unos niveles de seguridad equivalentes a los exigidos por el artículo 30, apartado 3, letra a), y que sea notificado a la Comisión por el organismo público o privado a que se refiere el artículo 30, apartado 1, del Reglamento (UE) Nº 910/2014"; esto es, cualquier proceso de evaluación equivalente a Criterios Comunes y los perfiles de protección de la norma CEN EN 419 211, a discreción del organismo de certificación designado –en nuestro caso, sería el Organismo de Certificación del Centro Criptológico Nacional–, que es quien debe tomar la decisión acerca de la metodología a emplear y comunicarla al ejecutivo europeo[728],

technology — Security techniques — Evaluation criteria for IT security — Part 2. (Tecnología de la información — Técnicas de seguridad — Criterios de evaluación para la seguridad de la TI. Parte 2). ISO, 2008; e ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3 (Tecnología de la información — Técnicas de seguridad — Criterios de evaluación para la seguridad de la TI. Parte 3). ISO, 2008.

[727] ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation (Tecnología de la información — Técnicas de seguridad — Metodología para la evaluación de la seguridad de la TI.

[728] El Reglamento eIDAS no aclara si los productos certificados conforme a esta segunda opción serán únicamente considerados dispositivos cualificados en el Estado donde hayan sido certificados o si, por el contrario, dichos productos se podrán comercializar en otros Estados de la Unión como dispositivos cualificados. En nuestra opinión, se debe entender que dichos productos gozarán del beneficio de la libre circulación previsto en el artículo 4.2 del Reglamento eIDAS.

como ha sucedido en el caso de España y de Italia[729].

Además, el artículo 31.2 del Reglamento eIDAS prevé que "la Comisión establecerá, publicará y mantendrá una lista de dispositivos de creación de firmas electrónicas cualificados certificados", a partir de la información que deberán remitirle los Estados miembros (prevista en el artículo 30.1 del Reglamento eIDAS); norma que claramente persigue establecer un mecanismo administrativo de publicidad administrativa que aporte certeza a los prestadores y a los usuarios de los servicios de confianza, en especial a las partes que confían.

Finalmente, es imperativo hacer notar que el Considerando 56 del Reglamento eIDAS menciona que "el presente Reglamento no debe regular la totalidad del entorno del sistema en el que operen tales dispositivos. Por consiguiente, el objeto de la certificación de los dispositivos cualificados de creación de firmas debe limitarse a los equipos y programas informáticos empleados para gestionar y proteger los datos de creación de firma creados, almacenados o tratados en el dispositivo de creación de firmas", por lo que "el alcance de la obligación de certificación debe excluir a las aplicaciones de creación de firmas".

Este enfoque resulta altamente criticable[730] porque deja fuera del sistema de control público de garantías de la firma electrónica nada más y nada menos que a la aplicación que se emplea para crear la firma electrónica, por lo que dicha aplicación podría actuar de forma fraudulenta, mostrando un documento en pantalla, pero remitiendo – al dispositivo cualificado de creación de firma electrónica, para la creación de la firma – el resumen criptográfico de un documento diferente al que realmente se mostró[731].

Aunque parezca sorprendente, esta posibilidad está expresamente autorizada en las normas técnicas aplicables, como ETSI EN 319 102-1, dedicada a los procedimientos de creación y validación de las firmas digitales correspondiente a firmas electrónicas avanzadas.

---

[729] Cfr. https://ec.europa.eu/futurium/en/content/list-alternative-processes-notified-commission-accordance-article-303b-and-392-eidas. En el caso de España, los criterios para la evaluación mediante este método alternativo han sido publicados por el Organismo de Certificación en forma de Instrucción Técnica IT-009, disponible en https://oc.ccn.cni.es/index.php/es/documentos/normativa-y-legislacion/5-it-009-remote-qualified-electronic-signature-creation-device-evaluation-methodology.

[730] Esta disfunción había sido ya advertida por (Delos, Lacroix, & Graux, 2010, p. 39 y ss.), al indicar que no existía, bajo la DFE, ninguna obligación legal en orden a mantener las condiciones de seguridad del dispositivo seguro de creación de firma electrónica en una aplicación de creación de firma o una interfaz de usuario externa al mismo.

[731] Esto no es tan problemático en el caso de sello, al menos en algunos escenarios, aunque ciertamente podría generar problemas análogos.

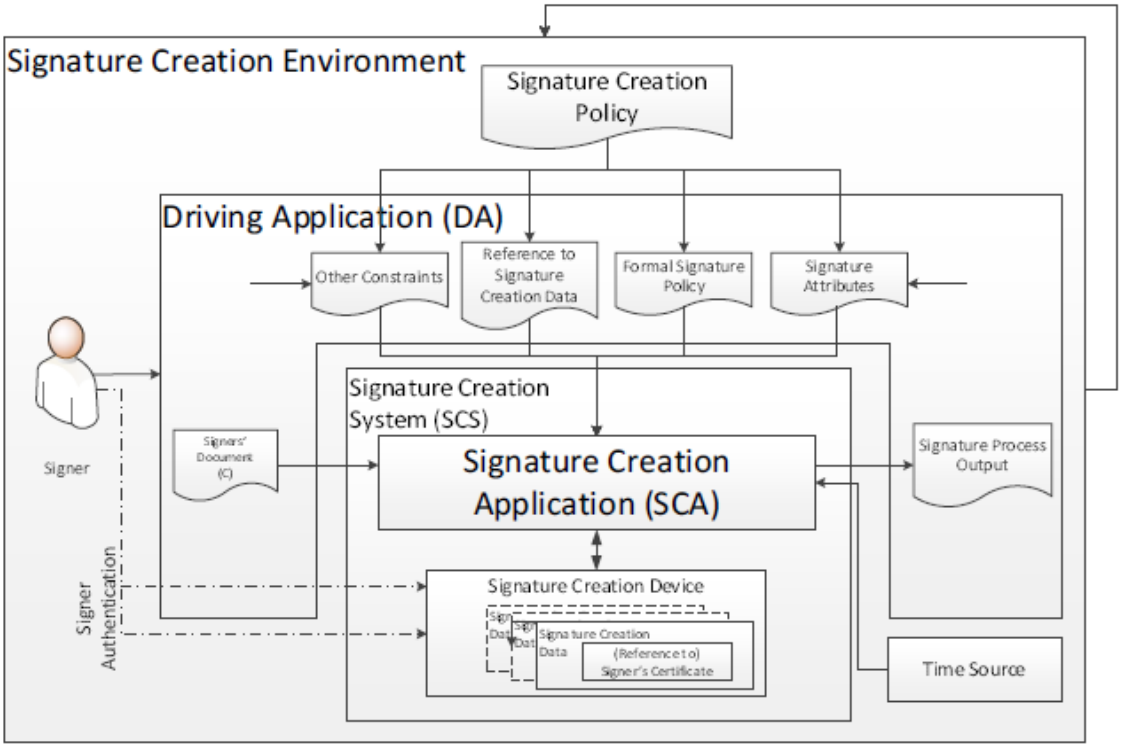


Ilustración 14. Modelo funcional de creación de firma electrónica (ETSI EN 319 102-1)

En dicha norma se establece un modelo funcional en el que se muestran los diferentes componentes que intervienen en la creación de la firma electrónica avanzada o cualificada (que lo será cuando el dispositivo sea cualificado), incluyendo la "*driving application*", que es la aplicación que representa el entorno de usuario que da acceso a la interfaz de firma electrónica, la aplicación de creación de firma propiamente dicha, y el dispositivo de creación de firma, que se pueden ver en la Ilustración 14.

Como se deriva de la sección 4.2.4 de dicha norma técnica, es perfectamente posible que la "*driving application*" se encargue de la remisión, del resumen criptográfico del documento, a la aplicación de creación de firma electrónica. En caso contrario, también conforme a dicha sección, será la aplicación de creación de firma la que produzca el resumen criptográfico para su entrega al dispositivo de creación[732].

En efecto, al alcanzar la certificación únicamente al dispositivo cualificado de creación de firma, queda fuera del marco de garantías precisamente lo más importante de la función social de la firma, que es la vinculación entre la declaración de voluntad con el texto sobre el que la misma recae, algo que es especialmente relevante dada la especial naturaleza del documento electrónico[733].

---

[732] El proceso es, realmente, algo más complejo, porque la firma digital se crea a partir de la representación del documento más la representación de los atributos de la firma, como la fecha alegada de firma, el certificado que respalda la firma y otros.

[733] Como ha explicado (Muñoz Soro, 2003, págs. 132-133), "hay que tener en cuenta que en el mundo real el firmante ve este documento en su integridad y que, además, lo que él ve coincide exactamente con lo que verá quien interprete posteriormente la firma", mientras que "por el contrario, el documento electrónico tiene fronteras difusas, ya que se materializa en ficheros informáticos cuya visualización por el usuario exige de la intervención de complicados programas, que pueden presentarlos en modos muy diferentes y

Ello no significa que la firma electrónica cualificada sea disfuncional, sino que las garantías técnicas intrínsecas a la misma no cubren verdaderamente toda su funcionalidad, algo que veremos debe ser tenido en cuenta en el momento de analizar su valor probatorio. Quizá sea preciso valorar, *de lege ferenda*, la conveniencia de extender el modelo de control público que anteriormente hemos presentado a las aplicaciones de firma electrónica también, en especial cuando las mismas se empleen para generar fuentes de prueba con presunción legal asociada, al objeto de no situar a los firmantes o creadores de sellos en situaciones de potencial indefensión.

Mientras ello no ocurra, en escenarios como la formalización de contratos en página web nos encontramos ante la generación de pruebas electrónicas que, aun con firma electrónica cualificada, son unilaterales, por lo que resulta extraordinariamente importante la intervención de un tercero interpuesto entre las partes[734], para la generación de una fuente de prueba los más eficaz posible.

4.2 LOS EFECTOS JURÍDICOS DE LA FIRMA Y SELLO ELECTRÓNICOS

4.2.1 La validez general de la firma y sello electrónicos

Debemos ahora explicitar una cuestión importante: toda firma o sello electrónicos, con independencia de su calificación como "ordinarios" o "simples", "avanzados" o "cualificados" sirven al mismo objetivo de atribuir el contenido del documento a la persona física o jurídica, y, por tanto, son legalmente válidos y, en función del caso, perfectamente aceptables[735].

En este sentido, el Considerando (22) del Reglamento eIDAS dice que "para contribuir al uso transfronterizo general de los servicios de confianza, debe ser posible utilizarlos como prueba en procedimientos judiciales en todos los Estados miembros"; y por su parte, el

utilizar entornos distintos a los del momento de generación de la firma".

[734] Para (Anguiano Jiménez J. M., 2016, pág. 134), que considera que las transacciones electrónicas son siempre entre ausentes, "[p]ara que las relaciones se produzcan, las partes que intervienen tienen que converger en un recurso informático que suele ser titularidad y estar controlado por una de ellas", poniendo como ejemplo "el acceso a páginas web donde se presta algún tipo de servicio", de modo que "[q]uien lo hace también tiene el control técnico de los recursos informáticos que conforman esa página web y en consecuencia es el único habilitado para generar una prueba electrónica de lo que en esa página web ocurre", añadiendo que "[t]ambién es el único que tiene la posibilidad de alterar o borrar los registros informáticos acreditativos de lo allí sucedido". Por ello, el autor indica que "la interposición resulta un recurso probatorio útil", que "debe ser tenido en cuenta en la implementación de estrategias probatorias". Así sucede en el caso de Logalty, por ejemplo, proceso diseñado por este autor, del que puede verse información en el Anexo A.5.4.

[735] Así lo enfatiza, en la doctrina francesa, (Caprioli, 2014, p. 102). Entre nosotros, (Madrid Parra, 2001, pág. 230) acertadamente ha hecho notar que "en el mundo de papel existen diferencias entre unas firmas y otras, pero no en cuanto a su validez, sino en cuanto a la seguridad", aclarando que "[c]uestión distinta es que se exija una especial solemnidad o su plasmación ante un fedatario público. Tanto en una modalidad como en otra de firma, puede haber supuestos de especial relevancia en los que incluso se requiera la presencia de un fedatario público en el acto de estampación de la firma, pero esto no afecta a la naturaleza o valor jurídico de la firma en sí (manuscrita o no) como medio, por ejemplo, de manifestación del consentimiento". Cfr. el artículo 17 bis de la Ley del Notariado de 28 de mayo de 1862, incorporado por artículo 115.1 de la Ley 24/2001, de 27 de diciembre, que parece manifestarse en contra de este criterio.

Considerando (49) del Reglamento eIDAS indica que "el presente Reglamento debe establecer el principio de que no se deben denegar los efectos jurídicos de una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla todos los requisitos de la firma electrónica cualificada".

En definitiva, el Reglamento eIDAS instaura una norma jurídica de no discriminación de la firma electrónica diferente de la firma electrónica cualificada, que también se extiende al sello electrónico no cualificado. Así se muestra en el artículo 25.1 del Reglamento eIDAS, cuando establece que "no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada", mientras que, en relación con el sello electrónico, el artículo 35.1 del Reglamento eIDAS indica que "no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho estar en formato electrónico o de no cumplir los requisitos del sello electrónico cualificado".

Por su parte, el artículo 3.9 de la LFE ya prohibía que se negaran efectos jurídicos a una firma electrónica que no reuniese los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica (regla que aplicaba tanto a la firma electrónica de una persona física o como de una persona jurídica). Dicho artículo fue dictado en trasposición del artículo 5.2 de la DFE, que ordenaba que "los Estados miembros velarán por que no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que: – ésta se presente en forma electrónica, o – no se base en un certificado reconocido, o – no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o – no esté creada por un dispositivo seguro de creación de firma".

Consecuencia de todo ello es que debemos partir de la validez, *a limine*, de toda tecnología de firma electrónica[736] y sello electrónico, porque lo relevante jurídicamente es poder atribuir, desde la perspectiva de la prueba, un contenido[737] a una persona física o jurídica, de acuerdo con las circunstancias del caso, con una situación concreta que varía en función de las solemnidades y de las formas exigidas para la producción de cada acto jurídico.

Cuestión diferente de la validez potencial será la de los efectos legales concretos de cada tipo de firma electrónica o sello electrónico, que queda en manos de cada legislador nacional[738], como veremos posteriormente.

---

[736] (Chou, 2015, p. 85), desde la perspectiva de la psicología, entiende que "para que las diferentes formas de firma electrónica puedan reemplazar completamente la tradición de firmar a mano, no sólo deberían poseer el mismo status legal, sino tener la misma influencia psicológica sobre el comportamiento humano", (la traducción es mía) algo que cuestiona de forma muy crítica, opinando –con base en diversos estudios empíricos– que las personas que firman electrónicamente tienen mayor tendencia a hacer trampa que las personas que firman a mano, que las firmas electrónicas evocar una menor auto-presencia que las firmas manuscritas, y que ello conduce a una mayor falta de honestidad. Nótese, sin embargo, que estos estudios no han empleado firmas electrónicas avanzadas, ni desde luego firmas electrónicas cualificadas.

[737] Típicamente, se tratará de una declaración de voluntad, de conocimiento, de deseo, etc. en el caso de la firma electrónica de persona física, a diferencia del caso del sello electrónico de persona jurídica, que legalmente no tiene esta connotación.

[738] El Considerando (22) del Reglamento eIDAS dice también que "corresponde al Derecho nacional definir

Este régimen jurídico no ha resultado particularmente novedoso en España, dado que el Tribunal Supremo español, como hemos indicado *supra*, había indicado la perfecta admisibilidad de los sistemas de firma electrónica de todo tipo, adelantándose en el tiempo a la aprobación de la primera legislación española sobre la materia, sin perjuicio de que haya sido más que conveniente elevar este principio (de no discriminación) a rango de ley formal.

En consecuencia, la diferencia real entre una simple firma o sello electrónicos, una firma o sello electrónicos avanzados o una firma o sello electrónicos reconocidos o cualificados no reside en su validez o admisibilidad jurídica, ni siquiera en su potencial eficacia[739], sino en el conjunto de requisitos técnicos necesarios para lograr o incluso garantizar jurídicamente unos efectos jurídicos concretos, en particular, por la vía de las presunciones legales, que invierten la carga de prueba, que se contienen en el Reglamento eIDAS y las que se puedan establecer en sede nacional (cfr. el Considerando (22) del Reglamento eIDAS).

Finalmente, sucede que una firma o sello electrónicos (sean ordinarios, avanzados o incluso cualificados) pueden, a pesar de ser válidos, no ser idóneos, ellos solos, para atribuir todos los elementos de producción de un acto a una persona física o jurídica, de modo que necesitaremos elementos y condiciones adicionales para asegurar la evidencia que ofrece el documento en forma electrónica[740]. Por ejemplo, para obtener certeza de la existencia del documento electrónico –generalmente pocos momentos después de su producción y firma electrónica– podemos añadir a la firma o sello electrónicos un sello de fecha y hora criptográfico, obteniendo un valor probatorio del documento electrónico superior al documento privado en soporte papel[741], mecanismo que el Reglamento eIDAS

---

los efectos jurídicos de los servicios de confianza, salvo disposición contraria del presente Reglamento", mientras que el Considerando (49) del Reglamento eIDAS indica que "sin embargo, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el presente Reglamento según los cuales una firma electrónica cualificada debe tener el efecto jurídico equivalente a una firma manuscrita".

[739] Porque si es admisible como prueba, potencialmente producirá efectos jurídicos, incluso aunque el legislador nacional no regule ningún efecto jurídico específico para estos instrumentos, o regule una eficacia de la firma electrónica no cualificada diferente a la equivalencia con la firma escrita de una persona física, o una eficacia diferente del sello electrónico no cualificado a la presunción de origen e integridad de datos de un documento o comunicación de una persona jurídica. Y en este contexto será particularmente relevante lo que establezcan regulaciones sectoriales o las partes.

[740] Nótese que el artículo 27.3 del Reglamento eIDAS ordena que "los Estados miembros no exigirán para la utilización transfronteriza de un servicio en línea ofrecido por un organismo del sector público una firma electrónica cuyo nivel de garantía de la seguridad sea superior al de una firma electrónica cualificada", y de forma similar, que el artículo 37.3 del Reglamento eIDAS ordena que "los Estados miembros no exigirán, para el uso transfronterizo en un servicio en línea ofrecido por un organismo del sector público, un sello electrónico cuyo nivel de seguridad sea superior al de un sello electrónico cualificado", por lo que, al menos en este caso, cualquier garantía extra que se requiera deberá no afectar a la posibilidad de uso de una firma o sello electrónico cualificado basado en un certificado cualificado. Por este motivo, en el Reglamento eIDAS ha desaparecido la denominada "excepción del sector público" contenida en el artículo 3.7 de la DFE, implementada en España mediante el artículo 4 de la LFE, que hoy se debe considerar inaplicado por el Reglamento eIDAS.

[741] El sello de fecha y hora se consideró, en el artículo 4 de la propia LFE, como una de las condiciones adicionales exigible al uso de la firma electrónica, noción que se ha reafirmado en el artículo 29.2 de la LAE, en el procedimiento administrativo, aunque parece haber decaído del artículo 26.2 de la LPAC.

regula como servicio de confianza independiente de la firma o sello electrónicos.

4.2.2 La eficacia de la firma y sello electrónicos

Desde el punto de vista de la eficacia, por tanto, y respecto a la firma electrónica cualificada, el artículo 25.2 del Reglamento eIDAS establece que "una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita", mientras que respecto al sello electrónico cualificado, el artículo 35.2 del Reglamento eIDAS determina que "un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado".

En ambos casos se trata de un efecto jurídico típico, que persigue la generación de seguridad jurídica para los usuarios de los sistemas de firma o sello electrónicos cualificados, que no precisan entonces regular el funcionamiento del sistema de firma o sello electrónico, ni obtener una previa autorización de uso de los mismos, en sus relaciones con terceros.

Por lo que se refiere a la firma electrónica, determinaba el artículo 3.4 de la LFE que la "firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel"; esto es, que la firma electrónica que cumple estos requisitos se "reconoce" legalmente como equivalente a la firma manuscrita[742]. Este artículo se dictó en trasposición del artículo 5.1 de la DFE, que ordenaba que "los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma: a) satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y b) sea admisible como prueba en procedimientos judiciales" y establecía, a juicio de la doctrina, el principio de equivalencia funcional entre firma electrónica y firma manuscrita[743].

El artículo 25.2 del Reglamento eIDAS mantiene el enfoque, como se puede ver, de determinar que el efecto jurídico típico de una firma electrónica cualificada será el equivalente al que tendría la firma manuscrita[744], por lo que se deberá poder emplear

---

[742] Pero cabe advertir acerca de la dificultad que podía suponer la prueba judicial de que un sistema era, efectivamente, de firma electrónica reconocida conforme a la LFE, dada la inexistencia en España –al menos en términos prácticos– de un sistema voluntario de acreditación de la actividad del prestador que expide el certificado reconocido (artículo 26 de la LFE), y de la posibilidad de uso de dispositivos seguros de creación de firma sin certificación de seguridad (artículos 27 y 28 LFE), aspectos a los que nos referiremos posteriormente.

[743] Así lo indica (Martínez Nadal, 2009, pág. 89).

[744] Para (Illescas Ortíz, 2001, pág. 185), "[é]sta es la voluntad legislativa al consagrar la regla de la equivalencia funcional", puesto que "[l]a esencia de la equivalencia radica precisamente en la fungibilidad de posiciones y no en la desigualdad de una respecto de la otra: ni la manuscrita ha de ser superior a la electrónica ni viceversa". Claramente se viene a referir a que la firma electrónica no debe aportar mayor valor de autenticidad al contenido en el que caso de la firma manuscrita a la que sustituye, posición que comparto plenamente. Otra cosa será el efecto jurídico que dicha firma manuscrita tenga, institución que se encuentra en una cierta crisis como instrumento de acreditación real del consentimiento. Esto ha sucedido especialmente en el caso de la contratación de determinados productos financieros complejos, como las participaciones preferentes. Ejemplifica esta situación la Sentencia de la Audiencia Provincial de Madrid 60/2015, que en su fundamento jurídico decimotercero afirma que "a) la firma de los documentos aportados

cuando una ley exija el requisito de firmar, al tiempo que el epígrafe 1 del propio artículo 25 prohíbe negar eficacia jurídica (potencial) a una firma electrónica que no sea cualificada.

Dicho epígrafe dispone que "[n]o se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada", en línea de continuidad con el artículo 5.2 de la DFE, que ordenaba que "[l]os Estados miembros velarán por que no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que: — ésta se presente en forma electrónica, o — no se base en un certificado reconocido, o — no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o — no esté creada por un dispositivo seguro de creación de firma", que dio lugar al artículo 3.9 de la LFE, el cual dispuso que "no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica", parecido –como se puede ver– a la formulación del artículo 25.1 del Reglamento eIDAS.

Como hemos avanzado anteriormente, esto significa que toda firma electrónica puede potencialmente recibir efectos jurídicos, no pudiendo ser ninguna tecnología discriminada por ser electrónica[745], algo que afectaría a la tutela judicial efectiva de forma evidente; pero también implica que el legislador sólo define un efecto jurídico típico en relación con la firma electrónica cualificada –que es precisamente actuar como equivalente de la firma manuscrita–, permitiendo a los Estado miembros establecer los efectos jurídicos que consideren oportunos en relación con las firmas no cualificadas[746].

En su consecuencia, resultaría contrario a Derecho realizar una interpretación *a sensu contrario* del efecto típico de las firmas electrónicas cualificadas en perjuicio de las firmas no cualificadas; esto es, no se puede considerar acertada una interpretación excesivamente rigorista de la LFE, que argumente que si "la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel" (artículo 3.4 de la LFE), entonces la firma electrónica no reconocida no tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel, sino un valor diferente[747]. De la misma forma, tampoco sería correcta la

---

por la parte demandada con el escrito de contestación permite constatar única y exclusivamente que fueron firmados, no que les fuera explicado su contenido con anterioridad al momento de la contratación; b) Tampoco justifica su entrega, de la que no existe constancia alguna, ni que la misma se produjera también con anterioridad bastante a la contratación, lo que hubiera permitido su examen detenido por los actores".

[745] Para (Dumortier & Vandezande, 2012a, p. 8), "la necesidad de las firmas electrónicas ha sido sobreestimada. En un contexto en línea, la mayoría de transacciones no son concluidas mediante el intercambio de documentos firmados. Al contrario, las personas navegan a través de procesos electrónicos y la principal necesidad, desde una perspectiva de confianza, es asegurar que dichos procesos pueden ser «reproducidos» posteriormente, en orden a reconstruir lo que sucedió en caso de incidente o disputa" (la traducción es mía).

[746] Cfr. los Considerando (22) y (49) del Reglamento eIDAS.

[747] (Martínez Nadal, 2009, pág. 93) se cuestionaba acerca del significado y alcance de la cláusula de salvaguardia de las firmas electrónicas que no cumplen los requisitos de las firmas electrónicas reconocidas en los siguientes términos: "Porque si no se les puede negar eficacia, ¿acaso significa que tienen la misma eficacia que las que cumplen tales requisitos? ¿Cuál es, entonces, y, en definitiva, la diferencia, a estos

interpretación que, partiendo de que "una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita" (artículo 25.2 del Reglamento eIDAS), considerase que una firma electrónica no cualificada no podrá tener un efecto jurídico equivalente al de una firma manuscrita.

Y no es correcta esta interpretación porque la firma electrónica que no sea cualificada podrá obtener también efectos jurídicos, a tenor de la regla de no discriminación contenida en la DFE, la LFE y hoy en el Reglamento eIDAS[748], algo confirmado por el TJUE en, al menos, un caso[749].

Como hemos avanzado, los Estados miembros podrán establecer efectos jurídicos en relación con las firmas electrónicas no cualificadas[750], con carácter general o en relación a casos concretos, o incluso no establecer regla alguna al respecto –en cuyo caso nos encontraremos ante firmas electrónicas de efecto atípico–, pero desde luego lo que no podrán hacer es denegar todo efecto jurídico a una firma electrónica no cualificada ni, en caso alguno, restringir su admisibilidad como prueba.

Dado que la definición de firma electrónica contenida en el artículo 3.10) del Reglamento eIDAS se refiere a "los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar", todos los Estados miembros deben respetar que una firma electrónica no cualificada pueda potencialmente recibir el efecto de "servir para firmar"; esto es, para ser empleada en

---

efectos, entre una firma que cumple los requisitos del art. 3.3 LFE y una firma que no cumple tales requisitos?", para responder que "probablemente la diferencia consista en que las firmas electrónicas en las que falta alguno o algunos de los requisitos de equiparación y a las que se aplica el artículo 3.9 no se beneficien de la equiparación de efectos con la firma manuscrita, y, por tanto, sea necesario demostrar, a través de procedimientos probatorios en ocasiones difíciles y costosos, sus efectos respecto de la autoría e integridad del mensaje firmado".

[748] Para (Illescas Ortíz, 2001, págs. 193-194), de hecho, "[l]a prohibición legal de que sean negados «efectos jurídicos» a la FE sencilla supone el reconocimiento de la producción de efectos jurídicos por la ficha firma. El hecho, además, de que tal reconocimiento haya sido formulado sin distinción alguna entre clases de efectos resulta inhabilitante para llevar a cabo distinciones ulteriores entre los efectos en cuestión", por lo que afirma que "[l]a FE sencilla, así pes, produce efectos jurídicos: todos los efectos jurídicos que la firma manual produce en el mundo del soporte en papel", aunque reconoce que la firma simple recibe el efecto jurídico, por ministerio de la Ley, de identificación, al que ya nos hemos referido.

[749] Cfr. Sentencia del Tribunal de Primera Instancia de 19 de octubre de 2006, en la que, en un caso (asunto T-311/04, Buendía Sierra contra la Comisión) en el que, entre otros motivos, el demandante alega la inexistencia de determinadas decisiones sobre recurso de reposición y concesión de puntos de promoción profesional (en el marco del artículo 45 del Estatuto de los Funcionarios de las Comunidades europeas y la Decisión relativa a las disposiciones generales de aplicación del citado artículo 45), basándose en la ausencia de textos firmados y documentos escritos, el Tribunal admite de forma natural el uso de la firma electrónica del documento digital correspondiente a las decisiones controvertidas, dado que "el Estatuto y las DGB 45 no imponen ninguna forma para la adopción de las decisiones en cuestión", en un magnífico ejercicio de antiformalismo.

[750] El Dictamen de la Abogacía del Estado 26/12, de 2 de abril de 2012, entiende "plenamente ajustado a la LFE que la normativa específicamente aplicable a las Administraciones Públicas regule el uso y la eficacia en el ámbito administrativo de aquellas modalidades de firma electrónica que no reúnan los requisitos de la firma electrónica reconocida", si bien la "admisión de modalidades de firma electrónica distintas de la firma electrónica reconocida o de la incorporada al documento nacional de identidad electrónico por las Administraciones Públicas requiere de una decisión administrativa *ad hoc* plasmada en la correspondiente disposición normativa en la que se concreten los supuestos y condiciones en los que se admite el uso de tales sistemas de firma electrónica" (Abogacía General del Estado, 2013, pág. 337 y ss.).

lugar de una firma manuscrita, porque en caso contrario estaríamos ante una infracción manifiesta del artículo 25.1 del Reglamento eIDAS.

Y ello suscita la duda acerca de qué otros efectos jurídicos pueden establecer los Estados miembros en relación con la firma electrónica no cualificada. Una posibilidad, que además se encuentra mencionada en el propio Reglamento eIDAS[751], sería establecer un efecto jurídico específico en relación con un determinado tipo de firma electrónica, en un contexto concreto, como por ejemplo sucede con la admisión del uso de determinadas firmas electrónicas no cualificadas en las relaciones entre los ciudadanos y las entidades del sector público[752], o en la regulación de sistemas de firma electrónica específicos de las entidades del sector público, sin la consideración de cualificados, pero con indudable efecto jurídico[753].

Otra posibilidad sería que el legislador nacional decida equiparar con carácter general determinadas modalidades de firma electrónica, no cualificada, a la firma escrita[754].

Por otra parte, cabe también preguntarse qué sucede en el caso de que un Estado miembro no establezca efecto jurídico alguno en relación con un sistema de firma electrónica no cualificada. Dado que, como hemos visto de forma reiterada, dicho Estado no puede denegar el efecto jurídico de la firma electrónica ni su admisibilidad como prueba, ello deja espacio para la autonomía de la voluntad de las partes que se relacionan con sujeción a las reglas del Derecho privado, en los términos y con las limitaciones a las que

---

[751] El Considerando (48) del Reglamento eIDAS indica que "aun cuando es necesario un alto nivel de seguridad para garantizar el reconocimiento mutuo de las firmas electrónicas, en determinados casos, como por ejemplo en el contexto de la Decisión 2009/767/CE(10) de la Comisión, deben aceptarse también las firmas electrónicas que tienen una menor garantía de la seguridad", lo cual supone establecer un efecto jurídico específico en relación con estas firmas electrónicas no cualificadas, que precisamente sustituyen a las correspondientes firmas manuscritas.

[752] Así ha sucedido en la LAE y en la LUTICAJ, a las que nos referiremos posteriormente, que han regulado el derecho subjetivo del ciudadano al empleo de sistemas de firma electrónica avanzada basada en certificado reconocido/cualificado en pie de igualdad con los sistemas de firma electrónica reconocida/cualificada, en los ámbitos administrativo y judicial, y se ha mantenido en los artículos 9 y 10 de la LPAC, con la incorporación, además, del epígrafe 11 al artículo 3 de la LFE, que establece que "todos los sistemas de identificación y firma electrónica previstos en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley de Régimen Jurídico del Sector Público tendrán plenos efectos jurídicos"; previsión que se mantiene en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza (disposición adicional segunda).

[753] Como también ha sucedido en la LAE y en la LUTICAJ, y se ha mantenido en la LRJSP, como veremos en detalle.

[754] Esto es precisamente lo que ha acabado sucediendo en Italia, donde el artículo 20.1-bis del *Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale*, en redacción dada por *Decreto legislativo 13 dicembre 2017, n. 217, Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*, establece que "el documento electrónico cumple con el requisito de la forma escrita y tiene la efectividad prevista por el artículo 2702 del Código Civil cuando incorpora una firma digital, otro tipo de firma electrónica calificada o una firma electrónica avanzada o, en cualquier caso, se forma, previa la identificación informática de su autor, a través de un proceso que tenga los requisitos establecidos por el AgID de conformidad con el artículo 71 con modalidades tales que garanticen la seguridad, integridad e inmutabilidad del documento y, de manera clara e inequívoca, su trazabilidad al autor" (la traducción es mía).

posteriormente nos referiremos[755].

Esta concepción doble se traduce en los niveles que caracterizan la eficacia de la firma electrónica: la regla jurídica de no discriminación, de acuerdo con la cual la parte a quien interesa la eficacia de una firma electrónica tiene derecho a que se practique una prueba suficiente, que determine si la firma electrónica era suficientemente fiable como para imputar el acto a la persona que la produjo; y la regla de equivalencia, que no elimina la necesidad de esta prueba, pero la reduce considerablemente, mediante la presunción de la especial idoneidad de determinada tecnología (la que se puede subsumir en el concepto jurídico de firma electrónica cualificada) para actuar sustantivamente como si fuera la firma manuscrita de dicha persona, con eficacia *erga omnes*.

Mientras que la regla jurídica de no discriminación permite la existencia de firmas electrónicas atípicas, cuyos efectos sustantivos serán definidos por las partes, pudiendo "servir para firmar [en ese caso particular]", la regla de equivalencia establece una firma electrónica típica que aporta seguridad jurídica a las partes que deciden utilizarla, debido a su idoneidad para "servir para firmar [en todo caso]". Y dada la necesidad de admitir el empleo de firmas electrónicas no cualificadas en determinados ámbitos, se observa que en efecto los Estados miembros establecen efectos típicos singulares a dichas firmas no cualificadas, limitados a su jurisdicción.

Los Estados miembros no sólo pueden establecer efectos jurídicos con respecto a las firmas electrónicas no cualificadas, sino que también pueden hacerlo en relación con las firmas electrónicas cualificadas, siempre que dichos efectos vayan más allá del efecto típico definido en el Reglamento eIDAS, como por ejemplo sucederá en el caso del establecimiento de una presunción de autenticidad de la firma electrónica cualificada[756].

No se puede concluir esta sección sin indicar que ninguna firma electrónica –ni siquiera la firma electrónica cualificada– puede emplearse en la absoluta totalidad de actuaciones personales, ya que el artículo 1.2 del Reglamento eIDAS, en línea de continuidad con la legislación anterior[757], aclara que el mismo "no afecta al Derecho nacional o de la Unión relacionada con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma"[758], por lo que nos podemos encontrar, en efecto, ante requisitos esenciales de forma[759] que impidan absolutamente el uso de la firma

---

[755] Cfr. el epígrafe 5.1 de este trabajo.

[756] Así sucede en el caso de la legislación procesal alemana, cuando la firma electrónica cualificada ha sido validada conforme al artículo 32 del Reglamento eIDAS, según se desprende de la sección § 371a (1) del Código alemán de Procedimiento Civil (*Zivilprozessordnung – ZPO*). En relación con esta cuestión, cfr. el epígrafe 4.3.2.3 de este trabajo.

[757] El artículo 1.2 de la LFE establecía que sus disposiciones "no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten". Cfr. el Considerando (21) del Reglamento eIDAS, que indica que "tampoco debe regular el presente Reglamento los aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos por el Derecho nacional o de la Unión. Por otro lado, no debe afectar a los requisitos nacionales de formato correspondientes a los registros públicos, en particular los registros mercantiles y de la propiedad".

[758] Como ha indicado (Martínez Nadal, 2009, pág. 42), "en ningún caso los notarios pueden ser sustituidos por un prestador de servicios de certificación, cuya función (a efectos identificativos) es distinta y, en cualquier caso, no está revestida de los atributos propios de aquellos".

[759] Esto debe interpretarse, como acertadamente ha señalado (Illescas Ortíz, 2001, págs. 94-95), en el

electrónica, incluso cuando la misma sea cualificada.

Y es que, en definitiva, corresponde al Derecho nacional establecer los efectos jurídicos que debe producir una firma manuscrita[760], en el ámbito de los requisitos de forma de los diferentes actos jurídicos[761], lo que va a condicionar el uso del correspondiente mecanismo de firma electrónica.

En efecto, resulta frecuente la exclusión de la posibilidad de emplear cualquier tipología de firma electrónica, incluida la firma electrónica cualificada, en determinados tipos de actuaciones jurídicas, por lo que hay que estar a lo que se determine conforme a la ley aplicable. Esta noción conecta con la idea de que quizá ninguna firma electrónica basada en claves criptográficas deba ser necesariamente considerada idónea para la realización de actos personalísimos[762]. Así sucede con la imposibilidad de realizar a distancia, con

---

sentido de que la normativa "en efecto, modifica de modo trascendental, según se ha repetido, el derecho hasta ahora aplicable a la forma y prueba de las voluntades negociales y no negociales así como a su declaración", pero que "[c]iertamente, lo que se mantiene inalterado […] respecto de la situación precedente es la necesidad de que la voluntad exista y se emita para que el contrato se perfeccione", reconociendo además que "ni el documento electrónico – los «datos electrónicos» – ni la FE que los rubrique son por el momento utilizables cuando se trata de una figura negocial o un acto jurídico para el que el derecho preexistente requiera formalidades públicas o dación de fe pública", por lo que "[p]ara dicha índole de documentos, en efecto, la FE no produce equivalencia funcional hasta que no intervenga una norma específica que así lo declare"; norma que llegaría con la Ley 24/2001, de 27 de diciembre, que modifica la Ley del Notariado de 28 de mayo de 1862, aunque la misma nunca se ha aplicado plenamente.

[760] (Gobert, 2015, p. 35).

[761] En relación con la forma, (Rodríguez Ayuso, 2018, págs. 105-106) ha indicado "que, con las nuevas tecnologías, se impone la obligatoriedad del soporte: mientras que el contrato tradicional podía celebrarse válidamente en forma escrita o hablada (sin necesidad, la primera, de forma especial, y, esta última, de soporte físico), el contrato electrónico, presente la forma que presente, ha de canalizarse, obligatoriamente, de manera electrónica (rasgo definitorio básico de este tipo de contratos). Por tanto, partiendo de la concepción restringida o limitada de la forma contractual, aun no siendo necesaria, *a priori*, su constancia en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica como presupuesto para la validez del contrato desde la concepción tradicional de esta exigencia (normalmente escritura pública ante fedatario), es evidente que la inobservancia de este requisito determina la inexistencia misma del contrato por ausencia de toda forma, de las electrónicamente posibles, de códigos encriptados o de lenguaje especial", por lo que considera que "[p]odemos hablar, pues, de una formalidad, si se quiere, más profunda o estructural que pretendida o legal, necesaria, en cualquier caso, para la validez del acto desde un punto de vista, no tanto ya jurídico, cuanto natural o sustancial", considerando que "el contrato electrónico responde, al mismo tiempo y de manera inseparable, a la doble finalidad de la forma *ad substantiam* y *ad probationem*: la primera, insistimos, por la necesidad del soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica como materialización necesaria de la inmaterialidad inherente del negocio jurídico analizado; la segunda, en fin, como medio necesario para la prueba, no ya de su validez (anterior), sino de su vida o existencia", a lo que se refiere como "formalismo indirecto o formalismo necesario de contratos jurídicamente no formales, como son los electrónicos".

[762] En concreto, (Bauzá Martorell, 2002, pág. 65 y ss.) se ha referido a los problemas que, a su juicio, pueden derivarse de la que denomina "escindibilidad" de la firma electrónica, indicando que "sólo la seguridad del par de claves a través de un dispositivo de identificación biométrica puede resultar idóneo para asegurar que el signatario de un documento mediante una clave es titular de la misma", lo que se traduce en un nivel de exigencia superior incluso al de la firma electrónica cualificada. También (Nieva Fenoll, 2009) considera que la firma electrónica basada en claves criptográficas plantea el problema de la "transferibilidad de la firma", incluso en el caso de la firma electrónica cualificada, por lo que considera a estos sistemas menos seguros procesalmente que la firma electrónica basada en métodos biométricos. De forma contundente, (Couto Calviño, 2007, pág. 10) recuerda que "la firma electrónica no es una firma, sino un procedimiento electrónico que puede cumplir una función equivalente, y ahí acaba su similitud con la firma manuscrita",

independencia del sistema de firma de que se disponga, actuaciones en las que intervienen fedatarios públicos, en los términos de la legislación notarial, y sin perjuicio de que dichas actuaciones sí podrían hacerse presencialmente –pero no a distancia– empleándose la firma electrónica cualificada[763].

A pesar de lo que se acaba de decir, debemos mencionar la importante excepción, en la práctica, de la legitimación notarial de la firma electrónica del acuerdo de aprobación de cuentas anuales y aplicación del resultado, exigible conforme al artículo 366.1.2º del Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil, y que ha sido sistemáticamente ignorada tanto en el desarrollo normativo del correspondiente procedimiento de depósito digital, tanto en soporte físico como mediante el oportuno sistema telemático, con el argumento de que el uso del certificado cualificado sustituía dicha legitimación notarial de firma electrónica, situación que se ha mantenido incluso después de que el Tribunal Supremo la haya desautorizado expresamente[764].

En el caso del sello electrónico vendría a suceder algo parecido con la firma electrónica,

---

por lo que, añade, "[n]unca puede ser un acto personalísimo e inmediato, sino que más bien es un acto artificial y mediato que no se puede efectuar personalmente". También (Valero Torrijos, 2013, pág. 72) considera que "a pesar de la denominación empleada por el legislador –firma– su funcionamiento se parece, más bien, al de un sello y, por lo tanto, en función de las medidas de seguridad que se adopten o no en su configuración y uso permitiría a otro sujeto distinto del titular suplantar la identidad de éste último".

[763] El artículo 17 bis.1 de la Ley del Notariado de 28 de mayo de 1862, añadido por el artículo 115.1 de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, establece que "los instrumentos públicos a que se refiere el artículo 17 de esta Ley, no perderán dicho carácter por el sólo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquél de conformidad con la Ley reguladora del uso de firma electrónica por parte de notarios y demás normas complementarias", aunque la Disposición transitoria undécima de la propia Ley, añadida por el artículo 115.2 de la citada Ley 24/2001, desactiva esa posibilidad cuando indica que "hasta que los avances tecnológicos hagan posible que la matriz u original del documento notarial se autorice o intervenga y se conserve en soporte electrónico, la regulación del documento público electrónico contenida en este artículo se entenderá aplicable exclusivamente a las copias de las matrices de escrituras y actas así como, en su caso, a la reproducción de las pólizas intervenidas".

[764] Cfr. (De Miguel Asensio, 2015, págs. 1008-1009). Se trata de una Sentencia dictada en relación con la Instrucción de 13 de junio de 2003, de la Dirección General de los Registros y del Notariado, complementaria de la Instrucción de 30 de diciembre de 1999, sobre presentación de las cuentas anuales en los Registros Mercantiles mediante procedimientos telemáticos (nunca formalmente derogada), que establecía las reglas para la legitimación notarial de la firma electrónica en este procedimiento. Esta Instrucción –en mi experiencia, jamás aplicada en la práctica– fue sustituida, o al menos eso cabe suponer, por la Orden JUS/206/2009, de 28 de enero, por la que se aprueban nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación, que "olvida" la existencia de la mencionada Instrucción de 2003, aunque mantiene –ya sólo en su Anexo II, relativo al formato de los depósitos digitales de cuentas– la exigencia de legitimación notarial de firmas del certificado de aprobación de cuentas y aplicación del resultado, prescindiendo completamente de la legitimación notarial de la firma electrónica. Dicha Orden fue derogada por la Orden JUS/471/2017, de 19 de mayo, por la que se aprueban los nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación, dictada al amparo de la habilitación legal prevista en la disposición final tercera del Real Decreto 602/2016, de 2 de diciembre, Orden que prescindió incluso de la exigencia de la legitimación notarial de la firma manuscrita, en un ejemplo de cómo la aprobación de un modelo oficial produce la inaplicación de una norma reglamentaria; en este caso, la contenida en el artículo 366.1.2º del Reglamento del Registro Mercantil. La actual Orden JUS/319/2018, de 21 de marzo, por la que se aprueban los nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación, ha mantenido esta lamentable situación.

aunque con la diferencia de que no existe, como en la firma electrónica, un efecto de equivalencia descrito legalmente; es decir, que el efecto típico del sello es, como hemos visto, acreditar la autenticidad del origen de los datos y su integridad, y no ser equivalente a ninguna figura previamente existente, como pudiera ser el "sello físico de persona jurídica".

Dada la inexistencia de este efecto de "equivalencia con", se pueden generar dudas razonables acerca de los actos para los que se puede emplear un sello electrónico (con independencia de si el mismo es ordinario, avanzado o cualificado), excepto cuando nos encontremos ante el requisito legal, sustantivo, de que una persona jurídica deba ofrecer una garantía de autenticidad del origen de los datos y de la integridad del contenido, como sucede, por ejemplo, en el caso de las facturas electrónicas[765]. Tampoco parece irrazonable acudir al empleo del sello electrónico en aquellos casos en que, como hemos visto anteriormente, exista una norma que prevea el uso de un sello (físico) de persona jurídica.

Sin embargo, aunque sabemos que para el Reglamento eIDAS el sello electrónico debe servir como prueba de que un documento electrónico ha sido expedido por una persona jurídica, aportando certeza sobre el origen y la integridad del documento –Considerando (59)– y para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores –Considerando (65)–, de ahí no se puede desprender que se pueda emplear para toda actuación jurídicamente vinculante para la persona jurídica, en especial a tenor de las normas de representación de los diferentes tipos de personas jurídicas.

Sorprende, a este respecto, que el Considerando (58) del Reglamento eIDAS establezca que "cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica", como si quisiera evitar que la existencia del sello pudiera afectar negativamente a la representación, en el sentido de discriminar negativamente la actuación del representante de la persona jurídica en cuestión.

Parece que para el legislador europeo un sello electrónico se pudiera emplear para toda actuación de una persona jurídica, pero hay que recordar que el Reglamento no afecta al Derecho nacional o de la Unión relacionado con la celebración y validez de los contratos u otras obligaciones legales o de procedimiento relativos a la forma, por lo que se deberá acudir al caso concreto para dilucidar si se puede o no emplear un sello para una determinada actuación.

De nuevo, los Estados miembros pueden determinar en su legislación los efectos jurídicos que produzcan los sellos electrónicos, y en este caso cabe prever que nos encontraremos ante dos tipos de normas: las que podrán regular efectos de sellos electrónicos diferentes

[765] En efecto, de acuerdo con lo establecido en el artículo 164.Dos de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido, que establece que "la factura, en papel o electrónica, deberá garantizar la autenticidad de su origen, la integridad de su contenido y su legibilidad, desde la fecha de expedición y durante todo el periodo de conservación", en redacción dada por el artículo 67.Cuatro de la Ley 17/2012, de 27 de diciembre, de Presupuestos Generales del Estado para el año 2013 (cabe imaginar que para adecuarse a la Directiva 2010/45/UE, de 13 de julio de 2010, por la que se modifica la Directiva 2006/112/CE relativa al sistema común del impuesto sobre el valor añadido. Esta obligación se desarrolla en el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.

a los cualificados, para casos concretos, y, a diferencia de la firma electrónica cualificada, las que autoricen el uso del sello electrónico cualificado para determinadas actuaciones, como por ejemplo, en el ámbito de las relaciones entre las personas jurídicas y las entidades del sector público[766], en el funcionamiento electrónico del sector público[767], en el caso de la factura electrónica[768], o incluso para formalizar actuaciones jurídicamente vinculantes para la persona jurídica en cuestión[769].

En caso de que los Estados miembros no establezcan normas específicas relativas a los efectos de los sellos electrónicos, o de autorización de su uso en aquellos casos donde se requiera legalmente la representación, cabrá también atender a lo que las partes pacten, dentro de su ámbito de autorregulación, o a la utilidad intrínseca del sello, que por ejemplo se podría emplear para la autenticación de comunicaciones remitidas por personas jurídicas, a la acreditación de las actuaciones de acceso o de recepción, o quizá a la formalización de condiciones generales de la contratación[770].

Al efecto jurídico principal que acabamos de exponer, añade el Reglamente IDAS un segundo efecto jurídico, idéntico en relación a ambas instituciones, cuando el artículo 25.3 ordena que "[u]na firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros", y el artículo 35.3, que "[u]n sello electrónico cualificado basado en un certificado cualificado emitido en un Estado miembro será reconocido como un sello electrónico cualificado en todos los demás Estados miembros".

Se trata de un efecto de reconocimiento transfronterizo, que como se puede ver se limita a las firmas electrónicas cualificadas o los sellos electrónicos cualificados que se basen en certificados cualificados expedidos en los Estados miembros. Sorprende esta referencia al certificado cualificado porque, como hemos visto, una firma o un sello sólo pueden ser cualificados cuando se basan en un certificado cualificado, al ser un elemento constitutivo del concepto legal.

Por ello, esta previsión sólo se entiende desde el punto de vista de que dicho certificado cualificado haya sido expedido en un Estado miembro, y no en un tercer Estado, algo que permitiría sustentar la posición de que las firmas o sellos electrónicos cualificados basadas en certificados cualificados expedidos en Estados que no sean miembros de la Unión no gozan, necesariamente, del efecto de reconocimiento transfronterizo como

---

[766] Cfr. los artículos 9 y 10 de la LPAC, a los que posteriormente nos referiremos.

[767] Cfr. los artículos 40 y 42 de la LRJSP.

[768] En este caso, el artículo 5.2 de la Ley 25/2013, anteriormente referida, admite el uso del sello electrónico avanzado basado en certificado cualificado.

[769] Así lo admite, de forma perfectamente natural, (Gobert, 2015, p. 39).

[770] En relación con este último caso, la Sentencia del Tribunal de Justicia (Sala Tercera) de 25 de enero de 2017, en el asunto BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG contra Verein für Konsumenteninformation (C-375/15), interpreta que un sitio de Internet puede constituir un soporte duradero cuando "permite al usuario de servicios de pago almacenar la información que se le envía personalmente de tal manera que esa información pueda ser consultada posteriormente durante un período de tiempo adecuado a su finalidad y reproducida sin cambios", siempre que quede "excluida toda posibilidad de modificación unilateral de su contenido por el proveedor de servicios de pago o por cualquier otro profesional al que se haya confiado la gestión del sitio de Internet", garantías que sin duda ofrece el sello electrónico avanzado y, en todo caso, el sello electrónico cualificado.

firmas o sellos cualificados.

Se trata de una norma que recuerda a alguna ley nacional, como la alemana, que partiendo de que sólo confería el efecto jurídico de la equivalencia con la firma manuscrita a las firmas electrónicas que fueran cualificadas conforme a la ley alemana de firma electrónica[771], únicamente consideraba equivalentes a éstas las firmas electrónicas cualificadas que se basaran en certificados electrónicos cualificados expedidos por prestadores establecidos en otros Estados que previamente se hubieran acreditado, incluidos los prestadores del Espacio Económico Europeo[772], norma que se podía considerar como un obstáculo a la libre circulación de las firmas electrónicas prescrito por la DFE.

Quizá por el desplazamiento de la legislación nacional operada por el Reglamento eIDAS se haya considerado necesario prever en el nivel europeo una norma como la contenida en el artículo 25.3, en relación con la firma electrónica, y en el artículo 35.3, en relación con el sello electrónico, pero dicha norma podría entrar en conflicto potencial con lo establecido en el artículo 14 del Reglamento eIDAS, en cuya virtud, y para todos los servicios de confianza, se prevé la posibilidad de declaración de su equivalencia mediante el reconocimiento por acuerdo entre la Unión y el tercer país u organizaciones internacionales.

En este caso, debemos entender que también la firma electrónica cualificada basadas en un certificado cualificado emitido en un tercer país con convenio deberá ser reconocida como una firma electrónica cualificada en todos los demás Estados miembros, porque en caso contrario se producirá el indeseable resultado de la inaplicación del artículo 14 del Reglamento eIDAS.

En este sentido, el artículo 24.4.ter del Código de la Administración Digital (CAD) italiano[773] prevé la extensión de los efectos de la firma electrónica cualificada a la firma electrónica basada en un certificado cualificado expedido por un prestador de servicios establecido en un tercer país, cuando se dé alguna de las siguientes condiciones: a) que el prestador que expide el certificado cumpla los requisitos del Reglamento eIDAS y esté cualificado en algún Estado miembro; b) que el certificado cualificado esté garantizado por un prestador (que expide certificados) establecido en la Unión Europea que cumpla los requisitos del mismo Reglamento; o c) que el certificado o certificador cualificado sea reconocido en virtud de un acuerdo bilateral o multilateral entre la Unión Europea y terceros países u organizaciones internacionales.

Respecto a los aspectos probatorios de la firma y sello electrónicos, lo primero que debemos indicar es que, de acuerdo con el artículo 3.5[774] de la LFE, se definía el

---

[771] Así se decía en el artículo 162a (1), del Código Civil alemán (BGB), hasta su muy reciente reforma por el artículo 11 (27) de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017, que ha eliminado esta referencia, por lo que ahora se debe considerar que la firma deberá cualificada conforme al Reglamento eIDAS, por ser el mismo de aplicación directa.

[772] Cfr. el artículo 23 de la *Signaturgesetz* de 16 de mayo de 2001, así como (Bierekoven, Bazin, & Kozlowski, 2004, págs. 7-8).

[773] En redacción dada por Decreto legislativo nº 179, de 26 de agosto de 2016, que –entre otros contenidos– adecua la legislación italiana al Reglamento eIDAS.

[774] En redacción dada por Ley 56/2007, de 28 de diciembre.

documento electrónico como "la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado"[775] y que, según el artículo 3.6 de la LFE, será soporte de documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la Ley en cada caso; documentos expedidos y firmados electrónicamente por funcionarios o trabajadores públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica[776]; y documentos privados.

El artículo 3.7 de la LFE aclaraba que los documentos anteriormente referidos "tendrán el valor y la eficacia jurídica que corresponda a su naturaleza respectiva, de conformidad con la legislación que les resulte aplicable"[777]; artículo que hay que interpretar a la luz del artículo 46 del Reglamento eIDAS, que indica que "no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en formato electrónico".

Cada uno de estos tipos de documentos puede incorporar la firma o sello electrónicos, pudiendo ser del nivel ordinario, avanzado, avanzado con certificado cualificado o cualificado, excepto cuando la legislación aplicable establezca un nivel mínimo. Nótese que, antes de la reforma de la LFE por Ley 56/2007, de 28 de diciembre, de medidas de impulso de la Sociedad de la Información, la definición de documento electrónico contenida en la citada Ley exigía que el documento estuviese firmado electrónicamente, lo cual había sido enérgicamente criticado por la doctrina[778].

---

[775] En su redacción originaria el artículo 3.5 de la LFE consideraba como documento el redactado en soporte electrónico que incorpore datos firmados electrónicamente. Esta misma definición se contenía en el anexo de la LAE.

[776] En la actualidad, hay que referirse a la LPAC y la LRJSP.

[777] Por ejemplo, en el caso de la fe pública notarial, hay que acudir a la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, modificada por Ley 24/2005, de 18 de noviembre, de reformas para el impulso a la productividad, cuyo artículo 106.1 regula la atribución y uso de la firma electrónica reconocida por parte de notarios y registradores de la propiedad, mercantiles y de bienes muebles, en el ejercicio de sus funciones públicas. Asimismo, en el caso del documento público administrativo, hay que estar a lo establecido en la LRJSP; y en el del documento público judicial, a lo establecido en la LUTICAJ.

[778] Entre otros, (Punzón Moraleda & Sánchez Rodríguez, 2008) habían indicado acertadamente que "una interpretación rigurosa de este precepto, tal y como quedó redactado con anterioridad a su derogación, suponía que únicamente podrían tener carácter jurídico aquellos documentos en los que se había insertado una firma electrónica, esto inclusive en contra de lo establecido en el artículo 24.2 de la Ley 34/2002, de 11 de julio —en adelante LCE—, en el que se afirma que «En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental». Aquí la interpretación que se hacía era que no era necesario, pese a estar prescrito, lo indicado en el apartado antiguo 5 de la LFE, y ello, simplemente, si tenemos en cuenta, primero, que el principio de equivalencia que resulta de la no necesariedad de firma manuscrita de determinados documentos que se redactan en soporte papel (arts. 1.228 y 1.229 del Código civil) —... ¿por qué entonces unas cargas superiores respecto de los documentos escritos?—, y en segundo lugar, que dicha redacción tampoco implicaba la posible derogación del art. 24.2 LCE en razón de lo expuesto con anterioridad, es decir, simplemente se optaba por un sistema diferente. Finalmente, en tercer lugar, el legislador con la redacción antigua del apartado 5 quería, a nuestro juicio, dejar bien claro, que existía sólo una auténtica equivalencia formal, y por ende procesal, entre el documento firmado con firma manuscrita y el documento electrónico cuando éste también estuviese firmado electrónicamente. Como se puede comprobar, existía una equivalencia en dos planos

En todo caso, tras la reforma del artículo 3.5 de la LFE ya no podía quedar duda alguna, en nuestro Derecho, acerca de la consideración de documento electrónico de toda información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado, y ello con independencia incluso de incorporar una firma o sello electrónicos. Lógicamente, con firma o sello electrónicos la prueba será más factible que sin ellos, y de ahí que con carácter general se predicase la posibilidad de emplear cualquier tipo de firma/sello electrónico, en función del nivel de riesgo de cada operación.

Desde una perspectiva procesal, en todo caso, debe quedar claro que nos encontramos ante una prueba documental, regulada en los artículos 317 y siguientes de la LEC, y no ante la prueba de instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso del artículo 384 de la propia LEC[779]. La diferencia es relevante,

---

distintos: por un lado, el establecido en la LCE, pues el documento electrónico que la parte contraria no hubiese impugnado, sería prueba plena en el proceso —de acuerdo con el art. 326 LEC para los documentos privados y con el 319 LEC para los públicos—, y por otro lado, el legislador en la LEC estaba pensando en la equivalencia entre la firma manuscrita —3.4 LFE— y la firma electrónica —3.5 LFE—."

[779] Cfr. (Montero Aroca, 2007, pág. 512 y ss). Más enérgico se pronuncia (Nieva Fenoll, 2009) cuando indica que "primero la Ley 59/2003, de 19 de diciembre, de firma electrónica, y después la Ley 41/2007, de 7 de diciembre, equipararon plenamente a efectos judiciales los documentos en papel y los documentos multimedia, reformando consecuentemente los arts. 267, 268, 318 y 326 de la Ley de Enjuiciamiento Civil. Por otra parte, esa Ley 41/2007 modificó diversos preceptos para permitir la tramitación telemática de los procedimientos judiciales. Tras estas reformas, los arts. 382 a 384, que trataban de poner una distancia entre el papel y el documento electrónico, han pasado a ser completamente sobreabundantes, y sería recomendable su derogación para evitar dudas y contradicciones. Mientras eso no ocurre, se les puede considerar tácitamente derogados por la lex posterior […]". (García Mas F. , 2010) también coincide en afirmar el muy relevante cambio de orientación en el tratamiento procesal del documento. Indica este autor que "no cabe la menor duda de que la Ley de firma electrónica cambia lo que yo había expuesto, entre otras razones, porque ahora dice algo que antes no decía en el Real Decreto-Ley de firma electrónica, y que ya empezó el camino de ese cambio legislativo en la Ley española de comercio electrónico, es decir, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. El apartado 2 de este art. 24 establece un principio que no está en la Ley de Enjuiciamiento Civil, y que además en la vigente ley o en la Ley de firma electrónica ha sido elevado a una categoría general, ya que se refiere no solamente a los documentos electrónicos donde esté incorporado un contrato, sino en general a todo tipo de documentos. Por ello, el legislador indica en la Ley de comercio electrónico que el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental, aplicándose las normas generales que la Ley de Enjuiciamiento Civil determina, según se trate de un documento privado o público electrónico. No se trata, como ya he defendido en otras ocasiones, de una simple prueba determinada por las reglas de la sana crítica y de apreciación por los Tribunales, sino una auténtica prueba documental, superando así los límites en los que la Ley de Enjuiciamiento Civil regulaba la prueba para los instrumentos electrónicos. Además, dando un paso adelante, el primer inciso del apartado 8 del art. 3 de la Ley de firma electrónica establece que el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio; con ello se extiende esa categoría del documento electrónico, y se regirá por las normas procesales probatorias de los documentos públicos o privados, según se trate, efectivamente, de un documento de una o de otra clase. En mi opinión, supone un salto cualitativo desde el Real Decreto-Ley de firma electrónica en cuanto a la conceptuación de la denominación de medio de prueba". (Ormazábal Sanchez, 2002) indicó que "el llamado documento electrónico no se adecuaba íntegramente a ninguno de ambos medios probatorios: ni era exactamente equiparable a un documento, aunque presentase múltiples semejanzas con él; ni el reconocimiento judicial era el cauce probatorio idóneo para traerlo al proceso", valorando positivamente la reconducción de los ficheros informáticos al medio de prueba previsto en el artículo 384 de la LEC, criticando el retorno al medio de prueba documental de estas fuentes de prueba, y añade que "[e]n este punto se plantea un interrogante de gran trascendencia: ¿cabe aplicar a estos instrumentos la regla de valoración legal propia del documento privado (art. 326.1 LEC), conforme a la cual, cuando su autenticidad no sea cuestionada por

ya que la documental hace prueba plena[780], siempre que el documento sea autentificado, mientras que la denominada "prueba informática" se valora a la sana crítica.

Nótese que no es el mismo el tratamiento en otros ordenamientos jurídicos, más estrictos, como el alemán, que únicamente aplica las reglas procesales de valoración de los documentos privados a los documentos electrónicos que incorporen firma electrónica cualificada[781], y no a los restantes.

Es precisamente esta prueba de la autenticidad de la firma electrónica la que se debe practicar en caso de "repudio" o "rechazo" del documento por parte de la parte a quien se imputa la misma, al igual que sucede en el caso de la firma manuscrita, que en caso de conflicto se sustancia mediante una prueba pericial caligráfica.

Hay que advertir que, debido al incipiente –y hasta tiempos muy recientes, escaso– uso de estos medios de prueba, se debe preparar especialmente su aportación[782]. Al efecto, la LFE determinó un tratamiento específico de la prueba de la autenticidad de la firma electrónica, en los casos de la firma avanzada y de la firma reconocida, olvidando sorprendentemente la firma electrónica simple u ordinaria. Sin embargo, de nuevo, aunque el tratamiento parecía muy diferente al principio, en realidad venía a ser el mismo.

Determinaba el artículo 3.8 de la LFE, en redacción dada por Ley 56/2007, de 28 de diciembre, al efecto, que "[s]i se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un

---

el adversario, deben tenerse por ciertos el hecho, acto o estado de cosas que documenten, la fecha y la identidad de los intervinientes?", para concluir que "[l]a similitud, en este aspecto, de los instrumentos informáticos con el documento tradicional me parece total y, por ende, creo que esta norma de valoración legal habría de aplicarse también a los documentos informáticos cuya autenticidad no haya sido cuestionada por el adversario. Es cierto, como hemos visto, que el precepto se remite a las reglas de la sana crítica. Pero lo hace, concretamente, a las reglas de sana crítica aplicables a aquellos según su naturaleza, una naturaleza, tratándose de instrumentos informáticos, muy afín a la de los documentos tradicionales, lo que permite trasplantar a aquellos las máximas de experiencia o reglas de la sana crítica positivizadas aplicables a éstos, una de las cuales es la de la autenticidad del documento no cuestionado".

[780] En la autorizada opinión de (Anguiano Jiménez J. M., 2016, pág. 131), en referencia a la aportación al proceso judicial de ficheros con propósito acreditativo, "[p]ara la consideración de estas aportaciones como prueba tasada se requerirá que la manifestación de voluntad que se acredita esté firmada por quien de emite", añadiendo que "[e]n caso contrario se considerará una aportación del 299 de la LEC que se valorará judicialmente en aplicación de las reglas de la sana crítica" y que "la condición documental se adquiere cuando el emisor de la manifestación de voluntad utiliza cualquiera de las modalidades de firma previstas en la vigente LFE".

[781] Cfr. la sección § 371a (1) del Código alemán de Procedimiento Civil (*Zivilprozessordnung – ZPO*).

[782] Como ha denunciado (Nieva Fenoll, 2009), "la realidad actual es que cuando en un expediente judicial aparece un documento multimedia, tiende a observársele como un objeto extraño al que hay que tratar con mil cuidados para que no se rompa, no se borre, no se altere su contenido, y otras muchísimas cautelas que harían reír a carcajadas a cualquier menor de edad, incluso de edad bastante temprana. Se tiene desconfianza por las copias en ese mismo formato aportadas por las partes de sus documentos, se suele omitir el cotejo de su contenido con todavía más facilidad que el cotejo del documento en papel, que poquísimas veces se hace realmente. Por añadidura, en no pocos casos se ordena la lectura y visionado del documento en el acto del juicio en el procedimiento ordinario, al amparo del art. 431 LEC, o en la vista del verbal, como si se tratara de un reconocimiento judicial. Y ello no es más que una pérdida miserable de tiempo, teniendo en cuenta que, como cualquier documento escrito —aunque previo el análisis del antivirus— las partes y el Juez deberían haberlo leído en privado antes de las respectivas vistas".

certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica", régimen que mejoraba la redacción anterior de la norma, pero que no estaba exento de problemas de enfoque[783].

El mismo artículo ordenaba también que "[l]a carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida", lo que podía resultar bastante gravoso para la parte que normalmente quería beneficiarse del valor probatorio de este artefacto[784].

La norma previó que, si dichas comprobaciones obtenían un resultado positivo, se presumiera la autenticidad de la firma electrónica reconocida[785] con la que se hubiera firmado dicho documento electrónico, siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. E incluso, si a juicio del tribunal la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros, tratamiento similar a la prueba de cotejo de letras; resultando preciso aclarar que la autenticidad de la firma electrónica reconocida sólo garantizaba que su equivalencia con la firma manuscrita se considerara probada.

También determinaba el mismo artículo 3.8 de la LFE que, si se impugnaba la autenticidad de la firma electrónica avanzada, se debía estar a lo dispuesto por el artículo 326.2 de la LEC, que permite el empleo de cualquier medio de prueba que resulte útil y pertinente, lo que nos llevaba al terreno de la prueba electrónica[786].

---

[783] En este sentido, a juicio de (Martínez Nadal, 2009, pág. 97), refiriéndose a la firma electrónica reconocida, "es posible que no sea suficiente, o incluso necesario, probar estos elementos para reconocer la validez de la firma electrónica. Pues lo que se está impugnando es la autenticidad de la firma; y por tanto debe probarse no tanto que la firma electrónica es reconocida sino que es auténtica", añadiendo que "efectivamente, podría darse el caso de que una firma fuera reconocida, por darse los requisitos anteriores, pero no fiera auténtica, p.ej. por haber existido una incorrecta identificación del solicitante del certificado, o, porque como consecuencia de la pérdida de la clave privada de firma, la firma ha sido realizada por un tercero no autorizado. […] Y, al contrario, podría darse el caso de una firma que resulta no ser reconocida, por incumplir alguno de los requisitos legales, pero, sin embargo, fuera auténtica, en la medida que, pese a ello, quedara garantizada la autoría y la integridad del documento electrónico". Desde una óptica de la mecánica procesal, (Elías Baturones, 2008, pág. 165) considera "que para tal comprobación sería conveniente y oportuno que por el Juzgado o Tribunal competente se librara oficio a dicho «prestador de servicios» a fin de que por el mismo se emitiera certificado oficial acreditativo de dichos extremos".

[784] En especial dada la desaparición de la presunción legal, contenida en el RDLFE, en cuya virtud se consideraba que una firma electrónica era reconocida; a saber, la acreditación voluntaria del prestador y la certificación del producto (Martínez Nadal, 2009, pág. 91). Aunque ambos mecanismos se mantuvieron en la LFE, esta ley no establecía presunción global alguna.

[785] Para (Gudín Rodríguez-Magariños, 2010, pág. 12), y a diferencia de lo que sucede con los demás sistemas de firma electrónica, en el caso de la firma electrónica cualificada, "el sistema de corroboración de la firma se aleja de los medios de confirmación pericial, para asemejarse al verdadero documento público, en el sentido de que lo que será objeto de corroboración no será el contenido mismo de la declaración como la autenticidad de la firma estampada", afirmación atinada, dado que en efecto una firma electrónica cualificada con una presunción *iuris tantum* de autenticidad parece situarse por encima de la firma manuscrita, salvo en el caso de la firma manuscrita legitimada notarialmente.

[786] Como ha indicado (De Urbano Castrillo, 2009), "la gran especialidad de esta prueba [electrónica], como se ha dicho, es que contiene un hardware y un software, es decir, los aspectos externos e internos del documento. En principio, en cuanto al hardware, puede resultar importante comprobar posibles incidencias en su fabricación, su acoplamiento y funcionamiento, máxime si existen varias terminales. Y, en cuanto al

A pesar de este doble tratamiento de la prueba de la firma electrónica, en ambos casos el tratamiento probatorio venía a ser el mismo, en caso de conflicto, ya que se debía acudir a una prueba pericial informática, que en su caso se podía simplificar o facilitar mediante la aportación, por los prestadores de los servicios de seguridad o de los servicios de certificación de la firma electrónica, o por lo fabricantes de la tecnología, de certificados que acreditasen, conforme a la normativa industrial o conforme a un esquema nacional de evaluación y acreditación de la seguridad de las tecnologías de la información, que los servicios y los productos empleados cumplían los requisitos de seguridad aplicables al caso concreto.

En el caso de la firma electrónica cualificada, el contenido de la pericia a realizar se encontraba determinado por la LFE[787], mientras que en el caso de la firma avanzada no se establecía criterio ninguno, dado que en aplicación del principio de neutralidad tecnológica, cualquier tecnología puede ser cualificada como firma electrónica avanzada, haga uso o no de certificados o dispositivos de firma, y por tanto difícilmente podía prever el legislador cómo se debe demostrar que una tecnología concreta no ha sufrido un problema de seguridad que la invalide como firma electrónica avanzada.

Esta segunda solución debe resultar también aplicable, en nuestra opinión, a la firma electrónica simple u ordinaria, al objeto de evitar la indefensión de la parte que combate la impugnación por falta de cauce procesal, resultando ciertamente criticable haber generado tal laguna legal.

Como hemos anticipado, la diferencia que realmente existe entre la prueba de la firma electrónica reconocida y de los restante tipos de firma electrónica era en la LFE, por tanto, el grado de definición de los aspectos a comprobar en la pericial informática, que en el caso de firma electrónica reconocida facilitaba la preparación de la prueba y, en su caso, la anticipación de la misma, y que además establecía la presunción de autenticidad de la firma electrónica reconocida una vez verificada, ventaja que debía tomarse en consideración como criterio de selección del nivel de firma requerido en un acto concreto.

Que no se definiera legalmente qué debe formar parte de la prueba pericial informática en los casos de la firma electrónica simple u ordinaria, y de la firma electrónica avanzada no significaba que la prueba no fuera posible o más compleja, sino que se debía estar al caso concreto[788] y, especialmente, a la definición de las medidas de seguridad de la

---

software, habrá que ver quién confeccionó el programa —si se trata de una cuestión relacionada con ello— y si quien aparece como titular del documento —por ejemplo quien lo firma digitalmente— es realmente el *dominus* del mismo, o se empleó su clave por un tercero, pongamos por caso. Sólo disponiendo de ese material, de los conocimientos personales suficientes —por ejemplo, del lenguaje básico y de expresiones técnicas del caso— y de la pericia judicial o informes de las partes, que expliquen lo sucedido y ofrezcan conclusiones claras y científicamente avaladas, podrá estarse en condiciones de efectuar una adecuada valoración de esos concretos medios de prueba", lo cual requiere de una importante especialización para la realización de la pericia.

[787] Incluyendo, entre otras cuestiones, la verificación de que el algoritmo de firma empleado correspondía a un sistema de firma electrónica reconocida, la verificación de la condición del dispositivo empleado como seguro, o la verificación de las prácticas del prestador del servicio que emitió el certificado como reconocido, algo tremendamente complejo, por otra parte, y que el Reglamento eIDAS ha solventado.

[788] A criterio de (Illescas Ortíz, 2001, pág. 196), plenamente aplicable en la actualidad, "el MD con FE sencilla ha de ser valorado con el conjunto de la prueba obrante en autos de acuerdo con las reglas de la sana crítica", a cuyo respecto "no debe olvidarse que el valor de la FE ha de ser ponderado de acuerdo con un cúmulo de circunstancias atinentes tanto al MD que atribuye cuanto a la finalidad perseguida por su

concreta tecnología que se iba a emplear como firma electrónica.

Para cerrar este marco, la disposición adicional décima de la LFE añadió un apartado tercero al artículo 326 de la LEC, que establece que cuando la parte a la que interese la eficacia de un documento electrónico lo solicite o cuando se impugne su autenticidad, se procederá de acuerdo con el artículo 3 de la LFE, que como hemos visto conecta también con el apartado segundo del artículo 326 de la LEC, previsión que se mantendrá vigente tras la aprobación del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, manteniendo en la LEC una referencia a la LFE una vez derogada ésta.

Como novedad sobre el régimen previsto en la LFE, el Reglamento eIDAS prevé en su artículo 26.4 que "la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a firmas electrónicas avanzadas", de modo que "se presumirá el cumplimiento de los requisitos de las firmas electrónicas avanzadas mencionadas […] en el artículo 26 cuando una firma electrónica avanzada se ajuste a dichas normas", previsión que también se contiene en relación con el sello electrónico avanzado en el artículo 37.4.

Estas normas presentan un gran interés[789] desde la perspectiva probatoria, dado que permiten facilitar la prueba de forma muy importante, mediante el establecimiento de la presunción de que una firma o un sello son efectivamente avanzados, por lo que no será necesario en estos casos demostrar que en el momento de generación de la firma o sello avanzado concurrieron todos los requisitos exigidos legalmente que, como hemos visto, no son pocos, por lo que supone una mejora sustancial con respecto al régimen previsto en la LFE al que nos acabamos de referir.

Para el establecimiento de estos números de referencia de normas se debe dictar un acto de ejecución mediante el procedimiento de examen, en los términos del artículo 48.2 del Reglamento eIDAS, acto de ejecución que de momento no se ha adoptado.

También establece el Reglamento eIDAS, y esto resulta más relevante desde la óptica de la prueba, el contenido del proceso de validación de la firma o sello electrónico cualificado (artículos 32 y 40), así como la posibilidad de implementarlo en forma de servicio de validación cualificado[790] (artículos 33 y 40), en ambos casos considerando la potestad de la Comisión de establecer normas de conformidad, el cumplimiento de las cuales presumirá que la validación se ha realizado correctamente.

En este caso, varía el régimen probatorio actual, ya que en virtud de la presunción ya no será necesario acudir a la prueba pericial a la que nos referíamos anteriormente, excepto en caso de impugnación, en cuyo caso la carga de la prueba recae sobre la parte que impugna, carga que puede ser muy difícil de levantar[791].

---

emisor y las características del negocio mediante el cual se perfecciona, ejecuta o consume; también habrá de ponderarse el grado de fiabilidad tecnológica de la FE sencilla empleada", por lo que, concluye, "[l]a sana crítica evocada, en efecto, excluye la atribución permanente de un valor absoluto para la FE sencilla con independencia de su modalidad y circunstancias del caso".

[789] Aunque las mismas también son relevantes en el contexto de la admisión transfronteriza de las firmas y sellos electrónicos, a la que posteriormente nos referiremos.

[790] Cfr. el epígrafe 4.3.2 de este trabajo.

[791] Sin perjuicio de que, como se ha expuesto en el epígrafe 4.1.3 de este trabajo, se pueda atacar igualmente

4.3 LOS SERVICIOS DE CONFIANZA EN SOPORTE DE LA FIRMA Y SELLO ELECTRÓNICOS

En este epígrafe presentaremos, sucintamente, los servicios de confianza tipificados en el Reglamento eIDAS en relación con la firma y el sello electrónico; esto es, el servicio de certificación de la identidad, el servicio de creación, el servicio de validación y el servicio de conservación.

4.3.1 El servicio de confianza de creación de la firma y sello electrónicos; la posibilidad de "delegar la firma o el sello" a un tercero

4.3.1.1 Caracterización del servicio

Una de las grandes novedades[792] del Reglamento eIDAS consiste en el servicio de creación de firma o sello por parte de un prestador de servicios, que habilita las operaciones relativas a la creación de la firma electrónica, mediante el dispositivo correspondiente, una opción que se ha venido denominando "firma delegada", o "firma centralizada", o "firma remota", o incluso "firma en la Nube", y que hasta la aparición del Reglamento eIDAS había generado dudas acerca de su legalidad.

Sin embargo, como expone el Considerando 51 del Reglamento eIDAS, "debe ser posible para el firmante confiar a un tercero los dispositivos de creación de firmas electrónicas cualificados", posibilidad que viene referida a diversos casos de uso, incluyendo la cesión de un dispositivo como una tarjeta criptográfica (típicamente para su uso desatendido), o, de forma más prometedora, al empleo de sistemas de clave privada centralizada (HSM) a que nos hemos referido anteriormente[793].

Asimismo, el Considerando 52 del Reglamento eIDAS aclara que "debido a sus múltiples ventajas económicas, debe desarrollarse la creación de firmas electrónicas a distancia con un entorno de creación de firma electrónica gestionado por un proveedor de servicios de confianza en nombre del firmante", posibilidad que es conceptualmente diferente a la anterior, y más amplia, al referirse no sólo a la gestión del dispositivo cualificado, sino a la creación de la firma, sea ésta avanzada o cualificada.

Estas normas suponen un claro avance respecto a la normativa anterior, que no parecía admitir la posesión de los datos de creación de firma por ninguna persona diferente del firmante[794], de modo que, y a tenor de las dificultades técnicas que ha planteado el despliegue de los dispositivos seguros de creación de firma electrónica hasta ahora

---

la validez de la firma electrónica cualificada porque la aplicación no ofrezca las necesarias garantías acerca de la visualización del documento a firmar.

[792] La LFE autorizó esta posibilidad en 2015, cuando fue modificada por la disposición final cuarta de la Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social, momento en que el Reglamento eIDAS ya estaba aprobado, pero aún no resultaba aplicable.

[793] Cfr. el epígrafe 1.3.1 de este trabajo.

[794] Con excepción, claro, de la clave de "firma" de persona jurídica, que en la exposición de motivos de la LFE admite la cesión de dichas claves, por su custodio, a terceros para su utilización.

comúnmente aceptados –tarjetas con microprocesador criptográfico– en especial en entornos de movilidad, es posible que esta opción facilite de forma muy importante la adopción de la firma o sello electrónico cualificado.

En su consecuencia, el Reglamento eIDAS permite la existencia del servicio de creación de firma o sello electrónico a distancia[795], pudiendo ser ordinaria, avanzada, avanzada basada en certificado no cualificado o avanzada basada en certificado cualificado, pero no considera el servicio cualificado de creación de firma electrónica cualificada o de sello electrónico cualificado como un servicio independiente, sino que el mismo deberá ser parte de un servicio cualificado tipificado en el propio Reglamento eIDAS que ofrezca un prestador cualificado.

O, por ser más preciso, y como veremos inmediatamente, lo que el Reglamento eIDAS permite es el servicio (siempre sin cualificación) de creación de firma o sello electrónico a distancia, firma o sello que podrá ser cualificado incluso aunque un tercero genere o gestione en su nombre los datos de creación correspondientes, empleando para ello un dispositivo remoto bajo la responsabilidad del prestador cualificado. Desde esta concepción, lo que el Reglamento eIDAS no permitiría es la existencia de un hipotético servicio cualificado de generación y gestión de claves por cuenta del firmante o del creador de sellos.

Este enfoque técnico de firma con clave centralizada es el que sustenta el sistema Cl@ve firma[796], que permite la obtención de un certificado de firma del DNI electrónico sin necesidad de disponer de la correspondiente tarjeta soporte, y que ya se emplea en diversos servicios de administración electrónica, y otros servicios análogos ofrecidos ya por diversos prestadores o autoridades en la Unión Europea[797].

La finalidad típica del servicio será, normalmente, permitir al firmante o creador de sellos proceder a la generación de la firma electrónica o del sello electrónico de forma remota, sin tener que disponer en su poder físico del correspondiente dispositivo de creación, en especial en el caso de un dispositivo cualificado.

Diferente del servicio de creación de firma o sello a distancia, que implica que el prestador disponga de los correspondientes componentes técnicos para la generación y/o gestión de los datos de creación de firma o sello por cuenta del usuario, es la posibilidad de que un firmante o creador de sello autorice a un tercero a utilizar los datos de creación de firma o sello, y que puede anticiparse bastante polémico.

No nos encontramos en este caso ante un prestador de servicios de confianza que genera o gestiona datos de creación de firma o sello que se mantienen bajo el control exclusivo, con un alto nivel de confianza, del firmante o creador de sellos, sino ante un negocio jurídico diferenciado, en cuya virtud se encomienda a un tercero la utilización de los datos de creación de firma o sello en cuestión, tercero que actuará por cuenta del firmante[798] o

---

[795] Cfr. el epígrafe 4.3.1 de este trabajo.

[796] Dicho sistema resulta accesible en http://clave.gob.es/clave_Home/dnin.html.

[797] Como, por ejemplo, sucede en Portugal, en una aproximación casi idéntica a la española. Cfr. https://www.autenticacao.gov.pt/cmd-assinatura;jsessionid=8D0D70676E0714F5C6B509ACCBCE2626.

[798] A esta posibilidad se había referido ya (Madrid Parra, 2001, págs. 198-199), que explica que "de hecho, con conocimiento o por descuido del titular, se podrá utilizar su firma electrónica por otra persona, cosa que no ocurre con la firma manuscrita. Esta sólo puede ser originalmente estampada en un documento de

del creador del sello.

Tal negocio jurídico[799], sustentado en la autonomía de la voluntad de las partes, será lícito en tanto en cuanto cumpla con los requisitos generales contenidos en la legislación, significativamente, el Código Civil español (en adelante, CC). En este sentido, conforme a lo establecido en el artículo 1255 del CC, "los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral ni al orden público", por lo que se deberá determinar previamente la existencia de alguna prohibición legal al respecto.

La posibilidad de que el firmante o creador de sellos pueda autorizar a un tercero la utilización de los datos de creación no se encuentra expresamente regulada en el Reglamento eIDAS, y tampoco se encontraba regulada en la normativa anterior (ni en la LFE, ni en la DFE[800] ni en el RDLFE), por lo que no puede hablarse de una autorización expresa al respecta, ni de que su ejercicio se encuentra autorizado pero con sujeción a condiciones específicas, como sucede en el caso de la generación y gestión de los datos de creación de firma y sello a la que antes nos hemos referido.

Pero esta posibilidad tampoco se encuentra claramente prohibida en la normativa, ni siquiera indirectamente, sino que el Reglamento eIDAS emplea una terminología que claramente ubica esta cuestión en el ámbito del riesgo del firmante o creador de sello.

Recuérdese, a tal efecto, que el artículo 26.c) del Reglamento eIDAS se refiere a que la misma debe "haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo", cuando podría haber dicho que los datos debían ser utilizados bajo su control exclusivo –en el mismo sentido, el artículo 36.c) del Reglamento eIDAS–; o el Anexo II, epígrafe 1.d) del mismo Reglamento, cuando determina que el dispositivo cualificado garantizará que "los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros" –aplicable *mutatis mutandis* a los sellos electrónicos–, cuando podría haber dicho que dichos dispositivos debían impedir el uso de los datos de creación

---

papel por su titular. De lo contrario se trataría de una falsificación. Si el titular de la firma manuscrita desea que otra persona firme por él, ha de recurrir a la representación. En el uso de la firma electrónica, ésa puede ser obviada mediante la simple entrega o puesta a disposición de la clave privada", y añade el mismo autor, que "[d]ejando al margen los supuestos delictivos de obtención fraudulenta de una firma electrónica, en la mayoría de los casos de «cesión voluntaria» de la firma electrónica sobre la base de la confianza en otra persona, será jurídicamente irrelevante que no haya sido el titular de la firma quien efectivamente la haya aplicado. Los efectos jurídicos le serán siempre imputados al titular. Se produce un fenómeno de «fungibilidad» en lugar de representación", valorando posteriormente el caso extremo de uso de la firma electrónica de una persona fallecida, que reconduce a la demostración de si existió o no representación.

[799] (Merchán Murillo, 2016, pág. 168), para quien "la firma electrónica cumple tres funciones: identificación, autenticación de la identificación y autorización/autenticación de la transacción", considera que "[l]a cesión voluntaria de la firma electrónica la podríamos colocar en la última de ellas, que es donde se produce, en lo que podríamos denominar, función de control (valor de control e incluso resultado del control) del dispositivo de firma electrónica", por lo que "[m]ediante la cesión de la firma se está otorgando un mandato indirecto o una representación, como resultado de una acción unidireccional o pluri-direccional, según el caso, pudiendo resultar, en la práctica, imposible deducir el valor de dicho mandato o representación".

[800] (Sorge, 2014, p. 131) así lo ha indicado.

por parte de terceros.

Tampoco la LFE estableció un deber legal de uso personal e intransferible de los datos de creación de firma electrónica (de persona física o de persona jurídica)[801], situando más bien la cuestión en el ámbito de la responsabilidad y, para ser más exactos, en el sentido de establecer una limitación de responsabilidad del prestador que expidió el certificado en caso de "negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos" (artículo 23.1.c) de la LFE), en cuyo caso el responsable será, lógicamente, el firmante (o, por analogía, el creador de sellos).

Cabría argumentar, en contra de la posibilidad de autorización de la utilización de los datos de creación de firma o sello por parte de un tercero, que la misma resulta incompatible con la propia definición de firma electrónica, por cuanto la misma, como hemos visto, debe identificar al firmante, y encontrarse vinculada tanto al firmante cuanto a lo firmado, pero lo cierto es que el legislador de la Unión podría haber configurado la utilización de los datos de creación de firma –no los de sello, por su propia naturaleza– como una actuación estrictamente personal, imponiendo la correspondiente obligación *ex lege*, y no lo ha hecho, sino que más bien ha hecho recaer las posibles consecuencias de la firma sobre él, como "firmante aparente", en base a la identidad contenida en el certificado, con independencia de que haya (o no) creado la firma.

Por tanto, cabe concluir que sería conforme a Derecho que un firmante o creador de sello autorizase a un tercero a la utilización de sus datos de creación[802], a salvo de lo que pueda disponer el legislador nacional[803].

---

[801] Algo que ha sido criticado por la doctrina, como, por ejemplo, puede verse en (Ortega Díaz, 2008, pág. 253).

[802] Para (Merchán Murillo, 2016, pág. 191), "[s]i bien, tanto Reglamento, Directiva y Ley, lo que pretenden es la capacidad de mantener las claves criptográficas privadas bajo el control exclusivo de uno, cualquiera de los signatarios pueden decidir renunciar a este control y permitir a otros a firmar en su nombre, de forma voluntaria", algo que para este autor nos sitúa "en el ámbito de la representación indirecta, considerada como verdadera representación", afirmando que "[p]or ello, puede determinarse que en el régimen de firma electrónica, la cesión voluntaria actual se encuentre recogida, implícitamente, dentro del esquema de la firma electrónica marcado en la «definición» legal, establecida en los Artículos 3 y 6,2 de la Ley".

[803] Más difícil es defender esta posición en ordenamientos, como el austríaco o el italiano, que en efecto han legislado en este sentido. En el primer caso, conforme a la sección § 5 de la Ley Federal sobre Firmas Electrónicas y Servicios de Confianza para Transacciones Electrónicas – *Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)*, promulgada por artículo 1 de la Ley Federal de 8 de julio de 2016, los firmantes y creadores de sellos, así como los prestadores cualificados de servicios de confianza que actúen bajo su mandato, deben custodiar diligentemente los datos de creación correspondientes, al objeto de impedir, de forma razonable, el acceso por terceros a dichos datos. La misma sección autoriza de forma expresa que se puedan compartir los datos de creación de sellos, lo que apunta a que no sería posible hacer lo mismo en el caso de los datos de creación de firma, pero ello no supone necesariamente que no sea posible autorizar a un tercero a utilizar dichos datos de creación de firma electrónica, cuando los mismos están custodiados por un prestador cualificado, porque dicha utilización no exige dar acceso a los datos de creación de firma electrónica. La sección § 16 (1) de la misma Ley tipifica, como sanción, el uso indebido, por cualquier persona, de los datos de creación de firma electrónica o sello electrónico sin el conocimiento o contra la voluntad del firmante o del creador de sellos, lo que abre la puerta a que dicho uso pueda ser debido, al estar autorizado. En el segundo caso, el artículo 32.1 del *Decreto legislativo 7 marzo 2005, n. 82, Codice*

La principal limitación que cabe imaginar a esta posibilidad reside en la hipotética prohibición que, al respecto, pueda establecer el prestador de servicios de confianza que expide al certificado[804], dado que en ese caso nos encontraremos ante un incumplimiento de una obligación del contrato de certificación, posiblemente considerada esencial por el prestador, y que conducirá, cuanto menos, a la revocación del certificado y, como ya se ha adelantado, a la exoneración de la responsabilidad por parte del prestador del servicio de confianza que expidió el certificado.

En este sentido, cabe recordar que el artículo 18.b) de la LFE –que ha sido desplazado parcialmente por el Reglamento eIDAS– obliga en su numeral primero a informar al firmante de la forma en que deben custodiarse los datos de creación de firma, por lo que normalmente nos encontraremos ante una obligación contractual, estrictamente personal e intransferible, de utilización de los datos de creación de firma.

Por tanto, para que se pueda implementar sin riesgo esta posibilidad de autorización de utilización de datos de creación de firma o sello a un tercero será importante que el prestador no establezca este tipo de prohibición.

Adicionalmente, será absolutamente imprescindible que el firmante o creador de sello legítimo pueda, en cualquier momento, conceder y retirar dicha autorización, y que además la autorización se encuentre limitada exactamente a una persona, a los efectos de disponer de la necesaria trazabilidad en la utilización de los datos de creación de firma o sello correspondientes.

Por último, es necesario indicar que esta autorización de la utilización de los datos de creación de firma o sello por parte de un tercero puede realizarse tanto cuando el firmante o creador de sellos posee físicamente del dispositivo –en su caso, cualificado– de creación de firma o sello (por ejemplo, entregando su tarjeta criptográfica al tercero), como cuando la gestión de los datos de creación de firma o sello se ha encomendado a un prestador de servicios de confianza, como acabamos de ver, pero lo que no se deberá hacer, por resultar excesivamente arriesgado para el firmante o creador de sello, es proceder a la copia de los datos de creación de firma o sello electrónico y su entrega a un tercero que no tenga esta condición de prestador de servicios de confianza.

Esta práctica sería, además, considerada ilegal en el caso de la firma o sello electrónica/o cualificada/o, por contravenir los requisitos del servicio a los que nos referimos a continuación.

---

dell'amministrazione digitale (CAD), en redacción dada por *Decreto legislativo 4 aprile 2006, n. 169*, obliga al titular del certificado de firma electrónica a garantizar la custodia del dispositivo de firma electrónica, y a utilizarlo personalmente. Posteriormente, el *Decreto legislativo 26 agosto 2016, n. 179* modifica de nuevo este artículo para extender la obligación personal de custodia también a los instrumentos de autenticación informática para la utilización de los datos de creación de firma electrónica, por lo que no cabe duda, en este caso, acerca de la voluntad de legislador en este sentido.

[804] Al respecto, (Ortega Díaz, 2008, pág. 250) recuerda que "el asegurar que la clave privada permanece, de forma exclusiva y segura, en poder de su titular se convierte en el pilar fundamental sobre el que se construye toda la fiabilidad del sistema de certificados", por lo que, para el autor, "[n]o es de extrañar, por tanto, que esta exigencia de seguridad sea recogida sistemáticamente en los contratos de certificación", de modo que "el suscriptor del certificado se compromete de adoptar las precauciones necesarias que eviten la puesta en peligro, la pérdida, la revelación o el uso no autorizado de su clave privada".

4.3.1.2 Los requisitos del servicio

Como punto de partida, el Considerando 51 del Reglamento eIDAS condiciona la posibilidad de que el firmante confíe a un tercero los dispositivos de creación de firmas electrónicas cualificados, a "que se apliquen los procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica y que la utilización del dispositivo cumple los requisitos de la firma cualificada", requisitos que ya conocemos con cierto grado de detalle[805].

Asimismo, el Considerando 52 del Reglamento eIDAS aclara que "a fin de garantizar que estas firmas electrónicas obtengan el mismo reconocimiento jurídico que las firmas electrónicas creadas en un entorno completamente gestionado por el usuario, los proveedores que ofrezcan servicios de firma a distancia deben aplicar procedimientos de seguridad de la gestión y administrativos específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante"; segundo caso en el que no sólo nos referimos a un gestor centralizado de claves, sino a todo el entorno de creación de la firma electrónica a distancia gestionado por un tercero mediante el correspondiente sistema fiable[806].

Más relevante resulta la frase final del Considerando 52 del Reglamento eIDAS, que contiene una potente limitación a esta posibilidad, cuando indica que "en el caso de una firma electrónica cualificada creada mediante un dispositivo de creación de firmas electrónicas a distancia, se aplicarán los requisitos aplicables a los proveedores de servicios de confianza cualificados contemplados en el presente Reglamento", que sabemos se refiere también a la creación del sello electrónico cualificado a distancia, por la aplicación *mutatis mutandis* al mismo de los requisitos de la firma electrónica cualificada.

En concreto, el apartado 3 del Anexo II del Reglamento eIDAS, aplicable tanto a dispositivos de creación de firma cualificados, como a dispositivos de creación de sello cualificados, indica que "la generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante sólo podrán correr a cargo de un prestador cualificado de servicios de confianza". Como ya dijimos anteriormente, dado que en el Reglamento eIDAS no considera la creación de firma o sello como un servicio que pueda ser objeto de cualificación, dicho prestador deberá encontrarse cualificado para prestar cualquiera de los servicios que sí pueden ser objeto de cualificación[807].

El Reglamento eIDAS no impone ningún requisito de independencia al prestador de este servicio, por lo que debe entenderse que esta posibilidad existe incluso en entornos corporativos, donde los datos de creación de la firma electrónica del empleado son gestionados en dispositivos de firma centralizada bajo la responsabilidad del empleador, por ejemplo, a condición de que se cualifique como prestador.

Por su parte, el apartado 4 del mismo Anexo determina que "sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de

---

[805] Cfr. el epígrafe 4.1.2 de este trabajo.

[806] Sobre los sistemas fiables, cfr. el epígrafe 6.2.5 de este trabajo.

[807] Cfr. el epígrafe 1.3.1 de este trabajo.

creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:

a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio".

Se trata de una previsión orientada a garantizar al máximo la seguridad de los datos de creación de firma o sello electrónico, en cuya virtud se restringen las operaciones que el prestador puede realizar sobre dichos datos. Más en concreto, la norma autoriza la duplicación de los datos de creación a los solos efectos de realizar una copia de seguridad de los mismos, pero con tres condiciones.

En primer lugar, el procedimiento de duplicación de los datos de creación de firma o sello electrónico no debe afectar negativamente a la posibilidad de que los citados datos de creación puedan ser protegidos de forma fiable frente a su utilización por terceros. De ello se desprende la necesidad de que el acceso a la versión duplicada de los datos de creación se encuentre bajo el mismo grado de control exclusivo de uso que los datos originales gestionados por el prestador.

En segundo lugar, los conjuntos de datos duplicados no deben ser de un nivel de seguridad inferior a los originales, con el objetivo evidente de impedir la sustracción de dichos datos, con la consiguiente posibilidad de suplantar la identidad del firmante o del creador de sellos, actuando en su lugar sin detección. Se trata de un requisito que se puede cumplir empleando técnicas de cifrado o de partición de claves en fragmentos antes de su almacenamiento en el exterior del dispositivo cualificado de creación de firma o sello.

En tercer, y último, lugar, se restringe la producción de estos conjuntos duplicados de datos de creación de firma o sello electrónico a los que sean estrictamente necesarios para mantener la continuidad del servicio.

Se trata, de nuevo, de una norma limitativa que persigue reducir la exposición de los datos de creación de firma o sello electrónico a riesgos, dado que cuanto menor sea el número de conjuntos de datos duplicados, menor será también la probabilidad de que terceros accedan a los mismos de forma ilegítima.

El Reglamento eIDAS no establece más requisitos específicos en relación con este servicio, al que resultan también aplicables los requisitos generales aplicables a los prestadores de servicios de confianza, sin cualificación o con ella[808].

Sin embargo, en sede nacional pueden establecerse requisitos específicos aplicables al servicio, como ha sucedido, por ejemplo, en Italia, donde el artículo 32 del Código de la

[808] Cfr., respectivamente, los epígrafes 6.1 y 6.2 de este trabajo.

Administración Digital (CAD)[809] ha establecido[810] una completa regulación de las obligaciones de los titulares y los prestadores de los servicios de firma electrónica cualificada; pero no del servicio de creación de sello electrónico cualificado, curiosamente, término más general que el de "certificadores" anteriormente empleado en la legislación italiana, y que por tanto ahora se refiere, con carácter general, a todos ellos, también a los que crean firmas electrónicas cualificadas a distancia.

Entre ellas, resultan de especial interés la obligación de uso estrictamente personal del dispositivo de creación de firma por parte del titular (el firmante); la obligación de prestador de adoptar todas las medidas organizativas y técnicas apropiadas para evitar daños a terceros; y, lo más relevante, el establecimiento de las obligaciones específicas de este tipo de prestador cuando el mismo expida los certificados[811].

Aunque estas obligaciones específicas se basan claramente en los requisitos que tradicionalmente se han exigido únicamente a los prestadores de servicios que emitían los

---

[809] Aprobado por Decreto legislativo nº 82, de 7 de marzo de 2005. Conforme al artículo 2.3 del CAD, en redacción dada por Decreto legislativo de 13 de diciembre de 2017, "[l]as disposiciones del presente Código y las Directrices relacionadas con el documento informático, las firmas electrónicas y los servicios de confianza mencionados en el Capítulo II, la reproducción y el almacenamiento de los documentos a que se refieren los artículos 43 y 44, la dirección digital y las comunicaciones electrónicas mencionadas en el Artículo 3-bis y en el Capítulo IV, y la identidad digital a que se refieren los artículos 3-bis y 64 se aplicará también a las personas, a menos que se disponga lo contrario" (la traducción es mía), por el que se aprueba el Texto refundido de las disposiciones legales y reglamentarias en materia de documentación administrativa.

[810] En redacción dada por Decreto legislativo nº 179, de 26 de agosto de 2016 y, más recientemente, Decreto legislativo nº 217, de 13 de diciembre de 2017.

[811] Dichas obligaciones se refieren a la comprobación de la identidad del solicitante del certificado, directamente o a través de terceros; la expedición y publicación del certificado en la forma o en los casos establecidos por las directrices del órgano de supervisión y de conformidad con la normativa de protección de datos; la incorporación al certificado cualificado en el momento de la solicitud, y con el consentimiento del tercero interesado, de los poderes de representación u otros títulos relativos a la actividad profesional o al cargo, previa comprobación de la documentación presentada por el solicitante certificando su subsistencia; el cumplimiento de las citadas directrices del órgano de supervisión; la información a los solicitantes, de manera clara y completa, sobre el procedimiento de certificación y los requisitos técnicos necesarios para acceder a ellos y sobre las características y limitaciones del uso de las firmas emitidas sobre la base del servicio de certificación; la publicación oportuna de la revocación y suspensión del certificado electrónico en determinados casos; la garantía de servicio de revocación y suspensión electrónico seguro y oportuno, así como del funcionamiento eficiente, puntual y seguro de los certificados expedidos, suspendidos y revocados; la determinación precisa de la fecha y hora de expedición, revocación y suspensión de certificados electrónicos; la prohibición de copiar y almacenar las claves de firma privada del sujeto al cual el proveedor de servicios de firma electrónica cualificada haya proporcionado el servicio de certificación; el suministro, empleando medios de comunicación duraderos, de toda la información útil para aquellos que requieren el servicio de certificación, incluyendo en particular los términos y condiciones relacionados con el uso del certificado, incluidas las restricciones de uso, la existencia de un sistema de acreditación facultativa, y los procedimientos de quejas y solución de controversias, información que puede transmitirse electrónicamente y debe redactarse en lenguaje claro y proporcionarse antes del contrato entre el solicitante y el prestador del servicio de firma electrónica cualificada; la utilización de sistemas fiables; o la garantía del funcionamiento correcto y de la continuidad del sistema, así como la comunicación inmediata al organismo de supervisión y los usuarios de cualquier mal funcionamiento que resulte en la interrupción, la suspensión o la interrupción del servicio. Además, el proveedor de servicios de firma electrónica cualificada deberá obtener los datos personales directamente de la persona a la que se refieran o, previo su consentimiento expreso, a través de terceros, y sólo en la medida necesaria para la expedición y el mantenimiento del certificado, suministrando la información requerida por el artículo 13 del Decreto Legislativo no. 196.

certificados, con la nueva redacción del CAD italiano ahora resulta aplicables también a los prestadores que ofrecen el servicio de creación de la firma electrónica cualificada, resultando obligados ambos prestadores al cumplimiento de las citadas obligaciones, sin perjuicio del modelo de responsabilidad frente a terceros de cada uno.

4.3.1.3 Los efectos jurídicos asociados al servicio

El Reglamento eIDAS no establece ningún efecto jurídico específico para este servicio, dado que el efecto jurídico se establece, como hemos visto, en relación con la prueba electrónica (la firma o sello electrónico) que se crea al hacer uso del mismo.

4.3.2 El servicio de confianza de validación de la firma/sello electrónico

4.3.2.1 Caracterización del servicio: el informe de validación

El servicio de validación permite la comprobación de una firma o sello electrónico, de forma que se determine su validez y, por tanto, su capacidad para producir los efectos jurídicos deseados.

Respecto a este servicio de confianza, en su modalidad cualificada, el Considerando (57) del Reglamento eIDAS indica que "la especificación de los requisitos exigibles a los prestadores cualificados de servicios de confianza que pueden brindar un servicio de validación cualificado a las partes usuarias que no desean o no pueden realizar por sí mismas la validación de las firmas electrónicas cualificadas debe estimular a los sectores privado y público para que inviertan en tales servicios", con el objeto de facilitar el empleo de la firma o sello electrónico.

Se trata de otra de las novedades del Reglamento eIDAS en relación con la DFE, que no regulaba servicio alguno al respecto, limitándose, en su Anexo III, a establecer una serie de recomendaciones para la verificación segura de la firma electrónica; recomendaciones que en la LFE se convirtieron en obligación, referida a los dispositivos de verificación de firma electrónica.

A pesar de resultar novedoso en el Reglamento eIDAS, se trata de un servicio que ha venido siendo ampliamente empleado en España, en especial en el ámbito de la Administración electrónica, y que se encuentra parcialmente regulado en el RDENI, resultando muy relevantes, al menos en volumen, experiencias como el servicio @firma[812], el servicio Validador del Consorci Administración Oberta de Catalunya o la plataforma Zain del Izenpe vasco.

La novedad del Reglamento es, en definitiva, la tipificación, la armonización y el fomento del servicio de validación, seguramente por la enorme complejidad técnica asociada a esta tarea, que hace francamente difícil a los terceros que reciben firmas o sellos electrónicos algo aparentemente tan simple como asegurarse de que son válidos, así como para crear un marco que permita consensuar las reglas para proceder a dicha validación de forma consistente en toda la Unión Europea.

Este último aspecto no es precisamente baladí, en especial en el caso de las firmas

[812] Cfr. (Martínez Gutiérrez, 2009, págs. 571-574) y, con mayor detalle, (Martínez Gutiérrez, 2011, págs. 439-443).

electrónicas transfronterizas, porque la ley aplicable a la creación y a la validación de la firma electrónica son diferentes, algo que en el modelo de la DFE ha generado problemas de reconocimiento transfronterizo de las firmas electrónicas; disfunción que debería resolver el enfoque de armonización del Reglamento eIDAS, al menos en el caso de la firma y el sello electrónico cualificado.

La validación se define en el artículo 3.41) del Reglamento eIDAS como "el proceso de verificar y confirmar la validez de una firma o sello electrónicos", mientras que los datos de validación se definen, en el artículo 3.40) del propio Reglamento, como "los datos utilizados para validar una firma electrónica o un sello electrónico".

Resulta interesante notar que este servicio se ofrece, normalmente, a una persona que recibe una firma o sello electrónico calificado, y precisa realizar este proceso de forma previa a confiar en dicha firma o sello electrónico cualificado. Esta parte usuaria se define, en el artículo 3.6) del Reglamento eIDAS, como "la persona física o jurídica que confía en […] el servicio de confianza", aunque realmente, como hemos avanzado, realmente precisa confiar en la prueba electrónica recibida (como una prueba de identificación electrónica, una firma o sello electrónico, o un sello de tiempo electrónico, o una certificación de entrega electrónica). Obviamente, el servicio también se puede prestar al firmante o al creador de sellos, para que posteriormente remita la firma o sello electrónico cualificado a terceros, o para conservarla junto con el documento o mensaje.

Nótese que, como en otros casos, se puede ofrecer un servicio cualificado, que cumplirá los requisitos que establece el Reglamento, o un servicio sin cualificación, en cuyo caso realmente los requisitos serán establecidos por el propio prestador.

En este sentido, hay que dejar claro que el proceso, y el correspondiente servicio cualificado, se refiere a la validación de la firma o sello electrónico cualificado, y no a la validación de otras tipologías de firma o sello electrónico, algo que responde a la imposibilidad de establecer requisitos para todas las posibles tecnologías que sustentan la prueba de atribución. Ello no significa que no se pueda "reutilizar" un servicio cualificado de firma o sello electrónico cualificado para la validación de una firma o sello electrónico avanzado basado en un certificado cualificado, algo relativamente simple dado que únicamente debe obviarse la comprobación de uno de los requisitos de la firma o sello, que además se informa en el certificado cualificado; más difícil resulta reutilizar este proceso cuando nos encontramos ante un certificado sin cualificación, por no encontrarse normalizada la información correspondiente al mismo, y así sucesivamente.

El enfoque del Reglamento eIDAS es, pues, muy pragmático y centra la cualificación en el proceso de validación de firma o sello electrónico cualificado, el más concreto y mejor definido en la normativa, tanto jurídica, como técnica. A continuación, analizaremos sucintamente estos requisitos, los cuales mostrarán la complejidad que subyace a este proceso, que –recuérdese– debe ser automático, y que consta de diversos elementos en juego.

En primer lugar, el artículo 32.1 del Reglamento eIDAS contiene algunas normas referidas a los certificados cualificados de firma o sello electrónico cualificado. En concreto, en el proceso de validación se debe verificar que el certificado que respalda la firma o sello electrónico cualificado era, en el momento de la creación de la firma, un certificado cualificado de firma electrónica ajustado al anexo I o al anexo III del

Reglamento eIDAS, respectivamente[813]. Se trata de un requisito que exige, como se puede fácilmente deducir, acceder al contenido del certificado y evaluar la completitud y corrección de dichas informaciones, o alternativamente, obtener información adicional acerca de los certificados, posiblemente de la lista de confianza publicada por el órgano competente[814], pero también poder determinar que esta información era correcta en el momento de creación de la firma, para lo cual es imprescindible determinar con certeza este aspecto, siendo muy relevante el uso de un servicio, eventualmente cualificado, de sellado de tiempo electrónico en un momento muy cercano al de creación de la firma o sello electrónico cualificado.

También debe ser objeto de comprobación que el certificado cualificado en cuestión había sido emitido por un prestador de servicios de confianza, lo que requiere de la comprobación de la información contenida en la lista de confianza anteriormente mencionada, a la fecha de creación de la firma o sello electrónico cualificado[815], y que era válido en el momento de la firma, para lo cual se requiere acceder a la información de estado de dicho certificado, de nuevo a la fecha de creación de la firma o sello electrónico; para lo cual también se debe comprobar el certificado empleado por el prestador para firmar el certificado del firmante o creador de sello, así como, en su caso, el certificado que a su vez hubiera firmado el certificado del prestador, y así hasta el inicio de la jerarquía, como se expuso en el capítulo técnico inicial[816].

En segundo lugar, el mismo artículo 32.1 contiene algunas exigencias relativas a algunas informaciones que deben mostrarse, de forma garantizada, a la parte usuaria, incluyendo los datos de validación de firma o sello, el conjunto único de datos que representa al firmante o creador de sellos en el certificado o una indicación clara acerca de haberse utilizado un seudónimo, en lugar de la identidad real del firmante.

Se trata de requisitos orientados a sustentar las garantías de la firma o sello electrónico asociadas a los datos contenidos en el correspondiente certificado, de modo que la parte usuaria pueda conocer[817] la identidad –en su caso, basada en seudónimo– del firmante o creador de sellos, y los correspondientes a los datos de validación de la firma o sello; esto es, la clave pública correspondiente a la persona identificada en el certificado en cuestión, dado que estos datos permiten determinar que una firma o sello es efectivamente avanzado.

En tercer lugar, el artículo 32.1 del Reglamento eIDAS se refiere a exigencias específicas de la firma o sello electrónico, entre las cuales la comprobación de que la firma o sello ha sido creada empleando un dispositivo cualificado –mediante la información contenida en el certificado correspondiente, o alternativamente la información indicada en la lista de

---

[813] Respecto a los concretos contenidos de los diferentes tipos de certificados, cfr. el epígrafe 2.1.2.1 de este trabajo.

[814] En relación con el contenido de este original mecanismo de publicidad administrativa, cfr. el epígrafe 7.1.4.1 de este trabajo.

[815] Esto es preciso porque el prestador puede haber perdido la cualificación en un momento posterior a la creación de la firma o sello electrónico, lo que no debe afectar a la validez de la firma o sello realizados antes de la pérdida de esta cualificación.

[816] Cfr. el Anexo A.1.2.5 de este trabajo.

[817] El numeral e) del artículo 32.1 del Reglamento eIDAS se refiere a que "en caso de que se utilice un seudónimo, la utilización del mismo se indique claramente a la parte usuaria en el momento de la firma", redacción que parece errónea dado que la parte usuaria no actúa en el momento de la creación de la firma.

confianza–, de que se ha mantenido la integridad de los datos firmados o sellados, y finalmente, de que en el momento de firma se han cumplido todos los requisitos previstos para considerar a la firma o sello como avanzado.

Esto último implica que el proceso de validación ha de ser capaz de comprobar la vinculación entre firma o sello y firmante o creador de sello, respectivamente; que la firma o sello identifica a firmante o creador de sello –lo que resulta redundante con la comprobación ya realizada del certificado–; el control exclusivo de los datos de creación de firma o sello –lo que sólo puede asumirse como correcto a partir de la constatación del uso del dispositivo cualificado, que ya sabemos que es puramente declarativa–; y la vinculación entre firma o sello y datos firmados o sellados.

Se trata de una redacción ciertamente oscura, que desde luego no facilita la comprensión del proceso –por no mencionar la enorme complejidad y coste que puede suponer una prueba pericial en estas condiciones–, problema que, como ya hemos visto en otros casos, sólo se mitiga gracias a la existencia de especificaciones y normas técnicas que concretan los diferentes requisitos, al objeto de que las diversas aplicaciones sean realmente capaces de validar la firma o el sello cualificado.

Al amparo de las recomendaciones contenidas en la DFE, se aprobó la especificación técnica CEN CWA 14171:2004, sobre procedimientos de verificación de firma electrónica[818], que ha sido recientemente actualizada en el TC 224 de CEN, para su conversión en la norma europea EN 419 111, partes 1, 4 y 5[819].

Más relevante, incluso, es la importante norma ETSI EN 319 102-1, que define de forma completa y minuciosa el proceso de validación de firma o sello electrónico, dada la posibilidad, que ya conocemos, de que la misma sea establecida a efectos de la acreditación de la conformidad del proceso. En efecto, el artículo 32.3 del Reglamento eIDAS prevé que "[l]a Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a la validación de las firmas electrónicas cualificadas", de modo que "se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la validación de una firma electrónica cualificada se ajuste a dichas normas", debiéndose estos actos de ejecución adoptarse "con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2"[820]; y sin que hasta hoy se haya establecido norma alguna.

En concreto, esta norma prevé tres modalidades del proceso de validación de firma o sello

---

[818] Esta especificación no se incluyó en la Decisión 2003/511/CE, de la Comisión, de 14 de julio de 2003, relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, por lo que una eventual certificación de las aplicaciones de validación no hubiera gozado ni del efecto de presunción de cumplimiento de requisitos legales ni del de libre circulación del producto.

[819] En concreto, EN 419111-1 – Protection profiles for signature creation and verification application - Part 1: Introduction; EN 419111-4 – Protection profiles for signature creation and verification application - Signature verification application - Part 4: Core PP; y EN 419111-5 – Protection profiles for signature creation and verification application - Signature verification application - Part 5: Possible extensions.

[820] Cfr. el epígrafe 1.4.2 de este trabajo.

electrónico[821] –de los cuales en este momento nos interesan dos[822]–, en función de las necesidades de la parte usuaria, que se construyen sobre una serie de procesos, más especializados[823], que se ocupan de validar los diferentes materiales que componen la firma o sello electrónico, en cada uno de los procesos de validación de firma o sello, en las condiciones establecidas, además, por una política de validación o en forma de restricciones de proceso[824].

La primera modalidad del proceso prevista es la validación de una firma o sello electrónico básico, que devuelve como resultado el estado de validez de la firma o sello en el momento de la validación. Esta clase de firma o sello se puede validar mientras el certificado no haya sido revocado ni haya expirado en el momento de la validación, por lo que no es suficiente para las firmas o sellos sujetos a obligaciones legales de conservación a largo plazo.

La segunda modalidad del proceso prevista es la validación de una firma o sello con tiempo y disponibilidad a largo plazo de materiales de validación, que devuelve como como resultado el estado de validez de la firma o sello en el momento temporal más antiguo en el que se puede demostrar su existencia, por lo que se puede emplear para comprobar la validez de una firma o sello incluso después de la revocación del correspondiente certificado. Además, cuando se incorporan estos materiales de validación, como las listas de revocación de certificados, este proceso dispone de ellos a largo plazo para dichas validaciones. Es preciso, con todo, hacer notar que esta firma o sello se podrá validar sólo mientras estos materiales de validación estén vigentes.

Finalmente, el epígrafe 2 del artículo 32 del Reglamento concreta que "[e]l sistema utilizado para validar la firma electrónica cualificada ofrecerá a la parte usuaria el resultado correcto del proceso de validación y le permitirá detectar cualquier problema que afecte a la seguridad", previsión que se centra en el producto –típicamente una aplicación informática– que implanta el proceso de validación, como se puede ver en la Ilustración 15.

[821] En virtud de lo establecido en el artículo 40 del Reglamento eIDAS.

[822] Por razones metodológicas, al tercero de ellos nos referiremos al presentar el servicio de conservación de la firma o sello electrónico. Cfr. el epígrafe 4.3.3.2 de este trabajo.

[823] Estos procesos ejecutan tareas como la validación del formato técnico de una firma o sello electrónico, la identificación del certificado de firma o sello correspondiente, la selección de parámetros técnicos para la validación de la firma o sello, la comprobación de la actualidad de la información de estado relativa al certificado, la comprobación de la validez del certificado en el momento de la validación, la comprobación de la integridad de la firma mediante las correspondientes operaciones criptográficas – empleando los datos de validación de firma o sello contenidos en el certificado –, la comprobación de la presencia de determinados atributos en la firma o sello electrónico, y la presentación de la validación de la firma o sello electrónico. Cfr. el epígrafe 5.2 de la norma ETSI EN 319 102-1.

[824] Un ejemplo de esta posibilidad se encuentra en el RDENI y su importante Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración, al respecto de la cual puede verse (Alamillo Domingo, 2012).

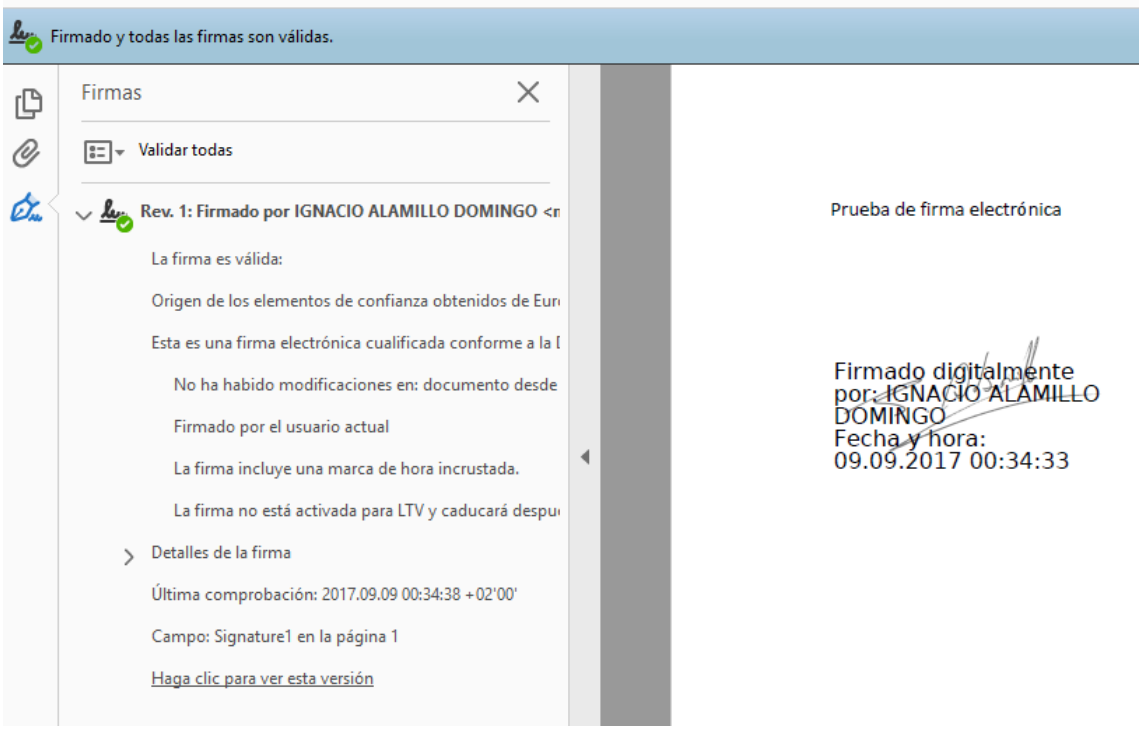


Ilustración 15. Ejemplo de visualización del resultado del proceso de validación de firma electrónica (elaboración propia)

En este sentido, es preciso aclarar que el proceso de validación de la firma o sello electrónico puede devolver tres resultados principales; a saber, "TOTAL-PASSED", cuando se han validado correctamente todos los elementos de la firma o sello electrónico; "TOTAL-FAILED", cuando ha fallado la comprobación criptográfica de la firma o sello, o se ha comprobado que la firma o sello fue creado después de la revocación o expiración del certificado, o que la firma o sello es sintácticamente incorrecto; y finalmente "INDETERMINATE", cuando alguna comprobación ha fallado, pero de ello no se desprende que la firma o sello sea necesariamente inválido, como por ejemplo cuando se valida una firma respaldada por un certificado expirado, porque en realidad dicha firma podría ser válida, siempre que se pueda determinar que fue creada antes de la expiración del certificado, algo que se podría acreditar si el documento y la firma han sido, por ejemplo, conservados en un archivo de la Administración Pública con las suficientes garantías.

4.3.2.2 Los requisitos del servicio

Como hemos visto, el Reglamento eIDAS define los elementos esenciales del proceso de validación de una firma o sello electrónico cualificado en los artículos 32.1 y 40, respectivamente, por lo que el servicio cualificado ofrecido deberá garantizar su cumplimiento.

En efecto, conforme al artículo 33.1.a) del Reglamento eIDAS –aplicable también al sello electrónico en virtud de lo establecido en el artículo 40 del propio Reglamento–, "[s]olo podrá prestar un servicio de validación cualificado de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que […] realice la validación de conformidad con el artículo 32, apartado 1 […]", proceso al que nos hemos referido en el

epígrafe inmediatamente anterior.

Adicionalmente, conforme al numeral b) del mismo artículo 33.1 del Reglamento eIDAS, se requiere al prestador del servicio que "permita que las partes usuarias reciban el resultado del proceso de validación de una manera automatizada que sea fiable, eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador cualificado de servicio de validación".

La norma se refiere a una suerte de informe de validación de la firma o sello electrónico, que va a servir como prueba electrónica justificativa de haberse realizado la citada validación.

Respecto a lo que debería incluir el citado informe, de nuevo resulta relevante la ya mencionada norma ETSI EN 319 102-1, que define los contenidos principales del resultado del proceso de validación de firma o sello electrónico, en sus diferentes variantes, puesto que también en este caso existe la posibilidad de que la misma sea establecida a efectos de la acreditación de la conformidad del servicio.

De esta forma, el artículo 33.2 del Reglamento eIDAS prevé que "[l]a Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas al servicio de validación cualificado al que se refiere el apartado 1", de modo que "se presumirá el cumplimiento de los requisitos establecidos en el apartado 1 cuando la validación de una firma electrónica cualificada se ajuste a dichas normas", debiéndose estos actos de ejecución adoptarse "con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2"[825]; y sin que hasta hoy se haya establecido norma alguna.

La norma prevé la posibilidad de que el informe sea de procesamiento automático, sin perjuicio de que la información sea presentada de forma comprensible para las partes usuarias que lo requieran, incluyendo informaciones como una indicación del estado correspondiente a los resultados del proceso de validación[826], una indicación de la política de validación o del conjunto de condiciones aplicables a la validación, la fecha y hora de la firma o sello que fue determinada en la validación y los datos de validación empleados para ello[827], la modalidad de proceso de validación empleada y determinadas informaciones adicionales, en función del resultado.

El Reglamento eIDAS no establece más requisitos específicos en relación con este servicio, al que resultan también aplicables los requisitos generales aplicables a los prestadores de servicios de confianza, sin cualificación[828] o con ella[829].

4.3.2.3 Los efectos jurídicos asociados al servicio

El Reglamento eIDAS no establece ningún efecto jurídico expreso y específico para este servicio, pero es innegable que el resultado del servicio –el informe de validación– es un elemento especialmente orientado a la facilitación de la prueba (administrativa o judicial) de la firma o sello electrónico cualificada, en especial desde el punto de vista de la parte

[825] Cfr. el epígrafe 1.4.2 de este trabajo.

[826] Para los que la propia norma establece sus valores y la semántica asociada.

[827] Como, por ejemplo, la fecha y hora de un sello de tiempo sobre la firma o sello electrónico, que demuestra su existencia en tal momento.

[828] Cfr. el epígrafe 6.1 de este trabajo.

[829] Cfr. el epígrafe 6.2 de este trabajo.

usuaria, que en muchas ocasiones precisará asistencia para estas tareas, así como a la libre circulación de las firmas y sellos electrónicos cualificados dentro de la Unión Europea. Se trata, en sí mismo, de una prueba electrónica relativa a la prueba electrónica que es la firma, en relación con el documento o mensaje firmado.

Sin embargo, este efecto jurídico implícito del servicio se dará, con su máxima intensidad, cuando la Comisión Europea establezca las correspondientes normas técnicas de proceso y servicio, puesto que el valor de disponer de un informe de validación con valor de presunción de conformidad con los requisitos legales correspondientes está fuera de toda duda.

Sin embargo, el hecho de que no se establezca, en el Reglamento eIDAS, un efecto jurídico específico para este servicio de confianza no significa que no se pueda establecer en sede nacional.

En este sentido, podemos citar los artículos XII.34 y XII.35[830] del Código de Derecho Económico belga, que establecen que la parte usuaria de una firma o sello electrónico cualificado disfrutará de la presunción de validez de dicha firma o sello electrónico cualificado si, ante de confiar en la firma o el sello, procede a su validación empleando un servicio cualificado conforme al Reglamento eIDAS[831]; lo cual es conceder, por cierto, más valor presuntivo a la firma o sello cualificado validado por tercero que la firma o sello cualificado validado por uno mismo.

Otro ejemplo de legislación nacional que otorga un efecto jurídico, en este caso al proceso de validación de la firma electrónica cualificada, y por tanto también al correspondiente servicio de confianza, lo encontramos en la nueva redacción de la sección § 371a (1) del Código alemán de Procedimiento Civil (*Zivilprozessordnung – ZPO*)[832], conforme a la cual la autenticidad aparente de una declaración en formato electrónico resultado del examen de la firma electrónica cualificada conforme al artículo 32 del Reglamento eIDAS sólo podrá ser cuestionada cuando haya serias dudas acerca de que dicha declaración haya sido realizada por la persona responsable.

---

[830] Incorporados por los artículos 20 y 21, respectivamente, de la *Loi du 21 julliet 2016, mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII "Droit de l'économie électronique" du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique*.

[831] Estos artículos no se encuentran aún en vigor, según dispone el *Arrêté royal fixant l'entrée en vigueur de la loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique; 14 septembre 2016*.

[832] Dada por artículo 11 (15) 3 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017). En su versión anterior, la sección § 371a (1) del ZPO venía a decir lo mismo, pero en relación a la firma que resultaba conforme a lo establecido en la Ley Marco para la Firma Electrónica (*Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)*, de 16 de mayo de 2001).

Como se puede ver, también en este caso se establece una clara presunción *iuris tantum* respecto a la validación, que beneficia especialmente a los prestadores cualificados para este servicio, lo cual resulta un claro incentivo a la adopción del servicio.

4.3.3 El servicio de confianza de conservación de la firma y sello electrónico

4.3.3.1 Caracterización del servicio

El servicio de conservación de firma o sello electrónico permite ampliar la fiabilidad de los datos de validación de la firma o sello electrónico cualificado más allá de su período de validez tecnológica inicial, necesidad que deriva de la tecnología criptográfica empleada, que pierde fortaleza a medida que transcurre el tiempo, principalmente por el incremento de la capacidad de cálculo y por la posible aparición de ataques que puedan afectar negativamente a los algoritmos[833].

Esta necesidad conecta con la existencia de documentos o mensajes de duración superior al de una firma o sello electrónico, por lo que hay que mantener[834] su validez jurídica, necesidad que identifica con bastante claridad el Reglamento eIDAS en su Considerando (61), cuando indica que la norma "debe garantizar la conservación a largo plazo de la información, es decir, la validez jurídica de la firma electrónica y los sellos electrónicos durante períodos de tiempo prolongados, garantizando que se puedan validar independientemente de la evolución futura de la tecnología", puesto que de otro modo se podrían ver afectadas las garantías de autenticidad e integridad del documento al que se han incorporado dichas firmas electrónicos y sellos electrónicos.

Este objetivo se podrá lograr acudiendo a diversas técnicas[835], incluyendo la incorporación, de forma protegida, de informaciones adicionales a la firma o sello electrónico o el empleo de repositorios de documentos firmados, que han sido inicialmente reguladas actualmente en la normativa nacional –como, por ejemplo, en España en la normativa de administración electrónica[836]–, que cabe imaginar quedará superada por la regulación europea, aplicable también al sector privado.

Antes de entrar en los requisitos del servicio, conviene hacer notar que el Reglamento eIDAS, a diferencia de la creación y validación de firma y sello electrónico, no regula cómo pueden el firmante o creador de sellos, o la parte usuaria (por ejemplo, el receptor del documento o mensaje firmado o sellado) conservar dicha firma o sello electrónico cualificado, algo francamente criticable por la evidente incompletitud que supone dicha

---

[833] Cfr. el epígrafe 6.2.6 y el Anexo A.1.2.3 de este trabajo.

[834] (Muñoz Soro, 2017, pág. 46) considera que "la conservación de documentos electrónicos auténticos no puede limitarse a una mera custodia pasiva, sino que para mantener su validez a lo largo de periodos extensos de tiempo es precisa la realización de determinadas operaciones y el cumplimiento de exigentes requerimientos técnicos".

[835] Se puede ver una experiencia de éxito en nuestro país referida al servicio de conservación en (Nualart Mercadé, 2008), aunque el mismo excede de lo que estrictamente es conservación de la firma o sello electrónico.

[836] Para un análisis completo del régimen previsto en el RDENI y su importante Norma Técnica de Interoperabilidad de Política de firma electrónica y de certificados de la Administración, véase (Alamillo Domingo, 2012), *in toto*.

laguna.

Quizá para evitar este problema, la legislación alemana autoriza[837], con carácter general a firmantes, creadores de sellos, partes usuarias y, por supuesto, prestadores de servicios que, cuando sea preciso, se puedan volver a proteger los datos que incorporen una firma electrónica cualificada, un sello electrónico cualificado o un sello de tiempo electrónico cualificado empleando medidas apropiadas, antes de que el valor de las firmas, sellos o sellos de tiempo disminuya a lo largo del tiempo; medidas que deberán encontrarse alineadas con las tecnologías más recientes[838].

4.3.3.2 Los requisitos del servicio

En este marco, el artículo 34.1 del Reglamento eIDAS –aplicable también al sello electrónico en virtud de lo establecido en el artículo 40 del propio Reglamento–, ordena que "[s]olo podrá prestar un servicio cualificado de conservación de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que utilice procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de la firma electrónica cualificada más allá del período de validez tecnológico", en una redacción que viene a contener dos requisitos para la prestación del servicio, de corte genérico, referido al empleo de procesos y tecnologías que permitan esta ampliación de la fiabilidad de la firma o sello más allá de su periodo de validez tecnológico.

Como se puede ver, el servicio se ordena a resolver un problema estrictamente técnico, en particular referido a la pérdida de seguridad de los algoritmos criptográficos empleados para la firma y sello electrónico cualificado, por lo que el requisito es únicamente disponer de la correspondiente tecnología, y aplicar el correspondiente proceso.

Resulta, sin embargo, criticable que no se establezca ningún requisito respecto a dicha tecnología o al proceso asociado, dado que de esta forma resulta francamente difícil para los operadores jurídicos determinar el alcance de las obligaciones asociadas al servicio.

Como en el servicio de validación de firma y sello electrónico cualificado, también en este caso podemos referirnos a las especificaciones y normas técnicas y, en concreto, a la ya menciona norma ETSI EN 319 102-1, que identifica tecnologías y contiene procesos para la creación y validación de firmas y sellos electrónicos, de forma que se pueda lograr este objeto de ampliación del periodo de validez técnica de estas pruebas electrónicas.

Más en concreto, esta norma, y en relación con las normas de formato de firma y sello electrónico[839], prevé la posibilidad de crear una clase de firma electrónica que ofrece disponibilidad a largo plazo e integridad de materiales de validación, mediante la adición de sellos de tiempo electrónico u otras tecnologías a una firma o sello electrónico avanzado, de forma que gracias a los mismos se pueda comprobar la validez de una firma o sello incluso –y en esto se diferencia de la segunda modalidad de proceso de validación– aunque haya expirado toda la información necesaria para la validación de los elementos que respaldan la firma, bien porque los certificados del prestador del servicio de confianza han expirado, bien porque se ha producido una pérdida crítica de la fiabilidad de alguno

[837] Cfr. la sección § 15 de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017).

[838] Previsiblemente, presumiéndose ello cuando este proceso se realice

[839] Cfr. ETSI EN 319 122, ETSI EN 319 132 y ETSI EN 319 142.

de los algoritmos criptográficos empleados.

Sería en este último caso en el que realmente podríamos hablar, de forma estricta, de conservación más allá del periodo de validez tecnológico de la firma o del sello, dado que el caso de la expiración del certificado que respalda la firma no predica nada acerca de la validez tecnológica de la firma o sello, que puede seguir siendo perfectamente adecuado y seguro. Dicha expiración podrá afectar, en función del caso, a la validez –o más correctamente, a la eficacia– jurídica de la firma o sello electrónico, pero sólo en caso de que no se pueda levantar la carga procesal con respecto a esta prueba electrónica.

De forma correspondiente, la norma ETSI EN 319 102-1 contiene una tercera modalidad del proceso de validación, prevista para la validación de esta clase de firma o sello, por lo que el servicio de validación podrá también procesar estas firmas o sellos electrónicos.

El Reglamento eIDAS no establece más requisitos específicos en relación con este servicio, al que resultan también aplicables los requisitos generales aplicables a los prestadores de servicios de confianza, sin cualificación o con ella[840].

Una duda importante que plantea este servicio es si el mismo implica que la conservación física del objeto de firma o sello deba correr necesariamente a cargo del prestador, o la pueden realizar el firmante o creador de sellos, o la parte usuaria; es decir, si esta conservación es un requisito del servicio.

A tenor de la dicción literal del Reglamento eIDAS, se puede entender que sería conforme al mismo un servicio que simplemente aplicara el proceso tecnológico previsto en las normas técnicas –por ejemplo, la adición de un sello cualificado de tiempo electrónico de archivo a la firma o sello electrónico cualificado–, devolviendo posteriormente la firma o sello modificada a la persona usuaria del servicio.

En contra de esta posibilidad se podría oponer que la denominación del servicio implica, en efecto, la obligación de conservación del objeto de firma o sello electrónico, pero dicha interpretación parecería excesiva, dado que nada más en el Reglamento la apoya. En este caso, además, seguramente se planteará el debate acerca del rol de las tradicionales instituciones de archivo[841] de documentos.

Más correcto parece la interpretación, que encuentra apoyo en las normas técnicas anteriormente aludidas, en cuya virtud la conservación física del objeto de firma o sello sería una opción técnica más para la ampliación del plazo de validez técnica de dicha firma o sello, alternativa o complementaria a la adición de sellos de tiempo electrónico de archivo, conforme al ejemplo anteriormente expuesto.

Esta interpretación ha sido expresamente adoptada por algún organismo de supervisión, como el francés[842], y es la que también adopta nuestra legislación del sector público, en

---

[840] Cfr. los epígrafes 6.1 y 6.2, respectivamente, de este trabajo.

[841] Para (Muñoz Soro, 2017, pág. 47), "[d]ada la dificultad y el coste que supone la creación de un servicio cualificado de confianza, cabe suponer que serán estas entidades las que se constituyan como prestadores de servicios cualificados de conservación de firmas y sellos electrónicos", aunque también admite que los archivos puedan limitarse a la conservación del documento, externalizando las operaciones de conservación de firma y sello a terceros.

[842] Cfr. los *Critères d'évaluation de la conformité au règlement eIDAS. Services de conservation qualifiés des signatures et des cachets électroniques qualifiés*, de 3 de enero de 2017, de ANSSI.

concreto en la Norma Técnica de Interoperabilidad de Política de firma y de sello electrónicos y certificados de la Administración, aprobada por Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas[843].

De forma consiste con lo que se acaba de indicar, tampoco es un requisito del servicio proceder a la conservación del documento o mensaje firmado o sellado, aunque ciertamente pueda resultar conveniente[844]; algo que en algún Estado ha supuesto la regulación, en sede nacional, del correspondiente servicio de confianza de archivo electrónico, como en Bélgica.

4.3.3.3 Los efectos jurídicos asociados al servicio

Como en otros casos, tampoco en este caso el Reglamento eIDAS establece ningún efecto jurídico expreso y específico para este servicio. A pesar de ello, el servicio produce un innegable efecto jurídico en el ámbito probatorio, facilitando la prueba de la firma o sello electrónico cualificado, en especial cuando haya transcurrido un plazo significativo de tiempo, y en todo caso, cuando se haya puesto en cuestionamiento la seguridad de alguno de los algoritmos en que se basó.

Ello resulta especialmente importante en documentos o mensajes que requieren un largo plazo de conservación, aunque hay que tener presente que la necesidad de conservar la firma o sello electrónico encuentra su límite natural en los plazos de prescripción y caducidad de las acciones, dado que puede tener poco sentido mantener el valor de la prueba electrónica cuando ya no se puede generar discusión procesal alguna acerca de la autenticidad de la firma o sello electrónico.

[843] Sobre este instrumento, cfr. (Alamillo Domingo, 2012) *in toto*, aunque referido a la versión anterior de la norma técnica en cuestión.

[844] Así lo recomienda, por ejemplo, el organismo de supervisión francés, aludiendo a la posible pérdida de validez técnica de algoritmo de resumen que, como sabemos, vincula al documento con la firma o sello. Para (Gobert, 2015, p. 37), el servicio de conservación de firma o sello electrónico viene a ser el embrión del servicio de archivo electrónico.

CAPÍTULO 5. LA REGULACIÓN DEL USO DE LA FIRMA ELECTRÓNICA Y DEL SELLO ELECTRÓNICO EN RELACIONES JURÍDICAS CONCRETAS

En este Capítulo, y después de haber presentado, en el Capítulo 4, el régimen jurídico aplicables a las fuentes de prueba electrónica relativas a la atribución de documentos a las personas físicas y personas jurídicas, y, en el caso de las primeras, también del consentimiento, esto es, ahora que conocemos la regulación jurídica generalmente aplicable a la firma electrónica y al sello electrónico, debemos dirigir nuestra atención a la particularidades que se presentan en relación con estas fuentes de prueba desde una perspectiva sectorial.

En efecto, en función del ámbito donde se vaya a emplear la firma electrónica o el sello electrónico encontraremos importantes concreciones en relación con dicho uso, que serán menores en las relaciones sujetas al derecho privado, donde la intervención del derecho público presenta una menor justificación y, por tanto, intensidad; y mayores en el caso de las relaciones con las entidades del sector público, en especial en la actividad formalizada.

Por consiguiente, el epígrafe primero de este Capítulo analiza el régimen de uso de la firma electrónica y del sello electrónico en aquellas relaciones sujetas al derecho privado, donde prima la autonomía de la voluntad de las partes, sin perjuicio de las excepciones que puedan establecerse, normalmente en atención a la necesaria protección de la parte débil.

Por su parte, en el epígrafe segundo se aborda el complejo régimen de uso de estas fuentes de prueba en el sector público español, que presenta una interesante evolución histórica digna de análisis, motivo por el cual se estudia la regulación de las denominadas condiciones adicionales al uso de la firma electrónica, hoy extintas, la regulación del uso de la firma electrónica y del sello electrónico en el procedimiento administrativo y judicial, por parte de ciudadanos, y, finalmente, la regulación del uso de estos por parte de las entidades del sector público, comparándose, por su indudable interés, el régimen anterior y posterior a la denominada "reforma del sector público".

5.1 EL RÉGIMEN DE USO DE LA FIRMA Y SELLO ELECTRÓNICOS EN LAS RELACIONES SUJETAS AL DERECHO PRIVADO

En este epígrafe analizaremos el régimen de uso de la firma y sello electrónicos *inter privatos* y, en concreto, y como hemos avanzado, y a reserva de los efectos jurídicos típicos que el Reglamento eIDAS establece en relación con la firma y sello electrónico cualificados, la posibilidad de que las partes hagan uso de su autonomía de la voluntad para regular dicho uso.

A estos efectos, hay que traer a colación el artículo 3.10 de la LFE, que establece que "a los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas", artículo que no tiene equivalente en el Reglamento

eIDAS, pero que no se puede considerar inaplicado por el mismo, sino al contrario[845]; y que ha desaparecido en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, sin que de ello tampoco pueda entenderse que se haya establecido una prohibición en este sentido.

En efecto, para las partes firmantes de un contrato, por ejemplo, una firma electrónica no cualificada puede ser perfectamente empleada como si fuera una firma manuscrita, y para ellos[846], dicha firma electrónica no cualificada debería tener la misma eficacia que la firma manuscrita; algo que deberá ser considerado por el Juez, dada la regla de no discriminación hoy contenida en el artículo 25.1 del Reglamento eIDAS a la que nos hemos referido anteriormente[847], pero sólo desde la perspectiva sustantiva, dado que las normas procesales no son disponibles por las partes.

Corresponde, sin embargo, al legislador nacional la potestad de modular el alcance de esta posibilidad, inclusive estableciendo límites a la autonomía de la voluntad de las partes[848].

Así sucede, por ejemplo, el artículo VII.78[849] del *Code de droit économique* belga, que

---

[845] El Considerando (16) de la DFE indicaba que "no se precisa un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado celebrados entre un número determinado de participantes", así como que "en la medida en que lo permita la legislación nacional, ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas"; esto es, el efecto que tendrán entre las mismas.

[846] (Illescas Ortíz, 2001, pág. 195) ya había notado que "[e]n cualquier caso, cuando por vía contractual se pacte la ampliación de los efectos de la FE sencilla aludida anteriormente, ha de tenerse en cuenta el universal efecto relativo de los contratos consagrado para España en el artículo 1.257.1 del Código Civil", de modo que "[e]llo ha de impedir que *a priori* efectos adicionales al de la identificación del emisor y la atribución del MD signado a tal emisor puedan ser aducidos frente a terceros ajenos al pacto de ampliación de los efectos probatorios de la FE sencilla", situación que se ha agravado al no establecerse, en el Reglamento eIDAS, efecto alguno para la firma electrónica no cualificada.

[847] Cfr. el epígrafe 4.2.2 de este trabajo.

[848] (Martínez Nadal, 2009, pág. 93) indicó, al respecto del artículo 3.10 de la LFE, que "esta previsión, en principio, puede resultar positiva para evitar determinados resultados excluyentes que puede provocar, como hemos visto, la regla de equiparación del art. 3.3 LFE", pero que "no obstante, puede resultar más problemática en aquellos supuestos en que las partes no se hallen en situación de igualdad, pudiendo dar lugar a imposiciones abusivas".

[849] En redacción dada por el artículo 9 de la *Loi 18 avril 2017, portant dispositions diverses en matière d'économie*, que modifica ligeramente la redacción anterior, dada por el artículo 17 de la *Loi 26 octobre 2015, modifiant le Code de droit économique et portant diverses autres dispositions modificatives*. La redacción original, dada por *Loi 19 avril 2014, portant insertion du livre VII "Services de paiement et de crédit" dans le Code de droit économique, portant insertion des définitions propres au livre VII et des peines relatives aux infractions au livre VII, dans les livres I et XV du Code de droit économique, et portant diverses autres dispositions*, se refería simplemente a la posibilidad de emplear una firma escrita o una firma electrónica, que debía ser conforme a la *Loi 9 juillet 2001, fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification*. La referencia a la firma cualificada se ha incorporado por artículo 29 de la *Loi 21 juillet 2016, mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII "Droit de l'économie électronique" du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique*.

regula la formalización del contrato de crédito al consumo[850], autorizando, junto al uso de la firma electrónica cualificada, el uso de cualquier otra firma electrónica, pero siempre que la misma garantice la identidad de las partes, su consentimiento al contenido del contrato de crédito y el mantenimiento de la integridad de dicho contrato, resultando la carga de la prueba necesariamente a cargo del profesional – y no del consumidor – y, lo que es más relevante, pudiendo el Rey puede establecer criterios para este propósito.

Esta normativa afecta a lo establecido en el artículo 1322, segundo párrafo[851], del *Code Civil* belga, que considera que un conjunto de datos electrónicos que se puedan atribuir a una persona determinada y que garanticen la integridad del contenido del acto satisface los requisitos de una firma escrita, algo muy importante porque esta regla se aplica con carácter general a la celebración de contractos por medios electrónicos a distancia, en virtud de lo establecido por el artículo XII.15[852] del *Code de droit économique*, en igualdad de condiciones que la firma electrónica cualificada.

Conforme a este enfoque, se puede dictar normativa específica relativa al tipo de firma electrónica a emplear en los contratos de crédito al consumo y los contratos de crédito hipotecario, debiendo ajustarse los profesionales a dichas normas, normas que parecen encontrar su legitimación en la protección de los consumidores.

Otro ejemplo lo encontramos en el Derecho alemán, aunque con una visión mucho más restrictiva, cuando la sección § 126a del *BGB* –Código Civil– impone el uso de la firma electrónica cualificada para la autenticación del soporte electrónico que sustituya a su correlato en soporte físico, cuando la normativa exija el uso de la forma escrita (*Schriftform*), aunque dicho requisito no es aplicable a la forma textual (*Textform*) prevista en la sección § 126b del *BGB*, ya que la misma no requiere, de hecho, de firma alguna.

A pesar de lo anterior, la sección § 127 (3) del *BGB* autoriza, excepto cuando se infiera la intención contraria de las partes, el uso de firmas electrónicas no cualificadas para cumplir el requisito de la forma electrónica –y, por tanto, de la forma escrita–, pero también indica que, en este caso, se puede posteriormente exigir la incorporación de una firma electrónica cualificada, o el registro notarial del contrato, lo que supone un potente límite a la autonomía de la voluntad de las partes, en especial en escenarios donde no resulte viable acudir a la firma electrónica cualificada, caso que se solicite la misma posteriormente, dado que en estos casos sólo podrá acudirse al citado registro notarial del contrato.

Nótese, sin embargo, que la reciente modificación del numeral 13 de la sección 309 del *BGB* prohíbe imponer a los adherentes a condiciones generales de la contratación requisitos de forma superiores, en sus declaraciones y comunicaciones con los predisponentes, al uso de una *Textform*, conforme a lo dispuesto en la ya mencionada

---

[850] En sentido similar se expresa el artículo VII.124 del *Code de droit économique* en relación con la formalización del contrato de crédito hipotecario.

[851] Incorporado por el artículo 2 de la *Loi 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire*.

[852] Incorporado por el artículo 3 de la *Loi 15 décembre 2003, portant insertion du Livre XII, "Droit de l'économie électronique" dans le Code de droit économique, portant insertion des définitions propres au Livre XII et des dispositions d'application de la loi propres au Livre XII, dans les Livres I et XV du Code de droit économique*, que en este punto traspone la Directiva 2000/31/CE, por cierto; modificado por el artículo 30 de la Ley de 21 de julio de 2016, antes mencionada.

sección 126b del *BGB*, por lo que en estos casos no será posible imponer el uso de la *Schriftform* y no se precisará firma alguna, y en caso de considerarse necesario disponer de alguna prueba del consentimiento, podrá pactarse el uso de cualquier clase de firma electrónica, siempre que el mismo no genere ningún obstáculo al ejercicio de los derechos de la parte débil.

Es evidente que se trata de un enfoque altamente restrictivo, que marca una clara preferencia por la firma electrónica cualificada o la forma escrita en soporte papel, pero no por otras tecnologías de firma electrónica.

Otro ejemplo, finalmente, lo encontramos en el derecho italiano, más en concreto, en el artículo 21.2-bis[853] del *Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (CAD)*, que impone el uso de la firma electrónica cualificada o de la firma digital en relación con doce actos jurídicos –principalmente relacionados con los derechos reales– previstos en el artículo 1350 del Código Civil, bajo pena de nulidad contractual, permitiendo el uso de otros tipos de firma electrónica, siempre que los mismos cumplan lo establecido en el artículo 20.1-bis del propio *CAD*.

En definitiva, a reserva de que la normativa se oponga, la autonomía de la voluntad de las partes permite la autorregulación del uso de los sistemas de firma electrónica no cualificada –así como de otros servicios de confianza, como por ejemplo el sello electrónico de persona jurídica, o el sello de tiempo electrónico– en sus relaciones jurídicas, sin que se precise una norma jurídica que específicamente habilite esta posibilidad.

Obviamente, el espacio para la autonomía de la voluntad de las partes va a verse limitado, como ya hemos visto en el ejemplo del derecho alemán, por los límites establecidos por el derecho del consumo, o el derecho laboral. En el caso español, resulta especialmente importante la posible consideración de dicho acuerdo como una cláusula abusiva, en los términos establecidos por el artículo 82 del TRLGDCU, que en su epígrafe 1 las caracteriza como aquellas "estipulaciones no negociadas individualmente y todas aquéllas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe causen, en perjuicio del consumidor y usuario, un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contrato", lo que incluye, en todo caso, aquellas que impongan indebidamente al consumidor la carga de la prueba, como se concreta en el epígrafe 2 del artículo 88 del mismo TRLGDCU, que considera en todo caso como abusiva la cláusula que suponga "la imposición de la carga de la prueba en perjuicio del consumidor y usuario en los casos en que debería corresponder a la otra parte contratante".

En este sentido, una cláusula relativa al uso de un sistema de firma electrónica no cualificada que imponga al consumidor la carga de la prueba será claramente considerada como abusiva[854], pero también deberá recibir esta consideración aquella, más sutil, que

---

[853] En redacción dada por artículo 21 del *Decreto legislativo 13 dicembre 2017, n. 217, Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*.

[854] Resultando la misma nula de pleno derecho y debiéndose tener por no puesta, conforme al artículo 83 del TRLGDCU y, además, constituyendo infracción en materia de defensa de los consumidores y usuarios,

obligue al consumidor a declarar que una firma electrónica no cualificada lo es, como hemos podido comprobar en algunos casos reales[855], dado que en este caso se produce, indirectamente, la misma inversión de la carga de la prueba.

Y también podrá resultar dudosa la cláusula predispuesta en que se "pacte" la equivalencia de una técnica de comunicación a distancia con la firma manuscrita, a cuyo efecto resulta interesante referenciar la Sentencia del Tribunal Supremo, Sala Civil, número 705/2015, de 23 de diciembre de 2015, que declara nula una cláusula predispuesta, por abusiva, en la que un Banco pactaba con su cliente la equivalencia entre la aceptación telefónica de una oferta con la firma manuscrita[856], al considerar que "se opone a lo dispuesto en los artículos 6 a 9 de la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores. En concreto, omite la remisión por escrito o en soporte duradero de las condiciones generales, y no hace mención a su remisión y recepción, que parece dar por supuesta, al referirse solo a las condiciones particulares. De donde resulta la vulneración de los arts. 88.2 y 89.1 del TRLGDCU en relación con el artículo 17 de la Ley 22/2007, al imponer al consumidor una manifestación de conformidad tácita con la recepción de unas condiciones generales y particulares que podría no haber recibido previamente y entrañar una inversión de la carga de la prueba sobre unos extremos cuya acreditación debería corresponder al banco"[857].

5.2 EL RÉGIMEN DE USO DE LA FIRMA Y SELLO ELECTRÓNICOS EN EL ÁMBITO DEL SECTOR PÚBLICO ESPAÑOL

En este epígrafe estudiaremos, por su importancia respecto al uso efectivo de los sistemas de firma electrónica, el régimen legal de uso de dichos sistemas –y de los correspondientes servicios de confianza– en el ámbito del sector público español, sin duda alguna el principal consumidor de estos servicios en la actualidad, régimen que se encuentra principalmente previsto en la legislación nacional, así como parcialmente en el

---

prevista en el artículo 49.1.i) de la misma norma.

[855] Por ejemplo, una importante aseguradora que opera en España incluye una cláusula en la que el consumidor debe aceptar que el sistema de firma electrónica – ni siquiera avanzada – que le suministra la compañía es un sistema de firma electrónica reconocida (hoy, cualificada), dada la evidente presunción de autenticidad que la misma recibe, y que supone la inversión de la carga de la prueba, excepto en el (seguramente extraño) caso de que el consumidor se aperciba del "engaño".

[856] El tenor literal de la cláusula en cuestión era el siguiente: "El Banco podrá ofertar al Titular la formalización de contratos y servicios mediante llamada telefónica a cualquiera de sus números de teléfono, fijos o móviles, que figuren en los registros del Banco. El Titular podrá aceptar la oferta del Banco mediante el contacto telefónico con el Banco. La aceptación de la oferta a través del referido contacto telefónico equivaldrá a todos los efectos a la firma manuscrita del Titular, y supondrá que el Titular ha recibido las condiciones particulares del mismo y que las acepta en su totalidad. Los correspondientes contratos se entenderán formalizados a partir del momento en que se produzca dicha aceptación. Todo ello sin perjuicio de cualquier otra documentación que el Titular y el Banco pudieran suscribir recogiendo la aceptación por el Titular de las condiciones contractuales".

[857] Sería interesante ver qué hubiera pasado de haberse acreditado la previa puesta a disposición de las condiciones generales y de las condiciones particulares, por ejemplo, acudiendo a un servicio de entrega electrónica certificada, en especial, cualificado.

Reglamento eIDAS.

Han sido diversas las normas nacionales que han establecido regulaciones específicas referidas al uso de la firma y el sello en el ámbito del sector público, entre las cuales encontramos normas de orientación general como la propia LFE, la LAE, la LUTICAJ, la LPAC y la LRJSP, así como también normas sectoriales, como en materia de contratación, de facturación al sector público y otras. A ellas nos referiremos a continuación.

5.2.1 El régimen inicial de uso de la firma electrónica en el sector público: las denominadas "condiciones adicionales"

La LFE dispuso en su artículo 4[858] determinadas especialidades en el uso de la firma electrónica en la Administración, conocidas en la DFE de forma genérica como "la excepción del sector público" y, en este sentido, su apartado 1 decía que "esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares", una norma que, en puridad, no parece necesaria, atendido el fundamento competencial de la LFE en el artículo 149.1 de la Constitución Española, competencias 8ª, 18ª, 21ª y 29ª, posteriormente complementada y ampliada de forma importante por la LAE –hoy sustituida por la LPAC y la LRJSP– y la LUTICAJ[859], pero que seguramente respondía a la previsión de la DFE de uso de la firma electrónica en las relaciones con el sector público[860], dada la especial relevancia de la forma de producción de los actos administrativos en el tradicional soporte papel[861].

Tras esta declaración genérica de sujeción a la LFE, el segundo párrafo del apartado 1 del artículo 4 de la LFE concretaba que "las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos", indicando también que "dichas condiciones podrán incluir, entre otras, la imposición de fechas

---

[858] Este artículo se debe entender inaplicado desde la entrada en aplicación del Reglamento eIDAS.

[859] Hay que recordar el carácter de leyes especiales de estas normas con respecto a la LFE.

[860] En concreto, el Considerando (19) de la DFE establecía, seguramente con un excesivo optimismo, especialmente visto en retrospectiva, que "la firma electrónica se utilizará en el sector público en el marco de las administraciones nacionales y comunitaria y en la comunicación entre dichas administraciones y entre éstas y los ciudadanos y agentes económicos, por ejemplo, en la contratación pública, la fiscalidad, la seguridad social, la atención sanitaria y el sistema judicial". Aunque ciertamente la Comisión impulsó el marco normativo apropiado para ello, lo cierto es que el impacto de uso de la firma electrónica avanzada ha sido más bien modesto, con excepciones singulares, aunque de gran volumen, como las relaciones con la Agencia Estatal de Administración Tributaria.

[861] Como explica (Valero Torrijos, 2013, pág. 62), "[l]a actuación de las Administraciones Públicas se ha venido realizando hasta ahora a través de la intervención directa de personas físicas, ya en su condición de titulares de órganos administrativos ya, de forma más genérica, como personal al servicio de aquéllas", de modo que "[e]n los casos en que se requiere específicamente el ejercicio de una competencia, el titular del órgano asume formalmente la decisión adoptada estampando su firma manuscrita ante un documento escrito, expresión a través de la cual se manifiestan normalmente los actos administrativo", por lo que en la adopción del soporte electrónico exigirá, de forma ineludible, la de la firma electrónica, con las previsiones adicionales que se consideren apropiadas para este entorno sectorial.

electrónicas sobre los documentos electrónicos integrados en un expediente administrativo", y finalmente definiendo la fecha electrónica como "el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados".

Estas condiciones adicionales al uso de la firma electrónica en el procedimiento administrativo, como se puede rápidamente intuir, suponían una alteración potencial importante del régimen liberal de uso de la firma electrónica, y exigían un adecuado tratamiento para cumplir su objetivo declarado, y no convertirse en un elemento de distorsión del mercado, especialmente desde la perspectiva de la creación de entidades de certificación públicas, inclusive en diversos niveles de la Administración[862].

Las condiciones adicionales se configuraron legalmente, siguiendo la DFE[863], como mecanismos legítimos de restricción potencial a la libre prestación y circulación de servicios de firma electrónica, por lo que resultaba necesario limitar el uso de esta posibilidad, y así lo hizo el legislador en el apartado 2 del artículo 4 de la LFE, disponiendo que "las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común", por cuanto la justificación jurídica de la citada restricción se podía encontrar, efectivamente, en el interés superior que representa el procedimiento administrativo, el cual exige garantías adicionales a las mínimas que puede ofrecer un mercado con calidades muy diversas, en especial desde la perspectiva de la admisibilidad, en las relaciones *inter privatos*, a acuerdos relativos al uso de la firma electrónica, que hemos tenido ya ocasión de analizar.

Además, el apartado 2 del propio artículo 4 de la LFE continuaba diciendo que "estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo", siguiendo a la DFE fielmente. Esta regla había sido, sin embargo, interpretada de forma ciertamente amplia por los Estados miembros de la Unión Europea, lo cual había afectado a la realización de la promesa de libre circulación de servicios y a la competencia efectiva[864].

---

[862] Cfr. al respecto, el análisis de iniciativas que autonómicas que realiza (Munar i Pascual, 2003), *in toto*.

[863] El artículo 3.7 de la DFE estableció que "los Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate. Estas prescripciones no deberán obstaculizar los servicios transfronterizos al ciudadano".

[864] (Dumortier, Kelm, Nilsson, Skouma, & Van Eecke, 2003, págs. 40 y ss., p. 99. y p. 148 y ss.), advirtieron sobre las dificultades de interpretación de algunos de los requisitos del artículo 3.7 de la DFE, como la necesidad de que las condiciones adicionales se refieran sólo a las características específicas de la aplicación de que se trate. Asimismo, indican que el establecimiento de condiciones generales de carácter general para todas las aplicaciones de administración electrónica puede afectar seriamente a la libre competencia del mercado de servicios y productos de firma electrónica, en cuyo caso la Comisión Europea debería intervenir, de acuerdo con lo establecido en la DFE y en el artículo 86 del Tratado de la Comunidad Europea. En concreto, dichos autores explicitan el riesgo de que las agencias públicas restrinjan sus aplicaciones a determinados certificados nacionales, en clara infracción del art. 3.7 de la DFE (como ha

En efecto, como tendremos ocasión de verificar *infra*, algunas de las condiciones adicionales exigidas en el ámbito de la administración electrónica[865] impidieron absolutamente el empleo de certificados expedidos por prestadores establecidos en otros Estados miembros de la Unión Europea, en una posible infracción del artículo 4 de la LFE y del artículo 3.7 de la DFE, del que trae causa.

Resulta especialmente importante resaltar la aparición, con posterioridad a la LFE, de normativa de la Unión Europea especialmente enfocada al uso transfronterizo de la firma electrónica, en particular la Directiva 2006/123/CE, relativa a los servicios en el mercado interior, a partir de la cual la Comisión adoptó dos Decisiones[866] de extraordinaria importancia porque determinación de un conjunto de requisitos que obligan a los Estados miembros a admitir, en cuanto destinatarios de documentos electrónicos, el uso de los sistemas de firma electrónica allí descritos[867], limitando la capacidad de los citados Estados para establecer condiciones adicionales que pudieran afectar negativamente a dichas Decisiones.

Respecto a la aprobación de las condiciones adicionales, el artículo 4.3 de la LFE previó que "las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica", regla sin embargo posteriormente alterada por el artículo 23.3 del RDLAE[868], que indica que "las condiciones generales adicionales a que se refiere el artículo 4.3 de la Ley 59/2003, de 19 de diciembre, se aprobarán mediante real decreto aprobado por el Consejo

---

venido sucediendo en España hasta la LAE. En el ámbito de las relaciones con la AEAT, hasta la Orden HAC/1181/2003, de 12 de mayo, únicamente se podía emplear el certificado Clase 2 CA de la FNMT-RCM).

[865] Por ejemplo, la exigencia de inclusión dentro del certificado de un extranjero del NIF español que tiene asignado – impuesta en aplicación de la Orden HAC/1181/2003, de 12 de mayo, hoy derogada – impedía de forma práctica que dicho extranjero pudiera emplear su sistema nacional de firma electrónica para realizar trámites con la AEAT.

[866] Se trata de la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las «ventanillas únicas» con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior, modificada por la Decisión de la Comisión 2010/425/UE, de 28 de julio de 2010, por la que se modifica la Decisión 2009/767/CE en lo relativo al establecimiento, el mantenimiento y la publicación de listas de confianza de proveedores de servicios de certificación supervisados o acreditados por los Estados miembros (cfr. el epígrafe 7.1.4.1 de este trabajo) y la Decisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE, relativa a los servicios en el mercado interior.

[867] Nótese que la Decisión 2011/130/UE se refiere a documentos producidos por las Autoridades competentes, que deben ser admitidos por las restantes Autoridades en la Unión Europea, mientras que la Decisión 2009/767/CE tiene un alcance más genérico, aplicable también a otros documentos que presentan los ciudadanos a las Autoridades competentes.

[868] Este artículo, curiosamente, no ha sido derogado en la reforma del RDLAE motivada por la aprobación de la LPAC y la LRJSP. Seguramente se debe entender inaplicado desde la entrada en aplicación del Reglamento eIDAS, al menos en lo referido a las condiciones adicionales que permite establecer.

de Ministros a propuesta conjunta de los Ministerios de la Presidencia[869] y de Industria, Turismo y Comercio[870], previo informe del Consejo Superior de Administración Electrónica". Nos referiremos inmediatamente a este artículo.

Finalmente, el apartado 4 del artículo 4 de la LFE indicó que "la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica", previsión de carácter general que no requiere de ulterior comentario en este momento[871].

5.2.2 El régimen de uso de la firma electrónica por parte de los interesados

5.2.2.1 El derecho a la admisión general de sistemas de firma electrónica, con anterioridad a la reforma del sector público

En el ámbito de la LAE y de la LUTICAJ, y en cierto modo en el marco del esquema de condiciones adicionales al uso de la firma electrónica a las que nos acabamos de referir, la admisión de los sistemas de firma electrónica de los interesados[872] se había previsto, con carácter general, en relación a aquellos sistemas que se basan en certificados electrónicos, y sin perjuicio del uso de otros sistemas, aunque con un cierto carácter residual.

Como ya hemos avanzado al referirnos a la identificación electrónica, y en el marco del artículo 6.2 de la LAE[873], el artículo 13.1 de la propia Ley determinaba que "las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos", referencia a la LFE que, a partir de 1 de julio de 2016 debía entenderse realizada ya a las previsiones del Reglamento eIDAS, anteriormente analizadas.

Y concretaba el apartado 2 del propio artículo 13 de la LAE[874], que "los ciudadanos

---

[869] Esta competencia, en la actualidad, correspondería al Ministerio de Hacienda y Administraciones Públicas.

[870] Esta competencia, en la actualidad, correspondería al Ministerio de Industria, Energía y Turismo.

[871] En relación con la aplicación de esta previsión a los certificados de empleados público, cfr. el epígrafe 2.1.4.3 de este trabajo.

[872] Conforme al Dictamen de la Abogacía del Estado 26/12, de 2 de abril de 2012, "el valor de los distintos tipos de firma electrónica diferentes de la firma electrónica reconocida vendrá dado por la circunstancia de que la Administración los haya admitido; una vez que la Administración haya admitido un determinado sistema de firma electrónica distinto de la firma electrónica reconocida, ese sistema de firma electrónica admitido por la Administración tendrá validez jurídica" (Abogacía General del Estado, 2013, pág. 351).

[873] Recordemos que su epígrafe g) establecía el derecho de los ciudadanos "a obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública", y su epígrafe h), el de "la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas".

[874] En su redacción por Ley 15/2014, de 16 de septiembre. En su redacción original, este apartado se refería a los "sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido,

podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

a) En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.

b) Sistemas de firma electrónica avanzada basados en certificados electrónicos reconocidos.

Las Administraciones Públicas deberán admitir todos los certificados reconocidos incluidos en la "Lista de confianza de prestadores de servicios de certificación" (TL) establecidos en España, publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen".

En sentido análogo, también la LUTICAJ ha establecido, en su artículo 4.2.f), el derecho de los ciudadanos a "utilizar los sistemas de identificación y firma electrónica del documento nacional de identidad o cualquier otro reconocido para cualquier trámite electrónico con la Administración de Justicia en los términos establecidos por las leyes procesales", y en su artículo 6.1.d), el derecho de los profesionales del ámbito de la Justicia a "utilizar los sistemas de firma electrónica del Documento Nacional de Identidad o cualquier otro reconocido, siempre que dicho sistema le identifique de forma unívoca como profesional[875] para cualquier trámite electrónico con la Administración en los términos establecidos por las leyes procesales".

Adicionalmente, el artículo 14.1 de la LUTICAJ concreta que "la Administración de Justicia admitirá, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y resulten adecuados para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos".

Sistemas que se concretan, como en la LAE, en el apartado 2 del propio artículo 14 de la LUTICAJ, que indica que "sin perjuicio de lo dispuesto en los artículos 4 y 6 de la presente Ley y en todo caso, con sujeción estricta a lo dispuesto por las leyes procesales, los ciudadanos y profesionales del ámbito de la Justicia podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con la Administración de Justicia:

a) Los sistemas de firma electrónica incorporados al Documento Nacional de Identidad,

---

admitidos por las Administraciones Públicas", en una dicción más amplia, que también permitía la admisión de sistemas de firma avanzada no basada en certificado, o de firma electrónica avanzada basada en certificado no reconocido.

[875] Nótese la diferencia de tratamiento en cuanto al sistema de firma electrónica considerado admisible para los ciudadanos y para los profesionales. Puesto en el contexto de los sistemas de firma electrónica avanzada basada en certificado electrónico reconocido, se aprecia que en el primer caso el legislador se está refiriendo a certificados individuales (de persona física, de persona jurídica o de entidad sin personalidad jurídica); mientras que en el segundo sólo se refiere a certificados individuales y, además, con un atributo específico. Para (Cotino Hueso & Montesinos García, 2012, pág. 187), la "diferencia se explica por las limitadas cualidades del DNI electrónico".

para personas físicas.

b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones públicas.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen".

Nótese, tanto en la LAE como en la LUTICAJ, el empleo de la forma imperativa del verbo "admitir", en línea con el derecho de ciudadanos[876] –y, en su caso, profesionales– al uso de los sistemas de firma electrónica, que no constituye, pues, una decisión discrecional o de concesión graciable por la Administración, sino una verdadera obligación jurídica[877], exigible siempre que se cumplan las condiciones legales establecidas en la normativa aplicable[878].

El legislador de la LAE y de la LUTICAJ podría haber empleado otros verbos menos exigentes, si no hubiese querido imponer una verdadera obligación a la Administración[879]. Por otra parte, tratar la admisión de sistemas de firma electrónica como una cuestión puramente discrecional afectaría a las legítimas expectativas de las personas adquirentes de sistemas de firma electrónica basada en certificados, expectativa que deriva directamente de la DFE y de la LFE, y que podría dar lugar a potentes distorsiones del mercado, como había venido sucediendo con la admisión exclusiva del certificado dela FNMT-RCM en las relaciones con la AEAT y otras entidades públicas, que venía a apoyar –seguro que de forma involuntaria por los gestores públicos correspondientes– un monopolio *de facto* no amparado ni por el derecho comunitario ni por la legislación española.

Es cierto que el artículo 13.2 de la LAE parecía matizar la obligación[880] de admitir los sistemas de firma electrónica que se contiene en el apartado 1 de ambos artículos, por

---

[876] (Martín Delgado, 2012, págs. 554-555), opina que las personas jurídicas y las entidades sin personalidad jurídica no gozan en la LUTICAJ del derecho a la admisión de sus sistemas de firma electrónica, debido a la omisión de una definición de ciudadano que las incluya, a diferencia de la LAE, omisión que considera "muy criticable, por cuanto supone retroceder y no incorporar a este ámbito el avance producido en el marco de las relaciones jurídico-administrativas", si bien también reconoce que "las mismas actuarán en juicio normalmente asistidas por abogado y procurador, con lo que la omisión tiene efectos limitados".

[877] En este sentido, resultaba clarificadora la exposición de motivos de la LAE cuando indicaba que "también se establece la obligación para cualquier Administración de admitir los certificados electrónicos reconocidos en el ámbito de la Ley de Firma Electrónica", manifestación menos asertiva en la exposición de motivos de la LUTICAJ, que sencillamente alude a que, en cuanto a los ciudadanos, "se contempla la posibilidad de uso de diversos sistemas de firma electrónica además del incorporado al Documento Nacional de Identidad", diferencia de intensidad que puede venir motivada por el diferente nivel de madurez tecnológica en la Administración de Justicia, o porque ya no considerase el legislador tan importante afirmar este derecho, más ampliamente extendido que en el momento de redacción de la LAE.

[878] Que incluyen los requisitos establecidos directamente en la propia LAE y LUTICAJ, así como las condiciones adicionales que se puedan establecer para salvaguardar las garantías de cada procedimiento.

[879] Como se ha avanzado anteriormente, en la DFE se partía del necesario uso de la firma electrónica en las relaciones con el sector público.

[880] No así la LUTICAJ, que no contiene esta referencia "a lo que cada Administración determine", sino una referencia a la sujeción estricta a las leyes procesales.

cuanto indicaba que el uso de los sistemas de firma electrónica se realizará "de acuerdo con lo que cada Administración determine", pero en nuestra opinión ello no implicaba que la decisión de admitir o no un sistema de firma electrónica fuera puramente discrecional de cada Administración, dado que ello implicaría vaciar de contenido el derecho reconocido en el artículo 6.2.h) de la LAE, y en los artículos 4.2.f) y 6.2.d) de la LUTICAJ.

En ambas leyes, resulta llamativo que no se garantizase ningún tratamiento privilegiado[881] en relación con la admisión de la firma electrónica reconocida, a pesar de que la LFE –y ahora el Reglamento eIDAS– la configuraba como la única firma electrónica directamente equivalente a la firma manuscrita[882], con el valor probatorio reforzado derivado de la presunción establecida por la LFE, y justamente en el momento en que se empezaba a disponer de un volumen masivo de unidades de DNI electrónico, que es precisamente una firma electrónica reconocida, y de hecho especialmente segura.

De hecho, puede indicarse que sólo el DNI electrónico recibió un tratamiento privilegiado, derivado de la obligación general de aceptación[883] del mismo que se contiene en el artículo 16 de la LFE, y que se plasmaba en la no necesidad de admisión previa del mismo[884]. Las referencias que se realizaban en los artículos 13.2.a) y 14 de la LAE a que el DNI electrónico se podrá utilizar "en todo caso y con carácter universal" resultaban bastante reveladoras de la voluntad del legislador de la LAE, en detrimento de las restantes firmas electrónicas reconocidas, que en la LFE reciben el mismo valor y

---

[881] Hay diversas razones, sin embargo, que avalan este tratamiento, en especial a la luz de la normativa de la Unión Europea que, en el marco de la Directiva de servicios, impone a los Estados miembros la obligación de admitir los sistemas de firma electrónica avanzada basada en certificado supervisado, como tendremos ocasión de analizar detalladamente.

[882] Sin perjuicio de que también otros tipos de firma electrónica también puedan producir efectos y sustituir las firmas manuscritas, como ya hemos analizado.

[883] En otro lugar me he referido a los efectos del DNI electrónico sobre el mercado de la certificación. Cfr. (Alamillo Domingo & Urios Aparisi, 2004). No he alterado ni un ápice esta opinión, y efectivamente la experiencia ha demostrado la inviabilidad de comercializar certificados de persona física (sin atributos extra, como la representación o la colegiación), y la desaparición total de la competencia en este caso. Sólo iniciativas públicas financiadas a cargo del presupuesto público –en particular el certificado Clase 2 CA o de la FNMT-RCM o el certificado idCAT del Consorcio AOC– pueden hoy convivir con el DNI electrónico, y en nuestra opinión sencillamente por su mayor facilidad de uso, que ciertamente deriva de su menor seguridad técnica. En sentido similar, (Dumortier, Kelm, Nilsson, Skouma, & Van Eecke, 2003, pág. 149) indican que el establecimiento, por las Administraciones Públicas, de servicios de certificación para su uso exclusivo en los procedimientos administrativos resulta posible, pero que el uso de dichos servicios para otros usos resulta inadmisible en términos de competencia efectiva, constituyendo una barrera al mercado interior. También (Martínez Nadal, 2009, pág. 279) considera, al referirse al DNI electrónico, que "la coexistencia de estos operadores privados con una autoridad de certificación pública que emite certificados altamente fiables, admisibles para usos generales y probablemente gratuitos o de bajo coste para el solicitante, puede resultar cuanto menos problemática desde el punto de vista empresarial, mientras que desde el punto de vista jurídico habría de analizarse su incidencia en los principios legales (de origen comunitario) que consagran la libre competencia en el mercado de los prestadores de servicios de certificación".

[884] Nótese que cuando el legislador se refiere al DNI electrónico no lo cualifica nunca de sistema "admitido", cosa que sí hace de forma expresa cuando se refiere a los restantes sistemas de firma electrónica avanzada. Además, en la LUTICAJ el legislador se refiere, en los artículos 4.2.f) y 6.2.d) al derecho a "utilizar los sistemas de firma electrónica del Documento Nacional de Identidad o cualquier otro reconocido", lo cual sólo puede generar mayor confusión en este ámbito.

efectos jurídicos de firma electrónica que el DNI electrónico.

Se trató de un cambio importante de enfoque con respecto al régimen anterior – en el que se venía considerando que sólo se podría emplear la firma electrónica reconocida, que era la única que se podía considerar directamente equivalente a la firma escrita –, que derivó principalmente de la aplicación de los principios de seguridad y proporcionalidad que informan la LAE[885] y la LUTICAJ[886], y que obligó a replantear gran parte del debate sobre los tipos y niveles de firma electrónica adecuados para cada procedimiento, pasando de la exigencia de la firma electrónica reconocida en base al principio de estricta equivalencia funcional, a la necesidad de realizar un análisis de riesgo para establecer el nivel de equivalencia material entre el procedimiento presencial existente y su versión electrónica.

Concretaba el artículo 15.1 de la LAE que "los ciudadanos, además de los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, referidos en el artículo 14, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos", previsión absolutamente redundante con los artículos 13.2.b) y 14 de la LAE, concretando en su epígrafe 2 que "la relación de sistemas de firma electrónica avanzada admitidos, con carácter general, en el ámbito de cada Administración Pública, deberá ser pública y accesible por medios electrónicos", la cual "incluirá, al menos, información sobre los elementos de identificación utilizados así como, en su caso, las características de los certificados electrónicos admitidos, los prestadores que los expiden y las especificaciones de la firma electrónica que puede realizarse con dichos certificados".

Este segundo epígrafe fue interpretado, en línea con la redacción original del epígrafe 2.b) del artículo 13 de la LAE, en el sentido de que permitía a cada Administración decidir discrecionalmente admitir los certificados reconocidos que considerase oportuno, discriminando al resto de certificados reconocidos, por lo que fue derogado, con ocasión de la modificación de dicho epígrafe, por el artículo 24.2, segundo apartado, de la Ley 15/2014, de 16 de septiembre, reforzando el derecho a la admisión de todos los certificados reconocidos.

Desde luego llama la atención la generosidad con la que el legislador de la LAE parecía estar dispuesto a admitir los sistemas de firma electrónica, aspecto con el que nos encontramos, en principio, de acuerdo, dado que con ello se preserva la neutralidad tecnológica[887]. Además, la referencia expresa a los sistemas basados en certificado electrónico reconocido, apuntaba de forma evidente al empleo de los certificados de firma electrónica no basados en dispositivo seguro de creación de firma, muy extendidos en la práctica.

Esta diversidad de sistemas de firma electrónica disponible en el mercado podía implicar un excesivo –e injustificado– esfuerzo técnico y económico por parte de la

---

[885] Artículo 4, apartados f) y g), y artículo 27.5, ambos de la LAE.

[886] Aunque dichos principios no se mencionan de forma explícita en la LUTICAJ, cfr. artículo 33.4 de la propia LUTICAJ, análogo al correlativo 27.5 de la LAE.

[887] La legislación española parecía en este punto bastante correcta. (Dumortier, Kelm, Nilsson, Skouma, & Van Eecke, 2003, pág. 149), consideran que una legislación que exigiese en términos estrictos el uso de sistemas de firma electrónica reconocida sería incompatible con la DFE. Parece que esta posición ha sido acogida con carácter general en el Derecho comunitario y español.

Administración Pública receptora de firmas electrónicas, de forma que la LAE contenía previsiones destinadas a concretar, de todos los sistemas de firma electrónica avanzada potencialmente admisibles, cuáles debían serlo en cada caso concreto –esto es, qué sistemas de beneficiaban de este "derecho de admisión"–, con base en un análisis de riesgos, pero siempre que normativamente no se hubiere impuesto un sistema de firma electrónica específico para dicha actuación.

5.2.2.2 La imposición normativa de sistemas de firma electrónica para actuaciones concretas

En algunos casos, la normativa aplicable ha optado por la imposición de sistemas específicos de firma electrónica, en relación con actuaciones concretas, limitando la posibilidad del órgano competente de acudir a un análisis de riesgos para tomar dicha decisión.

Por ejemplo, la legislación reguladora de la contratación del sector público ha venido exigiendo el uso de la firma electrónica cualificada, aunque con una cierta vacilación a lo largo de las sucesivas reformas que la misma ha sufrido.

En efecto, y con el antecedente directo del artículo 7.1 del Decreto 96/2004, de 20 de enero, por el que se regula la utilización de los medios electrónicos, informáticos y telemáticos en la contratación de la Generalitat de Cataluña, la disposición adicional decimonovena 1.f) de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público (LCSP/2007) previó la necesidad de emplear una firma electrónica reconocida conforme a la LFE para todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tuvieran efectos jurídicos y se emitiesen tanto en la fase preparatoria como en las fases de licitación, adjudicación y ejecución del contrato.

Esta previsión se mantuvo en el Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público (TRLCSP), en su disposición adicional decimosexta 1.f), hasta su modificación por Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público, se refirió a la "firma electrónica avanzada reconocida" –hoy, una firma electrónica cualificada–, en una dicción bastante extraña que ha generado dudas acerca de si seguía siendo exigible el máximo nivel de firma electrónica previsto en la LFE o no.

En todo caso, la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP/2017), que de nuevo incorpora en términos casi idénticos la regulación del TRLCSP, ha variado el régimen legal expuesto, pero sólo en el sentido de remitir a Orden ministerial la determinación de "las condiciones de utilización de las firmas electrónicas en los procedimientos de contratación del Sector Público", a pesar de que esta previsión se enmarca en un modelo enfocado al análisis de riesgos[888].

[888] Sobre esta cuestión, cfr. (Alamillo Domingo, 2017, pág. 384 y ss.), donde explico que, conforme a lo establecido en el artículo 22.6.c) de la Directiva 2014/24/UE, "será el legislador nacional o, en su defecto, cada poder adjudicador el que deba determinar en qué casos exige o no la firma electrónica – aunque cabe pensar que se exigirá siempre que exista una declaración de voluntad– y el tipo de firma electrónica a

También en conexión con la contratación del sector público, la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público exige que las facturas electrónicas incorporen, al menos, una firma electrónica avanzada basada en un certificado reconocido[889] –hoy, un certificado cualificado–, autorizando también (con anterioridad a la aprobación del Reglamento eIDAS, pero con un clara inspiración en la Propuesta de Reglamento) el uso de un sello electrónico avanzado de persona jurídica o de entidad sin personalidad jurídica, basado en un certificado reconocido que reúna los requisitos previstos en el artículo 5.2 de la Ley 25/2013[890].

5.2.2.3 La concreción de la admisión de sistemas de firma electrónica

Las notas principales que determinaban con carácter general la posibilidad de la efectiva admisión, por la Administración, de los diferentes sistemas de firma electrónica eran las siguientes: de un lado, el cumplimiento de la LFE –y, desde el 1 de julio de 2016, también del Reglamento eIDAS– por los sistemas a emplear, cuyos caracteres generales hemos expuesto anteriormente y, en concreto, el empleo de certificados electrónicos que cumplieran lo establecido en la LAE, dada la preferencia de la LFE por estos mecanismos; y, de otro, la adecuación de los citados sistemas para la función de garantía de la autenticidad e integridad de los documentos electrónicos; es decir, la determinación de la idoneidad del sistema para el caso concreto.

5.2.2.3.1 La verificación del cumplimiento de la legislación de firma electrónica

Los sistemas de firma electrónica a admitir, en especial aquellos basados en certificados[891], debían ser conformes con la legislación reguladora de aquélla, como es

---

emplear, en el marco de seguridad –que ya hemos visto se encuentra en el Esquema Nacional de Seguridad– y de la legislación de procedimiento administrativo", pudiéndose incluso "permitir el uso del sello electrónico avanzado basado en certificado cualificado, y el sello electrónico cualificado, para la actuación directa de las personas jurídicas –la mayoría de los operadores económicos– en sus comunicaciones y actuaciones con los poderes adjudicadores. Diversos Estados de la Unión, como Bélgica o Alemania, ya permiten de forma expresa esta opción en los procedimientos de contratación". En contra de esta posición parece haberse mostrado (Martínez Gutiérrez, 2009, pág. 153), cuando indica que "con la regulación establecida en el artículo 22.6.c) de la DCPUE […] el legislador comunitario parece optar únicamente por sistemas de firma electrónica avanzada o reconocida en los que se garantiza un alto nivel de seguridad y para los que se establecen requisitos adicionales que aseguren un adecuado nivel de interoperabilidad en materia de firma electrónica, fundamentalmente cuando no vayan a emplearse los formatos de firma estándar contenidos en la propia normativa comunitaria". En mi opinión, el legislador lo que hace es imponer exigencias de interoperabilidad cuando se emplee firma electrónica avanzada, pero sin limitar la capacidad de cada poder adjudicador de decidir si requiere de ese mecanismo, en función del riesgo.

[889] Esta firma deberá ser conforme al artículo 10.1 a) del Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, que se refiere a la "firma electrónica avanzada de acuerdo con lo dispuesto en el artículo 2.2 de la Directiva 1999/93/CE […] basada, bien en un certificado reconocido y creada mediante un dispositivo seguro de creación de firmas […] o bien, en un certificado reconocido", referencia que hoy debe entenderse realizada al Reglamento eIDAS.

[890] Estos requisitos han quedado claramente absorbidos, desde el 1 de julio de 2016, por el Reglamento eIDAS, hasta el punto de que debe considerarse que el artículo 5.2 citado ha quedado inaplicado.

[891] Y es que, como hemos visto, de acuerdo con el artículo 15.1 de la LAE, "los ciudadanos, además de los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, referidos en el artículo

lógico. Dicha verificación resultaba precisa, como resulta fácil de ver, a efectos de confiar en el sistema de firma electrónica a admitir, y corresponde a la Administración actuante realizarla; verificación del cumplimiento que podía resultar bastante compleja, especialmente porque, como hemos visto, la actividad de prestación de servicios de certificación no se encontraba sujeta por la LFE a autorización previa[892], y además no se había dictado ningún reglamento de desarrollo de la LFE que concretase o detallase las condiciones de prestación de dichos servicios.

No hay que olvidar, sin embargo, que en la LFE los prestadores de servicios de certificación debían comunicar el inicio de su actividad a la autoridad administrativa competente para su supervisión –actualmente la Secretaría de Estado de Sociedad de la Información y Agenda Digital, del Ministerio de Economía y Empresa[893]–, de acuerdo con lo que establecía el artículo 30 de la citada ley, y que dicha información era publicada por el supervisor en su sede electrónica, en forma de base de datos consultable[894] y en forma de Lista de Servicios de Confianza (o TL[895]) firmada electrónicamente por el citado órgano, lista que se ha mantenido y potenciado en el Reglamento eIDAS, según hemos podido ya analizar.

En definitiva, en la LAE se previó la admisión potencial de todos los sistemas de firma electrónica, pero también se limitó el derecho de uso de los sistemas de firma electrónica a los certificados expedidos por prestadores que al menos hubieran comunicado al supervisor el inicio de su actividad, asumiendo que en dicho caso los certificados cumplían lo establecido en la LFE, asunción que podría, por supuesto, resultar incorrecta, pues la posibilidad de ser supervisado no equivalía a cumplimiento efectivo de la legislación[896].

Además, el artículo 21 de la LAE reguló, en su apartado 1, criterios para la admisión en

---

14, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos", previsión absolutamente redundante con los artículos 13.2.b) y 14 de la LAE.

[892] Hasta la entrada en aplicación del Reglamento eIDAS, que como hemos visto sí que crea un sistema de autorización administrativa previa, aunque sólo para los servicios cualificados.

[893] Conforme al artículo 16 del Real Decreto 355/2018, de 6 de junio, por el que se reestructuran los departamentos ministeriales.

[894] Dicho servicio de consulta se encuentra disponible en la sede electrónica del Ministerio, accesible en la dirección https://sedeaplicaciones.minetur.gob.es/Prestadores/.

[895] *Trusted List* española, disponible en la sede electrónica del Ministerio, y que a su vez se encuentra referenciada en la TL de la Unión Europa, publicadas inicialmente en cumplimiento de lo establecido en la Decisión de la Comisión 2009/767/CE, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas, y, desde el 1 de julio de 2016, del artículo 22 del Reglamento eIDAS (cfr. el epígrafe 7.1.4.1 de este trabajo).

[896] Aunque el supervisor realmente era meticuloso en los procedimientos de comunicación de inicio de la actividad, lo cierto es que su capacidad de "no darse por comunicado" o de influir de forma profunda en la configuración del servicio de certificación objeto de la comunicación, resultaba ciertamente limitada, en ausencia de un Reglamento de desarrollo de la LFE que concretase los detalles técnicos de la actividad de prestación de servicios de certificación. En todo caso, dado que la LAE, desde su reforma por Ley 15/2014, de 16 de septiembre, impuso a las Administraciones la obligación de admitir todos los certificados contenidos en la TL para la firma electrónica, se había reforzado el incentivo legal de constar en dicha TL por parte de los prestadores, lo cual a su vez tuvo el efecto de incrementar el poder regulador indirecto del supervisor.

general, de forma reglada, mientras que, por el contrario, en el apartado 2 reguló la admisión de otros sistemas de firma electrónica empleados por las AAPP, en este caso bajo principios de reconocimiento mutuo y reciprocidad.

En este sentido, el apartado 1 del artículo 21 disponía que "los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por las Administraciones Públicas como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones Públicas la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas".

En nuestra opinión, el artículo 21.1 de la LAE establecía un marco razonable y equilibrado dentro del cual se podía considerar un "derecho de admisión" de la firma electrónica[897]. Obviamente, sólo los certificados electrónicos reconocidos garantizan una calidad en la identificación del firmante[898], por lo que no parecía haber nada que objetar en este punto. Asimismo, la condición de gratuidad en el uso promovía de forma efectiva la admisión del certificado, que no estaría garantizada en caso de que la Administración debiera pagar un coste al prestador[899], y que ha sido expresamente impuesto, como ya hemos indicado anteriormente, por el Reglamento eIDAS con carácter general.

Tampoco se podía objetar a la condición de puesta a disposición, por el prestador, de la información "que sea precisa", que se refería a la información sobre el estado de revocación del certificado, si bien generaba mayor inseguridad que deban hacerlo "en condiciones que resulten tecnológicamente viables[900]", texto de una cierta oscuridad. En efecto, aunque la LFE no imponía un formato técnico ni de certificado ni de mecanismos de información de estado de vigencia de los certificados, todos los prestadores que operaban en el mercado se basaban en los mismos estándares, por lo que en general se debía considerar que todos los certificados emitidos en España resultaban potencialmente admisibles.

---

[897] Cfr. (Martín Delgado, 2010, pág. 495 y ss.), quien indica, por una parte, que la LAE no contiene ninguna disposición que regule las condiciones que deben cumplir los certificados para poder ser admitidos, si bien posteriormente analiza las condiciones del artículo 21 de la LAE, que encuentra excesivamente vagas. Cfr. también (Martín Delgado, 2012, pág. 518 y ss.) en relación con el tratamiento de esta cuestión en la LUTICAJ.

[898] Esta manifestación es cierta incluso en el caso de certificados reconocidos con seudónimo, ya que el prestador del servicio de certificación conoce la identidad real.

[899] En este caso se plantearían problemas de diversa índole, especialmente en el caso de prestadores privados de servicios de certificación: ¿quién decidiría los precios?, ¿existiría un debe de admitir certificados a todos los prestadores? o ¿serían aceptables modelos de negocio como el de la FNMT-RCM, en el que las Administraciones usuarias abonan un coste ligado al volumen de población residente, en lugar de pagar por el número de certificados electrónicos efectivamente expedidos? La aplicación de la propia legislación de contratos del sector público, en nuestra opinión, impondría la obligación de tratar esta admisión como una cuestión contractual sujeta a la ley, cuyo tratamiento resultaría extraordinariamente complejo. En nuestra opinión, en este escenario sencillamente el derecho de admisión sería sencillamente inviable y quedaría vacío de contenido.

[900] La explicación a este requisito deriva a la ausencia de normativa legal o reglamentaria que concrete, desde un punto de vista técnico, las obligaciones de suministro de información de estado de certificados. Dada la diversidad de mecanismos técnicos disponibles, incluyendo listas de revocación de certificados (CRL), servicios en línea de información de estado de certificados (OCSP, SCVP, XKMS) o incluso depósitos web de consulta manual, parece necesario prever alguna restricción en este sentido.

Sin embargo, y en el marco de las condiciones generales al uso de la firma electrónica previstas en el artículo 4 de la LFE, al que nos hemos referido anteriormente, el apartado 1 del artículo 23 del RDLAE indica que "los prestadores de servicios de certificación admitidos deberán cumplir las obligaciones de la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como las condiciones generales adicionales a que se refiere el apartado 3", ampliando de forma importante las posibilidades de limitar el derecho de admisión previsto en el artículo 21.1 de la LAE, que acabamos de analizar; y sin que nada se diga acerca de la aprobación de condiciones adicionales, generales o particulares, por parte de otras Administraciones públicas, ni tampoco respecto de la aprobación de condiciones adicionales particulares por los órganos u organismos de la Administración General del Estado.

Cabe pensar, en cualquier caso, que esta posibilidad resultaba plenamente posible, excepto cuando el procedimiento viniera regulado por normas imperativas de la Unión Europea, como hemos visto sucede en el caso de la Directiva de servicios; y que el instrumento normativo apropiado sería un reglamento[901], atendido el efecto de restricción que supone para los ciudadanos la limitación de uso de posibilidades tecnológicas perfectamente legítimas, pero que la Administración no considera adecuadas para un concreto procedimiento administrativo.

En cualquier caso, debía considerarse como una condición adicional general, aplicable a los prestadores cuyos certificados se admitan ante la Administración General del Estado, la prevista en el artículo 23.2 del RDLAE, que dispone que "los prestadores de servicios de certificación deberán facilitar a las plataformas públicas de validación que se establezcan conforme a lo previsto en este real decreto, acceso electrónico y gratuito para la verificación de la vigencia de los certificados asociados a sistemas utilizados por los ciudadanos, la Administración General del Estado y sus organismos públicos", en línea con lo que establecía el artículo 21.1 de la LAE, hoy derogado, y el artículo 24.4 del Reglamento eIDAS[902].

Asimismo, se debían también considerar condiciones adicionales generales, en este caso aplicables a los prestadores cuyos certificados se admitan por cualquier Administración pública española, las que determina el artículo 19 del RDENI[903], bajo el título de "aspectos de interoperabilidad relativos a los prestadores de servicios de certificación".

El artículo 19 del RDENI estableció tres categorías de condiciones generales adicionales. En primer lugar, desde la perspectiva de la interoperabilidad organizativa, el epígrafe 2

---

[901] Nótese que es el RDLAE el que concreta este instrumento, ya que la LFE sólo se había referido al órgano que las aprobaba, sin detallar el tipo de norma.

[902] Este artículo establece que "[…] los prestadores cualificados de servicios de confianza que expidan certificados cualificados proporcionarán a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente".

[903] Este artículo, que además se dicta conforme a lo establecido en el RDLAE –algo bastante criticable, por cuanto el RDLAE sólo resulta de aplicación a la Administración General del Estado, mientras que el RDENI tiene carácter básico– tampoco no ha sido derogado con ocasión de la aprobación de la LPAC y la LRJSP. También se debe entender inaplicado desde la entrada en aplicación del Reglamento eIDAS, y en ningún caso resulta aplicable a prestadores de servicios establecidos en otros Estados miembros de la Unión Europea.

del artículo 19 del RDENI obliga a los prestadores que expiden certificados a organizar la prestación de su servicio a una serie de condiciones mínimas[904] orientadas a facilitar el uso de los certificados por parte de las Administraciones Públicas; en segundo lugar, desde la perspectiva de la interoperabilidad semántica, el epígrafe 3 del artículo 19 del RDENI obliga a los prestadores a establecer plantillas de certificados, conforme a una sintaxis y una semántica concretas, y exigiendo el establecimiento de reglas de unicidad a los efectos de la identificación; finalmente, y desde la perspectiva de la interoperabilidad técnica, el epígrafe 4 del artículo 19 del RDENI exige a los prestadores una serie de elementos técnicos mínimos[905], llamando la atención la sujeción de los estándares a emplear a lo establecido en el propio RDENI[906], así como la obligación de incluir determinados contenidos dentro de los certificados.

El artículo 23 del RDLAE y el artículo 19 del RDENI contienen, como se puede ver, una importante cantidad de exigencias, que cabe considerar como condiciones adicionales al uso de la firma electrónica por las Administraciones Públicas, cuya aplicación a prestadores establecidos en otros Estados miembro resulta absolutamente incompatible con el Reglamento eIDAS[907], por lo que cabe concluir que ambas normas –que no se han derogado con ocasión de la aprobación de la LPAC y de la LRJSP y, por tanto, se encuentran formalmente vigentes– habrían quedado inaplicadas por el citado Reglamento eIDAS, al menos para dichos prestadores extranjeros[908].

Por su parte, el apartado 2 del artículo 21 de la LAE dispuso que "los sistemas de firma electrónica utilizados o admitidos por alguna Administración Pública distintos de los basados en los certificados a los que se refiere el apartado anterior podrán ser asimismo admitidos por otras Administraciones, conforme a principios de reconocimiento mutuo y

---

[904] En concreto: a) Establecimiento de los usos de los certificados expedidos de acuerdo con un perfil dado y sus posibles límites de uso; b) Prácticas al generar los certificados que permitan posteriormente la aplicación de unos mecanismos de descubrimiento y extracción inequívoca de los datos de identidad del certificado; c) Definición de la información de los certificados o relacionada con ellos que será publicada por parte del prestador, debidamente catalogada; d) Definición de los posibles estados en los que un certificado pueda encontrarse a lo largo de su ciclo de vida; y e) Los niveles de acuerdo de servicio definidos y caracterizados para los servicios de validación y de sellado de fecha y hora.

[905] En concreto: a) Los estándares relativos a políticas y prácticas de certificación y generación de certificados electrónicos, estado de los certificados, dispositivos seguros de creación de firma, programas controladores, dispositivos criptográficos, interfaces de programación, tarjetas criptográficas, conservación de documentación relativa a los certificados y servicios, límites de los certificados, conforme a lo establecido en el artículo 11; b) La incorporación, dentro de los certificados, de información relativa a las direcciones de Internet donde se ofrecen servicios de validación por parte de los prestadores; y c) Los mecanismos de publicación y de depósito de certificados y documentación asociada admitidos entre Administraciones públicas.

[906] Esta sujeción implica una potente restricción a la libertad de los prestadores de elegir los estándares, ya que los mismos deberán ser preferentemente abiertos, o de uso generalizados por los ciudadanos, y en cualquier caso encontrarse previamente aprobados en el Catálogo previsto en la norma.

[907] En efecto, los prestadores no pueden ser obligados a cumplir, después de la aprobación del Reglamento eIDAS, requisitos adicionales a los previstos en la propia legislación reguladora de su actividad, por lo que cualquiera "norma" en este sentido deberá ser considerada como voluntaria.

[908] Mantener la aplicación de esta normativa sólo a los prestadores españoles podría resultar defendible en términos del derecho de la Unión, al no afectar a las operaciones transfronterizas, pero puede hacerles menos competitivos frente a prestadores extranjeros, en función del caso.

reciprocidad".

Se trataba, por tanto, de una admisión discrecional, a diferencia del caso anterior, que debía entenderse reglada. Esta distinción se encontraba plenamente justificada, ya que la regla del artículo 21.1 de la LAE regulaba una relación entre el ciudadano[909] y la Administración que admitía su certificado reconocido; mientras que la regla del artículo 21.2 de la LAE regulaba una relación interadministrativa en la que una Administración admitía un documento firmado con un sistema no admisible (por no cumplir las condiciones del artículo 21.1 de la LAE) empleado por otra Administración, lo cual se sujetaba, lógicamente, a principios de reconocimiento mutuo y recíproco[910].

Por lo que respecta a la LUTICAJ, que en este punto se aleja algo de la LAE, su artículo 22.1 indica que "los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por la Administración de Justicia como válidos en las relaciones con la misma, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones competentes en materia de justicia la información que se precise en condiciones que resulten tecnológicamente viables, bajo principios de reconocimiento mutuo y reciprocidad y sin que suponga coste alguno para aquéllas".

Los certificados cuya admisión resulta obligatoria deben ser, como en la LAE, certificados reconocidos, tal y como los define y regula la LFE, expedidos por prestadores de servicios de certificación que cumplan sus obligaciones legales, como hemos tenido ocasión de analizar anteriormente; previsión que resulta razonable, dada la ausencia de garantía respecto a la identificación en los certificados no reconocidos[911].

Asimismo, para que los certificados resulten admitidos, el prestador de servicios que lo emitió debe poner a disposición de la Administración la información que se precise, como en el caso de la LAE, en condiciones que resulten tecnológicamente viables, texto de una especial oscuridad, que se debe esclarecer acudiendo a los estándares habituales de

---

[909] Más habitualmente, por criterio práctico, el prestador que expide el certificado será el que solicite la "admisión" de su sistema de firma electrónica, dado que incrementa el valor de su propio servicio.

[910] Como ejemplo temprano –de hecho, anterior a la LAE– de reconocimiento mutuo, se puede mencionar el Convenio de cooperación tecnológica entre el Ministerio de Justicia y el Departamento de Justicia de la Generalitat de Catalunya para la implantación y ejecución de la presentación telemática de escritos y notificaciones –sistema LexNET– en las oficinas judiciales de Cataluña, firmado el 5 de mayo de 2006, y publicado por Resolución 2006/3165/JUS, de 28 de septiembre, mediante el cual se admiten en el ámbito de cada parte los certificados utilizados por la otra parte, de forma recíproca y sin coste alguno, técnica que supone una salida al problema del modelo de negocio de la FNMT-RCM, por causa del que los usuarios de certificados CERES se encuentran excluidos del "derecho" de admisión. Como es conocido, en el modelo de negocio de la FNMT-RCM los terceros verificadores de certificados deben adherirse a un convenio (si son entidades públicas) o a un contrato (si son ciudadanos o empresas), y abonar un precio por el derecho a hacer uso de certificados; de forma que los terceros sin convenio no pueden ni siquiera acceder a la información de estado de vigencia de los certificados. Los restantes prestadores de servicios de certificación, por el contrario, únicamente cobran al firmante por el suministro del certificado y, en su caso, del dispositivo de firma, resultando gratuito el acceso a la información de estado para todos los verificadores. Adicionalmente, cfr. (Coello de Portugal Martínez del Peral, 2003, pág. 99 y ss.), que critica el uso de la figura del convenio administrativo por parte de la FNMT-RCM para la prestación de sus servicios, que califica de contrario a la legislación de contratos.

[911] Y por supuesto, igualmente en el caso de los sistemas de firma electrónica que ni siquiera emplean certificados electrónicos.

certificación, como vimos anteriormente.

A mayor abundamiento, la información a suministrar debe serlo bajo principios de reconocimiento mutuo y reciprocidad, y sin que suponga coste alguno para las Administraciones competentes, punto en el que el artículo 22.1 de la LUTICAJ se aleja de la LAE, mediante una redacción imprecisa y desafortunada, en particular por la mezcla de dos casos que resultan claramente heterogéneos. Efectivamente, resulta sencillamente absurda la aplicación de los principios de reconocimiento mutuo y reciprocidad a la admisión de los certificados cuando la misma es solicitada por los ciudadanos o por los prestadores que les suministran certificados[912].

En definitiva, y como hemos expuesto en otro lugar[913], de todo ello se desprendía que el paradigma legal de certificado de ciudadano a emplear en las relaciones con las Administraciones Públicas haya sido el denominado certificado reconocido en soporte software, como por ejemplo el certificado idCAT emitido por el Consorci Administració Oberta de Catalunya o el certificado Clase 2 CA emitido por la FNMT-RCM dentro de su proyecto CERES, ampliamente extendidos en ambos casos, supuestamente dentro de la libre concurrencia que exigía la LFE.

Esta nueva aproximación no impedía, por supuesto, que los ciudadanos y, más en concreto, las empresas, decidieran adquirir sus propios sistemas de firma electrónica reconocida, algo que siempre resulta muy recomendable, dado que se trata de su clave privada y, por tanto, de su propio riesgo[914].

5.2.2.3.2 La determinación de la adecuación del sistema de firma electrónica

La segunda condición que establecía la LAE, y también establece la LUTICAJ, para el uso de un sistema de firma electrónica es que el mismo resultase adecuado para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

Dicha previsión aparece, a primera vista, como una redundancia en relación con la primera condición, puesto que todos los sistemas de firma electrónica conformes con la LFE y el Reglamento eIDAS deberían ya ser adecuados para la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos. Al menos es lo que dicta la intuición.

Sin embargo, como hemos estudiado, en realidad nada más alejado de la realidad: la LFE permitía la existencia de sistemas de firma electrónica que muy laxamente identifican a los firmantes[915]; por lo que sólo los sistemas basados en certificados cualificados ofrecen

---

[912] Sí, en cambio, puede resultar aceptable la norma en relación con los certificados expedidos a magistrados, jueces, secretarios judiciales, fiscales, abogados del estado y funcionarios al servicio de la Administración de Justicia y otros entes públicos.

[913] Cfr. (Alamillo Domingo & Urios Aparisi, 2010, pág. 665).

[914] Como hemos visto, esta opción es la más segura jurídicamente en cuanto a la efectiva admisión, pero no la única, por lo que en nuestra opinión se deberá hacer uso de la potestad discrecional de admisión de otros sistemas de firma electrónica prevista legalmente.

[915] Y, además, con la nueva definición de firma y sello electrónico contenida en el Reglamento eIDAS, no es ya necesario que dichos sistemas identifiquen a la persona en cuestión.

realmente una garantía estricta sobre la identidad de los firmantes[916].

Por tanto, resulta que efectivamente, además de comprobar que el sistema de firma electrónica era conforme con la legislación reguladora, se debía evaluar su funcionalidad para determinar si era o no adecuado para su uso en el procedimiento electrónico de que se trate, a partir de los principios de seguridad mínima y de proporcionalidad.

En este caso, la dificultad estribaba en disponer de criterios que ayuden en la determinación del "nivel de" firma electrónica que se requiere en cada una actuación concreta. Una metodología que permitiera la realización de este análisis de adecuación de uso de un sistema de firma electrónica para una actuación electrónica concreta debía, por tanto, considerar los siguientes pasos de evaluación:

- En primer lugar, se debía evaluar la existencia de normativa jurídica que imponga un nivel concreto de firma electrónica a utilizar, a la que anteriormente nos hemos referido.
- En segundo lugar, se debía evaluar el derecho del ciudadano a emplear la firma electrónica avanzada basada en certificado[917], que desde luego existía claramente a tenor de lo establecido en los artículos 6, 13.2, 15 y 21 de la LAE, y en los artículos 14.2.b) y 22 de la LUTICAJ.
- En tercer lugar, se debía evaluar el nivel de seguridad del activo documental de acuerdo con las dimensiones de seguridad del Esquema Nacional de Seguridad, dentro del nivel mínimo marcado por la ley, para determinar necesidades adicionales de seguridad.
- En cuarto lugar, se debían considerar los requisitos de interoperabilidad del RDENI y las NTI dictadas en su desarrollo que resulten aplicables al sistema de firma electrónica en cuestión[918].
- En quinto y último lugar, se debía valorar el cumplimiento de las condiciones adicionales que su hubiesen establecido en función de cada procedimiento, de acuerdo con lo establecido en el artículo 4 de la LFE.

Los sistemas de firma electrónica evaluados de esta forma resultaban, en principio, adecuados para la actuación de que se tratase, por lo que se podía adoptar la decisión en

---

[916] En este sentido, resulta llamativa la crítica feroz de (Boix Palop, 2010), por ciento refiriéndose a diversas alteraciones de la neutralidad tecnológica, cuando indica que "la continuada y reiterada tendencia a pedir firma digital vigente hasta la fecha demuestra, sin dudas, un grado de exigencia mucho mayor en el procedimiento electrónico que en el ordinario. […] Por extraños motivos asociados a un supuesto «miedo al fraude» que se asocia, sin que se sepa muy bien por qué, a las actuaciones por vía electrónica, […] la fehaciencia parecía en todo casi indispensable. […] tardaremos un tiempo en desterrar totalmente la práctica de «hiperproteger» el procedimiento administrativo de manera desproporcionada y en todo caso muy superior a la exigida en otros casos"; posición con la que sólo estoy parcialmente de acuerdo.

[917] Como se muestra en una retrospectiva de diez años de uso de firma electrónica reconocida en los ámbitos de la administración electrónica, la facturación electrónica y la contratación pública electrónica, este tipo de firma electrónica vino a sustituir a la firma electrónica reconocida (Alamillo Domingo & Cuenca León, 2014, págs. 669-670).

[918] Y, en particular, las condiciones de la denominada "política de firma electrónica y de certificados", redactada de acuerdo con los requisitos de mínimos establecidos por la Norma Técnica de Interoperabilidad correspondiente.

su empleo.

5.2.2.4 La admisión transfronteriza de firmas y sellos electrónicos en relación con el acceso a servicios públicos

El Reglamento eIDAS ha establecido una serie de reglas para la admisión transfronteriza de las firmas y sellos electrónicos[919], que van a afectar a la libertad de los Estados miembros de regular las condiciones de uso de estos sistemas de prueba electrónica en las relaciones que se establezcan con las mismas[920].

Aunque no es la primera ocasión[921] en que en el derecho de la Unión se establecen criterios para facilitar la admisión transfronteriza de las firmas electrónica –y no de los sellos, algo del todo lógico porque los mismos no habían sido aún institucionalizados como tales–, sí que es la primera vez que se establece una regla de alcance general.

En primer lugar, los artículos 27.3 y 37.3 del Reglamento eIDAS disponen, con carácter general, que los Estados miembros no exigirán, para el uso transfronterizo en un servicio en línea ofrecido por un organismo del sector público, una firma o sello electrónicos cuyo nivel de seguridad sea superior al de una firma o sello electrónico cualificados. Se trata de una norma claramente orientada a garantizar la actuación transfronteriza de los ciudadanos de la Unión, que en sus Estados de residencia típicamente van a obtener, a lo sumo, un sistema de firma o de sello electrónico cualificado. Sin perjuicio de lo que se acaba de indicar, como es lógico este régimen se aplica también a las firmas y sellos producidos por las entidades del sector público, que deban ser admitidos por las entidades de sector público de los restantes Estados miembros.

Como ejemplo de una firma o sello electrónico de nivel de seguridad superior al cualificado, podemos citar la imposición obligatoria de un sello de tiempo electrónico cualificado sobre el contenido del documento firmado, o de un certificado de firma electrónica con atributos –como en el caso de la representación legal o voluntaria– o de un certificado de atributos, adicional al certificado cualificado de firma electrónica.

Podemos considerar este aspecto como una reacción al régimen legal anterior, que como hemos visto permitía de forma expresa el establecimiento de condiciones adicionales al uso de la firma electrónica en las relaciones con el sector público.

En segundo término, los artículos 27.2 y 37.2 del Reglamento eIDAS determinan que si un Estado miembro impone una firma o sello electrónicos avanzados basado en un

---

[919] (Polanksi, 2015, p. 778) ha hecho notar que se trata de una previsión legalmente novedosa, aunque esto sólo es cierto con carácter general, dado que ya existía la experiencia de la Directiva de Servicios.

[920] Estas reglas afectan al régimen de uso de la firma y el sello electrónico establecidas por la LAE y la LUTICAJ, y antes de la entrada en vigor de la LPAC y la LRJSP, a las que desde luego resultan aplicables.

[921] Como ya hemos avanzando, resulta muy notable la Decisión 2011/130/UE, de 25 de febrero de 2011 por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior, modificada por la Decisión de Ejecución 2014/148/UE de la Comisión, de 17 de marzo de 2014; pero también resulta digno de mención el artículo 7.6 del Reglamento (CE) Nº 1896/2006 del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 por el que se establece un proceso monitorio europeo, que exige – salvo excepción – el empleo de la firma electrónica avanzada para la autenticación de la petición de requerimiento europeo de pago, firma que "será reconocida en el Estado miembro de origen sin que sea posible establecer condiciones suplementarias".

certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas o los sellos electrónicos avanzados basados en un certificado y las firmas o sellos electrónicos cualificados por lo menos en los formatos o con los métodos contemplados en el apartado 5; mientras que, por su parte, los artículos 27.1 y 37.1 del mismo Reglamento establecen que si un Estado miembro impone una firma o sello electrónicos avanzados con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá las firmas o sellos electrónicos avanzados, las firmas o sellos electrónicas avanzados basados en un certificado reconocido y las firmas o sellos electrónicos cualificados por lo menos en los formatos o con los métodos contemplados en el apartado 5.

Como se puede ver en ambos casos, lo que persigue el legislador europeo es, de nuevo, garantizar que se puedan emplear los sistemas de firma o sello electrónico avanzado de que dispongan los usuarios –aunque no de firma o sello electrónico ordinario, que quedaría excluido de admisión para usos transfronterizos– cuando un Estado miembro imponga la obligación de uso de éstos.

La idea es que cuando un Estado exija un sistema de firma o sello electrónico avanzado el ciudadano pueda elegir emplear dicho sistema, o alternativamente, y a su elección, también un sistema de firma o sello electrónico avanzado basado en certificado cualificado, o también un sistema de firma o sello electrónico cualificado, pero siempre que los mismo cumplan con lo establecido en el apartado 5 de los artículos 27 y 37, que prevé la posibilidad de que la Comisión Europea establezca, mediante actos de ejecución, normas técnicas relativas a formatos de referencia o métodos alternativos, con base en instrumentos ya existentes como la Decisión 2011/130/UE, de 25 de febrero de 2011[922] por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

Estas normas técnicas han sido adoptadas por la Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, que esencialmente se refiere a los perfiles de base XAdES, CAdES, PAdES y con un contenedor con firma asociada (ASiC), definidos en las especificaciones técnicas ETSI TS 103 171 v.2.1.1, ETSI TS 103 173 v.2.2.1, ETSI TS 103 172 v.2.2.2 y ETSI TS 103 174 v.2.1.1, respectivamente; o al uso de métodos equivalentes descritos en la propia Decisión.

Los métodos equivalentes están previstos, en la Decisión, para permitir la verificación transfronteriza de las firmas electrónicas, o los sellos electrónicos, y exigen que "el Estado miembro en el que tenga su sede el proveedor de servicios de confianza utilizado por el firmante ofrezca a otros Estados miembros posibilidades de validación de firmas adecuadas, en la medida de lo posible, para el tratamiento automático" (artículo 2.1 de la

[922] Modificada por la Decisión de Ejecución 2014/148/UE de la Comisión, de 17 de marzo de 2014.

Decisión), como sucede, en España, con el servicio @firma.

Estas posibilidades de validación "parten de los requisitos para la validación de las firmas electrónicas y los sellos electrónicos cualificados a los que hacen referencia los artículos 32 y 40 del Reglamento (UE) Nº 910/2014", con el objetivo de "establecer requisitos comparables para la validación y para aumentar la confianza en las posibilidades de validación proporcionadas por los Estados miembros para otros formatos de firma electrónica o sello electrónico distintos de los comúnmente admitidos", según establece el Considerando (9) de la Decisión, por lo que aplicarán, salvo excepción –normalmente referida a la exigencia del dispositivo cualificado de creación de firma o sello–, los requisitos que se analizan con ocasión del estudio de este proceso y su correlativo servicio de confianza[923].

Hay que notar que, a diferencia de la previsión de los artículos 27.4 y 37.4 del Reglamento eIDAS, estas normas no presumen que la firma o sello sea efectivamente avanzado, sino que únicamente se refiere a la sintaxis informática que deben cumplir las firmas o sellos admisibles en operaciones transfronterizas, o los métodos equivalentes que resultan aceptables, por lo que cabe indicar que se trata de una actuación que responde a la necesidad de circulación de las pruebas de atribución dimanante de la construcción del Mercado Único Digital[924].

Esta regla es muy conveniente, ya que como sabemos existen potencialmente muchas y variadas tecnologías de firma o sello electrónico avanzado, y podría perfectamente suceder que los ciudadanos de un Estado dispusiesen de un sistema técnicamente incompatible con los sistemas de firma o sello electrónico avanzado de otros Estados. Gracias a esta norma, una persona que deba realizar una actuación transfronteriza para la que se imponga la firma o sello electrónico avanzado podrá acogerse al sistema que le ofrezca dicho Estado o emplear el sistema conforme a la norma técnica establecida por la Comisión; esto es, al menos las firmas o sellos en formato XAdES, CAdES o PAdES, en el nivel de conformidad B, T o LT, o los métodos equivalentes ya mencionados.

Sin embargo, es también preciso reconocer que la Decisión de Ejecución (UE) 2015/1506 se limita, en todo caso, a sistemas de firma y sello electrónico avanzado – o cualificado – respaldados por el uso de los correspondientes certificados cualificados, por lo que no desarrolla todas las posibilidades previstas en los artículos 27.1 y 37.1 dado que no se refiere a la firma y el sello electrónico avanzado que no se base en un certificado, lo cual no deja de ser una forma de inaplicar el mandato legal.

En efecto, conforme a la norma, si el Estado miembro exige firma electrónica avanzada debería admitir la firma electrónica avanzada, o la firma electrónica avanzada basada en certificado cualificado, o la firma cualificada, pero tras la aprobación de la Decisión de Ejecución (UE) 2015/1506 dicho Estado admitirá firma electrónica avanzada (normalmente a sus nacionales), pero podrá exigir (a los extranjeros) el uso de una firma electrónica avanzada basada en certificado cualificado o de una firma electrónica cualificada.

---

[923] Cfr. el epígrafe 4.3.2 de este trabajo.

[924] Así se recoge en el Considerando (6) de la Decisión de Ejecución (UE) 2015/1506, que cita la Decisión de Ejecución 2014/148/UE, indicando que "[l]a finalidad del establecimiento de los formatos de referencia es facilitar la validación transfronteriza de las firmas electrónicas y mejorar la interoperabilidad transfronteriza de los procedimientos electrónicos".

Por tanto, aunque la regla es conveniente en términos de interoperabilidad, y puede considerarse razonable –frente a la dificultad de llegar a acuerdos sobre otros sistemas de firma o sello electrónico avanzado–, lo cierto es que supone un tratamiento diferente al previsto en el Reglamento eIDAS. Nada impide, sin embargo, que en el futuro se puedan incluir en la Decisión otros formatos de firma o sello electrónico avanzado que no se basen en certificados cualificados, o ni siquiera se basen en certificados, si ello resulta necesario.

5.2.2.5 El régimen de uso tras la reforma del sector público administrativo

La denominada "reforma del sector público" ha tenido impacto en el régimen de uso de la firma electrónica vigente hasta el momento, al que debemos referirnos en este momento.

En primer lugar, hay que decir que el artículo 13.g) de la LPAC mantiene el derecho de las personas con capacidad de obrar ante las Administraciones Públicas a la obtención y utilización de los medios de firma electrónica contemplados en la Ley, aunque veremos que con un régimen más restrictivo que el establecido en la LAE y en la aún vigente LUTICAJ.

En segundo lugar, y como ya hemos visto anteriormente, la LPAC regula de forma diferenciada la identificación y la firma o sello, estableciendo en su artículo 11.1 la regla general de la suficiencia de la identificación electrónica para la realización de cualquier trámite.

Como excepción al régimen general, el artículo 11.2 de la LPAC concreta que "las Administraciones Públicas sólo requerirán a los interesados el uso obligatorio de firma para: a) Formular solicitudes; b) Presentar declaraciones responsables o comunicaciones; c) Interponer recursos; d) Desistir de acciones; e) Renunciar a derechos", previsión a la que hay que añadir la exigencia de firma electrónica para el apoderamiento "apud acta" mediante comparecencia electrónica contenida en el artículo 6.5 de la propia LPAC.

En los restantes casos aplicará la regla general de que la simple identificación deberá ser suficiente para la actuación por el ciudadano, por lo que la Administración no deberá requerir, de forma obligatoria, ninguna firma electrónica.

Sin perjuicio de lo que se indica en la LPAC, cabe también la posibilidad de que en la legislación sectorial se mantengan o establezcan nuevas obligaciones de firma electrónica (a mi juicio, mediante ley formal), como ya hemos visto que sucede en la legislación de contratos del sector público, o de factura electrónica, que se solapan con la de procedimiento administrativo común.

En tercer lugar, en aquellos casos es que se pueda exigir la firma electrónica, el artículo 10.1 de la LPAC establece la regla general de que "los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento", regla que, desde la perspectiva del Reglamento eIDAS, resulta criticable, por cuanto podría limitar el derecho de uso de la firma electrónica no avanzada, dado que la misma no garantiza de forma necesaria la integridad e inalterabilidad del documento.

El epígrafe 2 del artículo 10, sin embargo, establece una regla especial para la relación con la Administración a través de medios electrónicos, en cuya virtud, "se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». A estos efectos, se entienden comprendidos entre los citados certificados electrónicos reconocidos o cualificados los de persona jurídica y de entidad sin personalidad jurídica.

b) Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

Cada Administración Pública, Organismo o Entidad podrá determinar si sólo admite algunos de estos sistemas para realizar determinados trámites o procedimientos de su ámbito de competencia".

Como ya vimos con ocasión del análisis del artículo 9 de la LPAC[925], cabe descartar la posibilidad de uso de los certificados de firma electrónica de persona jurídica, que han quedado inaplicados por el Reglamento eIDAS, por lo que esta previsión no ha llegado a entrar en vigor jamás.

Sin embargo, se admite con carácter el uso del sello electrónico de persona jurídica a efectos de firma, lo cual podría generar problemas dado que, como hemos visto anteriormente, un sello electrónico ofrece (en función de si es ordinario, avanzado o cualificado) garantías de la corrección del origen de los datos y de la integridad de los datos, pero no predica nada acerca de la expresión de la voluntad y del consentimiento de la persona jurídica, por lo que la regla especial contradeciría la general. Y, sin embargo, al admitirse en este artículo que el sello electrónico de persona jurídica "sirve para firmar", claramente se debe considerar como un sistema válido para la actuación de la persona jurídica en los casos en que la LPAC exige la firma electrónica.

Como también se puede ver, el artículo 10.2.c) de la LPAC permite a la Administración el empleo de cualquier otro sistema que considere válido, en los términos que se establezcan, previsión que cabe considerar favorablemente, ya que permite habilitar el uso de medios que firma o sello no avanzados o no cualificados, pero que resulten idóneos, como por ejemplo la firma electrónica manuscrita capturada en tableta digitalizadora, y por tanto, supone una corrección a la regla general del artículo 10.1, que era excesivamente estricta.

Además, el artículo 10.3 de la LPAC establece la regla de que "cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados", que constituye, de nuevo, una excepción a la regla general contenida en el artículo 10.1 de la propia Ley. En efecto, con la aplicación de esta regla especial, resulta que se puede admitir como sistema de firma electrónica un sistema de identificación electrónica que no acredite la integridad e inalterabilidad del documento, como por ejemplo Cl@ve PIN o Cl@ve Permanente.

[925] Cfr. el epígrafe 2.2.3 de este trabajo.

Esta regla viene a ser similar, en el fondo, a un supuesto más de la regla contenida en el artículo 10.2.c) al que nos acabamos de referir, y por tanto, se podría entender que resulta algo superflua, pero cabe imaginar que se ha incorporado a la LPAC por dos motivos: en primer lugar, para que quede claro que los mismos pueden ser empleados, eso sí, en los términos que se disponga en la normativa reguladora aplicable, remisión que cabe entender hecha a los instrumentos jurídicos de aprobación de Cl@ve o de otro sistema análogo, que son los que determinan la extensión y condiciones de uso de dichos sistemas; y en segundo lugar, y ello es más importante, porque los sistemas de identificación electrónica admitidos se extienden no sólo a los ciudadanos (nacionales o residentes en España), sino también a los de los restantes Estados miembros de la Unión, que por tanto podrán obtener el reconocimiento transfronterizo de su propio sistema nacional de identificación electrónica también a efectos de firma electrónica.

En relación con la decisión de uso de todos estos sistemas de firma, el artículo 10.2 de la LPAC también prevé, como en el caso de la identificación electrónica, que cada Administración decida qué medios de firma o sello admite en relación con cada trámite o procedimiento, decisión a mi juicio viene condicionada por lo establecido en el Esquema Nacional de Seguridad, dada su aplicación obligatoria en relación con los niveles de seguridad de los sistemas de información correspondientes.

Sin embargo, y a diferencia de lo que sucede en identificación electrónica[926], en este caso la Administración puede optar por no admitir el uso de ningún sistema de firma o sello electrónico avanzado o cualificado para su uso por el ciudadano.

Por este motivo, ya no cabe hablar, en la LPAC, del derecho subjetivo a la firma electrónica avanzada que existía claramente definido en la LAE, algo que en mi opinión resulta criticable. En efecto, con la LAE un ciudadano tenía el derecho a emplear un certificado de firma electrónica (con la excepción del certificado de entidad sin personalidad jurídica, cuya admisión era potestativa) en todos los casos, por lo que podía decidir no emplear otros medios eventualmente propuestos por la Administración. Y esto era sensato, porque el riesgo de un posible incidente de seguridad asociado a la firma de una persona, es de dicha persona, y por tanto la misma ha de poder decidir el sistema con el que quiere mitigar dicho riesgo.

Es claramente criticable que, con la nueva LPAC, se pueda dar la situación de que una persona jurídica se dote de un sistema de sello electrónico cualificado y se encuentre con la situación de que la Administración no está obligada a admitírselo en sus relaciones electrónicas con ella, y que le pueda incluso imponer un sistema de inferior seguridad.

De la interpretación conjunta de los artículos 9 y 10 de la LPAC, se deriva que una Administración puede perfectamente admitir a efectos de firma sólo los sistemas de identificación previstos en la Ley, por lo que en efecto se puede concluir que ha desaparecido el derecho al uso de la firma electrónica avanzada consagrado en la LAE, manteniéndose el derecho al uso del certificado electrónico, dado que necesariamente debe ser admitido como medio de identificación electrónica (cfr. artículo 9.2, último párrafo, de la LPAC).

Por ello, con la nueva Ley cabe esperar una progresiva sustitución o, cuanto menos,

[926] Donde recordemos que la elección por la Administración de un medio diferente al certificado electrónico de firma o sello (avanzado o cualificado) implica necesariamente también la admisión de dichos certificados para su uso por parte del ciudadano.

complementación, de los sistemas de firma (en menor grado, de los de sello electrónico) avanzada basada en certificado electrónico reconocido o cualificado, por la identificación electrónica basada en certificado electrónico reconocido o cualificado.

Muestra anticipada de ello es la Orden HAP/2194/2013, de 22 de noviembre, por la que se regulan los procedimientos y las condiciones generales para la presentación de determinadas autoliquidaciones y declaraciones informativas de naturaleza tributaria[927], que realiza una agresiva apuesta[928] al objeto de "reducir al máximo posible la presentación en papel de las autoliquidaciones y declaraciones informativas mientras se potencian nuevas vías de presentación como son las basadas en los sistemas de firma electrónica no avanzada definidos en la Resolución de 17 de noviembre de 2011 de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Agencia Tributaria".

Para ello, su artículo 2[929] autoriza a los sujetos obligados[930] la presentación electrónica de la práctica totalidad de las autoliquidaciones y declaraciones informativas indistintamente mediante una firma electrónica avanzada o mediante un sistema de identificación y

---

[927] Modificada por Orden HAP/455/2014, de 20 de marzo; Orden HAP/1846/2014, de 8 de octubre; Orden HAP/2762/2015, de 15 de diciembre; Orden HAP/365/2016, de 17 de marzo; Orden HFP/105/2017, de 6 de febrero y Orden HFP/255/2017, de 21 de marzo.

[928] Ampliada posteriormente por Orden HAP/2455/2013, de 27 de diciembre; Orden HAP/685/2014, de 29 de abril; Orden HAP/1136/2014, de 30 de junio; Orden HAP/2201/2014, de 21 de noviembre; Orden HAP/2178/2014, de 18 de noviembre; Orden HAP/2328/2014, de 11 de diciembre; Orden HAP/369/2015, de 27 de febrero; Orden HAP/1230/2015, de 17 de junio; Orden HAP/2118/2015, de 9 de octubre; Orden HAP/2762/2015, de 15 de diciembre; Orden HAP/2783/2015, de 21 de diciembre; Orden HAP/2835/2015, de 28 de diciembre; Orden HAP/296/2016, de 2 de marzo; Orden HAP/1349/2016, de 28 de julio; Orden HAP/1695/2016, de 25 de octubre; Orden HFP/1922/2016, de 19 de diciembre; Orden HFP/1978/2016, de 28 de diciembre; y Orden HFP/105/2017, de 6 de febrero; lo que trae cuenta de la importancia y extensión de estas políticas.

[929] En su redacción dada por Orden HAP/1846/2014, de 8 de octubre.

[930] En realidad, podríamos decir que en la gran mayoría de los casos lo impone taxativamente, dado que el artículo 3.1 de la misma Orden determina la obligación de realizar la presentación por Internet, y empleando necesariamente certificado reconocido, de "aquellos obligados tributarios que tengan el carácter de Administración Pública, o bien se encuentren inscritos en el Registro de Grandes Empresas regulado en el apartado 5 del artículo 3 del Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los Tributos, aprobado por el Real Decreto 1065/2007, de 27 de julio, bien estén adscritos a la Delegación Central de Grandes Contribuyentes o bien tengan la forma de sociedad anónima o sociedad de responsabilidad limitada", así como "en las autoliquidaciones del Impuesto sobre el Valor Añadido de aquellos obligados tributarios cuyo período de liquidación coincida con el mes natural, de acuerdo con lo establecido en los apartados 1.º, 2.º, 3.º y 4.º del artículo 71.3 del Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre, y en el supuesto del Modelo 430 "Impuesto sobre primas de seguros. Declaración-Liquidación", cualquiera que sea el obligado a su presentación". Asimismo, de acuerdo con el artículo 3.2 de la Orden, "también tendrá carácter obligatorio la presentación electrónica por Internet, […] en las presentaciones correspondientes al Impuesto sobre la Renta de las Personas Físicas y al Impuesto sobre el Patrimonio a realizar por las personas físicas que deban realizar la declaración del Impuesto sobre el Patrimonio", si bien en este caso podrán emplearse sistemas de firma avanzada o de identificación y autenticación basados en certificados electrónicos reconocidos, Cl@ve PIN o incluso número/s de referencia del borrador o de los datos fiscales previamente suministrados por la AEAT. De forma análoga, en el artículo 13 de la Orden, en relación con las declaraciones informativas.

autenticación, pero en ambos casos utilizando un certificado electrónico reconocido emitido de acuerdo a las condiciones que establece la LFE[931] que resulte admisible por la AEAT según la normativa vigente en cada momento; o alternativamente, y sólo en el caso de obligados persona física[932], también el sistema Cl@ve PIN. En sentido esencialmente idéntico se manifiesta el artículo 12 de la propia Orden, respecto a la presentación de determinadas declaraciones informativas.

Estos artículos resultan llamativos por diversas cuestiones, seguramente llamadas a marcar el inicio de una tendencia para el resto de Administraciones Públicas.

En primer lugar, por la equiparación entre la firma electrónica avanzada basada en certificado electrónico reconocido, y la identificación electrónica basada en el mismo certificado, dado que como indica la exposición de la Orden HAP/1846/2014, de 8 de octubre, "de acuerdo con los principios que fundamentaron la aprobación de la Orden HAP/2194/2013, de 22 de noviembre, y con la finalidad de facilitar y hacer más sencilla la presentación de declaraciones por vía electrónica a los obligados tributarios, se ha considerado conveniente introducir un nuevo sistema de presentación basado en el uso de certificados electrónicos reconocidos alternativo al de firma electrónica avanzada, eliminando con ello ciertas operaciones que en la práctica se ha puesto de manifiesto resultaban técnicamente complejas", por lo que "el ciudadano solo necesita disponer de un certificado electrónico reconocido que cumpla las condiciones que establece la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que resulte admisible por la Agencia Estatal de Administración Tributaria según la normativa vigente en cada momento".

Lo que sucede es que la identificación del ciudadano con su certificado se considera suficiente para las actuaciones de autoliquidación de los tributos, eliminándose la obligación de firmar electrónicamente, y todos los elementos de complejidad técnica que en efecto ello ha venido suponiendo. No resulta particularmente arriesgado aventurar que esta norma es reflejo de los enormes problemas asociados al empleo de determinados componentes técnicos, como en especial determinados tipos de aplicación informática de firma electrónica empleados en los procedimientos web, como los *applets* de firma empleados en las sedes electrónicas. Ciertamente se trata de una aproximación más neutral y, por tanto, alineada con el Reglamento eIDAS, y supone una orientación alejada de la producción documental y su autenticación por el ciudadano: una innovación jurídica –impulsada por la tecnología– en la que la autenticación de entidad sustituye a la autenticación de los datos.

En este escenario, hay que admitir que la persona física o jurídica que desee un elevado nivel de protección puede continuar apostando por los certificados electrónicos, y será la Administración la que deba construir mecanismos para acreditar la autenticidad de la expresión de la voluntad y la integridad del documento en cuestión. En la medida en que pueda hacerlo correctamente, el régimen de la LPAC se puede considerar más neutral tecnológicamente que el de la LAE, aunque podría resultar menos garantista.

Adicionalmente, esta restricción del derecho al uso de la firma o sello electrónico

---

[931] Hoy debe entenderse realizada la referencia no a la LFE, o no al menos únicamente a la LFE, sino también al Reglamento eIDAS, que regula también – y de forma preferencia a la LFE en caso de conflicto – los certificados cualificados de firma o sello electrónico.

[932] Pero únicamente cuando la misma no se encuentre obligada a la presentación con certificado, de acuerdo con lo establecido en el artículo 3.1 de la misma Orden.

avanzado tiene una consecuencia, que quizá no haya sido prevista por el legislador (o sí), derivada de los artículos 27 y 37 del Reglamento eIDAS: si el ciudadano español no tiene derecho al uso de la firma electrónica avanzada, tampoco lo tienen los ciudadanos de los demás Estados miembros de la Unión. Y ello es así porque los artículos 27 y 37 aplican cuando un Estado exige una firma electrónica avanzada o cualificada, pero no en otro caso, por lo que su finalidad no es tanto la de constituir un derecho general al uso de la firma electrónica avanzada o cualificada, sino la de evitar un trato discriminatorio en el que se exija más a un ciudadano o entidad de otro Estado de la Unión Europa que a uno del propio Estado[933].

Más recientemente, y en la misma línea de potenciación de la utilización de sistemas de identificación electrónica "para firmar", debemos referirnos a la Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.

La Resolución parte de la posibilidad reconocida en el artículo 10.3 de la LPAC de emplear los sistemas de identificación electrónica como medio de firma electrónica, a la que nos acabamos de referir, siempre que los mismos permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, complementando el sistema Cl@ve firma, servicio de confianza de creación de firma electrónica avanzada a distancia, que se basa en certificado cualificado del interesado.

Según declara la propia Resolución, las razones que justifican la habilitación de este sistema incluyen poder firmar sin tener que recordar una contraseña –que corresponde a Cl@ve Permanente, que se emplea como dato de activación de la firma electrónica remota– o evitar el empleo de las tecnologías concretas en el equipo del firmante, que generan dificultades técnicas de uso, significativamente, máquinas virtuales de Java y aplicaciones de creación de firma a instalar en dichos equipamientos.

A partir de estas razones, la Resolución tiene como objeto "establecer los criterios de uso y las condiciones técnicas de implementación de los sistemas de firma electrónica no criptográfica, previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre, que se considerarán válidos a efectos de firma en la Administración General del Estado y sus organismos públicos, así como en aquellas otras Administraciones Públicas que adopten estos criterios y condiciones técnicas", por lo que se orienta a ser un sistema de propósito general.

En ese sentido, nos encontramos ante un ejemplo de la potestad que tienen los Estados miembros para establecer efectos jurídicos de los sistemas de firma electrónica sin cualificación, posibilidad que recoge el Reglamento eIDAS –el cual únicamente establece el efecto jurídico, impuesto a los Estados Miembros, de que una firma electrónica cualificada tenga un efecto jurídico equivalente a una firma manuscrita (cfr. el artículo 25.2 del Reglamento eIDAS)– y que había sido apuntalada mediante el nuevo epígrafe 3.11 de la LFE. En efecto, mediante la aprobación de esta Resolución, lo que

[933] De forma similar a lo que establece el artículo 22.6 de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE, que residencia en cada Estado miembro, de acuerdo con un análisis de riesgos, la determinación de los casos en que se exige, o no, firma electrónica avanzada o cualificada, en cuyo caso deberá también admitirse la de los licitadores de otros Estados de la Unión.

verdaderamente sucede es que el Estado –en el marco de la habilitación que el legislador le confiere en el artículo 10.3 de la LPAC– determina que este concreto sistema de identificación "sirve para firmar", por lo que automáticamente queda encuadrado como sistema de firma electrónica (aunque no cualificada ni avanzada) conforme al artículo 3.10 del propio Reglamento eIDAS.

Respecto al uso de este sistema, el epígrafe III de la Resolución, en el marco de lo establecido por el Esquema Nacional de Seguridad, lo autoriza "cuando el sistema de información asociado al procedimiento haya sido categorizado, según el esquema nacional de seguridad, de categoría básica y aquellos de categoría media en los que no sea necesario utilizar la firma avanzada, cuando así lo disponga la normativa reguladora aplicable".

Como se puede ver, se trata de un sistema que, con carácter general, podrá emplear el interesado persona física para "acreditar la autenticidad de la expresión de su voluntad y consentimiento", como exige el artículo 10.1 de la LPAC, pero con dos exclusiones importantes: la primera, cuando el sistema de información sea categorizado como de nivel alto (en las dimensiones de seguridad de integridad y autenticidad, en relación con los activos documentales producidos por el interesado, por supuesto), en cuyo caso el Esquema Nacional de Seguridad impone de forma taxativa el uso de la firma electrónica cualificada; la segunda, cuando el sistema sea categorizado como de nivel medio, pero conforme a la normativa reguladora se exija la firma electrónica avanzada.

Esta normativa reguladora es diferente al propio Esquema Nacional de Seguridad, dado que el mismo no establece ningún criterio para diferenciar, dentro del nivel medio de seguridad, casos en que se emplee la firma electrónica avanzada. Un posible ejemplo sería la normativa sectorial reguladora de la facturación electrónica dirigida al sector público, o la normativa de contratación del sector público (al menos, en su versión actualmente vigente, dado que la Directiva (UE) 2014/24 flexibiliza el criterio, permitiendo acudir a técnicas de análisis de riesgos para tomar la decisión de imponer el uso de sistemas de firma electrónica avanzada, algo que sería más que deseable incorporar a la trasposición nacional de la misma).

Dado que el artículo 10.1 de la LPAC exige que los sistemas de firma electrónica, además de permitir acreditar la autenticidad de la expresión de la voluntad y el consentimiento del interesado persona física, también requiere que se acredite la integridad e inalterabilidad del documento, se podría perfectamente plantear la duda acerca de la posibilidad de empleo de cualquier sistema de identificación electrónica que no incorpore técnicas de integridad.

Sin embargo, el epígrafe 3 del artículo 10 de la LPAC, como sabemos, no impone estas exigencias de forma estricta en relación con el sistema de identificación que se empleará como sistema de firma, algo que resulta, por otra parte, perfectamente coherente con el Reglamento eIDAS, que tampoco exige a las firmas no avanzadas que aporten garantías de integridad e inalterabilidad de los datos firmados. Curiosamente, la Resolución analizada enfatiza que "en cualquier caso, todos los sistemas de firma electrónica admitidos deberán garantizar el cumplimiento de los requisitos recogidos en el apartado primero del artículo 10 de la citada Ley. Esto es, que estos sistemas permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, así como la integridad e inalterabilidad del documento", algo que ya hemos dicho que no va a garantizar, en sí mismo, el sistema de identificación en cuestión.

Ello tiene como consecuencia que las garantías de integridad e inalterabilidad deberán ser aportadas posteriormente por la Administración, que en definitiva es quien tiene la carga de la prueba, por lo que el sistema de firma electrónica no será únicamente el sistema de identificación electrónica que se declara admisible "para firmar", sino que también incluirá los elementos adicionales necesarios para garantizar el cumplimiento de las exigencias del epígrafe 1 del artículo 10 de la LPAC.

La Resolución lo reconoce de forma explícita cuando indica que "así, y en aplicación de lo dispuesto en el artículo 10.3 de la Ley 39/2015, de 1 de octubre, que faculta a las Administraciones Públicas a admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, siempre que así lo disponga la normativa reguladora, se procede con esta resolución a indicar los requisitos que se tienen que cumplir, no sólo con este objetivo, sino para asegurar también la integridad e inalterabilidad de los datos firmados, así como los requisitos para comprobar que se realizó dicho acto".

Nótese que, aunque el sistema de firma electrónica, globalmente considerado –descrito en los epígrafes V y VI de la Resolución–, ofrezca garantías de integridad e inalterabilidad de los datos firmados, de ello no se desprende –y ya sabemos que tampoco lo pretende la Resolución en cuestión– que nos encontremos ante un sistema de firma electrónica avanzada, porque no se cumplen los requisitos previstos al efecto en el artículo 26 del Reglamento eIDAS, entre otros motivos precisamente porque la integridad e inalterabilidad de los datos firmados no son inherentes a la firma generada por la persona física, sino que se producen a posteriori (y por la parte contraria, que posteriormente pretenderá atribuir la firma electrónica a la persona en cuestión).

En todo caso, en relación con estas garantías de integridad e inalterabilidad de los datos firmados, el epígrafe IV de la Resolución prevé tres casos diferenciados: la protección de la información presentada por el interesado; la protección de las evidencias necesarias para la verificación de la identidad, recopiladas inmediatamente antes del acto de la firma; y la protección de las evidencias del consentimiento explícito del interesado con el contenido firmado.

En los tres casos, el mecanismo de integridad es el mismo, y consiste en sellar dichas informaciones con el sello electrónico cualificado o reconocido del organismo y la adición de un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y su incorporación inmediata al sistema de información asociado a dicho procedimiento.

Resulta criticable la referencia al sello electrónico reconocido, por generar una posible confusión con respecto a los sellos electrónicos expedidos al amparo del artículo 18 de la LAE, y de los que jamás se ha podido decir que fueran "reconocidos", sino que a lo sumo se hubieran podido considerar equivalentes a "avanzados basados en certificados reconocidos"). Pero es que, además, los certificados reconocidos para sellos electrónicos dictados al amparo de la LAE –que ya era dudoso que fueran reconocidos conforme a la LFE, que sólo preveía esta posibilidad en relación con los certificados de firma electrónica–, se han debido de dejar de expedir a partir de la entrada en vigor del Reglamento eIDAS, dado que no se encuentran amparados por la medida transitoria prevista en el mismo, que sólo es aplicable a los certificados de firma electrónica de persona física. Por este motivo, hay que entender que la Resolución prevé el uso, exclusivamente, del sello electrónico cualificado del prestador del servicio de firma

electrónica objeto de análisis, en el sentido previsto en el Reglamento eIDAS, y que el término "reconocido" se emplea, exclusivamente, como sinónimo.

El uso de un sello electrónico cualificado es un aspecto que hay que valorar positivamente, dado que refuerza el nivel de garantía, protegiendo tanto al prestador del servicio de firma electrónica como a sus usuarios, que como hemos visto deben incorporar estas informaciones a sus correspondientes sistemas de información – y hasta cabe especificar que, al tener una indudable función probatoria, también se deberán incorporar a los correspondientes expedientes. En efecto, es preciso traer a colación que, conforme al artículo 35.2 del Reglamento eIDAS, "un sello electrónico cualificado disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado", por lo que su valor como mecanismo de garantía de la integridad, así como de atribución del contenido al órgano titular del sello, está fuera de toda duda.

Ello no significa, por supuesto, que el contenido al que se incorpora el sello sea verídico, ni que se establezca presunción legal alguna en su favor, ni mucho menos una inversión de la carga de la prueba con respecto a dicho contenido. Esto significa que la persona física puede impugnar la autenticidad, y la carga de la prueba corresponderá a la Administración, debiéndose proceder en los términos del artículo 384 de la Ley de Enjuiciamiento Civil, en su aplicación supletoria al procedimiento contencioso-administrativo, a lo que responde lo previsto en el epígrafe VI.2 de la propia Resolución.

El hecho de que se emplee un sello electrónico (en este caso, cualificado) también tiene la consecuencia de encontrarnos ante una actuación administrativa automatizada, por lo que el certificado en cuestión deberá cumplir las reglas establecidas al efecto en la normativa vigente. Resulta muy conveniente que en este caso se haya restringido el uso del mecanismo del código seguro de verificación, al menos para la colección y aseguramiento de los elementos con valor probatorio del sistema.

Sorprende negativamente, sin embargo, la extraña referencia al sellado de tiempo electrónico que, a su vez, protege el sello electrónico cualificado. En ese caso, en lugar de optarse por un sello cualificado de tiempo electrónico parece considerarse suficiente con un sello electrónico de tiempo basado en un certificado cualificado y, lo que es más sorprendente, emitido por un prestador supervisado.

El Reglamento eIDAS indica, en su artículo 41.3, que "los sellos cualificados de tiempo electrónicos disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas", por lo que el sello de tiempo electrónico que prevé la Resolución no gozará de este beneficio legal, que ciertamente resultaría muy necesario para aliviar la carga de la prueba en caso de conflicto.

Por otra parte, la noción de un "prestador supervisado" de sellado de tiempo es completamente ajena al Reglamento eIDAS, que únicamente establece controles con respecto a los "prestadores cualificados". Por ello, nos encontramos ante una previsión que puede generar bastantes problemas, al no poderse determinar aspectos clave como el contenido de la supervisión de un prestador no cualificado – y no tanto con respecto al organismo de supervisión, que sería el mismo en ambos casos.

En todo caso, al régimen anterior –de aseguramiento de las evidencias electrónicas que sustentan la firma electrónica, y que recae sobre el prestador del servicio de firma electrónica– el epígrafe IV de la misma Resolución prevé que "el organismo responsable

del procedimiento emitirá un justificante de firma sellado con su sello electrónico de órgano y generando el código seguro de verificación o CSV, que será el documento con valor probatorio de la actuación realizada", previsión de la que resulta criticable la ausencia del sello de tiempo electrónico en dicha acreditación, que es la que en definitiva recibe el firmante.

Con carácter general, todo ello viene a reforzar el protagonismo de la firma simple basada en una identificación electrónica –en su caso, basada en certificado cualificado– en detrimento de la firma electrónica avanzada o cualificada, que como hemos visto, tiene una mayor eficacia, especialmente desde la perspectiva de la prueba en el procedimiento administrativo o judicial, y sin perjuicio de lo que se pueda establecer en la legislación sectorial.

5.2.3 El régimen de uso de la firma y sello por las entidades del sector público español

La LAE y la LUTICAJ regularon no sólo el uso de los sistemas de firma electrónica por parte de los interesados, sino también por parte de las propias entidades del sector público[934], que ya hemos adelantado parcialmente al referirnos a la identificación electrónica[935], regulación que ha mantenido, en términos prácticamente idénticos, en la LRJSP.

El artículo 13.3 de la LAE determinaba que "las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.

b) Sistemas de firma electrónica para la actuación administrativa automatizada.

c) Firma electrónica del personal al servicio de las Administraciones Públicas.

d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes".

De forma casi idéntica, el artículo 14.3 de la LUTICAJ, vigente, indica que "la Administración de Justicia podrá utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzca:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede judicial electrónica y el establecimiento con ella de comunicaciones seguras.

---

[934] (Linares Gil, 2010) había afirmado la "conveniencia de que la regulación de la identificación y autenticación sea aplicable de modo unitario a todas las Administraciones Públicas", añadiendo que "no estamos ante materias propias de la autonomía organizativa de cada Administración Pública sino ante cuestiones propias del régimen jurídico de las Administraciones Públicas –¿cómo se exterioriza y formaliza la voluntad en la Administración Pública?– e incluso de procedimiento administrativo común al abordar requisitos de validez y eficacia de la actuación administrativa". Opinión que, desde luego, parece haber sido acogida plenamente en la reforma del sector público a la que posteriormente nos referiremos.

[935] Cfr. el epígrafe 2.1.4 de este trabajo.

b) Sistemas de firma electrónica para la actuación judicial automatizada.

c) Firma electrónica del personal al servicio de la Administración de Justicia.

d) Sistemas de intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo que específicamente se haya convenido".

Como se puede ver, ambos artículos se refieren indistintamente a sistemas que se emplean para la función de identificación electrónica y para la función de firma, como ya hemos visto sucede también en relación con los sistemas empleados por parte de los interesados.

Como comentario general a los diferentes sistemas, hay que hacer notar que la LAE se refería, y la LUTICAJ se sigue refiriendo, a sistemas para la autenticación de los documentos, considerando sistemas de firma electrónica y otros mecanismos que no tienen dicha calificación legal, como sucede con los sistemas de intercambio electrónico de datos en entornos cerrados de comunicación.

Sin embargo, el artículo 13.3.a) de la LAE se refería a los certificados empleados para la sede electrónica administrativa, y de forma análoga, lo hace el artículo 14.3.a) de la vigente LUTICAJ. A estos certificados nos hemos referido anteriormente, por lo que cabe dar aquí por reproducidas las consideraciones ya realizadas[936], debiendo recordarse únicamente que este certificado no se podía emplear "para firmar", sino únicamente para la garantía de la identidad de la sede en cuestión.

Nos centraremos, por ello, en los siguientes epígrafes, en los restantes sistemas previstos por la legislación que "sirven para firmar", incluyendo aquellos empleados en la actuación automatizada y no automatizada, con la advertencia previa de que también en este caso nos encontramos con diferente significados de esta expresión, dado que pueden disponer de firma electrónica tanto las personas físicas titulares de órganos administrativos cuanto las restantes que se integran en la organización de la entidad correspondiente, algo que tiene más relevancia de la que inicialmente pueda parecer[937].

5.2.3.1 La autenticación de la actuación administrativa automatizada

El artículo 13.3.b) de la LAE se refería a los denominados sistemas de firma electrónica para la actuación administrativa automatizada[938], que diferenciaba de la firma electrónica

---

[936] Cfr. el epígrafe 2.1.4.1 de este trabajo.

[937] (Valero Torrijos, 2016, pág. 2708) recuerda que "la principal diferencia entre los órganos y el resto de las manifestaciones estructurales que encontramos en el ámbito de las Administraciones Públicas se refiere a la imprescindible vinculación de los primeros con las competencias, de manera que, más allá de las matizaciones […] respecto de la regulación legal vigente, sólo aquéllos se encuentran habilitados para manifestar de manera vinculante la voluntad de la respectiva Administración". El mismo autor ha dicho, en relación con la hoy definición legal común de órgano administrativo, que se debe establecer "como criterio delimitador que la correspondiente unidad administrativa tenga atribuidas competencias específicas y propias con independencia de su naturaleza, es decir, que mediante el ejercicio de las mismas contribuya a la formación de la voluntad administrativa, incluso si su actuación tiene exclusivamente una relevancia interna o su intervención resulta meramente facultativa" (Valero Torrijos, 2016, págs. 2710-2711).

[938] Para (Valero Torrijos, 2013, pág. 67), "[p]or lo que se refiere a la exigencia de una intervención directa de las personas físicas en la actuación administrativa, el uso de medios electrónicos permite que las decisiones se lleven a cabo de forma automatizada, esto es, sin que aquélla tenga lugar, de manera que se adopten directamente por los sistemas informáticos conforme a una programación de las aplicaciones previamente establecida […] sin que la participación del personal al servicio de la Administración aporte muchas veces más que una simple rúbrica a modo de visto bueno que permite, en última instancia, realizar

del personal al servicio de las Administraciones Públicas, prevista en el mismo artículo 13.3.c). En sentido casi idéntico, como hemos visto, el artículo 14.3.b) de la vigente LUTICAJ se refiere también a los sistemas de firma electrónica para la actuación judicial automatizada, y el artículo 14.3.c), a la firma electrónica del personal al servicio de la Administración de Justicia.

Dada la identidad de supuestos, los analizaremos de forma conjunta, con la sola advertencia de que el régimen de la LAE ha sido modificado tras la aprobación del Reglamento eIDAS y la LRJSP, algo que no ha sucedido de forma expresa en la LUTICAJ (sin perjuicio de que la LUTICAJ también deba entenderse afectada por la aprobación del Reglamento eIDAS).

El artículo 18.1 de la LAE previó la posibilidad de que cada Administración Pública pudiera determinar, para la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada, la utilización de dos sistemas, a los que denominaba expresamente "firma electrónica". En el mismo sentido, con respecto a la actuación judicial automatizada, se expresa el vigente artículo 19.1 de la LUTICAJ.

El primer sistema era el "[s]ello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica" (artículo 18.1.a) de la LAE) y sigue siendo el "sello electrónico de la oficina judicial basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica" (artículo 19.1.a) de la LUTICAJ); mientras que el segundo sistema era el "[c]ódigo seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente" (artículo 18.1.b) de la LAE[939], sustituido por el actual artículo 42.b) de la LRJSP, que analizaremos) y sigue siendo el "[c]ódigo seguro de verificación vinculado a cada oficina judicial, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede judicial electrónica correspondiente" (artículo 19.1.b) de la LUTICAJ).

Por lo que se refiere al sello electrónico, el mismo debía basarse en un certificado electrónico que resultara conforme a la legislación de firma electrónica, que en el momento de aprobación de la LAE y de la LUTICAJ era la LFE[940]; norma que, como

---

una imputación formal de autoría de una decisión o, más bien, de un documento puesto que aquélla, en realidad, habrá sido adoptada a partir de los datos proporcionados por el sistema de información, sin que la persona física realice comprobación alguna ni modifique el resultado del tratamiento informativo que ha recibido", algo que, en mi opinión, permite cuestionar la necesidad o, incluso, corrección de uso de dicha firma manuscrita. La actuación administrativa automatizada ha generado ya un importante debate doctrinal, en relación con el cual se puede ver (Valero Torrijos, 2007, pág. 73 y ss.), (Martín Delgado, 2009, pág. 363 y ss.), (Alamillo Domingo & Urios Aparisi, 2011), *in toto*, o (Piñar Mañas, 2011, págs. 37-40); específicamente en el ámbito tributario, cfr. (Delgado García & Oliver Cuello, 2007).

[939] En el ámbito tributario, el artículo 84.2.b) del Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos se refiere al "[c]ódigo seguro de verificación vinculado a la Administración pública, órgano o entidad permitiéndose en todo caso la comprobación de la autenticidad e integridad del documento accediendo por medios electrónicos a los archivos del órgano u organismo emisor".

[940] En relación con el certificado de sello electrónico, cfr. el epígrafe 2.1.1 de este trabajo.

también sabemos, sólo regulaba las diferentes variantes de la firma electrónica, de las que la expedida a la persona jurídica era quizá la que más se podía aproximar a este concepto.

Con la aprobación del Reglamento eIDAS, la firma electrónica quedó restringida en sentido estricto únicamente a las actuaciones de personas físicas, por lo que ambos artículos debían ser reinterpretados para acomodarse a la nueva normativa, que sí regula el sello electrónico, como hemos también estudiado en detalle con anterioridad, debiéndose hacer notar que el Reglamento eIDAS no limita el uso del sello electrónico a las actuaciones automatizadas, a diferencia de la LAE y de la LUTICAJ.

En este sentido, el artículo 42.a) de la LRJSP, que resulta prácticamente idéntico al artículo 18.1.a) de la LAE, debe entenderse referido a certificados cualificados de sello electrónico conforme al Reglamento eIDAS, con las particularidades ya estudiadas en su momento[941]. No es ocioso decir, sin embargo, que existe una diferencia sutil entre ambos regímenes jurídicos, al exigirse en la LRJSP el uso de un certificado cualificado, exigencia no contenida en la LAE ni en el LUTICAJ, y que tiene como efecto la ineludible obligación de sustituir todos los certificados de sello electrónico expedidos al amparo de la LFE, dado que los mismos no pueden considerarse cualificados, ya que dicha cualificación sólo procede, como sabemos, en relación con los certificados de persona física, entre los que no se encuentran los certificados de sello electrónico previstos en la LAE y la LUTICAJ.

En todo caso, la normativa objeto de análisis constituye un ejemplo claro de norma jurídica –en este caso, nacional– que define efectos jurídicos específicos para un sello electrónico, adicionales en relación con aquéllos previstos para cualquier sello electrónico[942]. En efecto, dado que el Reglamento eIDAS no establece mayor efecto jurídico para un sello electrónico –incluido el sello electrónico cualificado– que la garantía de integridad y la corrección del origen de los datos, del Reglamento no se deduce que el mismo sea un mecanismo apropiado para la actuación de la Administración (automatizada o no), por lo que resulta preciso que el legislador nacional establezca esta

---

[941] Cfr. el epígrafe 2.1.4.2 de este trabajo.

[942] En este sentido, (Martín Delgado, 2009, pág. 362) ha indicado que "[t]oda actuación administrativa debe ser debidamente firmada como garantía de la identidad del autor de la misma y de que aquélla es expresión de la voluntad de éste, que asume su contenido. La actuación administrativa automatizada no es una excepción. En este caso, la firma es electrónica y, como ha sido mencionado, debe producirse mediante el empleo de dos sistemas de firma: el sello electrónico y el código seguro de verificación de firma. Aunque no es éste el momento para profundizar sobre el análisis de ambos instrumentos, interesa destacar que uno y otro pueden ser de titularidad del conjunto de la persona jurídica —la Administración actuante— o de alguno de los órganos que la forman. Sin la mediación de uno de ellos, sin la firma, no hay actividad administrativa válida, porque no existe imputación. A estos efectos es indiferente que el sello o el código sean utilizados por un funcionario, persona física, o por una aplicación informática de forma automatizada. Lo importante es que se produce la imputación por voluntad de la norma y que se aplica la ficción consistente en atribuir a la Administración o al órgano titular del sistema de firma (y, en este caso, desde él a la Administración) la autoría de tal actuación. Si la firma es del órgano y la competencia se atribuye legalmente al órgano —que, además, no puede renunciar a ella en aplicación del artículo 12.1 LPC—, el hecho de que quien firme o quien ejerza la competencia materialmente sea un sistema de información no es relevante a efectos de conceptualización". Sin embargo, creo que, en realidad, lo que ha sucedido es que simplemente se ha definido una nueva forma para la autenticación de la actuación, que no es reconducible a la tradicional institución de la firma manuscrita (y, por tanto, tampoco a su equivalente funcional, que es la firma electrónica), lo que implica dotar al sello electrónico de persona jurídica, como ya se ha dicho, de efectos jurídicos adicionales a los previstos en el Reglamento eIDAS.

posibilidad de forma expresa, aunque en este caso con el límite de que se emplee única y exclusivamente dentro del ámbito de una actuación administrativa automatizada.

Por lo que se refiere al código seguro de verificación[943], el mismo se configura como un sistema alternativo de "firma electrónica" de la Administración, también limitado a la actuación administrativa automatizada, caracterizado, en el actual artículo 42.b) de la LRJSP como aquel "vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente".

La legislación actualmente vigente no ofrece definición alguna de este código seguro de verificación[944], remitiendo a lo que se disponga en los términos y condiciones correspondientes, lo cual debería exigir la regulación de este mecanismo mediante la correspondiente disposición de carácter general[945], que podrá configurar como mejor considere el funcionamiento de este mecanismo, siempre que se cumplan determinas requisitos mínimos.

En primer lugar, y por la ineludible condición de tratarse de un sistema seguro empleado para la autenticación de documentos, parece imprescindible que dicho garantice la integridad y la corrección del origen de los datos; esto es, el código seguro de verificación deberá cumplir condiciones equivalentes a las establecidas en el Reglamento eIDAS para el sello electrónico, y por este motivo podrá recibir esta consideración legal, al menos en operaciones transfronterizas.

En efecto, el código seguro de verificación, desde la perspectiva de documentos administrativos que deban producir efectos transfronterizos, podrá ser reconducido –si se considera oportuno– a la figura del sello electrónico, pudiendo ser considerado ordinario o avanzado, pero en ningún caso se basará en certificado cualificado, por lo que no podrá ser un sello electrónico cualificado.

En segundo lugar, debe tratarse de un sistema que permita la verificación del documento mediante el acceso a la sede electrónica correspondiente, que cabe entender será la de la Administración Pública, órgano, organismo público o entidad de Derecho Público emisora del documento[946]. Como se puede ver, con este sistema, la posibilidad de

---

[943] Sobre los orígenes remotos de este sistema, ligados a la Agencia Estatal de Administración Tributaria, cfr. (Segarra Tormo, 2004, pág. 104 y ss.).

[944] (Gamero Casado, 2016, pág. 94), ha observado que "[e]ste concepto aparece en la Ley 11/2007, pero no se incorpora a ningún otro texto normativo, por lo que, tras la derogación efectiva de esta Ley el 2 de octubre, volverá a la condición de concepto jurídico indeterminado".

[945] En este sentido, y sólo para el ámbito de la Administración General del Estado, el artículo 20.3 del RDLAE ordena que "[l]a aplicación de este sistema requerirá una orden del Ministro competente o resolución del titular del organismo público, previo informe del Consejo Superior de Administración Electrónica, que se publicará en la sede electrónica correspondiente". En todo caso, en el artículo 42.b) de la LRJSP se ha añadido el inciso "en los términos y condiciones establecidos", texto que no aparecía en el artículo 18.1.b) de la LAE, lo que refuerza esta posición.

[946] Curiosamente, (Gamero Casado, 2016, pág. 94) caracteriza este sistema de forma diferente, al indicar que "[s]e trata de una tecnología con cuyo uso, cuando se genera o firma un documento electrónico, un original queda custodiado por un tercero de confianza, que se erige en notario digital", concepción que, a pesar de ser muy correcta, en mi opinión no encuentra acomodo en la actual normativa.

verificar la autenticidad del documento ya entregado al ciudadano o a otra Administración depende única y exclusivamente del emisor, algo que no sucede en los documentos administrativos producidos en papel.

Se trata de un sistema que, por este motivo, se debería emplear por parte de la Administración de forma restrictiva, siendo de una inferior calidad probatoria al sello electrónico avanzado basado en certificado cualificado, o de sello electrónico cualificado[947], en especial por la posibilidad que tiene la Administración de eliminar un código seguro de verificación de su sede electrónica[948], generando la apariencia de invalidez del documento que entregó al ciudadano o a otra Administración. Por tanto, lo recomendable sería limitar el uso de este sistema, algo que entra perfectamente dentro de la potestad de autoorganización de la Administración.

De emplearse este sistema, se debería hacer en casos absolutamente tasados y previstos en la legislación vigente, como precisamente su empleo en un documento firmado o sellado electrónicamente, a los solos efectos de facilitar su traslado al soporte papel[949], posibilidad prevista en el art. 27 de la LPAC.

El RDLAE desarrolla, para la Administración General del Estado, el funcionamiento de este sistema de "firma electrónica", estableciendo diversas reglas que tratan de mitigar –hay que suponerlo así, al menos– los riesgos jurídicos que presenta el uso de código seguro de verificación.

En primer lugar, conforme al artículo 20.2 del RDLAE, el sistema debe ofrecer una serie de garantías; a saber, el carácter único del código generado para cada documento, su vinculación con el documento generado y con el firmante, y la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento. Se trata de exigencias que recuerdan a las que ofrece el sello

---

[947] Así se reconoce, por ejemplo, en la Orden FOM/2159/2013, de 31 de octubre, por la que se regula el sistema de código seguro de verificación de documentos electrónicos del Ministerio de Fomento, que limita el uso exclusivo de este sistema sólo a las actuaciones administrativas comprendidas en sistemas de información clasificados como de categoría "Básica", debiendo además existir una justificación del órgano directivo del Departamento, a quien competa la actuación automatizada, para no utilizar medios de firma electrónica basada en certificados reconocidos (artículo quinto).

[948] Aunque alguna normativa explicite que la eliminación de un código sólo se puede realizar por decisión judicial o por la aplicación de la normativa vigente (como, por ejemplo, hace la Resolución de 16 de diciembre de 2015, de la Confederación Hidrográfica del Guadalquivir, sobre el uso del sistema de código seguro de verificación), lo cierto es que a la Administración le resulta posible proceder a la eliminación del código, algo que no puede hacer con un documento sellado electrónicamente respaldado por certificado electrónico. Por su parte, (Bauzá Martorell, 2016, pág. 791) admite que este sistema "en términos de garantía resulta claramente inferior al documento con sello electrónico", dada la posibilidad de que la Administración borre el código de su sede electrónica, por lo que "[a]sí en el CSV la prueba depende exclusivamente de la Administración, mientras que en el documento sellado sólo depende del ciudadano".

[949] Ejemplo de esta posibilidad es la Resolución de 20 de mayo de 2016, del Servicio Español para la Internacionalización de la Educación, sobre el uso del sistema de código seguro de verificación de este Organismo. En el ámbito autonómico, este enfoque lo encontramos en el Proyecto de Decreto por el que se regula el régimen jurídico de la Administración de la Comunidad Autónoma de Cantabria en el uso de medios electrónicos en su actividad administrativa y sus relaciones con los ciudadanos, cuyo artículo 7 sólo autoriza, con carácter general para las actuaciones administrativas automatizadas, el uso de sello electrónico basado en certificado cualificado; mientras que el artículo 28.1 del propio Decreto limita el uso del código seguro de verificación exclusivamente para garantizar la autenticidad de las copias en soporte papel producidas a partir de documentos electrónicos, mediante el acceso al archivo electrónico correspondiente.

electrónico avanzado, por lo que, si las mismas coincidieran –algo perfectamente posible, en función de la tecnología elegida para la implementación del código seguro de verificación–, el código seguro de verificación sería encuadrable en dicho concepto[950].

En efecto, normalmente esta tecnología hará uso de técnicas criptográficas –aunque diferentes de la firma digital, empleada en el caso de sello electrónico basado en certificado cualificado– para poder garantizar la vinculación del código con el documento, y su unicidad. Entre estas técnicas encontramos el uso de resúmenes criptográficos[951], uso de códigos de autenticación de mensaje con resumen criptográfico (HMAC)[952] y otras técnicas criptográficas *ad hoc*[953].

En segundo lugar, el epígrafe 3 del mismo artículo 20 del RDLAE especifica los contenidos mínimos que deberá tener la disposición de carácter general que regule la aplicación del sistema de código seguro de verificación; a saber, la descripción del funcionamiento del sistema, las actuaciones automatizadas a las que es de aplicación el sistema, los órganos responsables de la aplicación del sistema, las disposiciones que resultan de aplicación a la actuación, la indicación de los mecanismos utilizados para la generación del código, la sede electrónica a la que pueden acceder los interesados para la verificación del contenido de la actuación o documento, y el plazo de disponibilidad del sistema de verificación respecto a los documentos autorizados mediante este sistema[954].

---

[950] Más correcta resulta, a mi juicio, la caracterización de las garantías exigibles a estos sistemas que realiza el artículo 29.2 del citado Proyecto de Decreto por el que se regula el régimen jurídico de la Administración de la Comunidad Autónoma de Cantabria en el uso de medios electrónicos en su actividad administrativa y sus relaciones con los ciudadanos, que se refiere al carácter único y aleatorio de cada código generado para cada documento, así como una seguridad criptográfica equivalente a un sistema de sello electrónico avanzado basado en certificado cualificado; su vinculación con el documento generado y con el órgano o entidad emisor del mismo; y la posibilidad de acceder y verificar el documento durante todo el plazo en el que el documento pueda producir efectos jurídicos frente a terceros.

[951] Notable resulta, en este sentido, la Orden DEF/2594/2014, de 16 de diciembre, por la que se establece el sistema de utilización del código seguro de verificación de documentos electrónicos del Ministerio de Defensa, que produce un código de hasta 95 caracteres por hacer uso de algoritmos muy seguros como SHA-2-512.

[952] Como se explicita en el artículo sexto de la ya citada Orden FOM/2159/2013, de 31 de octubre, por la que se regula el sistema de código seguro de verificación de documentos electrónicos del Ministerio de Fomento, por ejemplo.

[953] Por ejemplo, el epígrafe 4 de la disposición adicional sexta de la Ley 7/2014, de 22 de diciembre, de Medidas Fiscales, de Gestión Administrativa y Financiera, y de Organización de la Generalitat, describe un algoritmo para la generación del código seguro de verificación de uso en el ámbito tributario, para actuaciones automatizadas y no automatizadas: "a) Se obtendrá la hora del sistema en milisegundos. Esto proporcionará una cadena de 15 caracteres. b) Se generará un número aleatorio de 21 dígitos. c) Se compondrá una cadena numérica por concatenación de los dos elementos anteriormente generados. d) Sobre el número anterior se aplicará una tabla de transformación que realice un cifrado y convierta la cadena numérica de entrada en una cadena de 24 caracteres alfanuméricos. e) Se eliminarán por usabilidad los caracteres correspondientes al dígito cero y a la letra «O» mayúscula y se separarán los 24 dígitos en tres bloques de 8 caracteres mediante el carácter «–». Los 27 caracteres resultantes formarán el CSV. f) En caso de obtener un CSV ya existente en el sistema, vinculado a otro documento, se repetirá el proceso comenzando con el apartado a) del algoritmo".

[954] Como ejemplo de aceptable aplicación de esta norma, cfr. la Orden HAP/1200/2012, de 5 de junio, sobre uso del sistema de código seguro de verificación por la Dirección General del Catastro, modificada por Orden HAP/2554/2015, de 25 de noviembre, aunque no cubre todos los contenidos exigibles. Mejor ejemplo constituye la Resolución de 4 de febrero de 2011, de la Presidencia de la Agencia Estatal de

A pesar de la claridad de la norma, en la mayoría de casos la citada disposición de carácter general apenas se limita a indicar el órgano al que se vincula el código seguro de verificación[955], y en la inmensa mayoría, simplemente no se regula ninguna de las condiciones exigibles[956], lo que podría afectar a la validez jurídica de las actuaciones realizadas mediante este sistema.

Quizá debido a las limitaciones indicadas, en especial respecto al valor probatorio menor, al menos potencialmente, que presenta el sistema de código seguro de verificación, pero en atención a la conveniencia de su uso en el cambio de formato y, en especial, de soporte[957], resulta frecuente encontrar normativa que hace uso de los dos sistemas, de forma combinada, de modo que se aplica un código seguro de verificación sobre un documento previamente autenticado con sello electrónico basado en certificado cualificado[958].

De todos modos, y con respecto a las actuaciones transfronterizas de los interesados[959], resulta preciso decir que ninguno de estos sistemas de autenticación de la actuación administrativa automatizada está expresamente previsto en la Decisión de la Comisión

---

Administración Tributaria, sobre uso de código seguro de verificación y por la que se crean sellos electrónicos del organismo. Quizá la norma más detallada al respecto sea la Orden FOM/2159/2013, de 31 de octubre, por la que se regula el sistema de código seguro de verificación de documentos electrónicos del Ministerio de Fomento.

[955] Así sucede en el caso de la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos, por ejemplo.

[956] Como en el caso de la Orden TIN/790/2010, de 24 de marzo, por la que se regula el envío por las empresas de los datos del certificado de empresa al Servicio Público de Empleo Estatal por medios electrónicos, o la Orden INT/3022/2010, de 23 de noviembre, por la que se regula el Tablón Edictal de Sanciones de Tráfico, por citar sólo dos ejemplos de los múltiples existentes.

[957] En este sentido, el artículo 27.3 de la LPAC ordena, en su numeral c), que "[l]as copias en soporte papel de documentos electrónicos requerirán que en las mismas figure la condición de copia y contendrán un código generado electrónicamente u otro sistema de verificación, que permitirá contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u Organismo público emisor". Aunque la norma no exige que se trate de un código seguro de verificación, normalmente debería serlo. Por ejemplo, en el ámbito tributario, cfr. el artículo 86 del Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.

[958] Cfr., por ejemplo, el artículo 10.2 de la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos, en relación con la expedición de consultas y certificaciones; o el Anexo III del Real Decreto 22/2015, de 23 de enero, por el que se establecen los requisitos de expedición del Suplemento Europeo a los títulos regulados en el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales y se modifica el Real Decreto 1027/2011, de 15 de julio, por el que se establece el Marco Español de Cualificaciones para la Educación Superior.

[959] Sobre las diferentes modalidades de los actos administrativos transfronterizos, a los que principalmente afectaría esta medida, (Bocanegra Sierra & García Luengo, 2008, págs. 10-11) explican que "[e]s una constatación irrefutable, en efecto, que, con cierta frecuencia, los actos administrativos son eficaces en espacios territoriales más amplios o más reducidos que los propios del ámbito de vigencia de las normas materiales que aplican, pudiendo la eficacia de un acto administrativo dictado en un país traspasar incluso las fronteras estatales en aplicación de una norma extranjera", lo que, añaden, "conduce al aislamiento —o al nacimiento— de una categoría jurídica de nuevo cuño"; actos que exigen, de forma ineludible, la interoperabilidad y el reconocimiento transfronterizo de los requisitos de forma aplicables a los mismos, a lo que parece responder, al menos en parte, esta Decisión.

2011/130/UE, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior (modificada por la Decisión de Ejecución de la Comisión, de 17 de marzo de 2014), por lo que no se podrán emplear para la emisión de documentos para las relaciones electrónicas con las entidades del sector público de los restantes Estados miembros de la Unión Europea[960], sin perjuicio de que se pueda realizar una interpretación generosa de la misma por parte de las citadas autoridades competentes, o de la necesidad de que se modifique, en el futuro, la citada Decisión, para admitir cualquiera de los sistemas de firma válidos en el Estado de producción del acto administrativo.

Mientras ello no suceda, entendemos que si la legislación del Estado donde deba producir efectos el acto administrativo transnacional admite el uso del sello electrónico en su ámbito nacional, deberá admitir, además de los sellos electrónicos de las entidades del sector público de dicho Estado, también los de los restantes Estados miembros, en las condiciones analógicas que ya conocemos[961], por lo que, en estos casos, se deberá emplear, cuanto menos, un sistema de sello electrónico avanzado basado en un certificado cualificado; y ello lleva a que el código seguro de verificación posiblemente no resulte admisible, ni siquiera aunque sea considerado como un sello electrónico avanzado, en atención a la tecnología subyacente al mismo.

Lo anteriormente indicado debe entenderse, por supuesto, sin perjuicio de normas especiales que regulen el reconocimiento transfronterizo de alguno de estos sistemas, como sucede, de forma singular, en el caso de las apostillas electrónicas reguladas en la Orden JUS/1207/2011, de 4 de mayo, por la que se crea y regula el Registro Electrónico de Apostillas del Ministerio de Justicia y se regula el procedimiento de emisión de apostillas en soporte papel y electrónico, dictada en el marco del Convenio XII de la Conferencia de La Haya de Derecho Internacional Privado por el que se suprimió la exigencia de legalización de los documentos públicos autorizados en el territorio de un Estado contratante y que debieran ser presentados en el territorio de otro Estado contratante. En este caso, la apostilla electrónica se incorpora a un registro electrónico para cuya consulta se requiere disponer del correspondiente código seguro de verificación[962].

5.2.3.2 La autenticación de la actuación administrativa no automatizada

Como ya se ha adelantado, el artículo 13.3.c) de la LAE se refería a la "[f]irma electrónica del personal al servicio de las Administraciones Públicas" para la identificación electrónica y para la autenticación de los documentos electrónicos de las Administraciones Públicas, previsión que posteriormente se desarrollaba en el artículo 19 de la propia Ley; una regulación que hoy ha quedado sustituida por la contenida en el artículo 43 de la LRJSP, que presenta algunos cambios significativos con respecto al régimen legal anterior, como la referencia expresa a los titulares de los órganos, la

[960] Así lo indica también (Bauzá Martorell, 2016, pág. 791).

[961] Cfr. el epígrafe 5.2.2.4 de este trabajo.

[962] Este código seguro de verificación, como hemos visto sucede de forma generalizada, no se regula conforme a las exigencias mínimas contenidas en el RDLAE.

posibilidad de emplear un seudónimo de la persona física o la desaparición de la referencia a la posibilidad de empleo del DNI electrónico para estas actuaciones.

Por su parte, el artículo 21 de la LUTICAJ contiene, y se mantiene vigente, una norma esencialmente idéntica a la contenida en el artículo 19 de la LAE, pero con un fuerte componente organizativo adicional, ya que regula las especialidades derivadas de la dotación de los sistemas de firma electrónica a magistrados, jueces, secretarios judiciales, fiscales, abogados del estado y funcionarios al servicio de la Administración de Justicia y otros entes públicos, que se realizará por el órgano que en cada caso prevé la norma; algo que se explica por la complejidad de la organización de la Administración de Justicia[963].

En primer lugar, el apartado 1 del art. 43 de la LRJSP ordena que, exceptuando los casos de identificación electrónica (art. 38 de la LRJSP, reconducible al servicio de confianza de certificado cualificado de autenticación de sitio web previsto en el Reglamento eIDAS) y de la actuación administrativa automatizada (arts. 41 y 42 de la LRJSP), "de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano o empleado público", firma electrónica que podrá ser cualificada, avanzada u ordinaria, en función del caso.

A diferencia de la previsión contenida en el artículo 19.1 de la LAE, que se refería a la "identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante", el artículo 43.1 de la LRJSP resulta aplicable a cualquier actuación, en una dicción más amplia, que permite extender su ámbito de aplicación sin problema a todos los empleados públicos, ejerzan o no competencias administrativas, algo que, además, resulta coherente con la lógica del funcionamiento electrónico de todo el sector público, y no sólo de las Administraciones Públicas en sentido estricto.

El apartado 2 del artículo 43 de la LRJSP atribuye a la Administración Pública, como no puede ser de otra forma, la potestad para determinar los sistemas de firma electrónica que debe utilizar su personal, concretando que los mismos podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios, una regla que resulta importante porque impacta, en particular, sobre el contenido de los certificados cualificados de firma electrónica, a los que ya nos hemos referido anteriormente[964].

Ciertamente, entre dichos sistemas pueden autorizarse, además de aquellos basados en el uso de certificados de firma electrónica[965], avanzada o cualificada, también otros. Entre ellos destaca con fuerza la práctica de asignar a los órganos y empleados públicos el uso

---

[963] En relación con el régimen jurídico de la firma electrónica del personal al servicio de la Administración de Justicia, cfr. (Linares Gil, 2012, pág. 493 y ss.). Es de imaginar que el régimen de la LUTICAJ resulte modificado en sentido similar a la LRJSP. Por lo que respecta a los letrados autonómicos, cfr. (Urios Aparisi, 2012, pág. 910 y ss.)

[964] Cfr. el epígrafe 2.1.4.3 de este trabajo.

[965] Considera (Gamero Casado, 2016, págs. 95-96) que "para garantizar la interoperabilidad, lo mejor que pueden hacer las Administraciones públicas es generalizar en su personal certificados reconocidos o cualificados, evitando el uso de otros sistemas de firma, especialmente cuando se trata de actuaciones que previsiblemente vayan a tener eficacia jurídica *ad extra* de la propia organización".

de sistemas de código seguro de verificación para su uso personal, ampliamente extendida[966], a pesar de las dudas que genera el empleo, por personas físicas, de sistemas que el legislador previó para la actuación administrativa automatizada[967]. Estos sistemas adolecen de las mismas limitaciones anteriormente expuestas, y por tanto cabe dar aquí por reproducidas las consideraciones ya realizadas al respecto.

También será posible, y en algunos escenarios resultará más que conveniente, la utilización por los empleados públicos de sistemas de firma manuscrita capturada electrónicamente[968], como por ejemplo en escenarios de movilidad como la inspección.

Diferente del caso de los sistemas de firma electrónica del personal a que nos acabamos de referir es el de la firma de las autoridades y los miembros de los órganos colegiados, personas que no tienen la condición de empleados públicos, y que por lo tanto no quedan sujetos a la anterior normativa. De ello no se desprende, a mi juicio, que no puedan disponer de firma electrónica, por supuesto, sino que será necesaria la aprobación de la correspondiente regulación, dentro del marco general previsto en los Esquemas Nacionales de Interoperabilidad y de Seguridad, cuyas previsiones resultan plenamente aplicables.

Aunque la decisión de la Administración relativa a los sistemas a emplear por parte de titulares de órganos y de empleados públicos no parece requerir de una disposición de carácter general, será muy conveniente reglamentar las cuestiones relativas a la gestión del ciclo de vida de estos sistemas de firma electrónica, incluyendo los tipos de sistemas de identificación y de firma electrónica, su titularidad y provisión, los contenidos y la expedición de los certificados cualificados para la identificación y la firma electrónica, la publicidad de los sistemas de identificación y firma electrónica, los derechos y deberes de las autoridades y los empleados públicos a los que se dote de sistemas de identificación y firma electrónica, así como el correspondiente marco sancionador, y la suspensión y revocación de sistemas de identificación y firma electrónica[969].

En otro orden de cosas, el artículo 45.1 de la LRJSP autoriza que "[l]as Administraciones Públicas podrán determinar los trámites e informes que incluyan firma electrónica

---

[966] El artículo 21.c) del RDLAE autoriza, en el ámbito de la Administración General del Estado, el uso personal de sistemas de código seguro de verificación, con sujeción al régimen correspondiente, y sin perjuicio de las correspondientes adaptaciones. Diversas disposiciones, que ya hemos indicado anteriormente, han hecho uso de esta posibilidad.

[967] Conforme al Dictamen de la Abogacía del Estado 26/12, de 2 de abril de 2012, "[d]el tenor literal de los artículos 13.3.b) y 18 de la LAECSP se desprende que los sistemas de sellado electrónico de Administración Pública y de Código seguro de verificación se circunscriben a las actuaciones administrativas automatizadas, que son objeto de definición expresa en el apartado a) del Anexo de la citada Ley […] sin que se aprecie fundamento jurídico suficiente para extender estos sistemas de firma a supuestos distintos de los expresa y deliberadamente previstos por el legislador, siendo significativo que el desarrollo reglamentario de la LAECSP (el ya citado Real Decreto 1671/2009) indique en su Preámbulo que «... se ha dispensado una atención especial a la autenticación en el seno de la actuación automatizada»" (Abogacía General del Estado, 2013, págs. 351-352).

[968] Se trata de un sistema al que ya nos hemos referido en el epígrafe 4.1.1.1 de este trabajo, y que deberá ser considerado como de firma electrónica simple u ordinaria.

[969] Constituye un excelente ejemplo de esta regulación la contenida en el Decreto 42/2017, de 22 de junio, por el que se regula el Régimen Jurídico de la Autorización y Uso de la firma electrónica de autoridades y empleados públicos de la Administración de la Comunidad Autónoma de Cantabria y su Sector Público.

reconocida o cualificada y avanzada basada en certificados electrónicos reconocidos o cualificados de firma electrónica", permitiendo a la Administración elegir el sistema que considere apropiado para cada trámite que requiera la firma electrónica, previsión que debe también entenderse aplicable al sello electrónico.

Se trata de una decisión, sin embargo, fuertemente condicionada por lo establecido en el epígrafe 5.7.4 del Anexo II del Esquema Nacional de Seguridad, dada su aplicación obligatoria en relación con los niveles de seguridad de los sistemas de información correspondientes.

En este sentido, será preciso el empleo de la firma electrónica cualificada, al menos, en relación con los sistemas de información de nivel alto en las dimensiones de integridad y autenticidad, que son los menos, mientras que los restantes casos puede adoptarse prácticamente cualquier tecnología de firma electrónica[970], algo que afecta a la interoperabilidad de los documentos firmados electrónicamente.

Sería ciertamente recomendable extender el empleo de la firma electrónica cualificada a todos los trámites de la Administración, dada la necesidad de aportar las suficientes garantías, y que resultará posible mediante la adopción de tecnologías concretas, como los sistemas de firma electrónica cualificada con claves centralizadas, a los que nos hemos referido con anterioridad.

Como se puede ver, el régimen de firma electrónica previsto para autoridades administrativas y empleados públicos no agota en absoluto la materia. Más bien al contrario, se podría decir que la misma no ha explorado innovaciones relevantes que pueden derivar de su uso, como, por ejemplo, el impacto que el uso de la firma electrónica presenta en figuras que encuentran su razón de ser en un mundo de soportes en papel, pero que podrían quedar obsoletas gracias a esta tecnología, como sucede con la delegación de firma o la refundición de actos de la misma naturaleza que afecten a varios interesados[971].

---

[970] (Valero Torrijos, 2013, págs. 155-156), valora la posibilidad de uso de "ciertas prácticas muy frecuentes en el día a día de la actividad administrativa como, por ejemplo, la incorporación a los documentos de firmas manuscritas digitalizadas o la utilización de sistemas de seguridad basados en un nombre de usuario y contraseña", dadas sus escasas garantías de seguridad, por lo que debe "rechazarse la utilización de los referidos ejemplos de firma electrónica *simple* para los documentos administrativos ya que, en última instancia, se podría estar facilitando la revisión encubierta de decisiones sin respetar los procedimientos legales de revisión", y considerando que "la plena validez y eficacia del documento administrativo electrónico nos remite necesariamente a la utilización de la firma electrónica avanzada o reconocida", aunque reconoce la admisibilidad de los restantes sistemas.

[971] Esta reflexión ha sido realizada por (Valero Torrijos, 2013, págs. 89-90), que, en relación con el primer caso, considera que "la delegación de firma –artículo 16 LRJAP– pierde gran parte de su sentido en la medida que sólo se transfiere la facultad de rubricar la decisión previamente adoptada por el titular del órgano competente, quien a través de la firma electrónica podría asumir, de manera masiva, la responsabilidad directa y material sobre las decisiones relativas al número de actos que se requiera"; mientras que, en relación con la segunda posibilidad, apunta que "la refundición de actos de la misma naturaleza que afecten a varios interesados contemplada en el artículo 55.3 LRJAP tampoco sería de gran utilidad con estas modalidades de actuaciones basadas en el uso de medios electrónicos; sobre todo si tenemos en cuenta que, al dictarse tantos actos individuales como supuestos de hecho existan, se evitarán en el futuro eventuales problemas desde la perspectiva de la protección de los datos personales en los supuestos em que se pretenda ejercer el derecho de acceso al contenido del acto o al expediente por parte de los interesados".

Más aún, la adopción de medios electrónicos para la actuación de los órganos –en particular, la firma electrónica– permite que dicha actuación pueda realizarse desde cualquier lugar, lo que indudablemente afecta a las normas de suplencia, y correspondiente delegación de la competencia, en caso de que el titular del órgano se encuentre ausente, y, en especial, fuera del ámbito territorial de ejercicio de las correspondientes competencias. Resulta difícil de justificar, a mi juicio, el mantenimiento de dichas normas, desde el momento en que se puede conceder acceso seguro a la documentación (y el expediente) para que el titular del órgano pueda proceder a la autentificación del correspondiente acto administrativo, mediante su firma electrónica[972].

Finalmente, y seguramente conocedor de la diversidad en materia de firma electrónica, el legislador ha establecido, en el apartado 2 del art. 45 de la LRJSP, una regla dirigida a la interoperabilidad interadministrativa de los documentos electrónicos que incorporen determinados sistemas de firma electrónica.

En efecto, como sabemos, la interoperabilidad de la firma electrónica viene determinada por la adopción de normas relativas a determinados formatos técnicos, por lo que las restantes firmas electrónicas no se benefician del reconocimiento interadministrativo. Claramente las firmas electrónicas basadas en claves concertadas, o las firmas electrónicas manuscritas, resultan tecnológicamente discriminadas en el actual modelo de interoperabilidad, construido en relación con la concreta tecnología de la firma electrónica basada en clave pública certificada.

El apartado 2 del artículo 45 de la LRJSP trata de resolver esta dificultad mediante la técnica de proteger el documento mediante el sello electrónico avanzado basado en certificado cualificado, o un sello electrónico cualificado, de la Administración, órgano, organismo público o entidad de derecho público que firmó el documento originalmente con el sistema de firma electrónica no interoperable.

Como se puede ver, nos encontramos ante una previsión legal de actuación administrativa automatizada, dada la referencia expresa al empleo del sello electrónico, y que no considera el uso del código seguro de verificación, hay que entender que por los problemas probatorios que en relación con el mismo se han puesto de manifiesto con anterioridad.

También llama la atención que esta autorización sólo se prevé cuando el emisor del documento deba remitirlo o ponerlo a disposición de otros órganos, organismos públicos, entidades de Derecho Público o Administraciones, y no de los ciudadanos, aunque la solución podrá desde luego ser la misma, toda vez que también son destinatarios de documentos firmados electrónicamente con sistemas de firma potencialmente diferentes de los basados en certificados cualificados.

Además, en el artículo 27 de la LPAC se permite, para la producción de copias auténticas a entregar a los ciudadanos, también el empleo del sistema de CSV, que es menos garantista que el sello electrónico basado en certificado cualificado (y mucho menos aún

[972] No parece que exista un obstáculo jurídico insuperable para considerar que titular del órgano que se encuentra desplazada fuera del territorio donde ejerce sus competencias no se encuentra ausente, al menos con la redacción del actual artículo 13 de la LRJSP, aunque más dificultad plantea el artículo 47.2, segundo párrafo, del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, que parece resultar de aplicación forzosa, pero que se podría soslayar mediante el correspondiente Reglamento Orgánico Municipal.

que el sello electrónico cualificado), como hemos podido ver en el análisis del artículo 42 de la LRJSP, por lo que lógicamente sería absurdo descartar el uso del sello electrónico para la interoperabilidad de los documentos firmados electrónicamente.

CAPÍTULO 6. LAS OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS

En el modelo regulatorio de los servicios de confianza, resulta preciso cumplir con una serie de obligaciones propias del servicio, incluyendo las referidas a los requisitos del servicio de confianza, y que serán objeto de análisis a lo largo de este Capítulo.

Las obligaciones del prestador de servicios de confianza se establecen en diversos planos normativos, de forma coherente con el modelo de gobernanza multinivel de la Unión Europea. De este modo, en el plano de la Unión Europea, el Reglamento eIDAS establece determinadas obligaciones que resultan aplicables a todos los prestadores de servicios de confianza, presten servicios cualificados o no, obligaciones comunes en relación con todos los servicios cualificados de confianza y, finalmente, requisitos específicos para determinados servicios cualificados de confianza.

Por otra parte, en el plano nacional, el legislador puede establecer obligaciones adicionales a todos los prestadores de servicios de confianza, en relación con servicios cualificados o no, siempre que no se opongan al régimen armonizado por el Reglamento eIDAS. Asimismo, y como es lógico, el legislador nacional es soberano para regular como considere oportuno los servicios de confianza, cualificados o no, que sólo gozan de reconocimiento nacional.

Analizaremos, en primer lugar, las obligaciones exigibles a todos los prestadores de servicios de confianza, con independencia de la cualificación del servicio, para, posteriormente, estudiar las obligaciones específicas ligadas a la prestación de servicios cualificados de confianza.

6.1 LAS OBLIGACIONES COMUNES A TODOS LOS PRESTADORES DE SERVICIOS DE CONFIANZA TIPIFICADOS EN EL REGLAMENTO EIDAS

Para el legislador europeo una de las condiciones importantes de generación de confianza es la existencia de un conjunto mínimo de obligaciones para cualquier prestador de servicios de confianza[973], con independencia de que los servicios sean cualificados o no, y que analizaremos a continuación.

A estas obligaciones legales previstas en el Reglamento eIDAS debemos añadir algunas expresamente previstas en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

[973] (Rodríguez Ayuso, 2018, pág. 310 y ss.) incluye también las obligaciones generales de cualquier prestador de servicios de la sociedad de la información, ya que considera que los prestadores de servicios de confianza son una subespecie de los prestadores de servicios de la sociedad de la información que prestan servicios de intermediación.

6.1.1 La protección de datos de carácter personal; el uso de seudónimos

El artículo 5 del Reglamento eIDAS, aplicable también al régimen de identificación electrónica, ordena que "[e]l tratamiento de los datos personales será conforme a lo dispuesto en la Directiva 95/46/CE", previsión que se reitera, en el caso de los servicios cualificados de confianza, al establecerse en el artículo 24.2.j) del mismo Reglamento eIDAS que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: […] j) garantizarán un tratamiento lícito de los datos personales de conformidad con la Directiva 95/46/CE"[974]; referencias que, a partir del 25 de mayo de 2018 deben entenderse realizadas al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD); así como a la legislación española que lo complemente, una vez haya sido aprobada.

Se trata, ciertamente, de dos previsiones normativas superfluas, dado que la normativa de protección de datos resultaría igualmente aplicable, aún en ausencia de ambas referencias.

Esta obligación existía ya en el artículo 8.1 de la DFE y, en España, en la LFE, cuyo artículo 17.1, aunque sólo referido al servicio de expedición de certificados, determinaba la necesidad de que el prestador de servicios de certificación adecuase su actividad a las prescripciones de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal y a su normativa de desarrollo, principalmente el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, obligación que también se imponía a los órganos administrativos en el ejercicio de sus funciones de supervisión y control estatal.

Aunque no se decía en la DFE ni en la LFE, los terceros destinatarios de documentos firmados también debían proteger adecuadamente los datos personales y, especialmente, tener en cuenta que la finalidad de los datos certificados que recibían era verificar la firma electrónica del suscriptor del certificado, y no podían utilizar estos datos para ninguna otra finalidad, sin el consentimiento expreso del suscriptor, por constituir un cambio de finalidad.

En sentido análogo, y aunque el Reglamento eIDAS tampoco se refiere de forma expresa a la aplicación de la normativa de protección de datos personales a las partes usuarias que confían en las mismas, ello no implica que no resulte aplicable dicha normativa con carácter general, por lo que el tratamiento de los datos personales incorporados a pruebas electrónicas sustentadas por servicios de confianza deberá ajustarse plenamente a la normativa.

Por lo que respecta a la aplicación del nuevo RGPD a los prestadores de servicios de confianza, diversas son las cuestiones de interés.

En primer lugar, y aunque resulte obvio, la aplicación de la normativa de protección de

[974] También el Considerando (11) indica que "los prestadores de servicios de confianza y el organismo de supervisión deben respetar asimismo los requisitos de confidencialidad y seguridad del tratamiento previstos en la Directiva 95/46/CE".

datos de carácter personal se limita a los datos de personas físicas (artículo 1.1 del RGPD) identificadas o identificables (artículo 4.1 del RGPD), por lo que no será aplicable, por ejemplo, a los datos de las personas jurídicas empleados para la prestación de servicios de confianza a las mismas, como sucede en el caso de los sellos electrónicos de personas jurídicas[975].

Más difícil será evitar la aplicación del RGPD a determinados datos incluidos en las pruebas electrónicas sustentadas por los servicios de confianza, como por ejemplo en el caso de los sellos de tiempo electrónico, que incluyen resúmenes criptográficos de los datos objeto de sellado.

Aunque un resumen criptográfico no revela, en principio, información alguna acerca del documento o los datos a partir del que se genera[976], no constituye con carácter general una técnica de anonimización[977], por lo que no permite inaplicar la normativa de protección de datos personales, aunque es cierto que reduce en gran medida la carga de su aplicación[978].

En segundo término, y como no puede ser de otra forma, los principios de protección de datos, recogidos en el artículo 5 del RGPD deben ponerse en relación con cada concreto servicio de confianza, dado que condiciona su prestación. En este sentido, el principio de licitud, lealtad y transparencia[979] conecta claramente con la aplicación estricta de los requisitos previstos para cada servicio de confianza, dado que en caso contrario nos encontraremos ante un tratamiento contrario a este principio.

También el principio de limitación de la finalidad[980] presenta una intensa relación con la tipificación de cada servicio de confianza, así como con la causa negocial que subyace a su contratación, de modo que la recogida de datos en relación con la prestación de un servicio de confianza sólo podrá tener como finalidad determinada, explícita y legítima del tratamiento precisamente la prestación del servicio de confianza, y con independencia de que se pueda producir, posteriormente, un cambio de finalidad.

Por lo que respecta al principio de minimización de datos[981], el mismo exige que el

---

[975] Sin embargo, la normativa resultará aplicable a los datos personales de los representantes de las personas jurídicas que se obtienen para la gestión administrativa del servicio.

[976] Cfr. el Anexo A.1.1.1 de este trabajo.

[977] Cfr. el epígrafe 4 del Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014 por el Grupo de Trabajo sobre Protección de Datos del Artículo 29 (0829/14/ES WP126).

[978] Por ejemplo, no será necesario identificar al titular de los datos personales que eventualmente se encuentren contenidos en el documento a partir del que se genera el resumen criptográfico (cfr. artículo 11.1 del RGPD), ni gestionar el consentimiento en caso de posibles cesiones (cfr. artículo 6 del RGPD).

[979] Conforme al artículo 5.1.a) del RGPD, "[l]os datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado […]".

[980] Conforme al artículo 5.1.b) del RGPD, "[l]os datos personales serán: […] b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales […]".

[981] Conforme al artículo 5.1.c) del RGPD, "[l]os datos personales serán: […] c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados […]". El artículo 8.2 de la DFE explicitaba este principio, en relación con el servicio de expedición de certificados de firma electrónica, al

tratamiento de datos personales en cada servicio se limite a los datos adecuados, pertinentes y estrictamente necesarios, por lo que se deberá diseñar el modelo informacional del servicio de forma apropiada[982], en especial cuando nos referimos a servicios de confianza que resultan en la publicidad de dichos datos de carácter personal, como sucede en el caso del servicio de certificación de firma electrónica de persona física, excepto cuando se hace uso de un seudónimo, posibilidad a la que nos referiremos posteriormente con más detalle.

El principio de exactitud[983] también presenta una gran importancia en relación con los servicios de confianza, dado que, como sabemos, la finalidad última de estos servicios es servir de sustento a las pruebas electrónicas, como en el caso de la firma electrónica basada en certificado, en cuyo caso deberá procederse a la revocación del certificado con datos personales inexactos, y nueva expedición de certificados con datos correctos.

El principio de limitación del plazo de conservación[984] presenta también gran relevancia en el ámbito de los servicios de confianza, de nuevo debido a su conexión con la prueba electrónica, por lo que el Reglamento eIDAS establece una obligación específica al respecto, en el caso de los servicios cualificados de confianza, al que nos referiremos posteriormente[985].

También el principio de integridad y confidencialidad[986] va a conectar con las exigencias de seguridad de los servicios de confianza, y con las obligaciones específicas de sistemas fiables de servicios cualificados de confianza, a las que también nos referiremos en breve[987].

---

indicar que "[l]os Estados miembros velarán por que los proveedores de servicios de certificación que expidan al público certificados únicamente puedan recabar datos personales […] en la medida necesaria para la expedición y el mantenimiento del certificado", previsión que se trasladó al artículo 17.2 de la LFE, en cuya virtud "[l]os datos [personales] requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica", previsión que, como se ve, amplía la previsión de la DFE a otros servicios diferentes de la expedición del certificado.

[982] En todo caso, el principio de minimización de datos conecta con los conjuntos de datos previstos para algunos servicios de confianza, como en el caso de los certificados de firma electrónica, en relación con los cuales el Anexo I del Reglamento eIDAS prevé los datos mínimos que deben contener, sin perjuicio de otros atributos, que lógicamente podrán incluirse en función del principio de finalidad. Cfr. el epígrafe 2.1.2.1 de este trabajo.

[983] Conforme al artículo 5.1.d) del RGPD, "[l]os datos personales serán: […] d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan […]".

[984] Conforme al artículo 5.1.e) del RGPD, "[l]os datos personales serán: […] e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales […]".

[985] Cfr. el epígrafe 6.2.7 de este trabajo.

[986] Conforme al artículo 5.1.f) del RGPD, "[l]os datos personales serán: […] f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas […]".

[987] Cfr. los epígrafes 6.1.3 y 6.2.5 de este trabajo.

Finalmente, el principio de responsabilidad proactiva[988] va a quedar absorbido por las estrictas exigencias que, en materia de responsabilidad, contiene el Reglamento eIDAS, en especial en el caso de los servicios cualificados de confianza.

En tercer lugar, el RGPD establece restricciones en relación con el tratamiento de determinadas categorías de datos personales, cuando en su artículo 9.1 prohíbe "el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física", prohibición que resulta, como no puede ser de otra forma, aplicable a la prestación de servicios de confianza.

En sentido similar, el artículo 17.4 de la LFE prohibió a los prestadores de servicios de certificación incluir en los certificados ningún dato de los indicados en el artículo 7 de la Ley Orgánica 15/1999, incluso con la solicitud previa y el consentimiento del firmante[989]; eso es, datos relativos a ideología, religión o creencias; afiliación sindical; raza, salud y vida sexual; e infracciones penales o administrativas.

Aun existiendo esta prohibición, parecería excesivo no admitir la posibilidad de emitir certificados a los miembros de un partido político, o de un sindicato, con el atributo de "miembros-de" dichas organizaciones, certificados que, aunque no informen expresamente de los datos prohibidos, ciertamente de forma implícita suministran esta información a los terceros; por lo que se debe valorar positivamente que esta prohibición no se haya incorporado al Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, dejando esta cuestión regulada estrictamente en el ámbito de la normativa de protección de datos de carácter personal.

Desde este punto de vista, es necesario decir que la prohibición contenida en el artículo 9.1 del RGPD no resulta aplicable en determinados casos previstos en el epígrafe 2 del mismo artículo 9, entre los cuales resultan de interés, en cuanto nos ocupa, que "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado" (numeral a) del artículo 9.2 del RGPD), aplicable con carácter general, pero siempre que el consentimiento se pueda retirar en cualquier momento; que "el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado" (numeral b) del

---

[988] Confirme al artículo 5.2 del RGPD, "[e]l responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo".

[989] Para (Ortega Díaz, 2008, págs. 129-130), "[p]ocas dudas existen acerca de lo acertado de esta decisión del legislador", en atención a que "[u]no de los mayores miedos generados en el ámbito de los certificados electrónicos era la posibilidad de que, determinados titulares de certificado, fueran obligados a poseer certificados en los que, contenidos estos datos a título de atributo, los mismos pudieran ser conocidos cada vez que se basaba en ellos una firma electrónico", citando como ejemplos el de una aseguradora que obligue a sus usuarios disponer de un certificado con su registro de infracciones administrativas, y el de una compañía aérea que exija un atributo que declare la salud mental del usuario.

artículo 9.2 del RGPD), aplicable al caso de certificados de empleados que incorporen biometría para el control de acceso, por ejemplo; o que "el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados" (numeral d) del artículo 9.2 del RGPD), en el caso ya mencionado de certificados expedidos a miembros de estas organizaciones.

En presencia de estas excepciones, por tanto, no deberá resultar problemático prestar servicios de confianza empleando estos datos, en especial en el caso de la expedición de certificados de firma electrónica, aunque ello dependerá del escenario concreto.

En cuarto lugar, debemos referirnos al uso de seudónimos, posibilidad expresamente previstas en el Reglamento eIDAS; esto es, nombres alternativos que un suscriptor de un certificado de persona física puede utilizar, en lugar de su nombre y apellidos reales, manteniendo la capacidad de producir firmas válidas y eficaces jurídicamente.

El uso de los seudónimos, que supone una cierta ruptura de la función clásica de identificación de la firma personal, se autorizaba ya, en relación con la expedición de certificados, en el artículo 11.1 de la LFE, que en su numeral e) permitía que la identificación del firmante se realizase mediante un seudónimo, que debía constar como tal de forma inequívoca, y que se regulaba posteriormente, en el artículo 17.3 de la LFE, en los siguientes términos: en primer lugar, el servicio sólo se podía prestar a solicitud del firmante; en segundo lugar, el prestador debía comprobar la identidad personal del firmante (de acuerdo con el artículo 13 de la LFE) y conservar la documentación acreditativa correspondiente; finalmente, el prestador deberá divulgar la identidad del firmante cuando lo solicitasen los órganos judiciales en el ejercicio de sus funciones y en el resto de casos que prevé el artículo 11.2 de la LOPD en que así se requiera (debiéndose entender que se refería a las comunicaciones al Defensor del Pueblo, al Ministerio Fiscal, a los Jueces y Tribunales, y al Tribunal de Cuentas, así como las instituciones correspondientes de las comunidades autónomas) [990].

Como se ha avanzado, el Reglamento eIDAS mantiene la posibilidad de uso de seudónimos en el caso de certificados de firma electrónica de persona física, indicando en su artículo 5.2 que "[s]in perjuicio de los efectos jurídicos que la legislación nacional contemple para los seudónimos, no se prohibirá su utilización en las transacciones electrónicas", previsión de carácter general que entra potencialmente en conflicto con normas sectoriales que puedan imponer la obligación de identificación real.

En este sentido, el Considerando (33) del Reglamento eIDAS indica que "[l]as disposiciones relativas al uso de seudónimos en los certificados no deben impedir a los Estados miembros exigir la identificación de las personas de conformidad con el Derecho nacional o de la Unión", como por ejemplo en el caso de la necesaria identificación de los interesados en el procedimiento administrativo, o en el caso de la identificación de nuevo cliente conforme a la normativa de prevención de blanqueo de capitales. En todos

[990] Esta norma debe ser complementada con el régimen de uso de seudónimos en los certificados de empleados públicos, a que nos hemos referido en el epígrafe 2.1.4.3 de este trabajo.

estos casos, y como no puede ser de otra forma, no podrá hacerse uso de la posibilidad de empleo exclusivo del seudónimo, debiéndose entender, por tanto, que el Reglamento eIDAS sólo se opondrá a una norma nacional que prohíba todo uso de seudónimo, con carácter general, no en casos sectoriales justificados. Por tanto, se deberá poder hacer uso de la identificación de persona física basada en seudónimo en aquellos casos en que no exista una norma de Derecho de la Unión o una norma nacional que exija la identificación real[991], algo que deja bastante espacio a la autonomía de la voluntad de las partes.

Diferente de lo anterior será el efecto que cada legislación nacional establezca en relación con el uso del seudónimo, caso que establezca alguno, así como la regulación complementaria que pueda establecer cada Estado miembro en relación con el tratamiento del seudónimo en el certificado.

En este segundo caso, el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza autoriza el uso de un seudónimo para la identificación del titular en los certificados cualificados expedidos a personas físicas en su artículo 6.1.a), estableciendo, en su artículo 8.1, que "[l]os prestadores de servicios electrónicos de confianza que consignen un seudónimo en un certificado electrónico deberán constatar la verdadera identidad del firmante o titular del certificado y conservar la documentación que la acredite", en línea con la normativa anterior – aunque sin que sea preciso ya que el servicio se preste exclusivamente a petición del firmante –, y manteniéndose también la previsión[992] de que "[d]ichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones que tienen atribuidas con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales".

Ciertamente, nos encontramos ante un tratamiento que, para ser lícito, deberá basarse en lo establecido en el artículo 6.1.e) del RGPD, que determina la licitud del tratamiento si "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento", para lo cual se precisa una base jurídica establecida en los términos del epígrafe 3 del artículo 6, que cumpla un objetivo de interés público y sea proporcional al fin legítimo perseguido.

La amplia referencia a las "otras autoridades públicas" contenida en el Anteproyecto puede, en este sentido, resulta problemática, debiéndose justificar el acceso –sin consentimiento, claro– a la identidad real en una base jurídica suficiente, dada la evidente dimensión constitucional del derecho de protección de datos y otras libertades en juego, por ejemplo, en cuanto al derecho constitucional al secreto de las comunicaciones electrónicas, en el caso del servicio de confianza de entrega electrónica certificada.

---

[991] En relación con esta cuestión, resulta muy interesante el enfoque adoptado en el Derecho alemán, que autoriza el uso de la firma con seudónimo en el ámbito tributario, pero siempre que la persona demuestre su identidad real a la autoridad financiera. Cfr. el artículo 5 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungs*gesetz), de 18 de julio de 2017, que modifica la sección § 87a del Código Fiscal.

[992] Una previsión muy similar se contiene en el nuevo artículo XII.26 del Código belga de Derecho Económico –Libro XII, relativo al Derecho de la Economía Electrónica–, añadido por artículo 8 de la Ley de 21 de julio de 2016, que no contiene esta referencia al RGPD.

También el titular de un certificado de firma electrónica con atributo de representante puede ser identificado mediante seudónimo, en línea con otras leyes, como la alemana, que permite esta opción siempre y cuando el representado lo admita expresamente, y que también la permite en el caso de certificados con atributo de pertenencia a una organización profesional, siempre que la misma autorice el uso del seudónimo[993].

Otras leyes nacionales, como la italiana[994], han previsto un plazo mínimo de conservación de la información acreditativa de la identidad real de la persona identificada mediante el seudónimo; en este caso, de veinte años, plazo que coincide con el previsto, con carácter general para cualesquiera otras informaciones del certificado cualificado.

En quinto lugar, a las personas físicas cuyos datos personales sean objeto de tratamiento conectado con la prestación de cualquier servicio de confianza corresponden los derechos reconocidos en el RGPD, pero ciertamente con algunos matices importantes, derivados de la finalidad última de los servicios de confianza; esto es, el sustento del valor y la eficacia de las pruebas electrónicas de la actuación.

Los derechos de información y acceso a datos de carácter personal, previstos en los artículos 13 a 15 del RGPD no presentar particularidades dignas de mención especial. En cambio, el derecho de rectificación previsto en el artículo 16 del RGPD implicará, en función del caso, la modificación del servicio de confianza, como, por ejemplo, la revocación y nueva expedición del certificado de firma electrónica de persona física.

Por su parte, el novedoso derecho de supresión (también denominado "derecho al olvido") previsto en el artículo 17 del RGPD, aunque plenamente aplicable[995] –dado que el tratamiento de datos de carácter personal en el marco de la prestación de servicios de confianza se basará, normalmente, en el consentimiento del interesado–, debe ser puesto en relación con la obligación de conservación de informaciones que se impone al prestador del servicio, a la que nos referiremos posteriormente[996], plazo durante el cual los datos no podrán ser suprimidos[997]; en un tratamiento análogo al del derecho de

---

[993] Cfr. la sección § 12 de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (eIDAS-Durchführungsgesetz), de 18 de julio de 2017.

[994] Cfr. el artículo 33.1 del *CAD*, en redacción dada por Decreto legislativo nº 235, de 30 de diciembre de 2010.

[995] En este sentido, la supresión procederá cuando "a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; […] e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento" (artículo 17.1 del RGPD).

[996] Cfr. el epígrafe 6.2.7 de este trabajo.

[997] Así, conforme al epígrafe 3 del artículo 17 del RGPD, no será aplicable ese derecho cuando el tratamiento sea necesario "para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento […]", como es el caso; aunque tampoco lo será cuando el tratamiento sea necesario "para la formulación, el ejercicio o la defensa de reclamaciones".

cancelación anteriormente existente.

Con respecto al derecho a la limitación del tratamiento previsto en el artículo 18 del RGPD, el mismo podrá implicar, en aquellos Estados que lo hayan regulado, la suspensión del certificado de firma electrónica –caso de impugnación de la exactitud de los datos contenidos en el mismo– o el mantenimiento de las informaciones a efectos estrictamente probatorios, en beneficio del interesado, algo especialmente relevante en relación con los mecanismos de información acerca del estado de la validez de los certificados, por ejemplo.

El también novedoso derecho a la portabilidad de datos, previsto en el artículo 20 del RGPD, debe considerarse aplicable a los servicios de confianza, en especial en atención a la naturaleza técnica de los citados servicios, si bien no existen a fecha de este trabajo normas técnicas para el intercambio de datos de personas físicas entre prestadores, ni desde luego se conocen procedimientos por parte de los prestadores (quizá porque aún no se encuentra en vigor este derecho…). Este derecho debe entenderse, como no puede ser de otra forma, sin perjuicio de que la transferencia implicará la previa baja del servicio de confianza.

En cierto modo, el Reglamento eIDAS, igual que la normativa anterior, contempla una suerte de derecho a la portabilidad de los datos en caso de cese del servicio, aunque de forma muy limitada, como tendremos ocasión de analizar[998].

Finalmente, el prestador del servicio de confianza puede ostentar dos posiciones jurídicas diferenciadas, dado que puede actuar como responsable del tratamiento[999] o como encargado del tratamiento[1000], algo que va a variar en función del caso concreto.

El prestador de servicios de confianza es responsable del tratamiento[1001] cuando ofrece directamente sus servicios a las personas físicas cuyos datos trata durante la prestación de servicio, como por ejemplo cuando expide un certificado de firma electrónica a una persona física; sin embargo, si el prestador es contratado por una empresa para expedir certificados a los trabajadores de dicha empresa, estará actuando como encargado del tratamiento de dicha empresa, que es el responsable del tratamiento con respecto a dichos trabajadores.

De forma análoga sucede con el servicio de confianza de entrega electrónica certificada, en el que el prestador del servicio actuará normalmente como encargado del tratamiento,

---

998 Cfr. el epígrafe 6.2.8 de este trabajo.

999 El artículo 4.7 del RGPD lo define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

1000 El artículo 4.8 del RGPD lo define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

1001 En el Considerando (24) de la Propuesta de Reglamento eIDAS se decía, sin embargo, que "[u]n proveedor de servicios de confianza es un responsable del tratamiento de los datos personales y, por tanto, ha de cumplir las obligaciones previstas en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", en un enfoque incorrecto que, por fortuna, no se trasladó al texto finalmente aprobado.

dado que habitualmente será contratado por el remitente de la comunicación objeto del servicio, que le suministrará los datos personales del futuro receptor de la citada comunicación[1002]; y que se trata del mismo tratamiento que existe actualmente en relación con los envíos postales físicos[1003].

Choca con este modelo la previsión contenida en el artículo 17.2 de LFE, en cuya virtud los prestadores que emitan certificados al público sólo pueden obtener datos directamente de los firmantes (suscriptores de certificados) o bien con su consentimiento previo y expreso, previsión que, correctamente en nuestra opinión, no se ha mantenido en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

Al contrario, hubiera sido deseable que se incorporase al Anteproyecto de Ley español una previsión como la contenida en el derecho alemán[1004], que autoriza a los prestadores la obtención y tratamiento de datos de carácter personal de terceros, y no del interesado, cuando resulte necesario para ofrecer el servicio de confianza, incluyendo las verificaciones precisas para dicho servicio, así como para mantener su validez jurídica.

6.1.2 La accesibilidad del servicio de confianza y de los productos para el usuario final utilizados en su prestación

Conforme al artículo 15 del Reglamento eIDAS, "[s]iempre que sea factible, los servicios de confianza prestados y los productos para el usuario final utilizados en la prestación de estos servicios deberán ser accesibles para las personas con discapacidad", obligación que especifica, para el ámbito de los servicios de confianza, el régimen ya existente en el nivel nacional; y que ya existía en la DFE y en la LFE.

En España, debemos hacer referencia al Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social y su normativa de desarrollo, principalmente contenida en el Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

En concreto, el artículo 24.1 de la citada Ley ordena que "[l]as condiciones básicas de accesibilidad y no discriminación para el acceso y utilización de las tecnologías, productos y servicios relacionados con la sociedad de la información y de cualquier medio de comunicación social serán exigibles en los plazos y términos establecidos

---

[1002] Existen excepciones posibles a lo que se acaba de indicar: la primera, cuando el receptor es identificado mediante un sello electrónico de persona jurídica, no será aplicable la normativa de protección de datos, dado que el certificado correspondiente no contiene datos personales; la segunda, cuando el remitente de la comunicación sea una persona física que no tiene la condición de responsable del tratamiento, por ejemplo por actuar en un ámbito exclusivamente personal o doméstico (artículo 2.d) del RGPD), en cuyo caso el prestador de servicios de confianza será considerado como responsable del tratamiento.

[1003] Cfr. el Informe 0309/2008, del Gabinete Jurídico de la Agencia Española de Protección de Datos, referido a la recepción de direcciones de personas físicas por correo o fax, para la realización de envíos.

[1004] Cfr. la sección § 8 (1) de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017.

reglamentariamente", término que la disposición adicional tercera, numeral a), de la propia Ley, fija en el 4 de diciembre de 2009, por lo que debe entenderse que esta obligación se encuentra plenamente vigente.

Por su parte, el Real Decreto 1494/2007 viene a "establecer los criterios y las condiciones que se consideran básicos para garantizar el acceso de las personas con discapacidad a las tecnologías, productos y servicios de la sociedad de la información […], de acuerdo con los principios de igualdad de oportunidades, no discriminación y accesibilidad universal", resultando aplicable a los servicios de confianza, y que afecta, de un lado, a la accesibilidad de la página de Internet del prestador de servicios de confianza (artículo 6) y, de otro, a la accesibilidad de los programas de ordenador (artículo 8), si bien en este caso el sujeto destinatario de la norma será realmente el fabricante, y sin perjuicio de que el prestador de servicios de confianza deba elegir, cuando los suministre en el marco de su actividad, programas informáticos que se encuentren alineados con lo establecido en dicha norma.

Curiosamente, el artículo 9 del citado Real Decreto ordena que "[d]e acuerdo con lo establecido en la disposición adicional novena de la Ley 59/2003, de 19 de diciembre, de firma electrónica, los servicios, procesos, procedimientos y dispositivos de firma electrónica deberán ser plenamente accesibles a las personas mayores y personas con discapacidad, las cuales no podrán ser, en ningún caso, discriminadas en el ejercicio de sus derechos y facultades por causas basadas en razones de discapacidad o edad avanzada", por lo que "será de aplicación lo establecido en los artículos 5, 6 y 8 de este reglamento a los servicios, procesos, procedimientos y dispositivos de firma electrónica".

Desde una perspectiva más práctica, en relación con la accesibilidad de la página web el prestador de servicios de confianza, la disposición transitoria única del Real Decreto aclara que "todas las páginas, actualmente existentes o de nueva creación, deberán cumplir la prioridad 2 de la Norma UNE 139803:2004 a partir del 31 de diciembre de 2008", norma que ha sido posteriormente sustituida por la Norma UNE 139803:2012: Requisitos de accesibilidad para contenidos en la Web, idéntica a la Guía de Accesibilidad de Contenido Web 2.0 del Consorcio W3C, aprobada como Norma Internacional ISO/IEC 40500:2012; y cuyo cumplimiento puede ser acreditado mediante cualquier medio de prueba válido en Derecho, así como mediante la certificación de accesibilidad de página web prevista en el artículo 7 del mismo Real Decreto.

Por lo que se refiere a los productos, el artículo 8 del Real Decreto sólo indica, en su epígrafe 2, que "[s]e deberán promover medidas de sensibilización y difusión para que los fabricantes de equipos informáticos y de programas de ordenador incorporen a sus productos y servicios, progresivamente y en la medida de lo posible, los criterios de accesibilidad y de «Diseño para todos», que faciliten el acceso de las personas mayores y personas con discapacidad a la sociedad de la información", declaración –ni siquiera de principios– tan laxa como la contenida en el propio Reglamento eIDAS, algo que ciertamente resulta criticable a medida que se despliega el uso de estos servicios de confianza a una parte cada vez mayor de la población, como en el caso del certificado electrónico del DNI electrónico.

Desde una perspectiva de normas técnicas voluntarias, la importante norma ETSI EN 319 401 incluye la ineludible referencia a la necesidad de cumplir con los criterios de accesibilidad, remitiendo a la norma ETSI EN 301 549, que recopila los requisitos en materia de accesibilidad a tener en cuenta en procedimientos de contratación pública, facilitando el cumplimiento de esta obligación.

6.1.3 La aplicación de medidas de seguridad y la notificación de incidentes de seguridad

Una de las novedades más relevantes del nuevo modelo regulatorio referido a los servicios de confianza, al que ya nos hemos referido, se refiere a las medidas de seguridad que deben obligatoriamente aplicar todos los prestadores[1005] y que, como sabemos, conectan directamente con la noción de servicio de confianza.

En este sentido, el artículo 19.1 del Reglamento eIDAS ordena que "[l]os prestadores cualificados y no cualificados de servicios de confianza adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan", las cuales, "[h]abida cuenta de los últimos avances tecnológicos, […] garantizarán un nivel de seguridad proporcionado al grado de riesgo", debiendo los prestadores adoptar "medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad […]".

Se trata de un enfoque de medidas de seguridad basado en criterios de análisis de riesgos –que debe partir de que los servicios de confianza cualificados deben garantizar un alto nivel de seguridad[1006] y garantizar, cuando corresponda, la protección de los derechos y libertades de las persona físicas cuyos datos son objeto de tratamiento[1007]–, y con la particularidad, anteriormente comentada[1008], de que la Comisión puede establecer una mayor especificación de las medidas de seguridad que deberán cumplir los prestadores, constituyendo dicha especificación un verdadero reglamento técnico obligatorio de servicio.

De momento la Comisión no ha hecho uso de esta potestad, sino que ha adoptado una posición de corte más liberal, encomendando a la Agencia Europea de Seguridad de Redes y de la Información (ENISA) la producción de una serie de guías voluntarias relativas a los servicios de confianza, cuyo valor interpretativo, como instrumento de *soft law* que son, resulta indudable.

En efecto, el prestador que se adhiera a dichas guías siempre estará en mejor posición para demostrar el adecuado cumplimiento, por su parte, de esta obligación de seguridad, que en caso contrario. Una de las guías de ENISA, en concreto, se refiere al marco de seguridad de los prestadores de servicios de confianza, e identifica – además de los elementos de un proceso de análisis de riesgos que se puede considerar apropiado para el

---

[1005] Para (Gobert, Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie, 2015, p. 31), se trata de la obligación troncal a todos los prestadores de servicios de confianza, y la más importante, derivada del "trauma" de DigiNotar.

[1006] El Considerando (28) del Reglamento eIDAS conecta confianza y seguridad elevada, cuando indica que "[p]ara aumentar en particular la confianza de las pequeñas y medianas empresas y los consumidores en el mercado interior y fomentar el uso de servicios y productos de confianza, deben introducirse los conceptos de servicios de confianza cualificados y de prestador cualificado de servicios de confianza con miras a indicar los requisitos y obligaciones que garanticen un alto nivel de seguridad de cualquier servicio o producto de confianza cualificado que se preste o utilice".

[1007] Para ello, el prestador del servicio debe identificar y aplicar las correspondientes medidas de seguridad, conforme al artículo 32 del RGPD, en el marco del artículo 25 del propio RGPD, relativo a la privacidad por diseño y por defecto.

[1008] Cfr. el epígrafe 1.4.2 de este trabajo.

Reglamento eIDAS, un catálogo de escenarios de riesgos[1009] a los que habitualmente deberán hacer frente los prestadores.

También es posible considerar criterios relevantes de seguridad previstos en las normas técnicas voluntarias reguladoras de los servicios de confianza, como por ejemplo ETSI EN 319 401[1010], aplicable con carácter general a todo servicio de confianza; ETSI EN 319 411, partes 1 y 2, aplicable a los servicios de expedición de certificados de firma electrónica, sello electrónico o autenticación de sitio web; ETSI EN 319 421, aplicable al servicio de sellado de tiempo electrónico, etc.

Como sabemos, dichas normas pueden ser establecidas por la Comisión Europea a los efectos de presumir el cumplimiento de los requisitos del servicio, incluidos los requisitos de seguridad, por lo que resultaría conveniente que dicha aprobación se produjese. Pero el valor práctico de estas normas, incluso sin esta aprobación por la Comisión, es muy importante, dado que son las normas que contienen los criterios para la evaluación de la conformidad[1011].

Es preciso, finalmente, recordar[1012] que el legislador nacional puede también establecer sus propias normas sobre medidas obligatorias de seguridad, siempre que no entren en colisión con las que pueda establecer la Comisión.

Igualmente resulta novedoso que el Reglamento eIDAS imponga a los prestadores de servicios de confianza la obligación de "informar a los interesados de los efectos negativos de cualquiera de tales incidentes" (artículo 19.1 *in fine*), obligación que se concreta en el epígrafe 2 del propio artículo 19, cuando se ordena que "[l]os prestadores cualificados y no cualificados de servicios de confianza, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, notificarán […] cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes", notificación que deberá realizarse "al organismo de supervisión y, en caso pertinente, a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos".

Se trata de una obligación orientada a garantizar que el organismo de supervisión pueda tener acceso a la información acerca de los incidentes de seguridad, aunque no de todos ellos, sino únicamente de aquéllos que tengan un impacto significativo, concepto que el Reglamento eIDAS no concreta, y que puede resultar problemático, dado que en caso de

---

[1009] Incluyendo el compromiso de una autoridad de certificación, el compromiso de los algoritmos criptográficos, el compromiso de una autoridad de registro, el compromiso de los servicios de revocación, la brecha de seguridad de datos personales, la suplantación, la pérdida de disponibilidad de los servicios de certificación, la alegación de repudio por parte del suscriptor del certificado, el compromiso de un par de claves de suscriptor, el compromiso de una autoridad de validación o el compromiso de una autoridad de sellado de tiempo.

[1010] Dicha norma considera la necesidad de realizar un análisis de riesgos, de disponer de una política de seguridad de la información, de establecer controles de seguridad organizativa, de segregación de funciones, de control de los recursos humanos, de control de acceso físico y lógico, de seguridad operativa, de seguridad de red, de gestión de incidencias, de recolección de evidencias, y de gestión de la continuidad; por lo que esencialmente puede considerarse como una norma de seguridad general.

[1011] Cfr. el epígrafe 7.1.1 de este trabajo.

[1012] Cfr. el epígrafe 1.4.2 de este trabajo.

discrepancia entre qué consideren como significativo el prestador de servicios y el organismo de supervisión, el primero puede enfrentarse a un posible procedimiento sancionador.

Nótese, además, que dicho impacto recaer sobre el servicio o sobre los datos de carácter personal, y que, en función del caso, puede ser preciso realizar más de una notificación. Así será, en todo caso, cuando se vean afectados datos de carácter personal, debiéndose realizar la notificación a la autoridad de control correspondiente, en los términos previstos en el RGPD[1013] y conforme al reparto de competencias en sede nacional[1014].

El Reglamento eIDAS también se refiere a la posibilidad de tener que realizar una notificación complementaria al organismo nacional competente en materia de seguridad de la información, en aquellos Estados donde se establezca uno, como por ejemplo en el caso de Alemania; y a la persona física o jurídica a la que se ha prestado el servicio de confianza, cuando la violación de seguridad o la pérdida de integridad puedan atentar contra la misma, notificación que –a diferencia de las anteriores– debe realizarse "sin demora indebida".

Esta última posibilidad persigue que la persona afectada conozca la incidencia y, en su caso, pueda adoptar las medidas que considere oportunas, inclusive de tipo resarcitorio frente al prestador; y para garantizar dicho conocimiento, el cuarto párrafo del artículo 19.2 del Reglamento eIDAS ordene que "[e]l organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad o la pérdida de integridad reviste interés público", potestad que requerirá de la correspondiente motivación, dado el evidente daño reputacional que se causará, en este caso, al prestador de servicios de confianza.

Se trata, de todos los casos, de mecanismos de información que persiguen corregir una de las principales disfunciones del mercado de la seguridad –en el que se puede ubicar a la prestación de servicios de confianza–, que es la fuerte asimetría informativa[1015] generada por la opacidad de las entidades que sufren incidentes de seguridad.

En España, el organismo de supervisión ha concretado algunos detalles de la obligación de notificación de incidentes de seguridad mediante una Guía disponible en su página web[1016], de forma similar a como ya vimos en relación con la notificación de servicios

---

[1013] Cfr. los artículos 33, 34 y 55 del RGPD, de los que resulta relevante el plazo para la notificación, que no debe ser superior a las 72 horas, notificación que no deberá realizarse si es "improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas". Asimismo, cuando el prestador de servicios de confianza actúe como encargado del tratamiento, parece que deberá realizar la notificación a través del responsable del tratamiento, aunque es más que probable, dado el tenor literal del Reglamento eIDAS en este punto, que la notificación a la autoridad de protección de datos sea realizada directamente por el prestador de servicios de confianza que actúa como encargado del tratamiento, a fin de evitar la comisión de una posible infracción, aspecto que debería ser previsto en el contrato de encargo del tratamiento.

[1014] En el caso del Estado español, normalmente la autoridad de control será la Agencia Española de Protección de Datos, aunque en el caso de prestadores públicos de servicios de confianza establecidos en Cataluña y País Vasco, la autoridad de control será la autonómica.

[1015] Así lo ha denunciado la doctrina. Cfr., por todos, (Anderson & Moore, 2007).

[1016] Que no en la sede electrónica; disponible en http://www.mincotur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Documents/Gu%C3%ADa%20Notificaci%C3%B3n%20de%20incidentes

cualificados de confianza, debiéndose emplear el mismo procedimiento electrónico que en este caso.

En cualquier caso, merece la pena indicar que en dicha Guía se establece un plazo de 24 horas para la notificación, que se cuenta desde que el prestador tenga conocimiento del incidente, en el que se debe aportar una información mínima[1017], y un segundo plazo de 1 mes, el que se deberá aportar la restante información sobre el incidente, "analizado exhaustivamente el incidente de seguridad, sus causas, consecuencias y medidas tomadas".

Se trata de un régimen que se regula en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, estableciendo, de una parte, la obligación de tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten (artículo 14.2), y, de otra, confirmando el plazo previsto en la mencionada Guía, puesto que, conforme al epígrafe 3 del mismo artículo 16, "[l]os prestadores de servicios ampliarán en un plazo máximo de un mes tras la resolución del incidente la información suministrada en la notificación inicial con arreglo a las directrices y formularios que pueda establecer el Ministerio de Energía, Turismo y Agenda Digital"[1018].

6.1.4 La publicación de información veraz

El artículo 9.1.a) del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza ordena a los prestadores "[p]ublicar información veraz y acorde con esta ley y el Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014", obligación de carácter general que parece apropiada y proporcionada a la necesidad de que los servicios de confianza sean realmente fiables.

La información a la que se refiere el artículo será, en particular, aquella prevista para el conocimiento del funcionamiento del servicio por parte de los futuros usuarios[1019], de los usuarios y también de las terceras partes que confían, así como la documentación de prácticas del servicio[1020].

6.1.5 El no almacenamiento ni la copia de las claves, excepto en caso de su gestión en nombre del titular

El artículo 9.1.b) del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza impone, a todos los prestadores de servicios de

---

%20de%20seguridad.pdf.

[1017] Esta información incluye: fecha y hora en la que se tuvo conocimiento del incidente; fecha y hora de finalización del incidente, en su caso, o de la previsión de su solución; datos de contacto de la persona responsable de la gestión del incidente; datos de identificación del prestador de servicios de confianza involucrado; descripción del servicio afectado; descripción, en su caso, de los datos personales afectados; breve descripción del incidente de seguridad; resumen de medidas adoptadas o que se prevén adoptar para contrarrestar el incidente; y, en su caso, consecuencias transfronterizas del incidente.

[1018] En la actualidad, el Ministerio de Economía y Empresa.

[1019] Cfr. el epígrafe 6.2.4 de este trabajo.

[1020] Cfr. el epígrafe 6.1.6 de este trabajo.

confianza, con o sin cualificación, el "[n]o almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, de sello o de autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular", ampliando el régimen establecido por el Reglamento eIDAS para la firma electrónica cualificada y el sello electrónico cualificado, que ya hemos analizado[1021], a los prestadores que ofrezcan este servicio en relación con la firma electrónica avanzada o el sello electrónico avanzado, de una parte; y a los prestadores de servicios que lo ofrezcan en relación con el certificado de autenticación de sitio web.

Esta obligación (de no hacer) trae cuenta de la normativa anterior[1022], y se encuentra implícita en el Reglamento eIDAS, interpretado *a sensu contrario*, pero sólo en relación con la firma electrónica cualificada y el sello electrónico cualificado, por lo que nos encontramos ante una importante ampliación de su contenido, al extenderse a prestadores sin cualificación, de un lado, y a los certificados de autenticación de sitio web, de otro.

De esta forma, se asegura el legislador español de que estos datos sólo son almacenados o copiados por un prestador de servicios de confianza que los gestione en nombre de su titular, en cuyo caso "se utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado", debiéndose además "custodiar y proteger los datos de creación de firma, de sello o de autenticación de sitio web frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad", todo ello conforme al segundo párrafo del artículo 9.1.b.) del Anteproyecto.

Se trata de una previsión que se inspira de forma bastante clara en el Considerando (52) del Reglamento eIDAS, aunque va más allá al imponer exigencias de seguridad[1023] y, lo que es más importante, de disponibilidad continua, que el Reglamento no impone ni siquiera en el caso de la firma electrónica cualificada o del sello electrónico cualificado.

Aunque el legislador los agrupa, lo cierto es que los tres tipos de certificados tienen exigencias legales diferentes, como ya sabemos. En efecto, los datos de creación de firma electrónica deben quedar bajo el control exclusivo del firmante; los datos de creación de sello electrónico, simplemente bajo el control del creador de sellos; y ningún requisito de control de la clave se establece en el Reglamento eIDAS en relación con la autenticación

---

[1021] Cfr. el epígrafe 4.3.1 de este trabajo.

[1022] El numeral j) del Anexo II de la DFE ordenaba a los proveedores de servicios de certificación que expidieran certificados reconocidos "no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves", mientras que el artículo 18.1.a), en su redacción original, obligó a todos los prestadores a "[n]o almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios". El numeral a) del epígrafe 1 del artículo 18 fue modificado por Ley 25/2015, de 28 de julio, que lo alineó de forma anticipada al Reglamento eIDAS. En relación con el régimen legal anterior, cfr. (Martínez Nadal, 2009, págs. 325-330), que identifica la dificultad de demostrar el cumplimiento, resultando conveniente realizar auditorías periódicas que revisen y controlen este punto. Para (Ortega Díaz, 2008, págs. 113-114) resultaba conforme a la LFE que la generación de claves fuera realizada por un tercero diferente del certificador y del usuario, aunque consideraba esta posibilidad demasiado arriesgada.

[1023] Estas medidas deben añadirse a las generales de seguridad previstas por la normativa. Cfr. el epígrafe 6.1.3 de este trabajo.

de sitio web. Por ello, el alcance y rigor de esta obligación debería ponerse en relación con lo anteriormente expuesto.

Por otra parte, esta obligación no aplicará cuando las claves se entreguen a un tercero sin la consideración de prestador de servicios de confianza[1024], para su gestión –lo que es posible en el caso de los datos de creación de firma electrónica avanzada, de sello electrónico avanzado y de autenticación de sitio web, pero no en el caso de la firma electrónica cualificada ni del sello electrónico cualificado[1025]–, por lo que esencialmente se trata de una obligación dirigida al prestador de servicios de confianza que haya generado las claves, o a un prestador de servicios de confianza que las gestione en conexión con un servicio de confianza diferente que ofrezca, como por ejemplo la entrega electrónica certificada.

En su consecuencia, y dado que, como acabamos de ver, la Ley no establece a terceros diferentes de los prestadores de servicios de confianza prohibición alguna de almacenamiento o gestión de claves en nombre de un suscriptor de certificados, resultará posible que una Administración Pública se dote de un certificado cualificado de autenticación de sitio web, para su sede electrónica[1026], y le encomiende las claves a un centro de servicios de hospedaje de sitios de Internet donde se encuentre la página web correspondiente a dicha sede electrónica.

Se trata de un régimen que resulta criticable, que muestra una cierta desconfianza hacia los prestadores de servicios de confianza, a los que se prohíbe lo que, en cambio, se permite a terceros, que ninguna obligación legal tienen al respecto, ni se encuentran sujetos a marco de supervisión alguno.

6.1.6 La declaración de prácticas del servicio de confianza

Finalmente, el artículo 10 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza viene a exigir a todos los prestadores el disponer de una declaración de prácticas que los servicios electrónicos de confianza, a la que define, en su epígrafe 1, como "[u]n documento en el que los prestadores de servicios electrónicos de confianza describen la forma en que prestan el servicio y aseguran el cumplimiento de las obligaciones legalmente exigibles, e informan al público sobre el modo correcto de utilización de sus servicios", documento que "estará disponible al

[1024] Motivo por el que quedará excluido de la aplicación de la normativa, al no ser la gestión de claves por cuenta de su titular un servicio de confianza tipificado en el Reglamento eIDAS. Cfr. el epígrafe 1.3.1 de este trabajo. Respecto al almacenamiento de la clave por el propio prestador de servicios de certificación, (Pérez Pereira, 2009, pág. 149) consideró legalmente viable sortear la prohibición acudiendo a "la posibilidad de que PSC firme con el titular del certificado un contrato de depósito, independiente del contrato de certificación, mediante el cual entrega algo (por ejemplos, los datos de creación de firma), mientras que el PSC los custodiará y guardará, según lo establecido en el código de comercio para los contratos de depósito; en cuyo caso, debería establecerse en el contrato que el PSC no tiene constancia de cuál es el contenido exacto del depósito (por ejemplo, si se entregan en un sobre cerrado, o incluidos en un soporte magnético)", posibilidad que podría ser considerada como un evidente fraude de ley por el órgano de supervisión, comparada con realizar un depósito notarial, por ejemplo.

[1025] Motivos legales aparte, no es posible porque estos datos se encuentran en el interior del dispositivo cualificado correspondiente, del que no pueden ser extraídos, como hemos visto en el epígrafe 4.1.3 de este trabajo.

[1026] Sobre este tipo de certificado, cfr. el epígrafe 2.1.4.1 de este trabajo.

público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita".

El epígrafe 2 del mismo artículo 10 concreta los contenidos de este documento para el caso del servicio de expedición de certificados, de modo que el mismo "describirá las condiciones aplicables a la solicitud y expedición de un certificado, incluida la celebración de un contrato; detallará los términos aplicables a la suspensión y extinción de la vigencia de los certificados, e informará sobre la existencia de un servicio de consulta sobre la vigencia de los certificados", y también "indicará las obligaciones del titular en el uso del certificado, la forma en que han de custodiarse los datos de creación de firma, de sello o de autenticación de sitio web, y los medios que los protegen, así como cualquier recomendación útil para garantizar una buena utilización del certificado".

Se trata de una obligación que trae cuenta de la normativa anterior, puesto que la LFE ya exigió a los prestadores de servicios de certificación que formulasen este documento[1027], con los contenidos mínimos previstos en el artículo 19 de la citada Ley.

A diferencia del régimen legal anterior, muy detallado y alineado con la especificación técnica de referencia en esta materia, que no es otra que la IETF RFC 3647 – algo que dificultaba su extrapolación a otros servicios de certificación diferentes de la expedición de certificados –, el artículo 10 del Anteproyecto adopta, en su epígrafe 1, un enfoque más neutral y abstracto, lo que permite adoptar una estructura de contenidos que resulte apropiada para cada servicio.

Ello se encuentra en línea con lo establecido en el nivel de autorregulación, significativamente en la norma técnica europea ETSI EN 319 401 v2.1.1 (2016-02), que también adopta un enfoque abstracto, apropiado para el tipo de servicio que se esté ofreciendo.

Conforme a esta norma[1028], la declaración de prácticas que formule el prestador deberá describir cómo se trata cada uno de los requisitos aplicables que consten en la política del servicio; identificar las obligaciones de todas las terceras partes que participen en la prestación del servicio de confianza; e incluir las prácticas correspondientes a la cesación del servicio[1029]; todo ello sin perjuicio de la existencia de otras normas técnicas que puedan concretar, para un servicio de confianza en concreto, los contenidos de esta declaración de prácticas.

Por lo que se refiere a la expedición de certificados, el mínimo legal que se establece es, en relación con la normativa anterior, también menor y se centra en los aspectos que el legislador considera que resultan de conocimiento esencial por parte de los clientes y las terceras partes que confían, en especial recogiendo la necesidad de informar acerca de

---

[1027] Para (Martínez Nadal, 2009, pág. 83), las lagunas existentes en la LFE, motivadas por la posición de neutralidad tecnológica que la misma adopta, "ponen de manifiesto la importancia de las declaraciones de prácticas de certificación, concepto acogido legalmente en la Ley de firma electrónica, como instrumento más ágil y dinámico para la regulación en detalle de estas cuestiones no reguladas legalmente". (Pérez Pereira, 2009, págs. 115-116) caracteriza las políticas y prácticas como instrumentos de autorregulación individual, dado que son redactadas por los propios prestadores, aunque advierte del riesgo que la misma "se desvirtúe debido a la concentración de empresas del sector". En mi opinión, la normalización de políticas de servicios de confianza abordada por ETSI realmente ha tenido una mayor afectación a estos instrumentos.

[1028] Cfr. su epígrafe 6.1.

[1029] Cfr. el epígrafe 6.2.8 de este trabajo.

obligaciones impuestas por la legislación española que van más allá del Reglamento eIDAS, como hemos visto en los epígrafes anteriores.

Se trata de un régimen que se superpone y complementa la obligación de suministrar determinadas informaciones con anterioridad a la contratación de un servicio cualificado, al que nos hemos referido ya[1030], y con la que debe coordinarse.

En todo caso, y por lo que respecta al contenido de la declaración de prácticas del prestador de servicios de confianza que expide certificados, sean cualificados o no, la norma técnica europea ETSI EN 319 411-1 complementa las exigencias generales de la norma EN 319 401, que antes hemos mencionado, con los siguientes elementos, recomendándose su estructuración conforme a la especificación técnica IETF RFC 3647: la jerarquía completa correspondiente a la infraestructura de clave pública; los algoritmos y parámetros empleados; o las prácticas relativas al uso de las claves de autoridad de certificación utilizadas para los certificados, las listas de revocación y los certificados.

Las prácticas de certificación no pueden considerarse, debido a su contenido técnico, como un instrumento contractual, pero ciertamente resultan vinculantes y obligatorias para el prestador, constituyendo una suerte de reglamento del servicio. Por este motivo, todos los contenidos obligacionales para el usuario del servicio deben constar en el correspondiente contrato de servicio, en los términos previstos por la legislación reguladora, y teniendo en cuenta que normalmente serán condiciones generales de la contratación; esto es, cláusulas no negociadas individualmente[1031].

6.2 LAS OBLIGACIONES ESPECÍFICAS DE LOS PRESTADORES DE SERVICIOS CUALIFICADOS DE CONFIANZA TIPIFICADOS EN EL REGLAMENTO EIDAS

Con carácter general, todos los prestadores cualificados de servicios deben asumir un conjunto de obligaciones, previsto en el artículo 24.2 del Reglamento eIDAS, con independencia del tipo de servicio de confianza que prestan, y que analizaremos en este epígrafe[1032]. También revisaremos las obligaciones que para estos prestadores y servicios se establecen, en sede nacional, en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

6.2.1 La información acerca de los cambios en el servicio de confianza

El artículo 24.2 del Reglamento eIDAS ordena que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: a) informarán al

---

[1030] Cfr. el epígrafe 6.2.4 de este trabajo.

[1031] (Pérez Pereira, 2009, pág. 117) considera que "[l]as Declaraciones o políticas de prestación del servicio se incorporan por remisión como una condición general más en el contrato celebrado, dado que se encuentran fácilmente y gratuitamente accesibles por los usuarios a través de la página web de Internet del prestador del servicio", lo que sólo encuentro viable en relación con las obligaciones del prestador, pero no del usuario, dada la dificultad de considerar que dichos textos superan las exigencias del control de incorporación de la legislación reguladora de las condiciones generales de la contratación.

[1032] Con excepción de aquellas que, por razones sistemáticas, sea objeto de tratamiento en otro lugar, como en el caso de la protección de los datos de carácter personal.

organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados […]".

Se trata de una previsión novedosa orientada a que el organismo de supervisión esté debidamente al corriente de las modificaciones en la prestación del servicio de confianza, al objeto de que pueda ejercer su función de supervisión. Dada la dicción literal del precepto, parece que todos los cambios deben ser objeto de comunicación al organismo de supervisión, con independencia de que los mismo sean sustanciales o, por el contrario, accesorios.

El Reglamento eIDAS no exige a la modificación de un servicio repetir el procedimiento de cualificación, a diferencia del inicio del servicio de confianza, por lo que la modificación se puede realizar de forma inmediata, sin que la misma se encuentre sujeta a autorización previa, ni resulte preciso acompañarla de una nueva evaluación de la conformidad, ni esperar a la respuesta del organismo de supervisión.

Otra cosa es que, a pesar de lo que se acaba de decir, pueda suceder que un prestador de servicios de confianza decida ser especialmente prudente –en especial si intuye que el organismo de supervisión puede considerar que el cambio contraviene la normativa aplicable– y, en su consecuencia, decida aplicar los cambios cuando reciba una respuesta afirmativa por parte del organismo de supervisión.

La información a remitir al organismo de supervisión debe ser suficientemente detallada como para que el mismo pueda evaluar el impacto el cambio sobre el servicio, por lo que, en su caso, se deberán remitir las versiones actualizadas de los documentos que en su día se presentaron al organismo de supervisión.

Esta información debe remitirse al organismo de supervisión mediante el procedimiento de notificación, a través de registro electrónico del organismo de supervisión, al que ya nos hemos referido, sin que en este caso se haya establecido formulario específico.

6.2.2 Los requisitos del personal y de los subcontratistas

El artículo 24.2 del Reglamento eIDAS ordena que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: […] b) contarán con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan a normas europeas o internacionales".

Se trata de una obligación que ya existía en el régimen legal anterior, aunque sólo aplicable a los servicios de expedición de certificados, y que ahora se extiende a todos los prestadores de servicios de confianza[1033], y que resulta apropiada a las necesarias

[1033] En este sentido, el numeral e) del Anexo II de la DFE, referido al prestador de servicios de certificación que expide certificados reconocidos, le ordena "emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas"; mientras que, por su parte, el artículo 20.1.c) exigía "[e]mplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos

exigencias de conocimiento técnico[1034] específico para la prestación del servicio, y que se extiende a diversos elementos.

Por una parte, es preciso que el personal propio o los subcontratistas posean conocimientos relativos a la prestación del servicio, conocimientos que necesariamente deberán encontrarse relacionados con los procedimientos del servicio, tanto administrativos como de gestión del servicio; procedimientos que deben corresponder, además, a normas europeas o internacionales, obviamente referidas a cada uno de los servicios, hayan sido o no establecidas por la Comisión Europea[1035] o, en su caso, por el Estado miembro de establecimiento del prestador del servicio[1036].

Por otra parte, el personal propio y los subcontratistas deben disponer de conocimientos específicos en materia de seguridad – tanto general cuanto de servicios de confianza y de protección de datos de carácter personal –, a fin de reducir el riesgo de incidente de seguridad.

El artículo 24.2.b) del Reglamento eIDAS se refiere también a la necesidad que el personal y los subcontratistas dispongan de cualificaciones y experiencia suficientes, en función de los diferentes roles que asuman, en el marco de las titulaciones oficiales existentes en cada momento, sin perjuicio de que en muchos casos se deberá acudir a certificaciones privadas, como, por ejemplo, en el caso de la seguridad de la información, o de la auditoría de sistemas.

El prestador de servicios de confianza, en su consecuencia, deberá disponer de un plan de formación que se refiera con un tratamiento adecuado a los elementos anteriores, normalmente en línea con los requisitos generales de las normas ISO/IEC 27002 y ETSI EN 391 401[1037], y los específicos de cada servicio, como por ejemplo EN 319 411-1[1038], en relación con el servicio de expedición de certificados de firma electrónica, sello electrónico o autenticación de sitio web.

Dicho plan deberá, además, encontrarse actualizado y adecuado a la evolución de los requisitos de seguridad y de los procedimientos del servicio, por lo que se debe considerar una periodicidad apropiada en la formación prevista, siendo también conveniente mecanismos de control que verifiquen que las actividades son realizadas por el personal

---

de seguridad y de gestión adecuados en el ámbito de la firma electrónica".

[1034] (Martínez Nadal, 2009, pág. 365) señalaba, con acierto, que "es conveniente que se incluya entre el personal cualificado personas con formación no sólo técnica sino también jurídica, dado el examen de documentación que en algunos casos habrán de realizar (a efectos de identificación del solicitante del certificado, examen de poderes de representación caso de certificados de atributos, etc); incluso, cabría añadir ahora, no sólo conveniente sino estrictamente necesario dada la rigurosa comprobación de identidad y otros elementos personales que se establece en el artículo 13 LFE, que implica una valoración de la validez y vigencia de la misma". Coincide en esta necesidad de formación jurídica (Ortega Díaz, 2008, pág. 143), "pues, en algunos casos, tendrán que realizar exámenes de documentación (a efectos de identificación del solicitante del certificado, examen de poderes de representación […])".

[1035] Lo que supone un interesante punto de interrelación entre el marco normativo formal y el de la autorregulación técnica. Cfr., al respecto, el epígrafe 1.4.2 de este trabajo.

[1036] Cfr. el epígrafe 1.4.4 de este trabajo.

[1037] Cfr. el epígrafe 7.2 de la norma.

[1038] Cfr. el epígrafe 6.4.4 de la norma.

en cuestión[1039].

6.2.3 Los requisitos de solvencia

El artículo 24.2 del Reglamento eIDAS ordena que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: […] c) con respecto al riesgo de la responsabilidad por daños y perjuicios de conformidad con el artículo 13, mantendrán recursos financieros suficientes u obtendrán pólizas de seguros de responsabilidad adecuadas, de conformidad con la legislación nacional", obligación que no resulta novedosa dada la existencia de una previsión análoga en el régimen legal anterior al Reglamento eIDAS[1040], aunque sólo limitada a los prestadores que expedían certificados, y que ahora se extiende a todos los prestadores de servicios de confianza[1041].

En este sentido, el artículo 20.2 de la LFE previó que "[l]os prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan"[1042], garantía que "podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros", y pudiéndose, finalmente modificar por Real Decreto "[l]as cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores".

El Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza no varía sustancialmente este modelo[1043], aunque modifica las cuantías, de

---

[1039] (Ortega Díaz, 2008, pág. 143) considera que "sería recomendable que los certificadores, dentro de esa actividad autorregulatoria a la que incita la LSSI, *ex* art. 19, desarrollen y secunden prácticas de personal que otorguen una seguridad razonable de que sus sistemas están siendo atendidos por empleados que cumplen sus obligaciones", dentro de las cuales "se establezcan procedimientos de supervisión, minuciosos y serios que inspecciones las actividades de todo el personal que esté vinculado a la actividad certificadora".

[1040] En este sentido, el numeral h) del Anexo II de la DFE, referido al prestador de servicios de certificación que expide certificados reconocidos, le ordena "disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado".

[1041] Para (Ortega Díaz, 2008, pág. 149), "[e]l problema de la solvencia financiera de los prestadores de servicios de certificación que emiten certificados reconocidos, y por tanto la indiscutible capacidad de éstos para responder patrimonialmente, ha sido uno de los problemas cuya solución se tornaba indispensable para la creación de un sistema de firma electrónica que generara un alto grado de confianza en el mercado".

[1042] (Martínez Nadal, 2009, págs. 377-378) critica este modelo, "por cuanto se limita a eventuales responsabilidades ocasionadas estrictamente «por el uso de los certificados que expidan» los prestadores; y es cierto que el uso de los certificados es uno de los principales supuestos generadores de responsabilidad para las entidades certificadoras (p.ej., emisión y uso de un certificado falso, por incorrecta identificación de titular o incorrecta comprobación de atributos incluidos en el mismo) per existen también otros supuestos generadores de responsabilidad derivados del desarrollo de la actividad de certificación electrónica (p.ej., mantenimiento y uso no autorizado de una copia de la clave privada por parte de la autoridad de certificación, generación de claves vulnerables, retraso en la revocación) que no estarían cubiertos por la garantía económica prevista en el art. 20.2 LFE si se interpreta literalmente". En el mismo sentido, (Ortega Díaz, 2008, pág. 150).

[1043] Quizá el cambio más notable es que, a diferencia de la normativa anterior, no se contiene ninguna referencia a la finalidad de la garantía, que deberá entenderse aplicable a cualquier caso, en línea con la

forma que se parte de una cuantía mínima de 1.500.000 euros, pero que se incrementa en 500.000 euros por cada servicio adicional, de modo que un prestador que ofrezca los nueve servicios de confianza tipificados en el Reglamento eIDAS que pueden ser objeto de cualificación[1044] deberá disponer de un seguro de 5.500.00 euros.

Se trata de una cantidad realmente elevada, en especial cuando se contrasta con las exigencias de otras leyes nacionales. Por ejemplo, la ley alemana establece la cantidad mínima de 250.000 euros[1045], 12 veces menor que en la LFE actualmente vigente y 22 veces menor que la establecida en el Anteproyecto, para un prestador que ofrezca todos los servicios; mientras que la ley italiana, la francesa, la belga y la del Reino Unido ni siquiera establecen una cantidad mínima al respecto.

6.2.4 La información previa a los futuros usuarios de los servicios

El artículo 24.2 del Reglamento eIDAS ordena que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: […] d) antes de entrar en una relación contractual, informarán, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización", obligación que tampoco resulta totalmente novedosa dada la existencia de una previsión análoga en el régimen legal anterior al Reglamento eIDAS[1046], aunque

---

crítica que había realizado (Martínez Nadal, 2009, pág. 378), a que antes nos hemos referido.

[1044] Cfr. el epígrafe 1.3.1 de este trabajo.

[1045] Cfr. la sección § 10 de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017.

[1046] En este sentido, el numeral k) del Anexo II de la DFE, referido al prestador de servicios de certificación que expide certificados reconocidos, le ordena, "antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado". Esta obligación se incluyó en el artículo 18.2 de la LFE, aunque de forma extendida a todos los prestadores de servicios que expedían certificados, a diferencia de la DFE, que, como se acaba de ver, la limitaba sólo a los prestadores que expedían certificados reconocidos. La información mínima exigible, a tenor del epígrafe 2 del artículo 18 de la LFE, incluye: "1.º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos, o, en su caso, de los medios que los protegen, así como información sobre los dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido. 2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo. 3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado. 4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial. 5.º Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad. 6.º Las demás informaciones contenidas en la declaración de prácticas de certificación".

sólo limitada a los prestadores que expedían certificados, y que ahora se extiende a todos los prestadores de servicios de confianza.

El Reglamento eIDAS se refiere a las condiciones precisas para la utilización del servicio de confianza en cuestión, obligación[1047] que se debe completar con la colección de informaciones que eventualmente se puedan prever en la legislación nacional y, en su caso, por el correspondiente contrato que se establezca entre las partes, y que no es objeto de exigencia legal alguna[1048].

En este sentido, la legislación alemana ha previsto la obligación de que los prestadores de servicios de confianza informen acerca de diversos extremos de interés, incluyendo las medidas que deben adoptar los usuarios para ayudar a proteger la seguridad de los servicios de confianza, del uso permitido de dichos servicios y de la existencia de otras informaciones disponibles para los usuarios, como las ofrecidas por los fabricantes de productos empleados en los servicios cualificados de confianza y por el organismo de supervisión; así como del hecho de que los datos que incorporen firma, sello o sello de tiempo cualificados pueden precisar de protección adicional, en línea con lo establecido en la propia Ley sobre conservación a plazo, antes de que se reduzca su valor de seguridad a lo largo del tiempo; y, finalmente, acerca de los efectos jurídicos de los servicios de confianza[1049].

Aunque el Reglamento eIDAS no indique cómo debe darse cumplimiento a esta obligación de información, cabe entender que la misma deberá realizarse conforme a la normativa general, por lo que, en el caso de que el futuro usuario del servicio tenga la condición de persona física usuaria final, se deberán aplicar las previsiones de la normativa de protección de consumidores –principalmente contenida, en España, en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU)–, por lo que la información deberá suministrarse en soporte papel o en un soporte duradero.

Además, respecto al contenido de la información, se deberán considerar las previsiones del artículo 97.1 del TRLGDCU, debidamente adecuadas a esta actividad; a saber, la identidad del prestador, incluido su nombre comercial; la dirección completa del establecimiento del empresario y el número de teléfono, número de fax y dirección de correo electrónico del mismo[1050], cuando proceda, con objeto de que el consumidor y

---

[1047] En relación con la normativa anterior, (Martínez Nadal, 2009, pág. 331) había indicado que "se trata, por tanto, de una obligación precontractual que todo prestador ha de cumplir respecto del solicitante de un certificado con el que, en virtud de la emisión, establecerá una relación contractual", añadiendo que "esta obligación de información precontractual se establece para todo solicitante de un certificado, tenga o no la condición de consumidor", reflexión que resulta plenamente aplicable a la previsión del Reglamento eIDAS.

[1048] Como ha puesto de manifiesto (Ortega Díaz, 2008, pág. 315), "el contrato de certificación electrónica jamás ha sido, en modo alguno, regulado en la normativa de firma electrónica", algo que tampoco ha sucedido en el Reglamento eIDAS en relación con los servicios de confianza, lo que debe ser valorado positivamente, a mi juicio, dado el enfoque de neutralidad de modelos de negocio ínsito en esta norma.

[1049] Cfr. la sección § 13 de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017.

[1050] La dirección de correo electrónico debe considerarse obligatoria, dada la aplicación de la Ley 34/2002

usuario pueda ponerse en contacto y comunicarse con él de forma directa[1051], rápida y eficaz, así como, cuando proceda, la dirección completa y la identidad del empresario por cuya cuenta actúa, si fuere el caso; si es diferente de la anterior, la dirección completa de la sede del empresario y, cuando proceda, la del empresario por cuya cuenta actúa, a la que el consumidor y usuario puede dirigir sus reclamaciones; el precio del servicio[1052], incluidos los impuestos y tasas[1053]; el coste de la utilización de la técnica de comunicación a distancia para la celebración del contrato, en caso de que dicho coste se calcule sobre una base diferente de la tarifa básica; los procedimientos de pago, entrega y ejecución, la fecha en que el empresario se compromete a ejecutar la prestación de los servicios, así como, cuando proceda, el sistema de tratamiento de las reclamaciones del empresario; la lengua o lenguas en las que podrá formalizarse el contrato, cuando ésta no sea la lengua en la que se le ha ofrecido la información previa a la contratación; cuando proceda, la existencia de asistencia posventa al consumidor y usuario, servicios posventa y garantías comerciales, así como sus condiciones; la existencia de códigos de conducta pertinentes y la forma de conseguir ejemplares de los mismos, en su caso; la duración del contrato, cuando proceda, o, si el contrato es de duración indeterminada o se prolonga de forma automática, las condiciones de resolución; cuando proceda, la duración mínima de las obligaciones del consumidor y usuario derivadas del contrato; y, finalmente, cuando proceda, la posibilidad de recurrir a un mecanismo extrajudicial de reclamación y resarcimiento al que esté sujeto el empresario y los métodos para tener acceso al mismo.

En los casos en que la prestación del servicio implique la entrega de un bien, como por ejemplo sucede en el caso del dispositivo calificado de creación de firma electrónica o sello electrónico, la información también deberá referirse, conforme dispone el artículo 97.1 del TRLGDCU, a la existencia de una garantía legal de conformidad para los bienes.

Cuando el servicio sea comercializado a distancia –que posiblemente será habitual, sin perjuicio de que también se pueda adquirir en las oficinas del prestador–, resultará necesario también informar acerca del derecho de desistimiento[1054], incluyendo sus

---

a los prestadores de servicios de confianza, que prevé esta información en su artículo 10.1.a).

[1051] Cfr. el artículo 10.1.a) de la Ley 34/2002.

[1052] El precepto también indica que "si el precio no puede calcularse razonablemente de antemano por la naturaleza de los bienes o de los servicios", se deberá informar acerca de "la forma en que se determina el precio, así como, cuando proceda, todos los gastos adicionales de transporte, entrega o postales y cualquier otro gasto o, si dichos gastos no pueden ser calculados razonablemente de antemano, el hecho de que puede ser necesario abonar dichos gastos adicionales". Igualmente, "[e]n el caso de un contrato de duración indeterminada o de un contrato que incluya una suscripción, el precio incluirá el total de los costes por período de facturación. Cuando dichos contratos se cobren con arreglo a una tarifa fija, el precio total también significará el total de los costes mensuales. Cuando no sea posible calcular razonablemente de antemano el coste total, se indicará la forma en que se determina el precio", algo que podría suceder fácilmente en servicios como el de expedición de sellos de tiempo electrónico y de entrega electrónica certificada.

[1053] En el caso de los servicios de confianza, será el tipo normal de IVA, del 21%.

[1054] Conforme al artículo 103.a) del TRLGDCU, el derecho de desistimiento no procederá "una vez que el servicio haya sido completamente ejecutado, cuando la ejecución haya comenzado, con previo consentimiento expreso del consumidor y usuario y con el reconocimiento por su parte de que es consciente de que, una vez que el contrato haya sido completamente ejecutado por el empresario, habrá perdido su derecho de desistimiento", algo que puede suceder con cierta frecuencia en los servicios de confianza. Piénsese, por ejemplo, en el servicio de entrega electrónica certificada, que es de ejecución instantánea.

condiciones, el plazo[1055] y los procedimientos para ejercer ese derecho, así como el modelo de formulario de desistimiento; así como, cuando proceda, la indicación de que el consumidor y usuario tendrá que asumir el coste de la devolución de los bienes[1056] en caso de desistimiento y cuando los bienes, por su naturaleza, no puedan devolverse normalmente por correo, el coste de la devolución de los mismos.

Las normas técnicas de actividad aprobadas por el ETSI vienen a concretar, en el plano de la autorregulación, la obligación prevista en este epígrafe[1057], previendo la obligación de aprobar y publicar diversos textos informativos, entre los cuales un texto de divulgación, una suerte de folleto informativo, que forma parte de los términos y condiciones contractuales, con una estructura y unos contenidos mínimos recomendados[1058] y accesible a través de Internet. En el caso de los certificados electrónicos, además, se deberá contener en los mismos la dirección de Internet donde se publica esta información, al efecto de facilitar su conocimiento por parte de los titulares de los certificados, pero también por las terceras partes.

A dichas informaciones debe añadirse, en España, la correspondiente declaración de prácticas del servicio de confianza, a la que ya hemos tenido ocasión de referirnos[1059].

Nótese, finalmente, que la LFE ordenaba, también en su artículo 18.2, que "[l]a información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos"[1060], previsión que no se encuentra en el Reglamento eIDAS ni tampoco se ha incorporado al Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

6.2.5 El empleo de sistemas fiables y las medidas contra la falsificación y el robo de datos

El artículo 24.2 del Reglamento eIDAS ordena que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: […] e) utilizarán sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan"[1061] y, asimismo, que

---

[1055] Conforme al artículo 102.1 del TRLGDCU, el plazo de ejercicio del derecho es de catorce días naturales, a contar desde el día de celebración del contrato (artículo 104.a) del TRLGDCU), excepto si "el empresario no ha facilitado al consumidor y usuario la información sobre el derecho de desistimiento", en cuyo caso, "el periodo de desistimiento finalizará doce meses después de la fecha de expiración del periodo de desistimiento inicial", a tenor del artículo 105.1 del mismo TRLGDCU.

[1056] Como el dispositivo cualificado de creación de firma o sello electrónico.

[1057] Cfr. el epígrafe 6.2 de la norma ETSI EN 319 401, aplicable a todos los servicios de confianza.

[1058] Cfr. en relación con el texto divulgativo del servicio de expedición de certificados (*PKI Disclosure Statement* o PDS), los epígrafes 4.3, 6.3.4.c) y el Anexo A de la norma ETSI EN 319 411-1.

[1059] Cfr. el epígrafe 6.1.6 de este trabajo.

[1060] En relación con esta obligación, (Martínez Nadal, 2009, pág. 339) criticaba que "[e]n cuanto a la forma de acceso a tal información relevante, en este caso en el precepto legal se habla simplemente de que dicha información debe estar disponible; por tanto, no exige una transmisión o entrega sino que parece suficiente una puesta a disposición que, además, curiosamente, será a instancia del tercero, lo que quizá puede interpretarse en el sentido de que será a instancia de parte (del tercero interesado) y para un caso en concreto y no necesariamente una puesta a disposición general para posibles terceros usuarios".

[1061] El apartado f) del Anexo II de la DFE exigía, en este sentido, a los prestadores de servicios de

"f) utilizarán sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que: i) estén a disposición del público para su recuperación solo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos, ii) solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados, iii) pueda comprobarse la autenticidad de los datos".

Se trata de dos de las obligaciones más relevantes para los prestadores, que se completa con la obligación prevista en el numeral g) del mismo artículo 24.2 del Reglamento eIDAS, en cuya virtud los prestadores "tomarán medidas adecuadas contra la falsificación y el robo de datos", y que constituyen buena muestra de la utilización de la regulación para promover la "economía de la seguridad"[1062].

Las tres obligaciones se refieren a la imprescindible fiabilidad de los sistemas tecnológicos empleados para la prestación de los servicios cualificados de confianza[1063], estableciendo una especificación de la norma general de seguridad que impone el artículo 19.1 del Reglamento eIDAS[1064], que conecta, en particular, con el uso de los correspondientes controles criptográficos, dado que los servicios de confianza se basan intensivamente en el uso de claves criptográficas.

La primera obligación persigue el uso de sistemas y productos protegidos, ellos mismos, contra toda alteración, de forma que los mismos sean íntegros. Es un aspecto de gran importancia, dado que la modificación de un producto, como por ejemplo una aplicación informática empleada para la expedición de certificados, podría resultar en una prueba incorrecta o directamente falsa, como de hecho ha sucedido en el escandaloso caso DigiNotar[1065].

Adicionalmente, dichos sistemas y productos son los responsables de garantizar, desde el punto de vista técnico, un nivel de seguridad y de fiabilidad suficiente a los procesos que

---

certificación "utilizar sistemas y productos fiables […] que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan", en una referencia explícita a los procedimientos criptográficos, que en el Reglamento eIDAS ha desaparecido – cabe suponer que para garantizar mejor la neutralidad tecnológica. Por su parte, el artículo 20.1.d) de la LFE ordenaba a los prestadores "[u]tilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte".

[1062] (Anderson & Moore, 2007, p. 6 y ss.), en especial en relación con la economía de las vulnerabilidades, que presenta una afectación clara a esta industria, como ha quedado demostrado en el caso DigiNotar (Hoogstraaten, y otros, 2012).

[1063] (Ortega Díaz, 2008, pág. 148) se pregunta si los sistemas fiables referidos en ambos numerales (se refiere a los de la LFE, que traen cuenta de la DFE) son diferentes o si son el mismo sistema, considerando que el legislador se refiere a un único sistema. Con el Reglamento eIDAS esta conclusión ya no tiene porqué ser apropiada.

[1064] Cfr. el epígrafe 6.1.3 de este trabajo. Recuérdese que este artículo indica que "los prestadores cualificados y no cualificados de servicios de confianza adoptarán las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizarán un nivel de seguridad proporcionado al grado de riesgo".

[1065] Este prestador holandés, hoy desaparecido, sufrió en 2011 un ataque basado en una alteración del programa informático empleado para el proceso de solicitud de certificados, que permitió la generación de una gran cantidad de certificados falsos (Hoogstraaten, y otros, 2012, págs. 43-45), que se destinaron al espionaje de las comunicaciones en Internet de cientos de miles de ciudadanos iraníes.

conforman el servicio de confianza, como no puede ser de otra forma, ya que es evidente que de otra forma poca confianza se va a poder depositar en el servicio, y menos valor se va a conceder a la prueba electrónica sustentada por dicho servicio.

Aquí se ve perfectamente bien la íntima relación entre seguridad y confianza, que resulta transitiva, de modo que se confía en una prueba electrónica porque se confía en el servicio de confianza que la sustenta, y se confía en dicho servicio porque sus procesos son suficientemente fiables, y para eso, la tecnología empleada debe ser segura y también debe ser fiable. Nos encontramos ante conceptos jurídicos claramente indeterminados, que sólo pueden llenarse de contenido concreto acudiendo a la experiencia, a la autorregulación técnica y las mejores prácticas, y a las recomendaciones e instrucciones de organismos de supervisión competentes y con personal altamente especializado.

La segunda obligación, relativa al uso de sistemas fiables para la conservación de los datos que se faciliten a los sistemas de confianza[1066], constituye una concreción de la obligación, más general, de uso de sistemas y productos fiables a la que nos acabamos de referir.

Se trata de una obligación que, como en otros casos, encuentra su antecedente en los sistemas de almacenamiento de certificados expedidos, cuya regulación se encontraba ya en la normativa anterior, de la cual constituye una generalización a todos los servicios de confianza, a los que resultará de aplicación de forma variable en función del tipo de servicio.

Por ejemplo, por lo que se refiere a que los datos estén a disposición del público para su recuperación solo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos, lógicamente será plenamente aplicable, como venía sucediendo en la DFE[1067] y la LFE[1068], a los servicios de expedición de certificados – dado que el acceso por el público al certificado[1069] se podía encontrar justificado por la necesidad de conocer la clave pública del titular de dicho certificado, a los efectos de comprobar una prueba de identificación, de firma o de sello electrónico, respectivamente, pero puede no tener sentido en servicios como la entrega electrónica certificada[1070]. En otros casos, como en el servicio de sellado de tiempo electrónico, en que no hay datos de carácter

---

[1066] Debe entenderse que las obligaciones se establecen en relación con los datos facilitados para su almacenamiento en el sistema fiable, sean datos suministrados por los usuarios del servicio al prestador, o simplemente incorporados por el propio prestador al sistema fiable. En el segundo caso, los datos típicamente van a referirse a las pruebas electrónicas generadas por el prestador, como certificados cualificados de firma, sello o autenticación de sitio web, sellos cualificados de tiempo electrónico, certificaciones de entrega electrónica, etc.

[1067] El numeral l) del Anexo II de la DFE se refería a que "los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado".

[1068] El epígrafe 20.1.g) de la LFE se refería a que dichos sistemas fiables "restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado", en una dicción más restrictiva que la de la DFE.

[1069] En efecto, la DFE y la LFE se referían al almacenamiento de los certificados expedidos, no a los datos facilitados por los usuarios al prestador del servicio de certificación, por lo que nos encontramos ante un verdadero cambio en el contenido de esta obligación.

[1070] En particular, este servicio se emplea para la prueba electrónica de las comunicaciones, amparadas por el secreto de las mismas, por lo que muy difícilmente se encontrarán casos en que el público pueda recuperar estas comunicaciones, que son los datos que se facilitan al prestador del servicio.

personal almacenados por el prestador, exigir el consentimiento podría resultar excesivamente limitativo, en especial si se entiende que aplica al resumen criptográfico a partir del que se ha creado el sello de tiempo electrónico, por ejemplo.

Por lo que se refiere a que solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados, de nuevo deberá interpretarse en función del tipo de servicio y de la naturaleza de las informaciones objeto de almacenamiento, dado que, con carácter general, las pruebas electrónicas – los certificados, los sellos de tiempo, los certificados de entrega… –, no son modificables, y una vez expedidas tampoco se debería proceder a modificar las informaciones que avalan sus contenidos, aunque se ha de poder realizarlas cuando se encuentre justificado; por lo que habrá que entender que, al menos en el caso de las modificaciones, se deberá aplicar esta previsión de forma muy restrictiva.

De nuevo, en la DFE[1071] y en la LFE[1072] esta obligación se podía entender aplicable a los propios certificados, algo que resultaría absurdo dada la imposibilidad de modificar un certificado, por lo que se debía entender que las anotaciones y modificaciones se referían a los metadatos de dichos certificados, una vez incorporados a los sistemas fiables de almacenamiento. Desde esta perspectiva, podría resultar una obligación ciertamente aplicable a cualquiera servicio de confianza.

Respecto a que se pueda comprobar la autenticidad de los datos almacenados en estos sistemas fiables, se trata de una obligación que también proviene de la normativa anterior[1073], y que ahora se generaliza a todos los servicios de confianza; obligación que se podrá implementar de diversas formas, por ejemplo, mediante el uso, por el prestador del servicio, de su propia firma o sello electrónico para proteger las informaciones. Típicamente ello ya es así, en las pruebas electrónicas generadas por el prestador, por imperativo legal[1074], pudiéndose emplear el mismo mecanismo, u otro –como el sellado de tiempo electrónico– para la protección de otras informaciones almacenadas, como los metadatos (por ejemplo, las anotaciones).

Destaca, en relación con los sistemas fiables para el almacenamiento de datos, que el Reglamento eIDAS haya prescindido de la obligación de que los dichos sistemas permitan que "el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados" (numeral l) del Anexo II de la DFE[1075]), quizá por no haber considerado necesaria esta concreción de las obligaciones, ya analizadas,

---

[1071] El numeral l) del Anexo II de la DFE se refería a que "sólo personas autorizadas puedan hacer anotaciones y modificaciones".

[1072] El epígrafe 20.1.g) de la LFE se refería a que dichos sistemas fiables permitan "impedir que personas no autorizadas alteren los datos", sin aclarar a qué datos se refiere.

[1073] El numeral l) del Anexo II de la DFE se refería a que "pueda comprobarse la autenticidad de la información", mientras que el epígrafe 20.1.g) de la LFE se refería a que dichos sistemas fiables permitan "comprobar su autenticidad", refiriéndose a los certificados reconocidos.

[1074] Recuérdese que el certificado cualificado, el sello cualificado de tiempo electrónico, o el envío y recepción en la entrega electrónica certificada, incorporan la firma o sello electrónico avanzado del prestador del correspondiente servicio.

[1075] El artículo 20.1.g) de la LFE se refería a que dichos sistemas fiables permitan "detectar cualquier cambio que afecte a estas condiciones de seguridad", sin especificar a quién se refiere, si al usuario final del servicio, al público en general, al personal del prestador, o a todos ellos.

respecto a la integridad de los sistemas, y la autenticidad de los datos, que ciertamente obligan a implantar mecanismos de detección –no únicamente de prevención– de las posibles infracciones de seguridad.

La tercera obligación, contenida en el artículo 24.2.g) del Reglamento eIDAS, se refiere a la adopción de medidas adecuadas para impedir la falsificación y el robo de datos. Por lo que respecta a la falsificación, se trata de una obligación que trae cuenta del régimen legal anterior[1076], y que se generaliza a todos los servicios de confianza, modulándose el rigor de la obligación en función el criterio de la adecuación.

De nuevo, se deberá diferenciar entre las pruebas electrónicas generadas por el prestador para su entrega a terceros, en cuyo caso normalmente el propio Reglamento eIDAS impone la obligación de protección de la prueba electrónica empleando el sistema de firma o sello electrónico avanzado de que disponga el prestador, pudiéndose incluso elevar el nivel de garantía utilizando sistemas de firma o sello electrónico cualificado; de otros datos que gestione o publique el prestador, inclusive los contenidos en los sistemas fiables para el almacenamiento de datos a que acabamos de hacer referencia.

Más novedosa es la obligación de adopción de medidas contra el robo de datos, que no existía en el régimen legal anterior, que viene a complementar la obligación dimanante de la normativa de protección de datos personales, algo que hay que valorar de forma positiva, dado que en muchos casos los prestadores gestionan datos de personas jurídicas. Se trata de una obligación de especial relevancia en servicios como la generación y gestión de datos de creación de firma o sello electrónico, dado que el robo de estos datos permite la suplantación de la identidad de sus titulares, y la atribución de documentos y comunicaciones fraudulentamente a los mismos; o en el caso de la entrega electrónica certificada, dada la obligación de mantener el secreto de las comunicaciones sustanciadas a través del servicio.

Como se puede ver del análisis anterior, se trata de obligaciones de formulación general, que no se concretan excesivamente, seguramente por la dificultad de proyectarlas sobre cada tipo de servicio de confianza, especialmente tratando de mantener un enfoque de neutralidad tecnológica.

Por ello, se trata de objetivos de seguridad que precisarán de la necesaria concreción técnica en cada tipo de sistema fiable, que deberá realizar el prestador, en el marco regulador, ya conocido[1077], de "negociación" con el organismo de evaluación de la conformidad y el organismo de supervisión, a los que hay que convencer, de forma previa y periódica, del efectivo cumplimiento de estas obligaciones de seguridad.

Puede ayudar en esto el artículo 24.5 del Reglamento eIDAS, que autoriza a la Comisión a establecer, mediante actos de ejecución, números de referencia de normas para dichos sistemas y productos fiables, de forma que el cumplimiento de dichas normas implica la presunción de cumplimiento de los requisitos legales[1078]; previsión que no resulta novedosa, porque el artículo 3.5 de la DFE ya había previsto esta misma competencia[1079],

---

[1076] Cfr. el numeral g) del Anexo II de la DFE, y el artículo 20.1.e) de la LFE.

[1077] Cfr. los epígrafes 7.1.1 y 7.1.2.2 de este trabajo.

[1078] Sobre esta competencia de la Comisión, cfr. el epígrafe 1.4.2 de este trabajo.

[1079] Este artículo prevé que "[l]a Comisión, con arreglo al procedimiento en el artículo 9, apartado, podrá determinar, y publicar en el Diario Oficial de las Comunidades Europeas, los números de referencia de las

en aplicación de la cual la Comisión adoptó la Decisión 2003/511/CE, de 14 de julio de 2003, relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE), que en relación con la letra f) del Anexo II seleccionó la especificación técnica CEN CWA 14167, partes 1 y 2[1080]; especificación que también fue adoptada por el SOG-IS[1081] a los efectos de facilitar el reconocimiento de los correspondientes certificados de evaluación de la seguridad de las tecnologías de la información en el ámbito del citado grupo de trabajo.

En virtud del Mandato de normalización M/460, de la Comisión Europea, se ha aprobado la especificación técnica CEN/TS 419 261[1082], referida a los requisitos de seguridad de los sistemas fiables que gestionan certificados en soporte de la firma electrónica, así como sellos de tiempo electrónico; mientras que, también en virtud del Mandato M/460, la especificación CEN CWA 14167, partes 1 a 4, ha sido evolucionada a la especificación técnica CEN/TS 419 221, partes 1 a 4[1083] y la futura norma CEN EN 419 221, parte 5, también referidas de forma específica a los perfiles de protección de los sistemas fiables que gestionan certificados en soporte de la firma electrónica y los sellos de tiempo electrónico.

En todo caso, aunque la DFE no contenía ninguna definición de sistema fiable, CWA 14167-1 lo definió como "un sistema de información o producto implementado como hardware y/o software que produce registros confiables y auténticos que están protegidos frente a la modificación, y adicionalmente, asegura la seguridad técnica y criptográfica de los procesos soportados por el mismo", definición que se mantiene idéntica en CEN/TS 419 261, cuyo valor interpretativo resulta importante, dado que tampoco el Reglamento eIDAS contiene definición alguna acerca de qué sea un sistema fiable.

Asimismo, CWA 14167-1 definió el dispositivo criptográfico en maquinaria (*hardware cryptographic device*) como "un dispositivo criptográfico basado en maquinaria que

---

normas que gocen de reconocimiento general para productos de firma electrónica. Los Estados miembros presumirán que los productos de firma electrónica que se ajusten a dichas normas son conformes con lo prescrito en la letra f) del anexo II y en el anexo III de la presente Directiva".

[1080] CWA 14167-1 (marzo de 2003): Security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System Security Requirements; y CWA 14167-2 (marzo de 2002): Security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: cryptographic module for CSP signing operations - Protection Profile (MCSO-PP). La especificación técnica CWA 14167-2 fue posteriormente dividida en dos especificaciones (CWA 14167-2 y CWA 14167-4) publicadas en 2004, así como complementada por la CWA 14167-3, también de 2004.

[1081] El acuerdo SOG-IS fue creado en respuesta a la Decisión del 31 de marzo de 1992 (92/242/EEC) del Consejo de la Unión Europea en el campo de la seguridad de los sistemas de información, y de la posterior Recomendación del Consejo del 7 de abril (1995/144/EC) sobre criterios comunes en la evaluación de seguridad de tecnología de la información.

[1082] En el futuro, será la norma europea CEN EN 419 261.

[1083] El detalle es CEN/TS 419 221-1:2016. Protection Profiles for TSP cryptographic modules - Part 1: Overview; CEN/TS 419 221-2:2016. Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup; CEN/TS 419 221-3:2016. Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services; y CEN/TS 419 221-4:2016. Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup.

genera, almacena y protege claves criptográficas y ofrece un entorno seguro para la ejecución de funciones criptográficas", definición que también se mantiene idéntica en CEN/TS 419 261, y que se emplea como tecnología principal de protección de las claves criptográficas empleadas para la prestación de los servicios de expedición de certificados y de sellos de tiempo electrónico.

En el contexto del mismo Mandato M/460 se ha aprobado la especificación CEN/TS 419 241[1084], relativa a los sistemas fiables en soporte de firma en servidor, a la que ya nos hemos referido anteriormente, y actualmente se trabaja en otras especificaciones técnicas relativas a los sistemas fiables para su empleo en otros servicios de confianza.

Como se puede apreciar, el enfoque normativo es permitir una potente autorregulación de la industria, en este caso, relativa a los productos que sustentan los sistemas fiables, mediante la producción de especificaciones técnicas y, posteriormente, verdaderas normas técnicas, que en caso de considerarse conveniente, pueden ser referenciadas por la Comisión Europea (o por cada Estado miembro si así lo prevé en sede nacional) al objeto de gozar de la presunción de cumplimiento de los requisitos jurídicos correspondientes, y evitar barreras a su libre circulación (al menos cuando la especificación o la norma haya sido referenciada por la Comisión Europea).

Es evidente que el incentivo para adoptar las normas es muy superior cuando las existen normas referenciadas por la Comisión (o por un Estado miembro, en su ámbito territorial) que presumen el cumplimiento de los requisitos legales, y sin embargo, la Decisión 2016/650, a la que ya nos hemos referido, ha derogado la Decisión 2003/511/CE íntegramente, sin incorporar en la misma ninguna referencia a las anteriores especificaciones técnicas, por lo que actualmente no existen productos que gocen de la presunción legal anteriormente referida. Quizá se hubiera debido mantener vigente la Decisión de 2003 en la parte relativa a las normas relativas a los productos y sistemas fiables, aunque como hemos visto la misma se encontraba muy desfasada, pero ciertamente es importante disponer de mecanismos para facilitar a los prestadores la acreditación del cumplimiento de sus obligaciones legales.

Pero, aun sin ser referenciadas por nadie, la existencia de especificaciones y, en especial, de normas técnicas para los sistemas fiables es muy relevante, porque sitúa al prestador que las adopta en una mejor posición para convencer al organismo de evaluación de conformidad y al organismo de supervisión acerca de la razonabilidad y adecuación de las medidas de seguridad que debe adoptar[1085].

Sin embargo, debemos preguntarnos sobre la forma de demostrar la conformidad con los requisitos contenidos en dichas normas, sobre lo que el Reglamento eIDAS nada dice. A diferencia de lo que sucede con los dispositivos cualificados de creación de firma electrónica o sello electrónico, que deben ser previamente sujetos a una certificación formal de su seguridad –atendiendo al contenido de las normas, normalmente será una certificación conforme a los denominados Criterios Comunes de evaluación de la seguridad de tecnología de la información–, en el caso de los sistemas fiables no se

[1084] Actualmente, ya se ha aprobado la norma EN 419 241:2018, que la sustituirá.

[1085] Por ejemplo, que la especificación técnica CEN/TS 419 241 –ya norma CEN EN 419241:2018– haya concretado técnicamente los criterios de seguridad que permiten mantener el control exclusivo de los datos de creación de firma y sello electrónico, ha sido muy importante para reducir los términos del debate con el organismo de evaluación y el organismo de supervisión, en una materia altamente polémica.

impone esta certificación.

Por este motivo, se deberá poder acudir, a estos efectos, a cualquier medio de prueba válido en Derecho, como se reconoce en la legislación industrial, pero asumiendo el coste extra de negociación con los organismos de evaluación de la conformidad y de supervisión, que no existe en el caso de productos certificados contra norma referenciada por la Comisión Europea, y es menor en el caso de productos certificados contra norma europea no referenciada, o contra norma no europea[1086].

6.2.6 El uso de algoritmos criptográficos concretos

El Reglamento eIDAS se basa, aunque no de forma explícita[1087], en el uso de cifras y sus correspondientes algoritmos y parámetros, así como en cuanto a la gestión de las claves criptográficas, tanto en lo referido a los sistemas fiables que debe emplear el prestador, cuanto a los dispositivos cualificados de firma/sello (que típicamente suministran los prestadores), y que trataremos en este epígrafe de forma conjunta, por razones metodológicas.

El Reglamento eIDAS, sin embargo, no concreta en su texto qué mecanismos criptográficos –esto es, qué cifras concretas, así como los algoritmos y parámetros particulares– se deben emplear, puesto que nos encontramos ante uno de los aspectos no armonizados y que, por tanto, permiten la regulación en sede nacional; pero dichas normas se establecen de forma indirecta, como veremos a continuación.

Algunos Estados miembros han establecido normas concretas en relación con los mecanismos criptográficos, como por ejemplo Alemania[1088] o Francia[1089], que

---

[1086] Como sucede, en el caso de los HSM, con FIPS 140-2, que es una norma norteamericana.

[1087] A diferencia de la DFE y la LFE, que se referían expresamente a la "seguridad criptográfica". Cfr. Anexo II.f) de la DFE, y el artículo 20.1.d) de la LFE, algo más neutral, al hacer la referencia a la seguridad criptográfica a "en su caso".

[1088] En este caso, el órgano competente es el organismo de supervisión de los servicios de confianza, que es la Agencia de la Red Federal de Electricidad, Gas, Telecomunicaciones, Correos y Ferrocarriles, (*Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*), que venía actuando al amparo de lo establecido en la Ley Marco para la Firma Electrónica (*Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)*, de 16 de mayo de 2001) y el Reglamento de la Ley de Firma Electrónica (Verordnung zur elektronischen Signatur (*Signaturverordnung – SigV*), de 16 de noviembre de 2001); más en concreto, en el anexo 1 de la misma, que prevé los algoritmos a emplear en los productos para la firma electrónica. Dichas normas han quedado derogadas con la aprobación de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017), sin embargo, lo que genera dudas acerca de si el supervisor mantendrá esta potestad, dado que el epígrafe § 2 (2) de la VDG prevé que las funciones en materia de evaluación de algoritmos criptográficos de la *Bundesamtes für Sicherheit in der Informationstechnik* (Oficina Federal de Seguridad de la Información) previstas por la legislación sectorial se mantengan a pesar de las competencias del organismo de supervisión. Nótese también que para el organismo de supervisión para la creación, verificación y validación de certificados de autenticación de sitio web es la Oficina Federal de Seguridad de la Información.

[1089] En este caso, el órgano competente es el organismo de supervisión de servicios de confianza, que es la Agencia Nacional de la Seguridad de los Sistemas de Información (*Agence nationale de la sécurité des systèmes d'information*), en el marco del Referencial General de Seguridad, que viene a ser el equivalente francés de nuestro Esquema Nacional de Seguridad, aprobado por el Primer Ministro, a propuesta de la Agencia Nacional de la Seguridad de los Sistemas de Información y de la Secretaría General para la

lógicamente resultan sólo obligatorios para los prestadores establecidos en dichos Estados[1090]. También España ha dictado normas concretas, aunque sólo para los servicios empleados para el funcionamiento del sector público y para el procedimiento administrativo electrónico.

En ausencia de normas nacionales, y en relación con la prestación de los servicios de confianza de expedición de certificados y de sellos de tiempo electrónico, las normas técnicas vienen a exigir el uso de las cifras, algoritmos y parámetros previstos en la especificación técnica ETSI TS 119 312, actualmente en su versión 1.2.1 (2017-05).

Así sucede, por ejemplo, en las especificaciones y normas referidas a sistemas fiables para servicios de confianza[1091], en las relativas a la generación y validación de la firma electrónica[1092] o a los dispositivos cualificados[1093], o en las que regulan la actividad correspondiente a la prestación de cada servicio de confianza[1094], que recomiendan el uso de determinadas cifras, algoritmos y parámetros, mediante el reenvío directo a dicha especificación.

ETSI TS 119 312 especifica, para su uso en los servicios de confianza y, por conexión, en las pruebas electrónicas que los mismos sustentan, una serie de conjuntos criptográficos, que se definen[1095] como la "combinación de un esquema de firma con un método de relleno y una función de resumen criptográfico", mientras que un esquema de firma se define como "un triplete de tres algoritmos compuesto por un algoritmo de creación de firma, un algoritmo de verificación de firma y un algoritmo de generación de claves", y un método de relleno (que no se define en la especificación), como un mecanismo de completado y codificación de la información de entrada del algoritmo de creación y/o verificación de firma.

Lo que resulta interesante de la especificación técnica ETSI TS 119 312 es que incorpora, aunque sólo desde su última versión[1096], las recomendaciones del Grupo de Trabajo sobre Criptografía del SOG-IS, que persigue el establecimiento de un esquema de evaluación criptográfica en el marco de la evaluación de la seguridad de las tecnologías de la información; por tanto, aplicable a los productos empleados para la prestación de los servicios de confianza, sean productos y sistemas fiables, o dispositivos de creación de firma o sello electrónicos.

Modernización de la Actuación Pública.

[1090] Y, en el caso de Francia, sólo en el caso de que el prestador se quisiera acreditar –conforme al régimen anterior al Reglamento eIDAS–, bien para la presunción de conformidad con la legislación de firma electrónica, bien para que sus certificados fueran admitidos para las relaciones electrónicas con y entre las Administraciones Públicas.

[1091] CEN/TS 419 261 o CEN/TS 419 241.

[1092] ETSI EN 319 122, ETSI EN 319 132 y ETSI EN 319 142.

[1093] CEN EN 419 211, partes 1 a 6.

[1094] ETSI EN 319 411, partes 1 y 2 o ETSI EN 319 421.

[1095] A pesar de esta definición, hay que notar que no todos los algoritmos de firma digital requieren el uso de un método de relleno.

[1096] Anteriormente, esta especificación técnica, y su precedente – ETSI TS 102 176 – recogían recomendaciones realizadas por la industria y la academia, principalmente.

El valor de este documento reside, principalmente, en contener los mecanismos criptográficos acordados entre todos los participantes, lo que facilita claramente la libre circulación (la interoperabilidad, dice ETSI TS 119 312) de los productos a los que nos acabamos de referir, aunque desde luego también apoya la defensa frente a un posible cuestionamiento acerca de la seguridad de un algoritmo criptográfico, y ayuda a demostrar el cumplimiento de las obligaciones de seguridad a las que antes nos hemos referido.

Estos mecanismos criptográficos acordados se agrupan, en este esquema, en función de su nivel de seguridad[1097], en mecanismos "recomendados", que son los que reflejan el estado del arte de la criptografía, ofreciendo un nivel de seguridad de 125 bits[1098], y mecanismos "heredados", que se encuentran ampliamente desplegados y que ofrecen al menos un nivel de 100 bits.

Vistos estos requisitos, debemos plantearnos diversas cuestiones estrictamente jurídicas, referidas a su grado real de obligatoriedad, y a las consecuencias de su eventual infracción, si es que cabe emplear este término.

En primer lugar, respecto al grado de exigibilidad de cumplimiento de los requisitos criptográficos contenidos en ETSI TS 119 312 por parte de los prestadores de servicios de confianza, y como ya hemos avanzado, resulta claro que en el Reglamento eIDAS no encontramos ninguna norma de obligación al respecto –de hecho, ni siquiera se menciona la criptografía–, pero también es cierto que la criptografía es la principal medida de seguridad subyacente a los servicios de confianza, y que tanto el artículo 19 como el artículo 24 del Reglamento eIDAS ordenan a los prestadores a tomar las medidas de seguridad "adecuadas" en cada caso, estableciendo un deber de diligencia que, en el caso de los servicios cualificados, es realmente muy elevada.

De hecho, en el caso de los prestadores de servicios cualificados, el artículo 13.1 del Reglamento eIDAS establece, en su párrafo tercero, una verdadera presunción de intencionalidad o negligencia, por lo que el riesgo se ubica claramente en el lado del prestador, que debe poder demostrar que ha adoptado dichas medidas adecuadas, algo que puede basarse en el cumplimiento, por el prestador, de las indicaciones de la normativa técnica, en especial cuando la misma haya sido establecida por la Comisión Europea, de acuerdo con la previsión contenida en el artículo 19.4.a) –medidas de seguridad de los prestadores de servicios de confianza– o en el artículo 24.5 del Reglamento eIDAS –normas de sistemas y productos fiables–, en especial porque en este último caso, como sabemos, se presumirá el cumplimiento de los requisitos legales correspondientes.

Es cierto, sin embargo, que la Comisión carece de competencias en materia criptográfica, por lo que la norma que referencie la Comisión será la que a su vez referencie esta especificación, que realmente recibe su valor principalmente del hecho de que la misma ha sido consensuada por el SOG-IS.

[1097] El epígrafe 1.3 del documento del SOG-IS define informalmente el nivel de seguridad como la complejidad temporal del mejor ataque conocido (conforme a algunas asunciones relativas a los recursos del adversario), incluyendo operaciones relativas a la escritura en memoria y el procesamiento de datos, de forma que el nivel de seguridad de un mecanismo no podrá ser inferior a la complejidad de memoria o de datos del mejor ataque conocido sobre el mecanismo en cuestión.

[1098] Por lo que se precisan 2^{125} operaciones para lograr romper la seguridad del mecanismo en cuestión.

Por tanto, formalmente el cumplimiento no resulta exigible de forma normativa, pudiendo el prestador elegir la política de uso de criptografía que mejor considere, bajo su responsabilidad –en un contexto donde tiene la carga de la prueba de la adopción de medidas adecuadas de seguridad–, pero con el incentivo de que, en caso de adherirse a las especificaciones adicionales o normas técnicas correspondientes, goza de protección legal por vía de presunción de adecuación al objetivo legal.

Lo cual nos lleva a la segunda cuestión, cuya respuesta ya ha quedado anticipada. No se podrá hablar de "incumplimiento" del Reglamento eIDAS por el hecho de no emplear los conjuntos criptográficos definidos en estas normas técnicas –lo cual es bastante relevante en el marco de un hipotético procedimiento sancionador– pero el prestador deberá entonces demostrar al supervisor que ha sido diligente en la selección de dichos conjuntos criptográficos y en el establecimiento de reglas de uso, porque en caso contrario el supervisor podrá entender que el prestador está infringiendo sus obligaciones de seguridad contenidas en los artículos 19.1 y 24.2; esto es, podemos concluir que no alinearse con la norma técnica correspondiente, que es de cumplimiento voluntario, se puede convertir en un indicio de infracción legal, y activar la correspondiente potestad sancionadora del supervisor.

Otra cosa es que, y ahí reside la tremenda potencia del enfoque regulatorio, los organismos que evalúan los productos empleados para los servicios de confianza (sean para sistemas fiables o para dispositivos cualificados de creación de firma o sello) exijan la utilización de los algoritmos criptográficos referenciados en ETSI TS 119 312 y el documento del SOG-IS como condición para obtener la certificación[1099].

Desde una perspectiva judicial, en caso de no alinearse con estas normas técnicas, el prestador cualificado deberá asumir el riesgo de que una prueba electrónica basada en sus servicios de confianza sea atacada con éxito, desvirtuándola, en cuyo caso se generará un daño resarcible de acuerdo con las reglas nacionales de responsabilidad contractual o extracontractual, en función de la persona dañada, pero con las especialidades del artículo 13.1 del Reglamento eIDAS, incluyendo la ubicación de la carga de la prueba de actuación diligente sobre el propio prestador.

Como hemos visto, las normas técnicas que desarrollan el Reglamento eIDAS, establecen recomendaciones tanto respecto de los requisitos de las claves de usuario que se contienen en el Anexo II, cuanto de las claves de los prestadores de servicios de confianza, dado que las citadas claves constituyen parte fundamental de los sistemas fiables a los que se refiere el artículo 24.2.e), así como de las medidas adecuadas de seguridad que deben adoptar los prestadores de servicios de confianza.

Sin embargo, y como hemos avanzado, también otras normas españolas establecen requisitos criptográficos que pueden recaer sobre los prestadores de servicios de

[1099] Se trata de un modelo idéntico al que se emplea en EEUU y Canadá en el marco de la norma NIST FIPS 140-2, sobre requisitos de seguridad para módulos criptográficos, muy ampliamente empleados en el marco de los sistemas fiables para los servicios de confianza; de hecho, el autor de este trabajo no ha encontrado jamás, en veinte años de actividad profesional en este campo, ningún módulo criptográfico con certificación europea, lo cual se traduce, simple y llanamente, en que las autoridades norteamericanas influyen de forma decisiva en los algoritmos que (no) se emplean en la Unión Europea, dado que nos resultan aplicables sus restricciones a algoritmos que consideren inseguros o, quizá, políticamente inconvenientes, como por ejemplo la versión alemana del algoritmo de firma digital basado en curvas elípticas (EC-GDSA, que sí se admite en el esquema del SOG-IS como mecanismo recomendado, aunque tiene un escaso volumen de uso, motivo por el que no se promueve su uso en ETSI TS 119 312).

confianza y, más en concreto, sobre aquéllos que sean titularidad o que presten servicios a las Administraciones Públicas: nos referimos a la aplicación de lo establecido en el RDENI, y en el RDENS; así como a la Norma Técnica de Interoperabilidad de política de firma y sello electrónicos y de certificados de la Administración, aprobada por Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas –que ha sustituido a la anterior, aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública–, y a los que conviene referirse sucintamente.

La política de firma y sello electrónico se refiere, en su epígrafe III.5 a las "reglas de uso de algoritmos", dentro de las denominadas "reglas comunes", en referencia a los algoritmos criptográficos en que se basa la firma electrónica. En concreto, la regla 1ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad ordena que "la política de firma y sello especificará las reglas de uso de algoritmos en los diferentes formatos así como la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma/sello electrónico, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares y lo previsto en las normas que se definan en aplicación del Reglamento (UE) 910/2014", incluyendo la política criptológica como parte esencial de la política de firma y sello electrónicos y de certificados.

Dos son los aspectos de los que debe ocuparse, por tanto, cada concreta política de firma electrónica; a saber, el establecimiento de las reglas de uso de algoritmos, y la determinación de la longitud de las claves empleadas por dichos algoritmos para las operaciones.

En relación con la primera cuestión, en el epígrafe III.5 de la Norma Técnica de Interoperabilidad se establecen dos categorías de seguridad a efectos de la determinación de los algoritmos criptográficos. En efecto, conforme al RDENI podrán aplicarse, a los "entornos de seguridad regulados por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/ 2015, de 1 de octubre, de Régimen Jurídico del Sector Público, de aplicación en los procedimientos de administración electrónica", los algoritmos referenciados por en las normas de formatos de firma y sello avanzado de los formatos aprobados por la Comisión Europea o por el ETSI[1100]; estableciéndose reglas más estrictas para los denominados entornos de alta seguridad[1101].

Esta determinación no está precisamente exenta de problemas, tanto debido a la oscuridad

[1100] La regla 2ª establece que "[p]ara los entornos de seguridad regulados por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/ 2015, de 1 de octubre, de Régimen Jurídico del Sector Público, de aplicación en los procedimientos de administración electrónica, se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014» o las especificaciones técnicas publicadas por los organismos de Estandarización Europeos. La definición de usos de algoritmos podrá contemplar diferentes posibilidades según lo establecido en las guías aplicables, como la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía, las normas ETSI TS 119 312 'Criptographic Suites for secure electronic signatures', o aquellas que las sustituyan".

[1101] La regla 3ª determina que "para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional (CCN) serán de aplicación las recomendaciones revisadas de la CCN-STIC 405 así como en la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía".

del precepto, cuanto por su indeterminación. En efecto, resulta difícil dilucidar las condiciones de aplicabilidad de ambos niveles de seguridad, debido a la ausencia de mayores indicaciones en la Norma Técnica de Interoperabilidad, pero ciertamente parece que el nivel de alta seguridad al que se refiere la regla se refiere a la una seguridad mayor a la que exige la realización de cualquier procedimiento administrativo, por contraposición a la regla anterior.

Del análisis de las especificaciones técnicas mencionadas en la regla 2ª del epígrafe III.5 de la Norma Técnica de Interoperabilidad se deduce la posibilidad de emplear cualquiera de los algoritmos allí identificados para la producción de firmas o sellos electrónicos avanzados y cualificados, por lo que resulta que el nivel genérico de seguridad cubre, en principio, todos los casos de uso de firma y sello electrónico en el procedimiento administrativo y, por tanto, no supone requisito adicional alguno para el prestador.

En todo caso, y dentro del nivel de seguridad del procedimiento administrativo, resulta preciso acudir al RDENS. Una vez determinado el nivel de seguridad requerido en las dimensiones de autenticidad e integridad, el anexo II de dicha norma determina la aplicación de las siguientes reglas criptográficas, contenidas en el epígrafe 5.7.4:

- En el nivel bajo, se empleará cualquier medio de firma electrónica de los previstos en la legislación vigente, por lo que, en principio, no se establecería restricción ninguna en cuanto a los algoritmos a emplear.
- En el nivel medio, se establece que los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada, y que en todo caso se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
- En el nivel alto, se indica que se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel medio, además del empleo de dispositivos seguros de creación de firma y, preferentemente, de productos certificados.

Respecto al "entorno de alta seguridad" referido en la regla 3ª del epígrafe III.5, parecería razonable hacer coincidir este entorno de seguridad alta con el nivel de seguridad alto del RDENS, de forma que los algoritmos acreditados serían utilizados en los dispositivos seguros de creación de firma, en su caso debidamente certificados – y así sucedía con la redacción contenida en la anterior versión de la Norma Técnica de Interoperabilidad – pero en realidad parece que este "entorno de alta seguridad", como se ha avanzado, nos encontramos ante un nivel más alto de seguridad que el nivel alto del RDENS.

En este sentido, la Guía/Norma de seguridad de la TIC CCN-STIC-807:2012 contiene los algoritmos acreditados por el Centro Criptológico Nacional para su uso únicamente dentro del Esquema Nacional de Seguridad –lo cual no es menor, dado que alcanza a la totalidad del sector público español, y a sus contratistas y colaboradores privados–, estableciendo recomendaciones de uso de algoritmos acreditados para firma electrónica, en relación con los diversos niveles de seguridad del Esquema Nacional de Seguridad, que los prestadores de servicios de confianza que ofrezcan sus servicios a las Administraciones españolas deberán cumplir.

Por su parte, la Guía CCN-STIC-405:2012 establece recomendaciones en cuanto a algoritmos criptográficos y parámetros asociados para obtener garantías de seguridad en la utilización de la firma electrónica, tanto por los dispositivos seguros de creación de firma electrónica como por los prestadores de servicios de certificación.

Sin embargo, a diferencia de la Guía/Norma CCN-STIC-807:2012, el alcance de la Guía

CCN-STIC-405:2012 se refiere a los Sistemas de las Tecnologías de la Información y las Comunicaciones (STIC) que manejan información nacional "clasificada" o que requieran de una "firma electrónica reconocida" en la Administración, por lo que el ámbito de su aplicación deberá ser más estricto incluso que en el ámbito del RDENS.

Los Esquemas Nacionales de Interoperabilidad y Seguridad, como acabamos de comprobar, plantean exigencias criptográficas que van más allá de las que se establezcan como mínimo exigible por el Reglamento eIDAS, por lo que cabe preguntarse por la consecuencia jurídica correspondiente, que se puede resultar diferente en función de la posición de la Administración obligada.

En primer lugar, si la Administración es la prestadora del servicio de confianza en cuestión el cumplimiento de estas exigencias adicionales resultará pleno, dado que les resulta aplicable directamente la normativa estatal.

En el segundo caso, si la Administración es adquirente del servicio de confianza, deberá trasladar estas exigencias al prestador de servicios mediante el oportuno contrato administrativo, lo cual podría afectar negativamente a la libre circulación de los servicios de confianza dentro del territorio de la Unión Europea, en una posible contradicción con lo establecido en el Reglamento eIDAS y de la normativa de contratación pública.

Este problema se podría dar en el caso de que una Administración española decidiera adquirir sistemas de firma electrónica cualificada, mediante el correspondiente procedimiento abierto con publicidad europea, en el que se excluyese una proposición de un licitador alegando que el dispositivo, aún certificado como cualificado, no emplea el uso de un algoritmo concreto impuesto por la normativa nacional, algo que cabe pensar no sucederá simplemente porque los fabricantes suelen permitir que cada cliente configure los dispositivos de modo que puedan emplear los algoritmos que se requieran en cada caso.

6.2.7 La conservación de informaciones relativas al servicio

El artículo 24.2 del Reglamento eIDAS ordena que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: […] h) registrarán y mantendrán accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio", añadiendo que "[e]sta actividad de registro podrá realizarse por medios electrónicos".

Se trata de una obligación que, como en otros casos, supone la generalización a todos los servicios de confianza de la obligación inicialmente establecida para el servicio de expedición de certificados, en relación con lo cual la DFE ordenaba al prestador, en el numeral i) de su Anexo II, "registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos"; norma que fue objeto de trasposición en el artículo 20.1.f) de la LFE, que obligaba a "[c]onservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo".

Como se puede ver, la LFE concretó algo más que la DFE la información pertinente, que debía incluir también la declaración de prácticas de certificación que se encontrara vigente en el momento de la expedición del certificado[1102], así como el plazo de conservación, que se estableció en el mínimo de quince años desde la expedición del certificado, aclarando también que el objetivo de la conservación de estas informaciones es permitir que puedan verificarse las firmas electrónicas efectuadas con el certificado[1103].

Se trataba de un plazo que parecía alineado con el plazo de prescripción de las acciones personales que no tuvieran señalado un término especial de prescripción, que en la redacción original del artículo 1964 del Código Civil –vigente en la fecha de aprobación de la LFE– era precisamente de quince años, habiéndose reducido el mismo, en virtud de la modificación de dicho artículo operada por la disposición final primera de la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento

---

[1102] (Ortega Díaz, 2008, págs. 146-147) incluye, entre las informaciones a conservar, no sólo la de la solicitud y la generada durante todo el ciclo de vida del certificado, sino también la relativa a la generación de claves. Para este autor, "sería extremadamente recomendable que esa cuestión fuera tratada en los procesos autorreguladores en el seno de la industria de la certificación", como de hecho ha sucedido, con especial intensidad en el caso de los certificados de servidor seguro con validación extendida del CA/Browser Forum.

[1103] Resulta llamativo la incorrecta expresión de la firma efectuada con el certificado, cuando, como sabemos, el certificado no se usa para firmar (en todo caso, los datos de creación de firma y el dispositivo de creación de firma servirán para ello), sino para publicitar de forma segura los datos de validación de la firma, por lo que se ha extendido la expresión de que la firma se basa en el certificado, que es algo más acertada, aunque realmente lo más correcto sería referirse a que la firma se basa en la clave pública certificada. (Ortega Díaz, 2008, pág. 147) enfatiza el origen de esta obligación en la prueba, refiriéndose a la importancia de la documentación, por ejemplo, acreditativa de la entrega de las claves.

Civil, al plazo de cinco años[1104] desde que se pueda exigirse el cumplimiento de la obligación, con la precisión de que, en las obligaciones continuadas de hacer o no hacer, el plazo comenzará cada vez que se incumplan.

El establecimiento de este plazo de quince años podía resultar aparentemente razonable, a la luz de la exclusión de la normativa de contratación electrónica prevista en el Título IV de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, pero en realidad planteaba problemas relevantes.

En primer lugar, por el inicio del cómputo del plazo desde la expedición del certificado, y no desde su expiración o revocación anticipada, algo que no es menor dado que un certificado podía durar, conforme al artículo 8.2 de la LFE, hasta cinco años[1105], lo cual implica que un contrato firmado el día anterior a la expiración del certificado sólo se beneficiaría de diez años de conservación de las informaciones correspondientes.

En segundo lugar, porque a pesar de lo dicho anteriormente, la firma electrónica resulta plenamente aplicables a los documentos públicos, y, de forma específica, también a los documentos públicos notariales[1106], lo cual nos refiere a negocios jurídicos con acción real y, por tanto, plazo muy superior de prescripción.

Todas estas reflexiones resultan directamente trasladables a los servicios cualificados de confianza, con las necesarias adaptaciones en función del tipo de servicio, y en relación con las informaciones propias de cada servicio, entre las que Reglamento eIDAS incluye los datos expedidos y recibidos por el prestados, sea de su cliente o de terceros, en conexión con la prestación del servicio.

Diversas son las notas dignas de consideración en relación con esta obligación: en primer lugar, que la misma se mantiene incluso después de la cesación de las actividades de prestación de servicios de confianza, por lo que se deberá considerar en el plan de cese,

---

[1104] El apartado VI del preámbulo de la citada Ley 42/2015 justifica la reforma diciendo que con la reforma "se obtiene un equilibrio entre los intereses del acreedor en la conservación de su pretensión y la necesidad de asegurar un plazo máximo", anunciando también que "[l]a disposición transitoria relativa a esta materia permite la aplicación a las acciones personales nacidas antes de la entrada en vigor de esta Ley, de un régimen también más equilibrado, surtiendo efecto el nuevo plazo de cinco años".

[1105] En redacción dada por la disposición final 6 de la Ley 9/2014, de 9 de mayo. Hasta dicha reforma, el plazo máximo de vigencia del certificado era de cuatro años. El mismo plazo máximo se mantiene en el borrador de Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, artículo 4.2.

[1106] Recuérdese que el artículo 17 bis.1 de la Ley del Notariado de 28 de mayo de 1862, añadido por el artículo 115.1 de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, establece que "los instrumentos públicos a que se refiere el artículo 17 de esta Ley, no perderán dicho carácter por el sólo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquél de conformidad con la Ley reguladora del uso de firma electrónica por parte de notarios y demás normas complementarias", aunque la Disposición transitoria undécima de la propia Ley, añadida por el artículo 115.2 de la citada Ley 24/2001, desactiva esa posibilidad cuando indica que "hasta que los avances tecnológicos hagan posible que la matriz u original del documento notarial se autorice o intervenga y se conserve en soporte electrónico, la regulación del documento público electrónico contenida en este artículo se entenderá aplicable exclusivamente a las copias de las matrices de escrituras y actas así como, en su caso, a la reproducción de las pólizas intervenidas".

al que luego nos referiremos[1107]; en segundo, que esta obligación ya no sólo se oriente a apoyar la prueba electrónica, en caso de su cuestionamiento, sino también a la continuidad del servicio, referencia que resulta más novedosa y, en cierto modo, sorprendente, al menos en el caso de algunos servicios[1108]; finalmente, aunque no se explicite previsión concreta alguna en el Reglamento eIDAS, lógicamente esta obligación deberá conciliarse con el cumplimiento de la normativa de protección de datos, impactando sobre el ejercicio del novedoso derecho de supresión.

El Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza mantiene, en su artículo 9.3.a), el término de quince años respecto a la conservación de las informaciones previstas en el artículo 24.2.h) del Reglamento eIDAS, pero en una formulación que podría dar a entender que se trata de un plazo, no de mínimos, sino de máximos, algo que podría resultar inconveniente, como se ha justificado antes.

En todo caso, y como novedad en relación con la normativa anterior, el inicio del cómputo de este plazo se produce en el momento de finalización del servicio prestado. Por ejemplo, en el caso de un certificado cualificado que dure cinco años, la información deberá conservarse veinte años en total.

6.2.8 La cesación del servicio

El artículo 24.2.a) del Reglamento eIDAS ordena que "[l]os prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados: a) informarán al organismo de supervisión […] de su intención de cesar tales actividades".

A dicha obligación se debe añadir la prevista en el artículo 24.2.i) del propio Reglamento eIDAS, en cuya virtud los prestadores "contarán con un plan de cese actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17, apartado 4, letra i)"; disposiciones que esencialmente se refieren al mantenimiento de "toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio", como hemos analizado en el epígrafe anterior.

Se trata de una cuestión de extraordinaria importancia, y que denota la preocupación del legislador por evitar que el cese, por cualquier motivo, de la actividad por el prestador pueda afectar negativamente al valor probatorio de los procesos a los que se han incorporado pruebas electrónicas producidas o basadas en servicios cualificados de confianza.

En efecto, si para la validación de una firma electrónica cualificada, por ejemplo, es preciso comprobar –como ya hemos estudiado[1109]– que el certificado cualificado que la respalda era válido en el momento de creación de dicha firma electrónica cualificada,

---

[1107] Cfr. el epígrafe 6.2.8 de este trabajo.

[1108] Por ejemplo, en el caso del servicio de entrega electrónica certificada, una vez realizado el envío y la entrega, no parece que resulte necesario conservar muchas informaciones a estos efectos de continuidad del servicio.

[1109] Cfr. el epígrafe 4.3.2.1 de este trabajo.

resulta preciso tener disponible dicha información incluso con posterioridad al cese de la actividad del prestador, porque de otro modo simplemente no será posible.

Por tanto, el cese del prestador de servicios puede implicar que no se tenga acceso a esta información, en particular las listas de revocación de certificados, lo que constituye un claro riesgo para los usuarios de los servicios, así como para las terceras partes que deben confían en las pruebas electrónicas.

Para ello, el plan de cese deberá, como indica el ya mencionado artículo 17.4.i) del Reglamento eIDAS, especificar "la forma en que se hace accesible la información" en cuestión.

Más allá de estas previsiones, el Reglamento eIDAS no concreta las diferentes acciones que deben realizar los prestadores, dejando espacio para la autorregulación y/o para la legislación nacional.

En todo caso, al sujetarse esta cuestión a la evaluación de la conformidad, se puede garantizar que –antes del inicio de la prestación de los servicios– existirán las necesarias garantías, evitándose el daño potencial en caso de cese de la actividad. A ello se refiere el Considerando (41) del Reglamento eIDAS, cuando indica que "[a] fin de garantizar la sostenibilidad y durabilidad de los servicios de confianza cualificados y de potenciar la confianza de los usuarios en la continuidad de dichos servicios, los organismos de supervisión deben verificar la existencia y la correcta aplicación de las disposiciones relativas a los planes de cese en caso de que los prestadores cualificados de servicios de confianza cesen en sus actividades".

Esta obligación resulta novedosa respecto al régimen contenido en la DFE, pero no tanto en sede nacional[1110], dado que el artículo 21 de la LFE ya se refería a las obligaciones del prestador de servicios de certificación que fuere a cesar en sus actividades, que venía legalmente obligado a "comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas", pudiendo "transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia"; comunicación que también debía realizarse al organismo de supervisión[1111].

La novedad, también en este caso, reside en el refuerzo de la obligación de mantener el acceso a las informaciones necesarias para validar las pruebas electrónica, que anteriormente se podía considerar implícita, pero que ahora se explicita a efectos de mayor confianza de los usuarios.

En el régimen de la LFE, el epígrafe 3 del artículo 21 preveía la obligación de los prestadores que fueren a cesar en el servicio de expedición de certificados de remitir al órgano de supervisión "la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f)", relativo al mantenimiento de la información durante quince años, debiendo por el órgano de supervisión mantenerse "accesible al público un

[1110] Cfr. (Martínez Nadal, 2009, págs. 380-386).

[1111] Comunicación que no sólo era necesaria en caso de cese efectivo, sino que también debía venir referida, como ha señalado (Ortega Díaz, 2008, pág. 128), a cualquier causa que eventualmente pudiera afectar a la continuidad de la actividad.

servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo", en sustitución, como puede verse, del prestador y al objeto de mantener la posibilidad de los terceros de comprobar el valor probatorio de una firma electrónica.

Por su parte, el artículo 9.2.c) del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza complementa la regulación contenida en el Reglamento eIDAS con diversas previsiones, en línea con el régimen anterior.

En primer lugar, se mantiene el plazo de dos meses para la comunicación del cese de actividad, tanto a los clientes como al órgano de supervisión. Asimismo, en segundo término, se mantiene la posibilidad de que el plan de cese pueda "incluir la transferencia de clientes a otro prestador cualificado, una vez acreditada la ausencia de oposición de los mismos", lo que podrán realizar en respuesta a la comunicación anteriormente indicada.

Aunque no se diga, es evidente que, en caso contrario, el prestador procederá a la extinción de la vigencia de los certificados cuya gestión de sea transferida a otro prestador, como además se recoge en el artículo 5.1.f) del propio Anteproyecto.

En sentido similar se pronuncia la sección § 16 de la Ley alemana de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017, con la particularidad de que, conforme al epígrafe (5) de la citada sección, el órgano de supervisión deberá mantener una infraestructura de confianza para la verificabilidad permanente de los certificados electrónicos cualificados y los sellos cualificados de tiempo electrónico de prestadores de servicios de confianza que hayan cesado en su actividad.

CAPÍTULO 7. EL RÉGIMEN ADMINISTRATIVO DE SUPERVISIÓN Y CONTROL APLICABLE A LOS SERVICIOS DE CONFIANZA

Tras haber estudiado, en los Capítulos precedentes, los diferentes tipos de fuentes de prueba electrónica sustentadas en servicios de confianza; esto es, la identificación electrónica basada en certificado, la firma electrónica avanzada o cualificada basada en certificado y el sello electrónico avanzado o cualificado basado en certificado, así como los requisitos legalmente establecidos en relación con los prestadores de servicios de confianza, y de los propios servicios de confianza que sustentan estas fuentes de prueba electrónica, es momento de profundizar en el régimen jurídico-administrativo de supervisión y control que se establece para garantizar el correcto funcionamiento de dichos servicios de confianza.

En el epígrafe primero de este Capítulo nos ocupamos del régimen jurídico del acceso a la actividad, tanto en relación con los prestadores y servicios cualificados, como con los que no disponen de esta condición, conforme al modelo mixto que hemos presentado en el Capítulo 1. En relación con esta cuestión, en primer lugar, se analiza el novedoso sistema de evaluación de la conformidad de los servicios de confianza, requisito previo y periódico exigible a los cualificados; en segundo lugar, el procedimiento administrativo de concesión de la conformidad por parte del órgano de supervisión; y, en tercero, la comunicación de inicio de la actividad de los prestadores que ofrecen servicios no cualificados. En el mismo epígrafe se estudia la publicidad de la cualificación, que permite el inicio de la prestación de servicio cualificado, y otras modalidades de publicidad de servicios, cualificados o no.

En el epígrafe segundo de este Capítulo, se aborda la actividad de supervisión posterior al acceso a la actividad por parte del prestador, incluyendo el contenido de esta actividad administrativa, con una especial atención a la retirada de la cualificación y a otras medidas no sancionadoras que persiguen la eficacia de la supervisión.

Finalmente, en el epígrafe tercero se trata el régimen administrativo sancionador propuesto, en el nivel nacional, en relación con la prestación de los servicios de confianza, para dar cumplimiento al mandato del Reglamento eIDAS.

7.1 EL ACCESO A LA ACTIVIDAD DE PRESTACIÓN DE SERVICIOS DE CONFIANZA

Como se ha presentado en el Capítulo 1, el modelo regulatorio del Reglamento eIDAS diferencia de forma nítida los servicios de confianza en función de su cualificación, sujetando los servicios cualificados a un régimen de autorización administrativa previa al inicio de la actividad, al tiempo que mantiene el modelo de acceso libre al mercado de los servicios sin cualificación, pero con un significativo control *ex post*.

Resulta necesario referirse, en este momento, al procedimiento previsto en el Reglamento eIDAS en relación con el acceso a la actividad de los prestadores de servicios cualificados, diferenciándose tres momentos relevantes: la evaluación previa de la conformidad del servicio, la notificación de la intención de prestar el servicio, y posterior concesión, en su caso, de la cualificación, y finalmente, la publicidad de la citada

cualificación.

Posteriormente nos referiremos a la posibilidad de que el prestador de servicios sin cualificación deba también realizar alguna comunicación al supervisor, a los efectos de facilitar su supervisión *a posteriori*.

7.1.1 La evaluación de la conformidad del prestador del servicio de confianza cualificado

El primer paso del procedimiento que debe realizar un prestador para lograr la obtención de la cualificación del servicio de confianza (y, por tanto, su propia cualificación como prestador) consiste en la superación de una evaluación de la conformidad del servicio de confianza.

Conforme al artículo 21.1 del Reglamento eIDAS, "[c]uando los prestadores de servicios de confianza, sin cualificación, tengan intención de iniciar la prestación de servicios de confianza cualificados, presentarán al organismo de supervisión […] un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad". Se trata de una obligación que formalmente sólo se impone a los prestadores sin cualificación, lo que genera la duda acerca de si la misma resulta también exigible en el caso de que un prestador que ya disponga de cualificación para uno o varios servicios, pero que desee iniciar la prestación de un servicio que no disponga de la cualificación.

La respuesta a esta cuestión debe ser, en mi opinión, necesariamente afirmativa, dado que de otro modo nos encontraríamos ante una inaceptable vía de prestación de servicios no autorizados. Cabe entender que la cualificación del prestador se refiere a cada uno de los servicios, por lo que un prestador estará cualificado para el servicio de expedición de certificados de firma electrónica, pero no para la expedición de sellos de tiempo electrónico. Por ello, en caso de que desee iniciar la prestación del servicio de expedición de sellos cualificados de tiempo electrónico, al no encontrarse cualificado para ello, deberá previamente obtener la aludida evaluación de la conformidad.

Asimismo, el artículo 20.1 del mismo Reglamento eIDAS prevé que "[l]os prestadores cualificados de servicios de confianza serán auditados, al menos cada 24 meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad", al objeto de "confirmar que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento".

Por tanto, la evaluación de la conformidad, que, como se puede ver, se impone sólo a los prestadores que ofrecen servicios cualificados de confianza, se debe producir en diversos momentos: antes de notificar la intención de prestar el servicio en cuestión, y posteriormente cada dos años[1112], mientras se preste el servicio.

Adicionalmente, conforme al artículo 20.2 del Reglamento eIDAS, "el organismo de supervisión podrá en cualquier momento […] solicitar a un organismo de evaluación de

[1112] Nótese que, conforme al mismo artículo, dicho informe de evaluación de la conformidad correspondiente deberá remitirse al organismo de supervisión en el plazo de tres días hábiles tras su recepción.

la conformidad que realice una evaluación de conformidad de los prestadores cualificados de servicios de confianza, corriendo con los gastos dichos prestadores de servicios de confianza, para confirmar que tanto ellos como los servicios de confianza cualificados que prestan cumplen los requisitos del presente Reglamento", potestad que –hay que entender– debe ser ejercida conforme al principio de buena administración y, en particular, mediante la adecuada motivación[1113], debido a la asunción del coste de dicha evaluación por parte del prestador afectado.

En los tres casos, la evaluación de la conformidad tiene la finalidad de acreditar, de forma independiente, el cumplimiento de los requisitos legales exigibles para la prestación de servicios de confianza cualificados.

De esta forma, el objeto de la evaluación de la conformidad se dirige a la verificación, tanto al inicio como de forma periódica, del servicio de confianza cualificado –así como de los productos que se emplean en el mismo–, por lo que el proceso de evaluación ofrece una garantía material acerca de que el servicio prestado cumple los requisitos establecidos legalmente, incrementando la confianza en el sistema.

Tal es la importancia de la evaluación periódica, y su remisión al organismo de supervisión, que el Anteproyecto de Ley reguladora de determinados aspectos de los servicios de electrónicos de confianza ha previsto, en su artículo 9.3.e) ordena, taxativamente, que "[l]os prestadores cualificados de servicios de confianza enviarán el informe de evaluación de la conformidad al Ministerio de Energía, Turismo y Agenda Digital[1114] en los términos previstos en el artículo 20.1 del Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014", añadiendo que "[e]l incumplimiento de esta obligación conllevará la suspensión de la cualificación al prestador y al servicio que éste presta, y su eliminación de la lista de confianza prevista en el artículo 22 del citado Reglamento hasta que se aporte el informe de evaluación", retirada de la Lista que no deberá considerarse como sanción[1115].

En definitiva, la evaluación de la conformidad se configura como un proceso que debe ser ejecutado, a tenor de lo dispuesto en el artículo 3.18) del Reglamento eIDAS, por un "organismo definido en el punto 13 del artículo 2 del Reglamento (CE) Nº 765/2008 cuya competencia […] esté acreditada en virtud de dicho Reglamento"[1116], dado que el informe que produzca se va a emplear en el procedimiento autorizatorio en que consiste la concesión de la cualificación, por parte del órgano de supervisión, como material técnico

---

[1113] Así se menciona expresamente en el Considerando (43) del Reglamento eIDAS, cuando indica que "[s]iempre que el organismo de supervisión exija que un prestador cualificado de servicios de confianza presente un informe ad hoc de evaluación de la conformidad, el organismo de supervisión debe observar, en particular, el principio de buena administración, incluida la obligación de motivar sus decisiones, así como el principio de proporcionalidad", por lo que "el organismo de supervisión debe justificar debidamente cualquier decisión por la que requiera una evaluación ad hoc de la conformidad".

[1114] Actualmente, el Ministerio de Economía y Empresa.

[1115] Cfr. el epígrafe 7.2.2 de este trabajo.

[1116] El citado Reglamento Nº 765/2008 define la evaluación de conformidad como el "proceso por el que se demuestra si se cumplen los requisitos específicos relativos a un producto, un proceso, un servicio, un sistema, una persona o un organismo" (artículo 2.12), y al organismo de evaluación de la conformidad como el que "desempeña actividades de evaluación de la conformidad, que incluyen calibración, ensayo, certificación e inspección".

de apoyo fundamental para la correspondiente decisión administrativa.

El Reglamento eIDAS exige, pues, claramente que el organismo de evaluación[1117] sea competente para realizar el proceso de evaluación de la conformidad, competencia que debe referirse precisamente al objeto de evaluación –que son los servicios de confianza– y que debe ser comprobada de forma independiente. Para ello, el organismo de evaluación de la conformidad debe ser acreditado por un organismo de acreditación nacional[1118], que es el garante último de la cadena de evaluación de la conformidad, por lo que el precisamente es objeto del Reglamento Nº 765/2008 el establecimiento de "normas sobre la organización y el funcionamiento de la acreditación de organismos de evaluación de la conformidad que llevan a cabo actividades de evaluación de la conformidad" (artículo 1.1).

Resulta especialmente relevante hacer notar que la acreditación se conceptualiza, en el Reglamento Nº 765/2008 necesariamente como una potestad pública, consistente en la "declaración por un organismo nacional de acreditación de que un organismo de evaluación de la conformidad cumple los requisitos fijados con arreglo a normas armonizadas y, cuando proceda, otros requisitos adicionales, incluidos los establecidos en los esquemas sectoriales pertinentes, para ejercer actividades específicas de evaluación de la conformidad", motivo por el cual indica el Considerando (15) del Reglamento que "es necesario prever que los Estados miembros velen por que se dote a los organismos nacionales de acreditación, de autoridad pública para el ejercicio de la actividad de acreditación, con independencia de su personalidad jurídica".

En España, el organismo nacional de acreditación designado es ENAC, en virtud de lo establecido en el Real Decreto 1715/2010, de 17 de diciembre, que parte de la actuación previa de ENAC al amparo de la Ley 21/1992, de 16 de julio, de Industria, desarrollada por Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y la Seguridad Industrial[1119], si bien era discutible que dicha normativa resultara aplicable a todas las actividades de servicios, dado su enfoque en los productos industriales[1120].

[1117] Sobre el régimen jurídico estas entidades, cfr. con carácter general, (Blanquer, 2006, pág. 219 y ss.).

[1118] El Reglamento Nº 765/2008 realiza una decidida apuesta porque en cada Estado miembro únicamente pueda existir un organismo nacional de acreditación (artículo 4.1), sin perjuicio de que su Considerando (11) enfatice que "[l]a creación de un organismo nacional de acreditación uniforme debe realizarse sin perjuicio del reparto de funciones en el seno de los Estados miembros". Sobre la noción de acreditación, cfr. (Izquierdo Carrasco, 2000, pág. 453 y ss.), aunque el sistema ha sufrido importantes ajustes posteriormente, en especial motivados por la Directiva de Servicios.

[1119] El Real Decreto 2200/1995 regulaba en sus artículos 14 a 19 el funcionamiento de las entidades de acreditación, y designaba a ENAC como entidad de acreditación en su disposición final tercera; normas que fueron derogadas por el Real Decreto 1715/2010, como es lógico.

[1120] Es cierto que la Ley 21/1992 se aplica a "los servicios de ingeniería, diseño, consultoría tecnológica y asistencia técnica directamente relacionados con las actividades industriales" (artículo 3.2), y con carácter supletorio, a actividades de servicios, como las turísticas. En todo caso, hay que hacer notar que el Real decreto 1715/2010 se dictó con base en los títulos competenciales recogidos en el artículo 149.1.13ª y 23ª de la Constitución, que atribuye al Estado la competencia exclusiva para establecer las bases y coordinación de la planificación general de la actividad económica y para dictar la legislación básica en materia de medio ambiente, según se desprende en la disposición final primera, declarada inconstitucional y nula por Sentencia del TC 20/2014, de 10 de febrero, pero por haber incluido a los verificadores medioambientales en la obligación de acreditación de ENAC, por lo que el Tribunal Constitucional entiende conforme al

Asimismo, al objeto de garantizar la libre circulación de los certificados de acreditación que expida el organismo nacional de acreditación (a los organismos de evaluación de la conformidad) y de los certificados de conformidad expedidos por los organismos de evaluación de la conformidad (a los prestadores de servicios de confianza, en nuestro caso), el Reglamento Nº 765/2008 establece, en su artículo 11, la presunción de conformidad de los organismos nacionales de acreditación que hayan superado la evaluación por pares prevista en el artículo 10 del mismo Reglamento, que es organizada[1121] por un organismo europeo a cargo de la denominada "infraestructura europea de acreditación" (artículo 14 y Anexo I), que actualmente es la organización conocida como Cooperación Europea para la Acreditación (EA), una asociación formada por los propios organismos nacionales de acreditación[1122].

El efecto de esta norma es que la evaluación de conformidad podrá ser realizada por cualquier organismo de evaluación de la conformidad acreditado en su Estado de establecimiento[1123], sin necesidad de obtener nuevas acreditaciones en los restantes Estados donde opere, dado que su acreditación goza de reconocimiento en toda la Unión.

Más en concreto, en el ámbito de la Cooperación Europea para la Acreditación (EA) se ha establecido un Acuerdo Multilateral de Reconocimiento entre organismos nacionales de acreditación que ofrece cobertura, entre otras, a la realización de las evaluaciones de conformidad de servicios en general, con base en la norma ISO/IEC 17065.

Sin embargo, como hemos visto anteriormente, es preciso que el organismo de evaluación

---

reparto competencial la sujeción de la evaluación de la conformidad de las restantes actividades, incluso las no industriales, a la citada acreditación. Curiosamente, este mismo conflicto se ha suscitado, de nuevo, con ocasión del Real Decreto 239/2013, de 5 de abril, por el que se establecen las normas para la aplicación del Reglamento (CE) n.º 1221/2009 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, relativo a la participación voluntaria de organizaciones en un sistema comunitario de gestión y auditoría medioambientales (EMAS), y por el que se derogan el Reglamento (CE) n.º 761/2001 y las Decisiones 2001/681/CE y 2006/193/CE de la Comisión, que de nuevo sujetó a los verificadores medioambientales a la acreditación y supervisión de ENAC (cfr. artículo 11, epígrafes 1 y 2, artículo 12, epígrafes 1 y 4, y disposición transitoria tercera), previsión declarada inconstitucional y nula por Sentencia del TC 141/2016, de 21 de julio.

[1121] Con base en la norma ISO/IEC 17011.

[1122] Esta previsión comunitaria encuentra su lógico reflejo en la disposición adicional única del anteriormente mencionado Real decreto 1715/2010, relativa a la presunción de conformidad para los organismos nacionales de acreditación y los organismos de evaluación de la conformidad acreditados por ellos, en cuya virtud, "[l]as Administraciones públicas, en el ejercicio de sus competencias, reconocerán la equivalencia de los servicios prestados por los organismos de acreditación de cualquier Estado miembro de la Unión Europea, siempre que dichos organismos se hayan sometido con éxito al sistema de evaluación por pares previsto en el Reglamento (CE) n.º 765/2008, de 9 de julio, del Parlamento Europeo y del Consejo, y aceptarán la validez de los certificados de dichos organismos de acreditación, así como las certificaciones emitidas por los organismos de evaluación de la conformidad acreditados por ellos", previsión que ciertamente es superflua dada la aplicación directa del Reglamento comunitario.

[1123] El Reglamento Nº 765/2008 prevé la opción de acreditarse en un Estado diferente en dos casos: cuando el Estado en el que se encuentre establecido el organismo de evaluación de la conformidad designe a un organismo nacional de acreditación de un tercer Estado miembro, cuando los organismos nacionales de acreditación mencionados en el párrafo primero no realicen acreditaciones en relación con las actividades de evaluación de la conformidad para las que se solicita la acreditación, o cuando los organismos nacionales de acreditación mencionados en el párrafo primero no se hayan sometido con éxito a la evaluación por pares prevista en el artículo 10 en lo que respecta a las actividades de evaluación de la conformidad para las que se solicita acreditación (cfr. artículo 7).

de la conformidad tenga competencia específica en servicios de confianza, tanto por lo que se refiere la forma de evaluar como al contenido material de la citada evaluación. Más aún, resulta conveniente la existencia de criterios comunes en cuanto a ambas cuestiones, para evitar el riesgo de que los prestadores de servicios de confianza decidan acudir a organismos de evaluación de la conformidad que apliquen criterios insuficientemente rigurosos.

El artículo 20.4 del Reglamento eIDAS responde a esta necesidad, cuando prevé la posibilidad de que la Comisión pueda adoptar normas relativas a la acreditación de los organismos de evaluación de la conformidad y para el informe de evaluación de la conformidad, así como sobre las disposiciones en materia de auditoría a emplear durante la evaluación de la conformidad en cuestión; competencia a ejercitar mediante el procedimiento de examen.

Aunque hasta la fecha no se ha hecho uso de esta posibilidad, en el ETSI se ha aprobado la norma EN 391 403 v2.2.2 (2015-08), que establece –partiendo de la norma ISO/IEC 17605– los requisitos que deben cumplir los organismos de evaluación de la conformidad de servicios de confianza, que cubre los contenidos del artículo 20.4 del Reglamento eIDAS anteriormente transcrito, lo que permite anticipar que, en su caso, la misma sería la norma candidata para referencia.

Sin que resulte procedente analizar el contenido de la norma ETSI EN 319 403, sí que es relevante mencionar que dicha norma recomienda la realización de auditorías de vigilancia periódicas, proponiendo que al menos se realice una auditoría anual, por lo que en general cabe esperar que se exija una auditoría completa cada dos años, y al menos una auditoría de seguimiento anual.

A lo que hay que sumar, en su caso, las auditorías extra que pueda exigir el organismo de supervisión, como por ejemplo en caso de que el prestador notifique su intención de realizar cambios en la prestación de un servicio cualificado (cfr. el artículo 24.2.a) del Reglamento eIDAS), o en caso de actuación por fallo de seguridad notificado (cfr. el artículo 19 del Reglamento eIDAS), o incluso por denuncia administrativa frente al prestador de servicios de confianza. Más dudoso será que el organismo de supervisión pueda solicitar, sin motivación ninguna, a un prestador que realice una nueva evaluación de conformidad.

De la norma también resulta relevante decir que la misma establece que la auditoría –en la que consiste la evaluación de conformidad– debe basarse en normas, en especificaciones técnicas públicamente disponibles y/o en requisitos regulatorios, apuntando al uso de las normas técnicas a que nos hemos referido al presentar el modelo regulatorio del Reglamento eIDAS[1124], sean o no establecidas por la Comisión Europea.

De ello no se desprende en absoluto que las normas sean legalmente obligatorias, dado que en dicho caso pasarían a ser reglamentos técnicos *de facto*, pero no es menos cierto que si un organismo de evaluación es acreditado para auditar conforme a unas normas técnicas concretas, puede suceder que no pueda auditar a un prestador que no se adhiera a las mismas, por entender que excede de su acreditación, algo que refuerza sobremanera el empleo de dichas normas por parte de los prestadores de servicios de confianza.

Cabe, por tanto, asumir que cuando existan normas de actividad bien establecidas, los

[1124] Como, por ejemplo, ETSI EN 319 401, ETSI EN 319 411, partes 1 y 2, ETSI EN 319 412, partes 1 a 5, ETSI EN 319 421, ETSI EN 319 422, etc. Cfr. el epígrafe 1.4.2 de este trabajo.

organismos de evaluación de la conformidad las adoptarán para su propia acreditación, por lo que los prestadores de servicios de confianza también apostarán por las mismas, antes que por otras normas o especificaciones técnicas.

En todo caso, mientras la Comisión Europea no haga uso de la posibilidad de establecer las normas previstas en el artículo 18.4 del Reglamento eIDAS, queda en manos del organismo de supervisión determinar los detalles relativos a la forma de realizar la evaluación de la conformidad, así como respecto del informe que deberá emitir el organismo de evaluación de la conformidad.

En el caso del supervisor español, esta determinación se ha realizado mediante la publicación, en la sede electrónica correspondiente, de una *Guía de notificación de servicios de confianza cualificados*[1125], en la que se incluyen los detalles del informe en cuestión. Para resultar admisible para el organismo de supervisión, el informe "ha de contener expresamente la confirmación de que tanto el prestador cualificado de servicios de confianza como los servicios de confianza cualificados que presta cumplen los requisitos establecidos en el Reglamento eIDAS" y "ser suficientemente detallado como para permitir concluir fehacientemente al organismo de supervisión si, tanto el prestador cualificado de servicios de confianza como los servicios de confianza cualificados que presta, cumplen o no los requisitos establecidos en el Reglamento eIDAS".

Asimismo, el informe debe ajustarse a la estructura y contenidos previstos en el Anexo I de la citada Guía, que como se puede ver de la lectura del mismo es realmente detallado, y además se entiende sin perjuicio de la posibilidad del organismo supervisor de requerir información adicional, de considerarlo oportuno para la realización de sus funciones.

Finalmente, cabe preguntarse acerca de la posibilidad de realizar una evaluación de la conformidad en relación con un servicio no cualificado, cuestión que debe ser respondida en sentido afirmativo. Dicho enfoque será interesante tanto desde la perspectiva de la supervisión *ex post* por parte del órgano de supervisión, cuanto como herramienta de márquetin.

Obtenido, pues, el preceptivo informe de evaluación de la conformidad por el prestador, es siguiente paso será iniciar el procedimiento para la obtención de la cualificación, de lo que nos ocuparemos en el siguiente epígrafe.

7.1.2 El procedimiento de concesión de la cualificación

El artículo 17.3.a) se refiere, entre las funciones del organismo de supervisión, a la de "supervisar a los prestadores cualificados de servicios de confianza establecidos en el territorio del Estado miembro que lo designa a fin de garantizar, mediante actividades de supervisión previas y posteriores, que dichos prestadores cualificados de servicios de confianza, y los servicios de confianza cualificados prestados por ellos, cumplen los requisitos establecidos en el presente Reglamento", de donde deriva el procedimiento de notificación previa de servicios de confianza cualificados, que culmina en la cualificación[1126].

[1125] Disponible en http://www.mincotur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/Notificacion.aspx.

[1126] Dado que la notificación es sólo, técnicamente hablando, un trámite del procedimiento, nos parece más exacto referirnos al procedimiento de cualificación.

Este procedimiento de cualificación se encuentra previsto en el artículo 21 del Reglamento eIDAS y, como se ha avanzado, se configura como una verdadera autorización, pues en efecto, el epígrafe 1 del artículo 21 indica que "[c]uando los prestadores de servicios de confianza, sin cualificación, tengan intención de iniciar la prestación de servicios de confianza cualificados, presentarán al organismo de supervisión una notificación de su intención junto con un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad" –informe al que ya hemos tenido ocasión de referirnos anteriormente–, a partir de la cual se tramitará el correspondiente expediente administrativo[1127], que finalizará mediante resolución concediendo o denegando la cualificación, procedimiento que, como es lógico, se tramitará conforme a lo establecido en la LPAC, así como conforme a los detalles de la Guía de notificación de servicios a la que antes nos hemos referido.

7.1.2.1 Solicitud de inicio del procedimiento

Respecto a la naturaleza jurídica de esta actuación del prestador correspondiente en notificar al organismo de supervisión su intención de prestar un servicio de confianza cualificado, nos encontramos ante lo que materialmente se trata de una verdadera solicitud de inicio de procedimiento administrativo de autorización a instancia del interesado, y no de una declaración responsable ni de una comunicación previa.

En efecto, conforme a lo establecido en el artículo 69.3 de la LPAC, estas dos posibilidades "permitirán, el reconocimiento o ejercicio de un derecho o bien el inicio de una actividad, desde el día de su presentación, sin perjuicio de las facultades de comprobación, control e inspección que tengan atribuidas las Administraciones Públicas", algo que entraría en contradicción con el artículo 21.3 del Reglamento eIDAS, en cuya virtud "[l]os prestadores cualificados de servicios de confianza podrán comenzar a prestar el servicio de confianza cualificado una vez que la cualificación haya sido indicada en las listas de confianza a que se refiere el artículo 22, apartado 1".

La solicitud de concesión de la cualificación deberá cumplir los requisitos generales de toda solicitud administrativa, incluida su firma[1128] (en su caso, electrónica) y ser presentada en el oportuno registro administrativo, conforme a las reglas generales[1129].

En este sentido, dado que normalmente el prestador de servicios de confianza será una persona jurídica, nos encontraremos ante un procedimiento de tramitación íntegramente y exclusivamente electrónica, en aplicación de lo dispuesto en el artículo 14.2) de la LPAC, aunque no será así cuando el prestador del servicio sea una persona física, dado que el epígrafe 1 del artículo 14 de la LPAC prevé el derecho de las personas físicas a elegir si se relacionan con las Administraciones Públicas empleando medios electrónicos o no.

[1127] El procedimiento se denomina de "recepción de notificaciones del artículo 21 del Reglamento (UE) Nº 910/ 2014 relativo a la identificación electrónica y los servicios de confianza y comunicaciones del artículo 30.2 de la ley 59/2003 de firma electrónica", con código SIA 990982.

[1128] Cfr. el artículo 11.2) de la LPAC, en relación con el artículo 66.1.e) de la propia LPAC.

[1129] Ello implica la utilización del registro electrónico creado y regulado conforme a los artículos 24 y siguientes de la LAE, o al registro tradicional regulado en el artículo 38 de la LRJPAC, y a partir del 2 de octubre de 2018, el uso del registro electrónico general que se cree al amparo del artículo 16 y concordantes de la LPAC.

Y en relación con este punto en concreto, llama la atención el hecho de que en la Guía de notificación de servicios de confianza cualificados se imponga el procedimiento electrónico a todos los prestadores, incluidos aquellos que son personas físicas. Ciertamente, el epígrafe 3 del artículo 14 de la LPAC permite imponer, en determinadas circunstancias[1130], la tramitación exclusivamente electrónica a las personas físicas, pero para ello se requiere de una disposición reglamentaria, que en este caso no se ha dictado[1131] –desde luego, esta *Guía de notificación de servicios de confianza cualificados* no tiene carácter normativo ninguno–, lo que implica la manifiesta ilicitud de esta imposición a las personas físicas por parte del organismo de supervisión.

En la misma línea, la *Guía de notificación de servicios de confianza cualificados* impone el uso exclusivo de un formulario electrónico, que necesariamente deberá obligatoriamente ser remitido a través de la sede electrónica del organismo de supervisión, con exclusión de todo otro registro.

Por lo que respecta a la imposición de la presentación exclusivamente en el registro electrónico del organismo de supervisión, la misma entra en colisión con la previsión contenida en el artículo 38.4 de la LRJPAC, que debe entenderse[1132] –aunque sólo para las personas físicas prestadoras de servicios de confianza, como ya hemos indicado– hasta el 2 de octubre de 2018, pero también con la regulación del artículo 16.4 de la LPAC, limitando el derecho al uso de la denominada vía indirecta de presentación contempladas en dichas normas.

En el caso de la imposición del registro electrónico a las personas físicas sin norma reglamentaria, ya hemos indicado que se trata de una actuación administrativa que se debe reputar ilegal; mientras que en el caso del artículo 16.4 de la LPAC el problema se planteará de mantenerse esta limitación desde el 2 de octubre de 2018, cuando el mismo entre en vigor.

La cuestión es que el artículo 16.4 de la LPAC permite la presentación electrónica de los escritos no sólo en el registro electrónico del órgano al que se dirijan, sino también "en los restantes registros electrónicos de cualquiera de los sujetos a los que se refiere el artículo 2.1" –esto es, las Administraciones territoriales y el sector público institucional– posibilidad que no existía en la LAE. Por tanto, desde que este artículo entre en vigor se deberá permitir la presentación de este formulario también por vía indirecta, sin perjuicio de que se pueda limitar esta posibilidad de elección mediante una norma que pueda desplazar la aplicación de la LAE, dado que no resultará aceptable proceder a dicha

---

[1130] Sobre esta posibilidad, cfr. (Cotino Hueso, 2017, págs. 497-516); del mismo autor, en relación con la LAE, (Cotino Hueso, 2010, pág. 220 y ss.). Antes de la aprobación de la LPAC, esta posibilidad se contenía en el artículo 27.6 de la LAE.

[1131] El registro electrónico del organismo de supervisión fue creado por Orden IET/1902/2012, de 6 de septiembre, por la que se crea y regula el Registro Electrónico del Ministerio de Industria, Energía y Turismo. Su artículo 5 prevé que se podrá "establecer mediante orden ministerial la obligatoriedad de comunicarse por medios electrónicos con el mismo en determinados procedimientos. La relación de procedimientos de tramitación electrónica obligatoria se mantendrá actualizada en la sede electrónica del Ministerio de Industria, Energía y Turismo"; orden que no se ha dictado nunca. El artículo 12 de la citada Orden IET/1902/2012 sólo impone la obligación de emplear el registro electrónico a las personas jurídicas.

[1132] Puede verse una crítica a la defectuosa técnica legislativa relativa a esta cuestión en (Martínez Gutiérrez, 2016a, págs. 55-60) y (Rego Blanco, 2017, págs. 1000-1001), entre otros.

limitación mediante cualquier norma reglamentaria[1133], y claramente no se puede realizar mediante una simple Guía como la publicada por el organismo de supervisión actualmente.

Además, dado que la prestación de servicios de confianza es una actividad económica evidente, resultará aplicable también la vía de presentación indirecta de la ventanilla única prevista en el artículo 18 de la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio[1134], en referencia al portal http://www.eugo.es[1135]. Sin embargo, y a pesar de tratarse de una actividad sujeta a autorización para el prestador extranjero que se quiera establecer en España, actualmente en la ventanilla única no se contempla la misma.

En relación con la imposición de un formulario normalizado, parece que ha de generar una menor problemática[1136], dado que el artículo 66.6) de la LPAC, que se encuentra vigente, establece que "[c]uando la Administración en un procedimiento concreto establezca expresamente modelos específicos de presentación de solicitudes, éstos serán de uso obligatorio por los interesados", pero en realidad la obligación de empleo de un modelo específico tiene el efecto potencial de limitar la vía de presentación electrónica indirecta, en función del modelo de implementación técnica que se adopte.

En concreto, si el modelo de uso obligatorio es un formulario que se encuentra implementado técnicamente en la aplicación informática del órgano destinatario del mismo, en lugar de ser un documento que se pueda descargar y cumplimentar de forma

---

[1133] Cfr. (Rego Blanco, 2017, págs. 1018-1021), que se refiere a los ejemplos de la normativa de contratación pública y de facturación electrónica dirigidas a las entidades del sector público, así como a la normativa tributaria. En este último caso, aunque ciertamente la Ley 58/2003, de 17 de diciembre, General Tributaria es, en este punto, esencialmente equivalente a la LRJPAC (cfr. el artículo 98), siendo el artículo 117.2 del Real Decreto 1065/2007 , de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, el que parece prever la posibilidad de aprobar modelos obligatorios, si bien realizando sólo una interpretación *a sensu contrario*. Sin embargo, los artículos 96.5, 98.6, y otros, de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio, parecen sustentar con mayor claridad esta tesis.

[1134] Así lo recuerda (Rego Blanco, 2017, pág. 1029).

[1135] Portal que parece configurarse como un punto de acceso que conduce al interesado hasta el registro electrónico correspondiente, pero que puede proceder al registro para otra Administración si la misma, por ejemplo, no dispone de registro electrónico, empleando en este caso el de la Administración General del Estado, en los términos recogidos en la Orden HAP/566/2013.

[1136] Nos referimos a que la ley permite con claridad imponer esta obligación, sin perjuicio de los graves problemas que puede plantear un uso deficiente, incorrecto o hasta abusivo de los formularios, como ha denunciado (Rego Blanco, 2014, págs. 605-614), en su completo análisis relativo a las maneras en que, en palabras de la autora, "las solicitudes generadas electrónicamente requieren una mayor inversión de tiempo de cumplimentación y originan un incremento de la carga administrativa teóricamente reducida con su implantación", incluyendo la inclusión de «campos llave»; la normalización de los datos que el usuario debe aportar en los campos obligatorios, sin ofrecer un elenco tasado de opciones de respuestas; la introducción de campos obligatorios que no se corresponden con ninguno de los requisitos sustantivos de la solicitud, de acuerdo con su regulación; rotular con ambigüedad los campos de la solicitud; impedir dar por terminada la solicitud y presentarla si no se cumplimentan los campos marcados como obligatorios en el formulario o no se hace convenientemente; y la verificación automatizada de datos por relación a otros campos que implique nuevas exigencias no previstas por la norma reguladora.

autónoma, sólo resultará materialmente posible rellenarlo y presentarlo precisamente en dicho registro electrónico, y no en los restantes.

Este régimen se puede considerar apropiado a lo establecido en el LAE, conforme al cual los registros electrónicos sólo pueden emplearse para relacionarse con la Administración que los creó[1137], motivo por el que la LAE impuso la obligación a todas las Administraciones Públicas de crear un registro electrónico, y sin perjuicio de la posibilidad de que las Administraciones colaboren de forma voluntaria para habilitar sus registros electrónicos propios para la recepción de las solicitudes, escritos y comunicaciones de la competencia de otra Administración que se determinen en el correspondiente convenio; pero no resulta conforme con la LPAC, que según hemos indicado generaliza la vía electrónica de presentación indirecta.

Es cierto que *prima facie* resulta difícil de entender que el legislador haya realizado esta extensión del derecho del interesado a la presentación electrónica en registro electrónico diferente al del órgano al que se dirige el escrito, porque el esfuerzo y coste de acceder electrónicamente a un registro u otro es esencialmente el mismo, pero como ha puesto de manifiesto la doctrina, existen razones que lo justifican[1138], si bien existe una serie de presupuestos necesarios para que su funcionamiento correcto resulte posible – entre los que se encuentra la existencia de puntos de acceso general y de registros electrónicos comunes en las diferentes Administraciones[1139], propuesta doctrinal que la LPAC recoge.

La aprobación de un formulario obligatorio debería realizarse, por tanto, de forma que no se limite esta garantía legal de presentación electrónica por vía indirecta, debiéndose apostar por formularios descargables en lugar de por aplicaciones integradas en la sede electrónica, algo que no parece tener visos de ocurrir en la mayoría de casos. No es, de momento, el caso del formulario de solicitud de concesión de la cualificación; aunque el mismo se puede descargar y cumplimentar en el equipo del prestador de servicios de confianza, no incorpora los campos para la firma, y como hemos visto, se exige su presentación exclusivamente en el registro del organismo de supervisión.

Respecto al contenido de la solicitud, resulta ciertamente prolijo en los detalles exigidos. El formulario contiene una primera sección dedicada a la identificación de solicitante, que sólo puede ser una persona física, que deberá identificarse mediante su NIF o NIE y apellidos y nombre, campos que resultan de cumplimentación obligatoria. Este enfoque resulta llamativo, dada la posibilidad prevista en la LPAC de autorizar la actuación directa del prestador persona jurídica, mediante su sello electrónico, como se deduce de los artículos 11.2 y 10.2 de la citada LPAC, como analizaremos con mayor detalle *infra*[1140],

---

[1137] Cfr. (Valero Torrijos, 2007, págs. 115-119).

[1138] Para (Valero Torrijos, 2007, pág. 116), "en los casos de presentación a través de Internet, la localización física del registro –circunstancia que en definitiva explica las diversas alternativas de presentación indirecta para facilitar la tarea al ciudadano– pierde gran parte de su significado en la medida que la actuación puede realizarse cómodamente sentad@ en el domicilio o puesto de trabajo con sólo hacer un *click* de ratón. Así pues, parece razonable que la presentación deba llevarse a cabo necesariamente a través del registro electrónico de la Administración titular; salvo que se trate de actuaciones que preceptivamente tengan que realizarse por medios telemáticos, en cuyo caso convendría articular una vía de presentación alternativa cuando aquél no funcionara correctamente o existieran problemas técnicos al efectuar la conexión".

[1139] Cfr. (Valero Torrijos, 2007, pág. 118).

[1140] Cfr. la sección 5.2.2.4 de este trabajo.

de la que no se hace uso en absoluto.

Opcionalmente, en esta primera sección se puede indicar el "CSV indicado en la copia de la escritura notarial de apoderamiento incluida en el Registro Electrónico de Apoderamientos, según el Convenio de colaboración entre la Administración General del Estado y el Consejo General del Notariado", debiéndose, en caso de no disponer del mismo, aportar el poder de representación.

Nos encontramos ante un caso de sustitución de la aportación del poder de representación, –documento público en soporte papel– por la trasmisión electrónica del mismo, posibilidad que, sin duda, hay que valorar positivamente, y que se incardina en el Registro Electrónico de Apoderamientos creado por el artículo 15 del RDLAE[1141], y desarrollado por Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos[1142].

En efecto, y como se indica en el Convenio de colaboración entre la Administración General del Estado (Ministerio de Hacienda y Administraciones Públicas) y el Consejo General del Notariado para la remisión telemática de documentos públicos notariales de apoderamiento y sus revocaciones al Registro Electrónico de Apoderamientos, de 23 de mayo de 2014, "siendo una de las funciones esenciales de los notarios proporcionar seguridad jurídica al tráfico jurídico civil, mercantil y administrativo, y siendo una de sus competencias la de autorización de las escrituras públicas de apoderamiento, en los términos previstos en los artículos 1280 del Código Civil y concordantes de la normativa administrativa especial, este convenio tiene por objeto establecer los mecanismos técnicos, informáticos y de seguridad jurídica para que por medios telemáticos el notario a través de su organización corporativa remita en formato telemático copia de los apoderamientos autorizados para que un apoderado pueda actuar temáticamente ante la Administración Pública en nombre de otra persona física o jurídica. Asimismo, se pretende que dicha remisión de tal documento se acompañe de una ficha o formato expresivo del índice único informatizado para que, a través de la oportuna concreción del sistema telemático correspondiente, pueda ser objeto de incorporación automatizada al Registro Electrónico de Apoderamientos"; convenio que fue modificado por Adenda de 13 de noviembre de 2014 para posibilitar la adhesión de cualquier Administración a este sistema, pero siempre que la citada Administración se haya adherido al Registro Electrónico de Apoderamientos del Estado.

En virtud del convenio, el Consejo General del Notariado –a través de su compañía tecnológica ANCERT– se obliga a la remisión de la copia electrónica de la escritura de apoderamiento o de constitución de la sociedad, al amparo de la previsión contenida en el artículo 17 bis de la Ley de 28 de mayo de 1862, del Notariado[1143], y los artículos 221

[1141] Inicialmente el Registro Electrónico de Apoderamientos se crea para uso exclusivo en las relaciones con la Administración General del Estado y sus organismos públicos vinculados o dependientes, limitación de que elimina mediante reforma del epígrafe 1 del artículo 15 por Real Decreto 668/2015, de 17 de julio.

[1142] Se trata de un régimen que se encuentra transitoriamente vigente hasta el 2 de octubre de 2018, en que entrará en aplicación el nuevo régimen de Registro Electrónico de Apoderamientos previsto en el artículo 6 de la LPAC, aunque cabe prever que el tratamiento será el mismo, aunque ya con efectos a todas las Administraciones Públicas.

[1143] Este artículo fue incorporado por el artículo 115.1 de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, y su epígrafe 3 establece que "[l]as copias autorizadas de las matrices podrán expedirse y remitirse electrónicamente, con firma electrónica avanzada, por el notario

y siguiente del Decreto de 2 de junio de 1944, por el que se aprueba con carácter definitivo el Reglamento de la organización y régimen del Notariado[1144], así como a disponer de un sistema de consulta de subsistencia de poder de representación, de forma que se pueda conocer, en cualquier momento, el estado de vigencia del mismo. De este modo, la persona física (actuando en nombre propio o en representación de tercero) comparece ante Notario y otorga el poder, cuya copia impresa incluirá el correspondiente CSV, que podrá declararse en lugar de aportar el soporte impreso en cuestión, para su solicitud y remisión íntegramente electrónicas[1145].

En una segunda sección, la solicitud exige la identificación del prestador de servicios de confianza que realiza la notificación, de nuevo ignorando la existencia –como ya hemos visto prevista en el Reglamento eIDAS– de personas físicas prestadoras de servicios de confianza.

De los datos que se exigen en esta sección, resulta llamativo el correo electrónico, obligatorio, previsión razonable dada la actividad profesional tecnificada que realizan estos prestadores, pero sin que el formulario ni la guía contengan indicación alguna en relación con la finalidad para la que se solicita este dato. Cabe imaginar que dicha finalidad será la de realizar comunicaciones electrónicas, así como, en su caso, notificaciones administrativas electrónicas, en relación con el procedimiento en cuestión, pero resulta criticable que no se informe de la misma, dada la previsión contenida en el artículo 66.1.b), en cuya virtud la solicitud deberá contener la "[i]dentificación del medio electrónico, o en su defecto, lugar físico en que desea que se practique la notificación. Adicionalmente, los interesados podrán aportar su dirección de correo electrónico y/o dispositivo electrónico con el fin de que las Administraciones Públicas les avisen del envío o puesta a disposición de la notificación".

A continuación, el formulario prevé la posibilidad de que el solicitante se niegue a que la Administración recabe la información electrónicamente mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, en cuyo caso se le informa de la necesidad de aportar la documentación por cualquier de los medios válidos en Derecho.

---

autorizante de la matriz o por quien le sustituya legalmente. Dichas copias sólo podrán expedirse para su remisión a otro notario o a un registrador o a cualquier órgano de las Administraciones públicas o jurisdiccional, siempre en el ámbito de su respectiva competencia y por razón de su oficio. Las copias simples electrónicas podrán remitirse a cualquier interesado cuando su identidad e interés legítimo le consten fehacientemente al notario".

[1144] En redacción dada por Real Decreto 45/2007, de 19 de enero, que, por cierto, sufrió un importante recorte derivado de la anulación de una cantidad significativa de artículos por diversas Sentencias del Tribunal Supremo, entre las cuales la de 20 de mayo, que elimina el plazo máximo de 60 días de validez de las copias autorizadas electrónicas.

[1145] Hay que hacer notar que la copia electrónica será autorizada mediante la firma electrónica cualificada del Notario autorizante, conforme establece el epígrafe 1 del propio artículo 17 bis, cuando indica que "[l]os instrumentos públicos a que se refiere el artículo 17 de esta Ley, no perderán dicho carácter por el sólo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquél de conformidad con la Ley reguladora del uso de firma electrónica por parte de notarios y demás normas complementarias", normas que se contienen en el artículo 109 de la Ley 24/2001, en redacción dada por Ley 24/2005, de 18 de noviembre, de reformas para el impulso a la productividad, y que la misma se deberá conservar electrónicamente en el correspondiente expediente electrónico del órgano titular del Registro Electrónico de Apoderamientos.

Se trata de la aplicación del derecho reconocido, en este sentido, en el artículo 53.1.d) de la LPAC, y concretado en el artículo 28 de la misma LPAC, pero su aplicación genera bastantes dudas.

En primer lugar, el artículo 28.1 prevé que "[l]os interesados deberán aportar al procedimiento administrativo los datos y documentos exigidos por las Administraciones Públicas de acuerdo con lo dispuesto en la normativa aplicable", mientras que, conforme al epígrafe 3 del mismo artículo 28, "las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable".

Desde este punto de vista, en la sección IV se contiene un listado bastante completo de datos y documentos que obligatoriamente deben ser aportados por el interesado. Entre ellos encontramos documentos que se citan en el Reglamento eIDAS, como el informe de evaluación de la conformidad, los modelos de contratos, el plan de cese, el seguro de responsabilidad civil o la certificación del dispositivo cualificado, por lo que no habría dudas acerca de la previsión normativa que sustenta su exigencia; pero también encontramos documentos que no se mencionan en la citada normativa, por lo que resulta más dudoso que se pueda exigir su aportación: así sucede en el caso de la Declaración de prácticas de certificación o documento análogo[1146], en las políticas de los diferentes servicios, o en los diferentes elementos técnicos de prueba.

Así, cuando por ejemplo se exige la aportación de una política de entrega electrónica, o de una política de conservación, nos encontramos ante documentos no previstos en normativa alguna, por lo que ciertamente el formulario conculca el derecho previsto en el artículo 53.1.d), así como en los epígrafes 1 y 3 del artículo 28 de la LPAC.

En algunos casos, nos encontramos, además, ante el problema de que se imponen documentos a aportar que afectan a la neutralidad tecnológica del propio Reglamento, como por ejemplo cuando se exige, en relación con el servicio de conservación, un certificado de resellado[1147]. Esta exigencia tan concreta, tan específica de una implementación tecnológica, puede resultar discriminatoria frente a los prestadores que decidan emplear otras tecnologías[1148], por lo que es criticable.

Sin embargo, hay que tener en cuenta que, como se expuso anteriormente[1149], un prestador de servicios de confianza puede adherirse voluntariamente a normas técnicas de servicios

---

[1146] La Declaración de prácticas de certificación es obligatoria, conforme al artículo 19 de la LFE, para los prestadores de servicios de confianza que expiden certificados, pero no se puede predicar lo mismo del documento análogo al que se refiere el formulario, por ejemplo, con respecto al servicio de validación de firma electrónica.

[1147] El resellado es una técnica de extensión de valor probatorio de informaciones protegidas por la aplicación de algoritmos criptográficos, que consiste en aplicar un (nuevo) sello de tiempo a dichas informaciones, empleando un algoritmo más robusto, a los efectos de poder demostrar que dichas informaciones existían en el pasado, y que se habían protegido con el algoritmo ahora poco seguro. En esta técnica, que se ha normalizado en las normas técnicas europeas de formatos de firma (CAdES, PAdES y XAdES), se puede basar un servicio de conservación, como veremos, pero también es posible que se base en otras técnicas diferentes. Sin embargo, en estas técnicas no se habla nunca de un "certificado de resellado", por lo que quizá incluso nos encontramos ante una referencia errónea.

[1148] Como, por ejemplo, sucedería en el caso de emplear *blockchain* para sustentar la prueba de existencia de las informaciones con valor probatorio, algo que podría ser más conveniente que las cadenas infinitas de sellos de tiempo.

[1149] Cfr. la sección 1.4.2 de este trabajo.

de confianza. Y podría bien suceder –y, de hecho, sucede– que dichas normas técnicas impongan de forma obligatoria el disponer de determinados documentos (como una política del servicio, o una declaración de prácticas, etc.), lo cual será objeto de la correspondiente evaluación de la conformidad. Aunque las normas técnicas, por ser voluntarias, no se puedan considerar como "normativa" a los efectos de los artículos 53.1.d) y 28, epígrafes 1 y 3, de la LPAC, en estos casos es evidente que el organismo de supervisión puede exigir su aportación.

En otro orden de cosas, el organismo de supervisión ha de poder tener acceso a la información suficiente para poder realizar sus funciones, empezando por la concesión de la cualificación, por lo que resulta evidente que, aunque inicialmente sólo solicite unos documentos concretos, deberá poder solicitar informaciones complementarias, con la debida motivación en caso de acceso a información de alta sensibilidad. Por ello, lo criticable es imponer documentos que puedan implicar un modelo tecnológico concreto a adoptar por parte del prestador, puesto que afecta negativamente a la neutralidad tecnológica que informa al Reglamento eIDAS.

En segundo lugar, el artículo 28.2 de la LPAC prevé que "[l]os interesados no estarán obligados a aportar documentos que hayan sido elaborados por cualquier Administración, con independencia de que la presentación de los citados documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate, siempre que el interesado haya expresado su consentimiento a que sean consultados o recabados dichos documentos", previsión que en este caso será aplicable con carácter bastante limitado, dado que, con carácter general, las documentos que exige este procedimiento no son elaborados por las Administraciones Públicas. Por ejemplo, la documentación relativa a la persona física se encontrará en el Registro Civil, fuera por lo tanto del alcance de la LPAC; mientras que la documentación del prestador con forma societaria privada se encontrará en el Registro Mercantil, de nuevo fuera del alcance de la LPAC.

Se podría, sin embargo, aplicar la previsión del artículo 28.2 de la LPAC a algunos casos concretos, como por ejemplo la no aportación del número de identificación fiscal (a partir del censo correspondiente de la Agencia Estatal de Administración Tributaria), o de la certificación del dispositivo cualificado de creación de firma o sello, aunque en este segundo caso sólo sería posible en caso de que el citado dispositivo haya sido certificado en España, dado que el organismo de certificación es una unidad de Centro Nacional de Inteligencia, y se trata de información pública. También se podría aplicar a la disposición de creación de una entidad pública que se constituya como prestador de servicios de confianza.

Finalmente, el artículo 28.3 de la LPAC también prevé que "las Administraciones Públicas no requerirán a los interesados datos o documentos […] que hayan sido aportados anteriormente por el interesado a cualquier Administración", en cuyo caso "el interesado deberá indicar en qué momento y ante que órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto".

En este caso –que tampoco parece vaya a resultar aplicable con carácter general, dado que los documentos que se exigen con la solicitud normalmente no habrán sido aportados a otras Administraciones Públicas, debido a su especificidad– llama la atención que el formulario de solicitud no contenga campo o casilla alguna para permitir el ejercicio del derecho en cuestión, lo que supone, como en el caso anterior, una infracción de la LPAC.

Quizá el único documento que se podría beneficiar de esta posibilidad es el seguro de responsabilidad civil, caso que por alguna razón haya sido aportado a otra Administración.

La tercera sección del formulario se dedica, propiamente, a la notificación del o los servicios de confianza para los que se solicita la cualificación. Para cada servicio a notificar, el formulario contiene, en primer lugar, el listado completo de los servicios de confianza que pueden ser objeto de cualificación, a los que nos hemos referido con anterioridad[1150], para su selección del tipo de servicio por parte del prestador[1151], con la particularidad de que se ofrece la posibilidad de indicar, en algunos servicios de confianza, si los mismo se prestan también conforme a lo establecido en la LRJSP.

Tal es el caso de la expedición de certificados cualificados de empleado público (que son una especialidad de los certificados cualificados de firma electrónica de persona física), de la expedición de certificados cualificados de sello (que son una especialidad de los certificados cualificados de sello electrónico de persona jurídica) y de la expedición de certificados cualificados de sede electrónica (que son una especialidad de los certificados cualificados de autenticación de sitio web).

Esta posibilidad resulta criticable, dado que implica someter al estricto procedimiento administrativo de cualificación a los elementos adicionales contenidos en dichos certificados –como los atributos adicionales que se añaden al nombre– y a determinados aspectos de gestión de los citados certificados; es decir, que se sujeta a autorización administrativa previa por parte del organismo de supervisión aspectos puramente voluntarios de los certificados, sin norma jurídica habilitante, situación que plantea diversos problemas jurídicos de calado a los que nos referiremos posteriormente, cuando analicemos el régimen jurídico de estos certificados.

Tras la indicación del tipo de servicio, se deben indicar la denominación exacta y la descripción del servicio, con una limitación de 1.000 caracteres y advertencia de que "cualquier incorrección técnica, formal o legal deberá ser objeto de rectificación", algo que resulta especialmente razonable para luchar contra algunas de las prácticas de creación de confusión que han adoptado algunos prestadores, que daban a entender que su servicio disponía de una validez o eficacia que en realidad no era tal.

Asimismo, se exige la inclusión de un OID para el servicio, OID que consiste en un identificador numérico que habitualmente se ha venido empleando para diferenciar entre diversos tipos de certificados, pero que no se emplea en otros servicios, como por ejemplo en la validación de firma o sello electrónico, ni en su conservación. Ciertamente, es posible asignar un OID a cualquier objeto, incluido un documento de política de servicio, pero sorprende que se solicite este contenido, al menos con carácter general, porque no se emplea de forma necesaria en la publicidad administrativa de los servicios, a la que posteriormente nos referiremos.

Finalmente, el formulario exige la inclusión del denominado identificador del servicio, especificando que se trata de un certificado en base64. Aunque ni el formulario ni la guía de notificación aclaran nada al respecto, dicho identificador debe identificar el servicio

[1150] Cfr. el epígrafe 1.3.1 de este trabajo.

[1151] La taxonomía de tipos de servicios cualificados de confianza se encuentra alineada con el acto de implementación que aprueba el formato de la Lista de confianza, a la que posteriormente nos referiremos.

de forma única y sin ambigüedad, y en caso de que el servicio se sustente en una infraestructura de clave pública, debe consistir en una clave pública asociada al servicio y que se emplee para verificar la autenticidad del servicio[1152]. Por ejemplo, puede tratarse de la clave pública para verificar la firma de los certificados de firma electrónica, sello electrónico y autenticación de sitio web emitidos por el prestador; o la clave pública para verificar la firma electrónica o el sello electrónico de los sellos de tiempo electrónico expedidos por el prestador.

Como se puede ver, de nuevo el formulario impone una visión restrictiva, al permitir únicamente la notificación de servicios de confianza que se basen en el empleo de claves criptográficas y, además, certificadas en el marco de una infraestructura de clave pública. Sin embargo, ello deriva directamente del enfoque global del sistema de Listas de confianza empleado para la publicidad administrativa de los servicios, a la que en breve nos referiremos, por lo que no se trata de una problemática que se pueda resolver exclusivamente en sede nacional.

Finalmente, el formulario de solicitud prevé la posibilidad de aportar documentación complementaria, en cumplimiento de lo establecido en el artículo 28.1 de la LPAC, así como de realizar las observaciones que se consideren oportunas.

A pesar de tratarse de un modelo bastante completo, su complejidad y, en especial, la casi totalidad falta de instrucciones detalladas respecto a algunos campos, puede implicar que el mismo se presente incompleto o que contenga errores, lo que motivará la correspondiente subsanación y mejora de la solicitud, conforme a las reglas comunes previstas en el artículo 68 de la LPAC. Lo mismo sucederá en caso de ausencia de alguno de los documentos exigidos con carácter obligatorio, sin que existan en estos dos casos especialidades dignas de comentario.

7.1.2.2 Instrucción, resolución y notificación del procedimiento

Presentada la solicitud, en los términos indicados anteriormente, el organismo de supervisión deberá proceder a la apertura del correspondiente expediente electrónico, en los términos del artículo 70 de la LPAC, procediendo a la instrucción del mismo, conforme a las normas comunes.

Esta fase se orienta a la comprobación de los hechos que justificarán, en su caso, la concesión de la cualificación; esto es, corresponde a las actividades de supervisión previa previstas en el artículo 17.3.a) del Reglamento eIDAS, "a fin de garantizar […] que dichos prestadores cualificados de servicios de confianza, y los servicios de confianza cualificados prestados por ellos, cumplen los requisitos establecidos en el presente Reglamento". Por este motivo, el artículo 21.2 del Reglamento eIDAS concreta que "[e]l organismo de supervisión verificará si el prestador de servicios de confianza y los servicios de confianza que presta cumplen los requisitos establecidos en el presente Reglamento, y en particular, los requisitos establecidos para los prestadores cualificados

[1152] Cfr. la sección 5.5.3 de la especificación ETSI TS 119 612 v2.1.1, referenciada por Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

de servicios de confianza y para los servicios de confianza cualificados que estos prestan", verificación que se produce en los términos establecidos por la legislación nacional de procedimiento administrativo, y con aplicación plena de las correspondientes garantías que el mismo supone.

El organismo de supervisión recibe toda la documentación, de la cual tiene especial relevancia el informe de evaluación de la conformidad producido por el organismo de evaluación de la conformidad al que hemos tenido oportunidad de referirnos con anterioridad[1153], materiales que le sirven como apoyo para sus tareas de comprobación, en relación con las cuales resultarán aplicables las reglas de valoración de la prueba contenidas en el artículo 77.1 de la LPAC, que remite a las reglas generales contenidas en la Ley de Enjuiciamiento Civil, así como las reglas especiales contenidas en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza[1154].

Este punto es interesante porque implica que, salvo imposición legal expresa –como en el caso de la certificación del dispositivo cualificado de creación de firma electrónica o de sello electrónico– en principio el prestador puede acudir a cualquier medio de prueba admisible en Derecho para demostrar que cumple con los requisitos que le afectan como prestador, o que afectan al o los servicios cualificados que pretende prestar. Así, por ejemplo, sucedería en relación con la demostración de que un sistema empleado por el prestador es fiable, obligación prevista en el artículo 24.2 del Reglamento eIDAS.

Cosa diferente es que, como hemos avanzado anteriormente[1155], la adhesión del prestador a normas técnicas, y la correspondiente acreditación de su cumplimiento, facilite en gran medida esta demostración, en especial si las citadas normas han sido establecidas por la Comisión Europea, dado que en ese caso implicarán una presunción de cumplimiento de los requisitos del Reglamento eIDAS que vinculará al organismo de supervisión.

En cualquier caso, hay que recordar en este momento que el prestador solicitante ha aportado el preceptivo informe de evaluación de la conformidad, que en principio acredita el cumplimiento de los requisitos legales, pero en caso de duda por el organismo de supervisión, que en absoluto está legalmente vinculado por dicho informe, podrá acudir a estos mecanismos.

Respecto al plazo del procedimiento, el tercer párrafo del artículo 21.2 del Reglamento eIDAS prevé que "si la verificación no ha concluido en el plazo de tres meses, el organismo de supervisión informará al prestador de servicios de confianza especificando los motivos de la demora y el plazo previsto para concluir la verificación", lo que se deberá hacer conforme a la legislación nacional aplicable al procedimiento. Nótese que este plazo de tres meses se computa hasta la publicidad del servicio en la lista de confianza, y no únicamente hasta que se haya dictado y notificado la correspondiente resolución, a tenor de lo establecido en el artículo 22.3, párrafo tercero, del Reglamento eIDAS[1156].

[1153] Cfr. el epígrafe 7.1.1 de este trabajo.

[1154] Estas reglas se refieren, en especial, al uso de laboratorios especializados. Cfr. el epígrafe 7.2.1 de este trabajo.

[1155] Cfr. el epígrafe 1.4.2 de este trabajo.

[1156] En efecto, dicho texto indica que "[s]i el organismo de supervisión concluye que el prestador de

En este sentido, el artículo 21.2 de la LPAC indica que "el plazo máximo en el que debe notificarse la resolución expresa será el fijado por la norma reguladora del correspondiente procedimiento", plazo que "no podrá exceder de seis meses salvo que una norma con rango de Ley establezca uno mayor o así venga previsto en el Derecho de la Unión Europea". Como ya hemos avanzado, el artículo 21.2 del Reglamento eIDAS prevé un plazo inicial de tres meses, que podrá ser objeto de ampliación, pero sin establecer la duración de dicha ampliación, ni fijar un plazo máximo, por lo que la más elemental seguridad jurídica exige aplicar el límite de seis meses previsto en la legislación nacional, a contar aplicando las reglas generales[1157]. Y sin que nada impida la tramitación de urgencia de este procedimiento, en los términos establecidos en el artículo 33 de la LPAC, cuando razones de interés público lo aconseje, posibilidad que exige la correspondiente motivación[1158].

Resultan aplicables al cómputo del plazo, como no puede ser de otra forma, las previsiones legales relativas a la suspensión del plazo máximo para resolver, en los términos previstos en el artículo 22 de la LPAC, y a la ampliación del plazo máximo para resolver y notificar, en los términos previstos en el artículo 23 de la LPAC.

La principal causa para la suspensión del plazo máximo de resolución es la prevista en el artículo 22.1.a) de la LPAC; esto es, "cuando deba requerirse a cualquier interesado para la subsanación de deficiencias o la aportación de documentos y otros elementos de juicio necesarios, por el tiempo que medie entre la notificación del requerimiento y su efectivo cumplimiento por el destinatario, o, en su defecto, por el del plazo concedido, todo ello sin perjuicio de lo previsto en el artículo 68 de la presente Ley". En efecto, el organismo de supervisión puede requerir, durante la verificación, informaciones adicionales al prestador en orden a la plena acreditación del cumplimiento de los requisitos, especialmente en relación con aspectos que no hayan sido objeto del informe de evaluación de la conformidad, o que lo hayan sido de forma insuficiente.

Otra posibilidad en orden a la suspensión del plazo máximo para resolver se encuentra en el numeral e) del artículo 22.1 de la LPAC; esto es, "[c]uando deban realizarse pruebas técnicas o análisis contradictorios o dirimentes propuestos por los interesados, durante el tiempo necesario para la incorporación de los resultados al expediente", aunque esta causa seguramente se dará sólo cuando el organismo de supervisión cuestione la idoneidad de

---

servicios de confianza y los servicios de confianza que este presta cumplen los requisitos a que se refiere el párrafo primero, el organismo de supervisión concederá la cualificación al prestador de servicios de confianza y a los servicios de confianza que este presta y lo comunicará al organismo a que se refiere el artículo 22, apartado 3, a efectos de actualizar las listas de confianza a que se refiere el artículo 22, apartado 1, a más tardar tres meses después de la notificación de conformidad con el apartado 1 del presente artículo".

[1157] Conforme a lo establecido en el artículo 31.2.c) de la LPAC, "[e]l inicio del cómputo de los plazos que hayan de cumplir las Administraciones Públicas vendrá determinado por la fecha y hora de presentación en el registro electrónico de cada Administración u Organismo. En todo caso, la fecha y hora efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el documento"; de forma análogo, el artículo 21.3 de la LPAC ordena que "[e]ste plazo y los previstos en el apartado anterior se contarán: […] b) En los iniciados a solicitud del interesado, desde la fecha en que la solicitud haya tenido entrada en el registro electrónico de la Administración u Organismo competente para su tramitación"; mientras que, conforme a lo establecido en el artículo 30.4 de la propia LPAC, "[s]i el plazo se fija en meses o años, éstos se computarán a partir del día siguiente a aquel en que tenga lugar la notificación o publicación del acto de que se trate, o desde el siguiente a aquel en que se produzca la estimación o desestimación por silencio administrativo".

[1158] Cfr. el artículo 35.1.e) de la LPAC.

alguno de los medios técnicos empleados por el prestador, como por ejemplo, si un determinado producto empleado por el prestador, que no se encuentre certificado contra una norma técnica reconocida por el organismo de supervisión, es un sistema fiable conforme al artículo 24.2 del Reglamento eIDAS.

Más difícil de imaginar, al menos en términos prácticos, es la aplicación de la causa de suspensión del plazo máximo para resolver contenida en el numeral g) de artículo 22.1 de la LPAC ("[c]uando para la resolución del procedimiento sea indispensable la obtención de un previo pronunciamiento por parte de un órgano jurisdiccional, desde el momento en que se solicita, lo que habrá de comunicarse a los interesados, hasta que la Administración tenga constancia del mismo, lo que también deberá serles comunicado"), pero dicha circunstancia se podría producir, por ejemplo, en caso de impugnación judicial de la certificación de un dispositivo cualificado de creación de firma electrónica o de sello electrónico empleado por el prestador que realiza la notificación, dado que en dicho caso el organismo de supervisión podría no admitir dicha certificación hasta la resolución del procedimiento judicial.

Finalmente, hay que considerar también las tres causas de suspensión del plazo máximo para resolver –en este caso, de aplicación obligada– previstas en el artículo 22.2 de la LPAC. En este sentido, la causa prevista en el numeral a) del artículo 22.2; esto es, "[c]uando una Administración Pública requiera a otra para que anule o revise un acto que entienda que es ilegal y que constituya la base para el que la primera haya de dictar en el ámbito de sus competencias, en el supuesto al que se refiere el apartado 5 del artículo 39 de esta Ley, desde que se realiza el requerimiento hasta que se atienda o, en su caso, se resuelva el recurso interpuesto ante la jurisdicción contencioso administrativa", se puede plantear, por ejemplo, en caso de que el organismo de supervisión considere ilegal una certificación de dispositivo cualificado de creación de firma electrónica o de sello electrónico, así como otra certificación que declare la presunción de conformidad de un producto con el Reglamento eIDAS, al vincular al organismo de supervisión, en el sentido de que dicha certificación constituye base para el dictado del acto de cualificación.

En todos los casos del artículo 22 de la LPAC sucede que se suspende el cómputo del plazo de tres meses o, en su caso, de ampliación por otros tres meses, como máximo, de lo cual se deberá dar cuenta en la correspondiente resolución, que será notificada al interesado en los casos legalmente previstos.

Por lo que se refiere a la ampliación del plazo para resolver y notificar, el artículo 23 de la LPAC la prevé con carácter excepcional, "cuando se hayan agotado los medios personales y materiales disponibles a los que se refiere el apartado 5 del artículo 21", en cuyo caso "el órgano competente para resolver, a propuesta, en su caso, del órgano instructor o el superior jerárquico del órgano competente para resolver, podrá acordar de manera motivada la ampliación del plazo máximo de resolución y notificación, no pudiendo ser éste superior al establecido para la tramitación del procedimiento".

En una aplicación estricta de este precepto, sólo en caso de agotamiento de medios personales y materiales se podría proceder a la ampliación de plazo prevista en el artículo 21.2 del Reglamento eIDAS, y en todo caso, de nuevo dicha ampliación no podría superar el plazo máximo de seis meses establecido para el procedimiento de cualificación.

La ampliación de plazo deberá ser, en todo caso, objeto de la correspondiente resolución,

debidamente motivada[1159] y que deberá ser notificada al interesado conforme a las normas legales, tanto por mandato del artículo 23.2 de la LPAC, como del artículo 21.2 del Reglamento eIDAS[1160].

Nótese que la *Guía de notificación* nada dice acerca de estas posibilidades, limitándose a contener una referencia genérica al artículo 21 del Reglamento eIDAS, y sin siquiera mencionar la posibilidad de extensión del plazo de tres meses (por otros tres meses), algo que supone una infracción bastante evidente de lo establecido en el artículo 21.4 de la LPAC.

Finalizada la verificación por el organismo de supervisión; esto es, instruido el procedimiento, e inmediatamente antes de la redacción de la propuesta de resolución, se sustancia el trámite de audiencia previsto en el artículo 82 de la LPAC, mediante la puesta de manifiesto del expediente electrónico, a la que se aplicarán los límites previstos[1161] en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, para que, en el plazo de entre diez y quince días puedan alegar y presentar los documentos y justificaciones que estimen pertinentes. A pesar de que la dicción literal de la ley pudiera inducir a pensar lo contrario, en este trámite ya se da vista al interesado del borrador de resolución, para que conozca el sentido de la resolución propuesta y pueda alegar lo que mejor le convenga.

Respecto a los límites contenidos en la legislación de transparencia, hay que recordar que los mismos son de aplicación estricta, especialmente dado que nos encontramos ante el acceso del propio interesado a su expediente, derecho conferido por el artículo 53.1.a) de la LPAC, cuando indica que los interesados "tendrán derecho a acceder y a obtener copia de los documentos contenidos en los citados procedimientos".

Ciertamente, no puede ser de igual –mucho menos, de peor– condición el interesado que accede a un expediente abierto del que es parte, que cualquier otro ciudadano que solicita acceso, dado que nos encontramos ante una de las regulaciones especiales del derecho de acceso a información pública previstas en la disposición adicional primera de la Ley 19/2013, cuyo epígrafe 1 indica que "[l]a normativa reguladora del correspondiente procedimiento administrativo será la aplicable al acceso por parte de quienes tengan la condición de interesados en un procedimiento administrativo en curso a los documentos que se integren en el mismo", motivo por el cual la citada Ley 19/2013 se aplicará de

---

[1159] Cfr. el artículo 35.1.e) de la LPAC.

[1160] Este último artículo sólo indica que "el organismo de supervisión informará al prestador de servicios de confianza especificando los motivos de la demora y el plazo previsto para concluir la verificación", pero dicha información deberá realizarse conforme a las reglas de procedimiento administrativo propias de la legislación nacional de organismo de supervisión, de lo que se deduce la necesidad de realiza una verdadera notificación.

[1161] Recuérdese que el artículo 14.1 establece los siguientes límites: "a) La seguridad nacional. b) La defensa. c) Las relaciones exteriores. d) La seguridad pública. e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios. f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva. g) Las funciones administrativas de vigilancia, inspección y control. h) Los intereses económicos y comerciales. i) La política económica y monetaria. j) El secreto profesional y la propiedad intelectual e industrial. k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión. l) La protección del medio ambiente"; a los que hay que añadir los límites relativos a la protección de datos de carácter personal previstos en el artículo 15 de la misma Ley.

forma supletoria a lo previsto, en este caso, por la LPAC[1162]. Sin embargo, de esta regla no se desprende la inaplicación de los límites previstos en la citada Ley 19/2013, dado que es la LPAC –la norma de aplicación preferente– la que establece su aplicación en su artículo 82.

Por este motivo, y como hemos avanzado, las citadas limitaciones deberán ser objeto de una interpretación estricta[1163], requiriendo una especial motivación, dado el efecto potencialmente generador de indefensión sobre un interesado al que se le limita el acceso a una información relevante del expediente, y que va a sustentar la resolución que recaiga en su caso, quizá limitando su derecho de acceso a la actividad, en caso de denegación de la cualificación.

Realizado este trámite, y dado que difícilmente tendrá sentido que el órgano acuerde –caso que legalmente pueda hacerlo, algo que resultaría muy dudoso– el trámite de información pública sobre el expediente, se podrá proceder ya al dictado de la correspondiente resolución, y su notificación, todo ello en soporte electrónico[1164], resultando oportuno aclarar que, en caso de superación del plazo inicial de tres meses sin que se haya publicado el servicio cualificado en la lista de confianza, o notificado la correspondiente resolución de suspensión o ampliación del plazo máximo para resolver, nos encontraremos ante el correspondiente silencio administrativo, que conforme a la previsión contenida en el artículo 24.1 de la LPAC, debe considerarse negativo, dado que el artículo 21.3 del Reglamento eIDAS claramente indica que "[l]os prestadores cualificados de servicios de confianza podrán comenzar a prestar el servicio de confianza cualificado una vez que la cualificación haya sido indicada en las listas de confianza a que se refiere el artículo 22, apartado 1", algo que no sucede en caso de simple ausencia de respuesta por parte del organismo de supervisión.

Finamente, frente a la resolución cabrá la presentación del correspondiente recurso administrativo, conforme al régimen general, que no presenta especialidades dignas de mención.

7.1.3 La comunicación de inicio de actividad de los prestadores sin cualificación

Una vez visto el régimen de cualificación, que orbita alrededor de la notificación, resulta preciso plantearse acerca de la posibilidad de establecer un régimen de comunicación previa en relación con los servicios de confianza no cualificados previstos en el Reglamento eIDAS[1165].

[1162] Véase el Criterio Interpretativo CI/008/2015, de 12 de noviembre, del Consejo de Transparencia y Buen Gobierno (estatal).

[1163] El artículo 14.2 de la Ley 19/2013 ya ordena, con carácter general, que "[l]a aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso".

[1164] Cabe dar por reproducida aquí la crítica realizada con ocasión de la imposición de la comunicación exclusivamente electrónica a las personas físicas que decidan prestar servicios cualificados de confianza.

[1165] En el caso de los servicios de confianza que se puedan establecer por la ley nacional, lógicamente se deberá estar a lo que la misma disponga. Éste no es el caso de España, que –al menos de momento– no regula servicios adicionales de confianza.

Como sabemos, el Reglamento eIDAS apuesta por un modelo donde las interacciones previas entre el prestador y el organismo de supervisión se prevén en el caso de los servicios cualificados, y no en los restantes. En este sentido, conforme al artículo 17.3.b) del Reglamento, las funciones del organismo de supervisión, en relación con los servicios no cualificados, se limitan a "adoptar medidas, en caso necesario, en relación con los prestadores no cualificados de servicios de confianza establecidos en el territorio del Estado miembro que lo designa, mediante actividades de supervisión posteriores, cuando reciba la información de que dichos prestadores no cualificados de servicios de confianza, o los servicios de confianza prestados por ellos, supuestamente no cumplen los requisitos establecidos en el presente Reglamento".

En una lectura estricta de la norma, se puede considerar que la intervención del organismo de supervisión sólo deberá producirse en caso de denuncia, aunque incluso en esta interpretación restringida se deberían considerar posibles otras formas de conocimiento, por el supervisor, de un supuesto incumplimiento por los prestadores de sus obligaciones, o de los requisitos aplicables a los servicios de confianza sin cualificación.

Cabe plantearse si sería compatible con el Reglamento eIDAS una norma jurídica nacional que imponga el deber jurídico, a los prestadores de servicios de confianza sin cualificación, de proceder a realizar algún tipo de comunicación acerca de los servicios sin cualificación que prestan.

Esta es la previsión que, de hecho, se contiene en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios de confianza, cuyo artículo 13 indica que "[l]os prestadores de servicios de confianza no cualificados no necesitan autorización administrativa para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Energía, Turismo y Agenda Digital[1166] en el plazo de tres meses desde que la inicien".

Esta posibilidad parece admisible a tenor de la previsión del Reglamento eIDAS que autoriza de forma expresa a los Estados miembros a mantener o establecer normas relativas a los servicios de confianza, siempre que no se refieran a aspectos armonizados, pero ciertamente deberá tratarse de una comunicación posterior, dado que la comunicación previa de inicio de actividad prevista en el artículo 69 de la LPAC tiene el carácter de autorización y, por tanto, resultaría incompatible con el derecho de la Unión.

Apoya esta interpretación el hecho de que, como hemos visto, los citados servicios sin cualificación puedan ser objeto de publicidad administrativa en la lista de confianza, para lo cual es indudable que los mismo han de poder ser conocidos por el organismo de supervisión.

No es el caso de España, sin embargo, que en la lista únicamente incluye servicios cualificados, sino que se limita a publicitarlos en su sede electrónica, como veremos en breve[1167].

[1166] En la actualidad, el Ministerio de Economía y Empresa.

[1167] Cfr. el epígrafe 7.1.5 de este trabajo.

7.1.4 La publicidad de la cualificación

7.1.4.1 Las listas de confianza (TL)

Concedida la cualificación, se debe necesariamente proceder a dar publicidad a la misma, lo cual se realiza mediante un instrumento técnico concreto, denominado "lista de confianza" (en adelante, "TL"), al que se refiere el artículo 22 del Reglamento eIDAS, publicidad que, como ya hemos avanzado, tiene carácter constitutivo –y no simplemente declarativo–, ya que en efecto únicamente se puede iniciar la prestación del servicio desde el momento en que se produce dicha publicidad.

Nótese que no nos encontramos ante un caso de publicación[1168] del acto administrativo de cualificación, sino ante un instrumento que publicita los servicios que han sido objeto de dicha cualificación.

En este sentido, el artículo 22.1 del Reglamento eIDAS ordena que "[c]ada Estado miembro establecerá, mantendrá y publicará listas de confianza con información relativa a los prestadores cualificados de servicios de confianza con respecto a los cuales sea responsable, junto con la información relacionada con los servicios de confianza cualificados prestados por ellos", publicación que, conforme al epígrafe 2 del mismo artículo, deberá producirse de manera segura, de modo que las listas serán firmadas o selladas electrónicamente y, lo que resulta más novedoso, "en una forma apropiada para el tratamiento automático".

En efecto, el mecanismo de publicidad administrativa que informa de los servicios cualificados se encuentra diseñado, por el legislador de la Unión, como un mecanismo de tratamiento automatizado, al objeto de permitir que las aplicaciones informáticas que hacen uso de los servicios de confianza puedan determinar, sin intervención humana, que un servicio dispone de cualificación o no. Se trata de una novedad relevante desde la perspectiva de los instrumentos de publicidad administrativa, que normalmente no se diseñan legislativamente para resultar de tratamiento puramente automatizado, como en este caso, y que responde a unas necesidades muy concretas[1169].

[1168] El artículo 45.1 de la LPAC prevé que "[l]os actos administrativos serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente", imponiendo la obligación de publicación en otros casos, ninguno de los cuales se corresponde con el procedimiento que estamos analizando. En efecto, como ya hemos tenido oportunidad de analizar, el Reglamento eIDAS deja al Derecho nacional la regulación de los procedimientos empleados por el órgano de supervisión, por lo que nada establece en este sentido. Tampoco el Anteproyecto de Ley reguladora de determinados aspectos de los servicios de confianza exige la publicación del acto administrativo.

[1169] Como han indicado (Delos & Lacroix, 2010a, p. 5), "la necesidad de las Listas de Confianza (TL) procede del hecho de que, en la práctica, persisten determinadas dificultades ligadas al uso de las firmas electrónicas cualificadas (QES) y firmas electrónicas avanzadas basadas en certificados cualificados (AdESQC), especialmente en un uso transfronterizo, las cuales debían ser resueltas. Las mismas incluían problemas relativos a la confianza en las firmas electrónicas generadas en otros Estados Miembros. Dicha confianza podría ser incrementada poniendo a disposición sobre el estado de supervisión/acreditación de los servicios de certificación que expiden certificados cualificados (QC) por los PSCs establecidos o acreditados en los Estados Miembros. Esta información es esencial para soportar la validación de las QES y las AdES basadas en QC en un contexto transfronterizo" (la traducción es mía), lo que dio lugar a la Decisión 2009/767 de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas con arreglo a la Directiva

Nótese que sólo los servicios cualificados de confianza son objeto de publicidad administrativa obligatoria, y no en cambio los restantes servicios de confianza; ello es coherente con el modelo regulatorio de autorización y control previo que instaura el Reglamento eIDAS únicamente en relación con los servicios cualificados. Esto implica, sin embargo, que en algunos Estados se ofrecerá información sobre todos los servicios de confianza[1170], mientras que, en otros, dicha información se limitará a los servicios cualificados.

Dado que, conforme a los epígrafes 1 y 2 del artículo 22 del Reglamento eIDAS, cada Estado miembro debe publicar listas de confianza, el epígrafe 3 del mismo artículo 22 ordena que "[l]os Estados miembros notificarán a la Comisión, sin retrasos indebidos, información sobre el organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales, y detalles relativos al lugar en que se publican dichas listas, los certificados utilizados para firmar o sellar las listas de confianza y cualquier modificación de los mismos", al objeto de que la Comisión pueda poner "a disposición del público, a través de un canal seguro, la información a que se refiere el apartado 3 en una forma firmada o sellada electrónicamente apropiada para el tratamiento automático".

Se trata de un mecanismo conocido como "lista de listas de confianza" (LOTL), también procesable de forma plenamente automatizada, y que persigue facilitar el acceso a las diferentes listas de confianza nacionales. Por ejemplo, si se recibe una firma electrónica cualificada basada en un certificado cualificado emitido en Alemania, será necesario conocer la ubicación en Internet de la lista de confianza publicada por el organismo de supervisión alemán, que normalmente no será conocido fuera de Alemania[1171], y menos aún dónde publica las listas. Por tanto, la aplicación informática que deba validar la firma electrónica en cuestión podrá consultar la "lista de listas de confianza" publicada por la Comisión Europea y obtener la localización de la lista de confianza alemana, pudiendo entonces acceder a la misma para comprobar que el certificado que sustenta la firma electrónica es cualificado.

Finalmente, el epígrafe 4 del artículo 22 del Reglamento eIDAS prevé que "[a] más tardar el 18 de septiembre de 2015 la Comisión, mediante actos de ejecución, especificará la información a que se refiere el apartado 1 y definirá las especificaciones técnicas y formatos de las listas de confianza, aplicables a efectos de los apartados 1 a 4", actos de ejecución que "se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2"; previsión que encuentra su fundamento claro en la dimensión claramente transfronteriza de las listas de confianza, lo que justifica su armonización como instrumento común.

Se trata de una de las normas relacionadas con el propio funcionamiento del marco regulatorio de los servicios de confianza que puede establecer la Comisión Europea[1172],

---

2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

[1170] Hay que entender que, si en un Estado se decide dar publicidad a los servicios de confianza no cualificados, se deberá informar acerca de todos los servicios de confianza de que tenga conocimiento el organismo de supervisión, algo que dependerá de que se imponga algún tipo de obligación de comunicación, algo sobre lo que volveremos más adelante. Cfr. el epígrafe 7.1.3 de este trabajo).

[1171] En realidad, seguramente tampoco será conocido en Alemania…

[1172] Cfr. el epígrafe 1.4.2 de este trabajo.

y que ha sido dictada por Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, "Decisión de listas de confianza eIDAS"), y cuyo contenido resulta preciso conocer, al objeto de precisar qué información contiene, y cómo se transmite dicha información.

Las listas de confianza no son, de todos modos, una innovación del Reglamento eIDAS, ya que las mismas existían ya desde la Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior [notificada con el número C(2009) 7806 (en adelante, "Decisión de listas de ventanilla única"), modificada por Decisión 2010/425/UE de la Comisión, de 28 de julio de 2010, por Reglamento (UE) Nº 519/2013 de la Comisión de 21 de febrero de 2013[1173], y por Decisión 2013/662/UE de Ejecución de la Comisión, de 14 de octubre de 2013.

La Decisión de listas de confianza de ventanilla única encontraba su justificación en la posibilidad de que los Estados miembros exijan, "sobre la base de una evaluación apropiada de los riesgos existentes y de conformidad con el artículo 5, apartados 1 y 3, de la Directiva 2006/123/CE […] para la realización de algunos procedimientos y trámites a través de las ventanillas únicas con arreglo al artículo 8 de la Directiva 2006/123/CE, el uso por el prestador del servicio de firmas electrónicas avanzadas basadas en un certificado reconocido, con o sin dispositivo seguro de creación de firma" (artículo 1 de la Decisión de listas de confianza de ventanilla única), por lo que "[a] fin de que del uso transfronterizo de las firmas electrónicas avanzadas basadas en un certificado reconocido resulte eficaz, debe reforzarse la confianza en estas firmas electrónicas con independencia del Estado miembro en que esté establecido el firmante o el proveedor de servicios de certificación que expida el certificado reconocido", lo que "podría conseguirse ofreciendo más fácilmente en una forma confiable la información necesaria para validar las firmas electrónicas, y en particular la información relativa a los proveedores de servicios de certificación que están supervisados/acreditados en un Estado miembro y a los servicios que prestan".

En definitiva, existía ya un instrumento definitorio de las listas de confianza, pero limitado a las operaciones transfronterizas en el ámbito de la Directiva de Servicios, por lo que no se tenía porqué aplicar a otras operaciones transfronterizas, ni tampoco en las operaciones en el nivel nacional o domésticas. Además, como es lógico teniendo en cuenta su fecha de aprobación, se trataba de un instrumento exclusivamente limitado a

[1173] Esta Decisión fue la que incorporó la noción de una lista de tratamiento automático. El Considerando (3) de dicha Decisión indica, en este sentido, que "[l]as pruebas han confirmado asimismo la necesidad de que los Estados miembros no solo publiquen versiones de sus listas de confianza legibles por personas, tal como exige la Decisión 2009/767/CE, sino también en formatos que puedan procesarse por máquina. En caso de que los Estados miembros cuenten con numerosos proveedores de servicios de certificación, el tratamiento manual de las versiones de las listas de confianza legibles por personas puede ser relativamente complejo y requerir mucho tiempo. La publicación de versiones procesables por máquina de dichas listas facilitará el empleo de las mismas, ya que permitirá su tratamiento informatizado y, de este modo, propiciará su utilización en el contexto de los servicios electrónicos públicos".

las firmas electrónicas avanzadas basadas en certificado reconocido, conforme a la DFE, o a las firmas electrónicas reconocidas, también conforme al marco de la DFE. Y precisamente por encontrarse alineada con la DFE, este mecanismo distinguía entre sistemas de supervisión (a posteriori, que era el modelo de la citada DFE) y sistemas voluntarios de acreditación.

Por lo demás, de la lectura de la citada Decisión, es evidente que la misma ha servido de inspiración plena para el régimen del Reglamento eIDAS, tanto respecto al contenido y formato de la lista nacional, como a la existencia de la "lista de listas de confianza", pero adecuando la misma al nuevo modelo regulatorio del Reglamento, y a la ampliación de servicios de confianza, más allá de la firma electrónica.

Debe entenderse que la Decisión de listas de confianza de ventanilla única, por tanto, ha quedado inaplicada tras la entrada en aplicación del Reglamento eIDAS[1174] el 1 de julio de 2016, a pesar de que la misma no haya sido formalmente derogada, algo que resulta criticable.

Entrando en el contenido de la Decisión de listas de confianza eIDAS[1175], lo primero que se debe resaltar es que la misma debe incluir las reglas específicas del Estado miembro, entre las cuales, al menos "las normas y políticas específicas del Estado miembro a las que se hace referencia que se siguen en la evaluación de los servicios de confianza incluidos en la lista, en cumplimiento del sistema de supervisión y, en su caso, del sistema de aprobación del Estado miembro" y "la descripción concreta del Estado miembro a la que se hace referencia acerca de cómo utilizar e interpretar el contenido de la lista de confianza con respecto a los servicios de confianza no cualificados que figuran en la lista y los servicios de confianza definidos a nivel nacional".

Esto se debe poner en relación con el párrafo segundo del Capítulo I del Anexo I de la Decisión de listas de confianza eIDAS prevé que "[l]os términos «aprobado», «acreditado» y «supervisado» utilizados en las presentes especificaciones también comprenden los sistemas de aprobación nacionales, pero los Estados miembros proporcionarán información adicional sobre la naturaleza de tales sistemas nacionales en su lista de confianza, incluida una aclaración con respecto a las posibles diferencias con los sistemas de supervisión aplicados a los proveedores de servicios de confianza cualificados y a los servicios de confianza cualificados que estos prestan", un texto de una cierta oscuridad, que parece prever la necesidad de informar de la existencia, en su caso, de diferentes modalidades de supervisión (incluida las diversas tipologías de aprobación) que existen en sede nacional con respecto a los servicios de confianza previstos en el Reglamento eIDAS, pero sin cualificación, o con respecto a los servicios de confianza con cualificación únicamente nacional, por tratarse de servicios de confianza creados por la legislación nacional y no recogidos, por tanto, en el Reglamento eIDAS[1176]; información que se debe realizar mediante el instrumento referenciado en este campo.

[1174] Esta inaplicación se puede entender confirmada dado que el texto obligatorio que exige emplear la Decisión de listas de confianza eIDAS en la información sobre el sistema rector de la citada lista incluye la frase "[l]a presente lista de confianza es la continuación de la lista de confianza establecida por la Decisión 2009/767/CE".

[1175] Se puede ver el detalle completo de los contenidos de la TL en el Anexo C de este trabajo.

[1176] Esta provisión no se refiere, como es lógico, a la cualificación, que goza de un régimen armonizado y, por tanto, uniforme en toda la Unión Europea. Ello no significa que todos los procesos de cualificación

A título de ejemplo, la TL italiana refiere a una descripción[1177] relativa al servicio de verificación de identidad referido a la tarjeta nacional de servicios, consistente en la expedición de un certificado no cualificado de identificación por parte de prestadores cualificados que expiden certificados cualificados de firma electrónica, tras la comprobación de la identidad del ciudadano por parte de una entidad pública. Otro ejemplo, incluso más significativo, lo encontramos en el caso de la TL danesa, que explica[1178] que los prestadores de servicios pueden cualificarse conforme al Reglamento eIDAS o acreditarse conforme al concepto denominado "OCES"[1179], para lo que deben establecer un convenio con la Agencia Danesa para la Digitalización (que además es el organismo de supervisión), y sin que estos certificados OCES puedan ser considerados cualificados.

En segundo lugar, cuando el tipo de servicio indicado en la TL se corresponde con una autoridad de certificación raíz nacional, en este campo debe constar una dirección de Internet en la que se informe acerca de la legislación nacional aplicable a la autoridad de certificación raíz nacional, y a las correspondientes reglas de gestión. Así sucede, por ejemplo, en la TL alemana, que registra trece autoridades de certificación raíz nacionales a nombre del *Bundesnetzagentur*, que es el organismo de supervisión nacional de servicios de confianza; o en la TL polaca, que registra al Banco Nacional de Polonia, como la autoridad de certificación raíz nacional para la infraestructura de firma electrónica segura, para lo cual dispone de dos autoridades de certificación de este tipo.

Finalmente, y superando la exigencia contenida en el Reglamento eIDAS, la Decisión en cuestión prevé la posibilidad de incluir, en la lista de confianza nacional, información acerca de servicios de confianza sin cualificación (artículo 2 de la Decisión), lo que se justifica tanto en "responder a las expectativas legítimas de otros proveedores de servicios de certificación que no expidan certificados cualificados, pero que ofrezcan servicios relacionados con las firmas electrónicas en el marco de la Directiva 1999/93/CE y que se incluyan en la lista antes del 30 de junio de 2016" (Considerando (4) de la Decisión) como en el hecho de que "los Estados miembros podrán añadir otros tipos de servicios de confianza definidos a escala nacional distintos de los definidos en el artículo 3, apartado 16, del Reglamento (UE) no 910/2014, siempre que esté claramente indicado que no están cualificados de conformidad con el Reglamento (UE) no 910/2014" (Considerando (5) de la Decisión).

Otra cuestión relevante de la Decisión de listas de confianza eIDAS es el reconocimiento expreso de la posibilidad –que en todo caso tienen los Estados miembros, dado que el Reglamento eIDAS no se opone a ello– de publicar "una versión legible por personas de la lista de confianza", en cuyo caso "se asegurará de que esa versión de la lista de confianza contenga los mismos datos que la versión apropiada para el tratamiento automático", debiendo estar firmada en los mismos términos que en el caso de la versión de tratamiento automático. Además, conforme al Capítulo IV del Anexo I de la Decisión,

---

sean idénticos en todos los Estados miembros, igual que sabemos que no todos los prestadores tendrán un régimen jurídico idéntico, sino que sólo es preciso informar del régimen jurídico de los servicios típicos sin cualificación, y de los servicios atípicos, también sin cualificación europea.

[1177] Cfr. https://eidas.agid.gov.it/TL/schemerules-IT.html.

[1178] Cfr. http://uri.etsi.org/TrstSvc/TrustedList/schemerules/DK/.

[1179] Se puede encontrar más información sobre este sistema en https://www.nemid.nu/dk-en/.

"deberá facilitarse en forma de documento PDF con arreglo a ISO 32000, que deberá estar formateado de acuerdo con el perfil PDF/A (ISO 19005)".

Se trata de una posibilidad más que razonable, dado que la versión de tratamiento automático hace uso de un vocabulario XML que presenta una cierta complejidad y, por tanto, puede resultar difícil de comprender para cualquier persona sin conocimientos especializados, y que se ha complementado mediante herramientas como el "navegador de listas de confianza" que opera la Comisión Europea[1180], que permite visualizar las citadas listas de forma simple, como se puede ver en la Ilustración 16.

Finalmente, también es conveniente indicar que "[l]as listas de confianza deberán incluir información tanto actual como histórica, desde la fecha de inclusión de un proveedor de servicios de confianza en las listas de confianza, acerca del estado de los servicios de confianza incluidos en la lista", algo que no se desprende directamente del mandato legal contenido en el artículo 22 del Reglamento eIDAS, pero que resulta muy importante en términos de comprobación de la validez de un servicio de confianza en el pasado, como por ejemplo cuando se quiere determinar si en cierto momento un certificado expedido por un prestador era cualificado o no.

Esta información histórica permite, entonces, la toma de decisiones con respecto a la validez de una firma electrónica sustentada en un certificado expedido por un prestador que ha cesado en su actividad, por lo que su relevancia para el servicio de confianza de validación[1181] de firma electrónica o de sello electrónico es absolutamente crucial.

[1180] Disponible en https://webgate.ec.europa.eu/tl-browser/#/

[1181] Sobre este servicio, cfr. el epígrafe 4.3.2 de este trabajo.

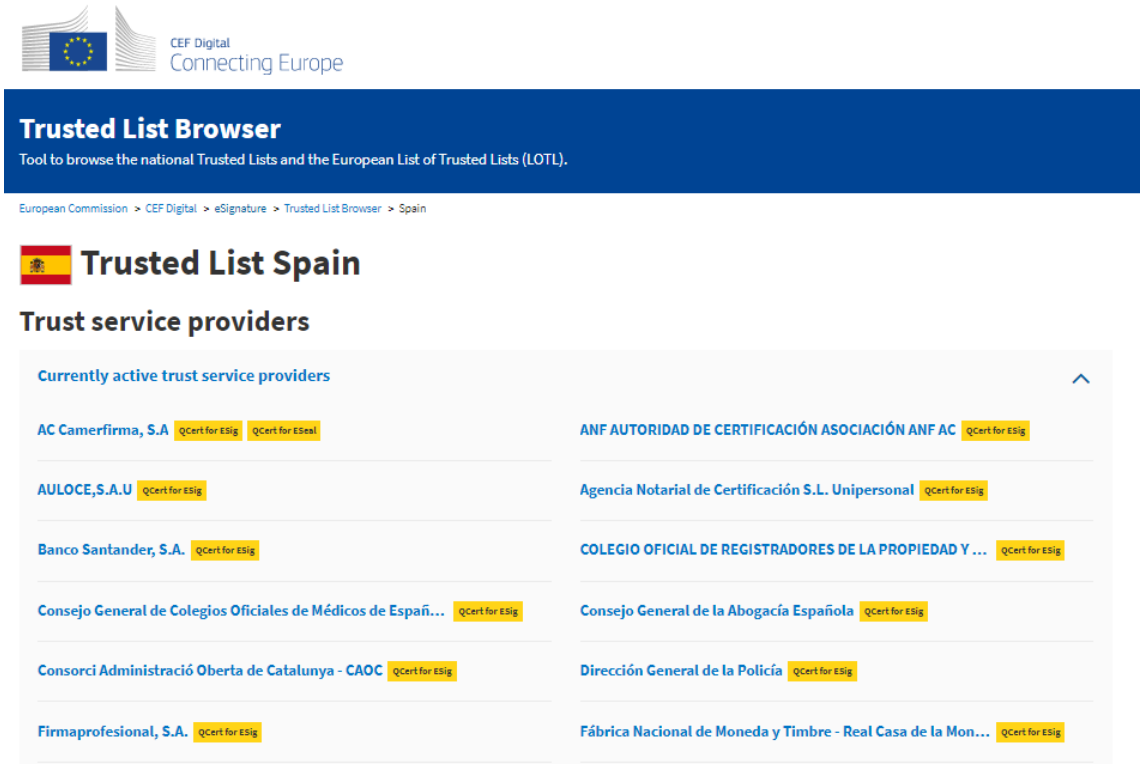


Ilustración 16. Navegador de listas de confianza de la Comisión Europea; detalle parcial de España (Portal de la Comisión Europea)

Respecto a la semántica de la lista de confianza, ya sabemos que el artículo 22 del Reglamento eIDAS se limita a indicar que en la misma se publicarán los servicios cualificados, por lo que al menos todos los servicios cualificados deben considerarse como tales, con independencia de los detalles concretos que ello implique en cada Estado miembro, puesto que, cono sabemos[1182], cada uno de ellos puede completar las previsiones del Reglamento eIDAS.

La citada Decisión, siguiendo el artículo 22.4 del Reglamento eIDAS, adopta una especificación técnica producida por el Instituto Europeo de Normas de Telecomunicaciones, ETSI TS 119 612 v2.1.1, mediante la técnica del reenvío directo[1183], convirtiéndola en obligatoria para sus destinatarios, que son los Estados miembros, por lo que nos encontramos ante un reglamento técnico. Y un reglamento técnico que condiciona de manera decisiva el contenido y la forma de la publicidad administrativa, que debe realizarse empleando el vocabulario XML que se contiene en dicha especificación.

Dado que, como hemos avanzado, se aplica en este caso la técnica del reenvío directo, y con indicación de la versión exacta de la especificación adoptada, sucede que las versiones que posteriormente pueda adoptar el ETSI de esta especificación técnica no

[1182] Cfr. el epígrafe 1.3.3 de este trabajo.

[1183] Conforme al primer párrafo del Capítulo II del Anexo I de la Decisión, "[l]as presentes especificaciones se basan en las especificaciones y los requisitos establecidos en la norma ETSI TS 119 612 v2.1.1 (denominada en lo sucesivo ETSI TS 119 612)".

resultarán aplicables en el ámbito de esta Decisión, requiriéndose de la modificación de la Decisión. De esta forma, la Comisión mantiene el control sobre las concretas obligaciones que impone a los Estados miembros, que de otro modo quedarían inmediatamente obligados a lo que decidiera la industria, que es en definitiva quien procede a realizar la normalización, especialmente en este caso, en que nos referimos simplemente a una especificación técnica (TS), y no a una verdadera norma técnica europea (EN). En este caso, además, esto es ciertamente importante, debido a que una de las informaciones incluidas en la lista es el "tipo de servicio de confianza"[1184], que debe estar plenamente alineado con las definiciones del Reglamento eIDAS, dado que es objeto de publicidad constitutiva.

Además, y dado el enfoque generalista de la especificación técnica ETSI TS 119 612, la Decisión de listas de confianza eIDAS establece requisitos específicos en relación con determinadas cuestiones de la citada especificación técnica, que tendrán prevalencia sobre ésta en caso de conflicto, aplicándose directamente dicha especificación en los restantes casos[1185].

Se trata de un enfoque que persigue –y así se desprende de diversas secciones de la especificación técnica ETSI TS 119 612– limitar la cantidad de información contenida en la TL, pero que reduce el valor del sistema de listas para conocer los verdaderos servicios que ofrecen los prestadores.

Por ejemplo, imaginemos que un prestador expide certificados de firma electrónica avanzada y cualificada, empleando una autoridad de certificación para ello, y diferenciando, en el caso de los certificados de firma electrónica cualificada, entre tipos de dispositivos cualificados de creación de firma electrónica, de modo que ofrezca certificados correspondientes a datos de creación de firma en tarjeta y datos de creación de firma en HSM gestionado por el propio prestador, además de los certificados en software. Si el citado prestador incluye dentro de los certificados que emite información procesable de forma automática indicando cuándo se emplea un dispositivo cualificado[1186], lo más posible es que el operador de la lista de confianza indique la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert, en la extensión `Qualifications`, sin diferenciar más. En este caso, la única forma de conocer las modalidades de servicio es conectarse a la página del prestador y leerse la información de políticas y/o prácticas, algo que puede suponer un esfuerzo desproporcionado que afecte a la prestación transfronteriza de servicios, inclusive debido a barreras idiomáticas.

[1184] Lo que se acaba de indicar no es en absoluto teórico ni baladí, sino al contrario, dado que existe una versión posterior de esta especificación, numerada como v2.2.1, en la que se ha incluido, como tipo de servicio de confianza, el de "gestión remota de dispositivo cualificado de creación de firma electrónica o de sello electrónico" que, como sabemos, no es considerado como tal por la Comisión Europea, en la interpretación que realiza del Reglamento eIDAS (cfr. el epígrafe 1.3.1 de este trabajo).

[1185] Conforme al segundo párrafo del Capítulo II del Anexo I de la Decisión, "[c]uando en las presentes especificaciones no se establezca ningún requisito específico, se aplicarán íntegramente los requisitos de las cláusulas 5 y 6 de ETSI TS 119 612. Cuando se establezcan requisitos específicos, estos prevalecerán sobre los requisitos correspondientes de ETSI TS 119 612. En caso de discrepancia entre las presentes especificaciones y las especificaciones de ETSI TS 119 612, prevalecerán las primeras".

[1186] Para ello se emplea una declaración normalizada en la norma ETSI EN 319 412, parte 5.

Pero lo más grave es que puede que en otro Estado miembro, la misma situación reciba un tratamiento diferente, si el correspondiente operador de la TL es muy estricto y considera necesario diferenciar el subconjunto de certificados que hacen uso de un dispositivo cualificado gestionado por el prestador en nombre del firmante. En este segundo caso –que ciertamente es más adecuado para la publicidad de los servicios ofrecidos por el prestador– se plantea el problema de que habría más de una forma de representar esta información dentro de la TL, algo que no facilita el uso de las listas de confianza para obtener información acerca de los servicios.

La primera forma es mantener la declaración general, anteriormente indicada, de la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert y añadir un filtro con el OID de los certificados cuyos dispositivos son gestionados por el prestador, en relación con los cuales se incluirá la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf; mientras que la otra forma es diferenciar todos los subconjuntos de certificados, mediante los correspondientes OIDs, indicando para cada uno de ellos el tipo de soporte. Las dos formas son correctas, aunque aportan menor grado de publicidad. En el primer caso, esencialmente se remite a lo que establezca el certificado, pero aclarando que los certificados que tengan cierto OID corresponden a datos de creación de firma gestionados por el prestador; mientras que en el segundo caso no es realmente necesario remitirse al certificado.

Resulta bastante evidente que el enfoque de las listas de confianza no es, por tanto, servir de instrumento general de publicidad administrativa, sino que más bien parece orientarse a facilitar la validación de las pruebas electrónicas generadas mediante los servicios de confianza, completando la información que precise el usuario que debe confiar en las mismas, y así se confirma en el párrafo tercero del Capítulo I del Anexo I de la Decisión de listas de confianza eIDAS, que aclara que "[l]a información que se proporciona en la lista de confianza está destinada principalmente a respaldar la validación de los tokens de servicios de confianza cualificados, es decir, objetos físicos o binarios (lógicos) generados o expedidos como resultado de la utilización de un servicio de confianza cualificado, por ejemplo, firmas electrónicas o sellos electrónicos cualificados, firmas electrónicas o sellos electrónicos avanzados admitidos por un certificado cualificado, marcas de tiempo cualificadas, pruebas de entrega electrónica cualificadas, etc".

Esto justifica plenamente, además, el enfoque de cualificación como autorización administrativa, de forma que sólo se autorice la prestación del servicio desde que el mismo aparece listado en la TL.

No nos encontramos, pues, con un instrumento de publicidad administrativa que permita acceder libremente a suficiente detalle de los servicios de confianza prestados en la Unión Europea, ni siquiera de los cualificados, sino de un instrumento útil para las personas que deben validar una prueba electrónica sustentada por un *token* de confianza. Es cierto que, en este contexto, el instrumento tiene una utilidad indudable para dicha persona, que ya tiene información relevante que necesita, a lo sumo, complementar, pero resulta criticable que no exista un mecanismo general de publicidad administrativa que contenga, de forma normalizada para toda la Unión Europea, la información completa.

De adoptarse este enfoque, sería más fácil, por ejemplo, la adquisición de servicios transfronterizos, que después de todo es uno de los objetivos del Reglamento eIDAS, por lo que sería deseable una evolución del modelo en este sentido.

7.1.4.2 La etiqueta de confianza "UE"

Un segundo mecanismo de publicidad, en ese caso exclusivamente previsto para los servicios de confianza[1187], es la etiqueta de confianza "UE" prevista en el artículo 23 del Reglamento eIDAS, que justifica su existencia en el Considerando (47) del Reglamento eIDAS, cuando indica que "[l]a confianza en los servicios en línea y la conveniencia de estos servicios son fundamentales para que los usuarios los aprovechen plenamente y confíen conscientemente en los servicios electrónicos", para cuyo fin "debe crearse una etiqueta de confianza «UE» que identifique los servicios de confianza cualificados prestados por prestadores cualificados de servicios de confianza", que "diferenciaría claramente los servicios de confianza cualificados de otros servicios de confianza, contribuyendo así a mejorar la transparencia del mercado".

A diferencia del mecanismo de lista de confianza, nos encontramos en este caso ante un mecanismo de anuncio por parte de prestador que obtiene la etiqueta de confianza "UE", cuyo uso "es voluntario[1188] y no debe implicar más requisitos que los establecidos en el presente Reglamento", según también aclara el Considerando (47) del Reglamento eIDAS. Desde esta perspectiva, el modelo de la etiqueta de confianza "UE" es claramente diferente de los sistemas de acreditación voluntaria de servicios de certificación que se contenían en la DFE, que precisamente se configuraron como autorizaciones singulares en atención al cumplimiento de requisitos específicos, adicionales a los mínimos establecidos en la normativa.

Conforme, pues, al artículo 23.1 del Reglamento eIDAS, "[u]na vez que la cualificación […] se haya incluido en la lista de confianza […], los prestadores cualificados de los servicios de confianza podrán usar la etiqueta de confianza «UE» para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan", previsión que se completa con la obligación, prevista en el epígrafe 2 del mismo artículo 23, en cuya virtud "[a]l utilizar la etiqueta de confianza «UE» para los servicios de confianza cualificados a que se refiere el apartado 1, los prestadores de los servicios de confianza garantizarán que en su sitio web exista un enlace a la lista de confianza pertinente".

Como en el caso de la lista de confianza, el Reglamento eIDAS ordena, en el artículo 23.3, que "[a] más tardar el 1 de julio de 2015 la Comisión, por medio de actos de ejecución, elaborará especificaciones relativas a la forma y en particular la presentación, composición, tamaño y diseño de la etiqueta de confianza «UE» para servicios de confianza cualificados", dada la evidente necesidad de que este mecanismo resulte uniforme para toda la Unión, acto de ejecución que se adopta por el procedimiento de examen, en el marco del Comité previsto en el artículo 48.2 del propio Reglamento eIDAS, y que se ha dictado por Reglamento de Ejecución (UE) 2015/806 de la Comisión, de 22 de mayo de 2015, por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados (en adelante, Reglamento etiqueta eIDAS).

[1187] Este mecanismo, como ha explicado (Gobert, Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie, 2015, p. 28), no se encontraba previsto en la Propuesta de la Comisión, sino que fue incorporado a petición del Parlamento Europeo.

[1188] Resulta verdaderamente sorprendente el escaso uso que realizan los prestadores españoles de este mecanismo de publicidad.

El Reglamento etiqueta eIDAS considera que ese mecanismo contribuye "a la transparencia en el mercado y fomentando por ende la confianza en los servicios en línea y la conveniencia de estos, aspectos esenciales para que los usuarios los aprovechen plenamente y confíen sin reservas en los servicios electrónicos" (Considerando 1), explicando a continuación el procedimiento seguido para la selección de la imagen de la etiqueta[1189], y que la misma ha sido "registrada como marca colectiva en la Oficina de Propiedad Intelectual del Reino Unido, por lo que está en vigor, es utilizable y está protegida", anunciando que también "será registrado también en los registros de la Unión e internacionales".

De forma sorprendente, y a pesar de este proceso –o no, dada la tradición en este sentido– la etiqueta de confianza eIDAS seleccionada es… ¡un candado!, el cual se puede ver en la Ilustración 17.

Ilustración 17. Etiqueta de confianza "UE", versiones en color (Reglamento de Ejecución (UE) 2015/806)

El Reglamento etiqueta eIDAS, además de establecer las normas de uso de la citada etiqueta, concreta que la misma "podrá ir acompañada de elementos gráficos o textuales que indiquen claramente los servicios de confianza cualificados para los que se utiliza, a condición de que no modifiquen la naturaleza de la etiqueta de confianza «UE» para servicios de confianza cualificados ni alteren el vínculo con las listas de confianza aplicables", al objeto de evitar posibles confusiones, como por ejemplo cuando un mismo prestador ofrece servicios cualificados y no cualificados.

7.1.5 Otras modalidades de publicidad administrativa

De forma adicional a las anteriores formas de publicidad, los Estados miembros pueden establecer otras modalidades para dar publicidad a los servicios de confianza que

[1189] En efecto, el Considerando (2) expone que "La Comisión organizó un concurso para estudiantes de arte y diseño de los Estados miembros, a fin de recibir propuestas sobre un nuevo logotipo. Un jurado de expertos seleccionó las tres mejores propuestas sobre la base de los criterios especificados en el pliego de condiciones técnicas y de diseño de la «e-Mark U Trust Competition». Se celebró una consulta en línea entre el 14 de octubre y el 14 de noviembre de 2014. El logotipo propuesto, elegido por la mayoría de los visitantes del sitio web durante dicho período y respaldado por una decisión final del jurado, debe ser ahora adoptado como nueva etiqueta de confianza «UE» para servicios de confianza cualificados".

supervisan, sean o no cualificados.

Por ejemplo, en el caso del Estado español, el organismo de supervisión ha establecido un sistema para suministrar información de los servicios cualificados, por una parte, y no cualificados, por otra[1190].

Dado que, en España, la lista de confianza no incluye información acerca de los servicios sin cualificación, esta interfaz es imprescindible para disponer de información acerca de los mismos, y que se puede ver en la Ilustración 18.

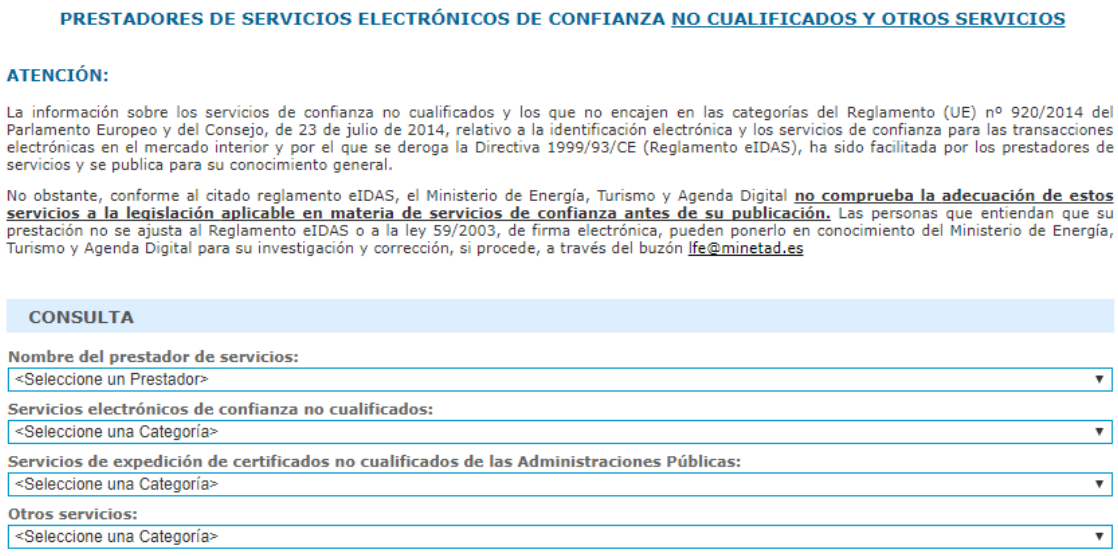


Ilustración 18. Interfaz de consulta de servicios no cualificados y otros servicios (España)

Cabe decir que en la lista de tipos de servicios de confianza no cualificados se echa de menos la referencia al servicio de creación de firma electrónica avanzada o de sello electrónico avanzado a distancia, al que ya hemos tenido ocasión de referirnos anteriormente[1191].

También llama la atención que esta interfaz incluya otros servicios diferentes a los servicios de confianza, algo heredado del régimen de la LFE, pero que no se debería mantener en el futuro, dadas las diferentes definiciones de servicios en ambas normas.

Y es que podía resultar razonable que el órgano de supervisión mantuviera información sobre cualesquiera servicios relacionados con la firma electrónica, porque podían entonces considerarse "servicios de certificación" conforme a la definición abierta de la LFE, pero desde luego ya no resulta aceptable en el modelo de lista cerrada del Reglamento eIDAS, a menos que dicha posibilidad se habilite por ley nacional, algo que el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza no realiza.

A título de ejemplo, en este listado de "otros servicios" se incluyen elementos como los

[1190] Sistema que encuentra su antecedente en el artículo 30.2 de la LFE, en relación con el cual puede verse (Martínez Nadal, 2009, págs. 513-514).

[1191] Cfr. el epígrafe 4.3.1 de este trabajo.

servicios de contratación electrónica certificada o de publicación electrónica certificada, entre otros, que no se encuentran regulados por la normativa de servicios de confianza, ni sujetos a la competencia del órgano de supervisión.

Por ello, es de imaginar que la derogación de la LFE implicará que el órgano de supervisión deje de publicar esta información.

7.2 LA SUPERVISIÓN DURANTE LA PRESTACIÓN DEL SERVICIO DE CONFIANZA

Una vez que el prestador ha accedido a la actividad, sea o no cualificado, el mismo se encuentra sujeto a la supervisión *a posteriori* que realiza el organismo nacional, como se desprende de lo establecido en el artículo 17.3 del Reglamento eIDAS.

En este epígrafe nos centraremos en el estudio de las diferentes manifestaciones de la actividad de supervisión, incluyendo los contenidos de esta actividad de supervisión, la retirada de la cualificación como consecuencia de las disfunciones en la actividad, y también la existencia de otras medidas en orden a garantizar la eficacia de la actuación supervisora. En el siguiente epígrafe nos centraremos en el régimen administrativo sancionador.

7.2.1 El contenido de la actividad de supervisión

Las funciones que se incluyen en esta supervisión se centran en la vigilancia de la correcta prestación de los servicios de confianza, con mayor intensidad en el caso de los servicios cualificados, en relación con los cuales el Reglamento eIDAS y la legislación nacional establecen requisitos específicos, y menor intensidad en los restantes servicios.

Como ya sabemos, el Reglamento eIDAS prevé diversos mecanismos para facilitar al organismo de supervisión en sus tareas de supervisión, en especial desde la óptica del necesario conocimiento de la actividad de los prestadores, entre los cuales la obligación de informar de todos los cambios en el servicio[1192], la presentación de los informes periódicos de evaluación de la conformidad[1193] o la notificación de incidentes de seguridad[1194].

Además, el artículo 17.4.e) del Reglamento eIDAS también permite al organismo de supervisión realizar auditorías –cabe imaginar que con sus propios medios–, o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la conformidad de un prestador cualificado de servicios de confianza, como también tuvimos ocasión de analizar[1195]; posibilidades a las que, en alguna legislación nacional, se añade la de exigir al prestador que realice sus propias evaluaciones y ofrezca las correspondientes evidencias[1196].

[1192] Cfr. el epígrafe 6.2.1 de este trabajo.

[1193] Cfr. el epígrafe 7.1.1 de este trabajo.

[1194] Cfr. el epígrafe 6.1.3 de este trabajo.

[1195] Cfr. el epígrafe 7.1.1 de este trabajo.

[1196] Así se establece en la sección § 4 (2) de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017).

Estos mecanismos resultan aplicables, con excepción de la obligación de notificación de incidentes de seguridad, únicamente a los prestadores cualificados, por lo que, en relación con los prestadores sin cualificación, normalmente el organismo de supervisión tendrá muy escasa información, incluso sujetando a dichos prestadores a la comunicación del inicio de su actividad; motivo por el que normalmente el organismo realizará supervisión reactiva, posiblemente en caso de incidente de seguridad o en caso de denuncia administrativa.

Adicionalmente, la ley nacional suele imponer a los prestadores de servicios de confianza obligaciones específicas de colaboración con el organismo de supervisión, incluyendo la entrega de documentación e informaciones relativas al servicio, así como en la inspección[1197], incluyendo la visita a las instalaciones correspondientes[1198].

Por lo que se refiere a la inspección, el artículo 16.1 del Anteproyecto prevé que el organismo de supervisión "realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de control", y atribuye a sus funcionarios adscritos "la consideración de autoridad pública en el desempeño de sus cometidos", por lo que, conforme a lo previsto en el artículo 77.5 de la LPAC, los documentos "en los que, observándose los requisitos legales correspondientes se recojan los hechos constatados por aquéllos harán prueba de éstos salvo que se acredite lo contrario" [1199], lo que genera una verdadera inversión de la carga de prueba en perjuicio del prestador solicitante de la cualificación, que deberá estar en disposición de levantar, en línea con el muy estricto régimen de responsabilidad civil previsto en el propio Reglamento eIDAS para los servicios cualificados de confianza.

Como es lógico, esta prueba deberá referirse a hechos directa y personalmente constatados por los citados funcionarios, como sucedería, por ejemplo, en el caso de acreditar las informaciones (o más bien, su ausencia) que debe publicar el prestador.

Asimismo, el epígrafe 2 del mismo artículo 16 del Anteproyecto prevé que el organismo de supervisión "podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de confianza", debiéndose considerar que sus pruebas no gozarán del efecto

---

[1197] Respecto a la función de inspección, (Palomar Olmeda, 2014, págs. 175-176) señala que la misma "necesita, de un lado, la habilitación legal para entender que el régimen sancionador se incluye dentro del régimen de regulación de una determinada actividad y, de otro, que para el ejercicio de esta competencia la sancionadora) lo común es establecer un determinado cuerpo de funcionarios o, en general, de empleados públicos sobre cuya actuación – debidamente documentada – se sustenta una potestad de investigación cuya documentación en actas goza de una presunción de veracidad e invierte la carga de la prueba sobre el cumplimiento o no de los requisitos establecidos para el ejercicio de la actividad". Dicha habilitación se encuentra establecida en el artículo 16.1 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

[1198] Cfr. la sección § 15 de la Ley Federal (austríaca) sobre Firmas Electrónicas y Servicios de Confianza para Transacciones Electrónicas – *Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)*, promulgada por artículo 1 de la Ley Federal de 8 de julio de 2016; o la detallada sección § 5 (1) de la Ley alemana de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017).

[1199] Cfr. (Blanquer, 2006, pág. 247 y ss.), que considera que nos encontramos, en estos casos, ante ficciones legales, y no ante presunciones.

privilegiado al que nos acabamos de referir, sin perjuicio de su valor intrínseco derivado del conocimiento pericial de dichas entidades, y debiéndose asumir que a costa de la propia Administración.

Finalmente, el epígrafe 3 del artículo 16 citado autoriza al organismo de supervisión "la realización de pruebas en laboratorios o entidades especializadas para acreditar el cumplimiento de determinados requisitos", añadiendo que "en este caso, los prestadores de servicios correrán con los gastos que ocasione esta evaluación". Se trata de una previsión especialmente relevante en caso de discrepancia, por ejemplo, sobre la consideración de determinados equipamientos del prestador como un sistema fiable o no, dada la complejidad y, consiguientemente, el elevado coste que dicha evaluación puede suponer.

Esta medida no se podrá tomar, como es lógico, en aquellos casos en que los productos se encuentren certificados por el órgano competente contra la norma técnica correspondiente, como ya hemos adelantado, siempre que la misma haya sido establecida por la Comisión Europea o, en su caso, en sede nacional, con el efecto presuntivo que ya conocemos[1200].

Se puede generar alguna duda acerca de las condiciones que deberán cumplir dichos laboratorios, pero las mismas son reconducibles al régimen general contenido en la legislación industrial, con la particularidad de que, en el caso de la evaluación de la seguridad de las tecnologías de la información, dichos laboratorios deberán encontrarse acreditados en el marco de dicho esquema[1201].

Desde una óptica más general y amplia que la de la estricta inspección, el artículo 18.1 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza prevé que "[l]os prestadores de servicios de confianza, la entidad nacional de acreditación, los organismos de evaluación de la conformidad, los organismos de certificación y cualquier otra persona o entidad relacionada con el prestador de servicios de confianza, tienen la obligación de facilitar al Ministerio de Energía, Turismo y Agenda Digital[1202] toda la información y colaboración precisas para el ejercicio de sus funciones", añadiendo a continuación que "[l]os prestadores de servicios de confianza deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.6 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa", pudiendo en sus inspecciones "ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas".

En este sentido, hay que traer a colación el artículo 18.1 de la LPAC, en el que se regula,

---

[1200] Cfr. los epígrafes 1.4.2, 4.1.3 (en la parte relativa a los dispositivos cualificados de creación de firma o sello), y 6.2.5, todos ellos de este trabajo.

[1201] En España, en el marco de la Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, que regula en su capítulo III los requisitos de acreditación de laboratorios. Los laboratorios actualmente acreditados se pueden ver en la página web del Organismo de Certificación del Centro Criptológico Nacional, en https://oc.ccn.cni.es/index.php?option=com_content&view=article&id=82&Itemid=81&lang=es.

[1202] Actualmente, el Ministerio de Economía y Empresa.

en el ámbito del procedimiento administrativo común, la colaboración de las personas[1203], aunque sólo en ausencia de Ley especial que la regule, impone a las personas –sean o no interesadas en el concreto procedimiento– el deber general de facilitar "a la Administración los informes, inspecciones y otros actos de investigación que requieran para el ejercicio de sus competencias, salvo que la revelación de la información solicitada por la Administración atentara contra el honor, la intimidad personal o familiar", entre otras excepciones, previsión que, aunque parece suponer una mejora en relación con el régimen legal anterior, no se encuentra exenta de polémica[1204].

El juego de las dos normas que acaban de presentar es diferente en función del sujeto del que se predique el deber de colaboración. En el caso de los sujetos mencionados en el artículo 18.1 del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, nos encontramos ante un régimen expresamente previsto por Ley, que constituye norma especial con respecto a la general contenida en el artículo 18.1 de la LPAC, por lo que ésta segunda no será aplicable; pero en el caso de otras personas a las que se requiera colaboración en relación con la aportación de información referida a un prestador, continuará siendo aplicable el régimen general de la LPAC.

Desde este punto de vista, es especialmente relevante notar que el régimen de la LPAC resulta más garante, al establecer las limitaciones legales ya apuntadas, que el del Anteproyecto, que no contiene límite ninguno. Parecería poco aceptable, en cualquier caso, una interpretación que excluyera la aplicación de los mencionados límites, dada la relevancia constitucional que éstos presentan.

Es, desde luego, preciso preguntarse hasta dónde alcanza este deber de colaboración de

---

[1203] (González Pérez & González Navarro, 2012, pág. 812), en relación con el artículo 39.1 de la LRJPAC, antecesor del artículo 18.1 de la LPAC, han caracterizado esta colaboración diciendo que "[e]stamos ante un *deber* –que es tal precisamente porque surge directamente de la Ley– y que se convierte en *obligación* de un individuo determinado, cada vez que la Administración pública necesite de ese apoyo del particular", fundamentado esta previsión tanto en la idea de solidaridad, pero también "en el interés general y, más concretamente, en la naturaleza vicarial –esto es, con vocación de servicio a ese interés general– que tiene aquélla", y que lleva a afirmar a dichos autores que ello incluye el caso "en que, además, el ciudadano investigado es el que ha de colaborar en esa investigación, porque, en la medida en que el resultado de esa investigación redunda en beneficio del sistema, a la larga redunda también en beneficio del investigado", posición que en mi opinión resulta limitada por los derechos fundamentales del investigado, en particular el de la tutela judicial efectiva. Estos autores, sin embargo, aprecian la inexistencia de infracción de obstrucción a la inspección cuando el investigado se limita a no decir la verdad (González Pérez & González Navarro, 2012, pág. 813).

[1204] Para (Carrillo Donaire, 2016, pág. 591) es preciso recordar que "[c]omo es sabido, los límites contemplados en el apdo. 1.º del artículo 18 de la LPAC cuentan con una regulación específica en la legislación de desarrollo de los derechos en él mencionados (honor, intimidad e imagen, respeto a la privacidad en el orden deontológico profesional, etc.), pero la enunciación del precepto legal no comprende toda la legislación concomitante que puede condicionar y limitar el ejercicio de este deber de colaboración, por lo que dicha relación no debe considerarse taxativa", señalando también que "tanto el Consejo de Estado como la Agencia Española de Protección de Datos, en los Informes evacuados en el curso de la tramitación del Anteproyecto de Ley, llamaron la atención sobre la conveniencia de explicitar como límite específico a este deber el derecho a la protección de datos, añadiendo –y esto nos parece de la mayor relevancia e igualmente extensible a las limitaciones que sí explicita el precepto y a las demás que puedan resultar aplicables– que sería igualmente preciso garantizar que se respete en todo caso el principio de proporcionalidad".

estos sujetos, y en especial del prestador de servicios[1205], dado que el mismo puede entrar en colisión con derechos fundamentales, tanto del prestador de servicios de confianza o de su personal, como, lo que es más importante, de las personas a las que ha ofrecido sus servicios el prestador en cuestión. Esta cuestión debe plantearse, además, desde una doble perspectiva, atendiendo a si el investigado es el propio prestador (situación que se encontrará sujeta al artículo 18.1 del Anteproyecto de Ley), o si, por el contrario, cualquier Administración Pública puede requerir a un prestador información acerca de una tercera persona, a la que se investiga en un procedimiento diferente (situación que entrará en el régimen del artículo 18.1 de la LPAC).

Por lo que se refiere a la primera perspectiva, parece evidente que el deber de colaboración encuentra un límite legal en el derecho a no incriminarse a sí mismo que asiste a las personas físicas a las que se solicite información, expresamente reconocido en relación con los servicios de confianza en diversas leyes nacionales, como la alemana[1206]. Aunque en la legislación española no se explicite esta posibilidad, debe entenderse que también existe, en aplicación de la legislación penal.

Aún dentro de esta primera perspectiva, relativa al ejercicio de la función de control –en su caso mediante la correspondiente actuación inspectora–, y también desde la segunda –en la que el investigado no es el prestador, sino un tercero–, resulta de la más absoluta importancia concretar hasta dónde puede llegar un requerimiento de información, dado que los servicios de confianza pueden contener datos reservados como, por ejemplo, los contenidos de un servicio de entrega electrónica certificada.

¿Podría, por ejemplo, el órgano de supervisión exigir a un prestador del servicio de entrega electrónica que le muestre las comunicaciones entre emisor y receptor, a los efectos de acreditar que presta correctamente el servicio? Más aún, ¿podría una Administración competente exigir a un prestador el acceso a las comunicaciones que, a su juicio, puedan tener relevancia en el ámbito de sus competencias?

Dada la definición legal de este servicio, que se dedica al aseguramiento de las comunicaciones electrónicas, parece que el servicio deberá garantizar el derecho constitucionalmente reconocido al secreto de las comunicaciones. En este caso, entiendo que esta solicitud de información se deberá tratar conforme a las previsiones de la Ley de Enjuiciamiento Criminal, requiriéndose, por tanto, mandamiento judicial para dichos accesos.

Asimismo, y como el Anteproyecto de Ley refiere, en el caso de acceso físico (o lógico) a las instalaciones del prestador, se deberá obtener el consentimiento del prestador, o bien el correspondiente mandamiento judicial, solución a la que se llegaría exactamente igual en aplicación del artículo 18.3 de la LPAC.

Además de lo expuesto, el epígrafe 3 del artículo 18 del Anteproyecto de Ley exige que "[a] más tardar el 1 de febrero de cada año, los prestadores cualificados de servicios de

[1205] (Rodríguez Ayuso, 2018, pág. 322 y ss.) considera aplicable a los prestadores de servicios de confianza las obligaciones de colaboración de los prestadores de servicios de la sociedad de la información que prestan servicios de intermediación, algo que a mi juicio puede resultar muy problemático, en especial en el caso del servicio de entrega electrónica.

[1206] Cfr. la sección § 5 (2) de la Ley alemana de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*.

confianza remitirán al Ministerio de Energía, Turismo y Agenda Digital[1207] un informe sobre sus datos de actividad del año civil precedente, con objeto de cumplimiento por parte de éste de las obligaciones de información a la Comisión Europea", estableciendo un deber general de reporte de los datos que en su momento se establezcan, debiendo al menos ser los necesarios para que el órgano de supervisión pueda, a su vez, informar de sus propias actividades a la Comisión[1208], según dispone el artículo 17.6 del Reglamento eIDAS, antes del 31 de marzo de cada año.

Finalmente, el artículo 17.4.j) del Reglamento eIDAS prevé que el organismo de supervisión tendrá la potestad de "requerir que los prestadores de servicios de confianza corrijan cualquier incumplimiento de los requisitos establecidos en el presente Reglamento", referida por tanto a ambas categorías de prestadores, y que debe entenderse extensiva a la corrección de cualquier incumplimiento de los requisitos que pueda establecer, de forma adicional o complementaria al Reglamento eIDAS, la ley nacional[1209].

El Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza otorga amplias, e indeterminadas, facultades al organismo de supervisión en su función de control, dado que, conforme a su artículo 15.2, "podrá acordar las medidas apropiadas para el cumplimiento del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, y de esta ley", pudiendo, además, "dictar directrices para la elaboración y comunicación de informes y documentos y para el cumplimiento de las obligaciones técnicas y de seguridad exigibles a los servicios de confianza".

Se trata de una previsión análoga a la contenida en otras legislaciones nacionales[1210], pero que no deja de llamar la atención por la extraordinaria amplitud que la misma presenta, y los posibles conflictos jurídicos que potencialmente puede generar un mal uso de la misma, dado que, en principio, el prestador de servicios de confianza que no cumpla con lo establecido en dichas directrices se encontrará en la necesidad de demostrar que, aun separándose de los criterios y recomendaciones incluidas en las mismas, cumple con lo establecido en la normativa legal.

Nos encontramos ante un potente instrumento de *soft law* público en sede nacional[1211], que concede un enorme poder al organismo de supervisión, aunque desde el mismo se encuentra, desde luego, limitado por el ordenamiento jurídico.

Dichos límites vienen referidos, en nuestra opinión, a lo establecido en las normas legales

---

[1207] Actualmente, el Ministerio de Economía y Empresa.

[1208] Nótese que, conforme al epígrafe 8 del artículo 17 del Reglamento eIDAS, "[l]a Comisión podrá, mediante actos de ejecución, definir los formatos y procedimientos relativos al informe a que se refiere el apartado 6", actos de ejecución que "se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2"; de modo que el contenido exigible al Estado miembro marcará el correlativo exigible a los prestadores de servicios de confianza.

[1209] Previsión que debería recogerse en dicha ley nacional, como sucede en el borrador de Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza, artículo 17.1.

[1210] Como, por ejemplo, se puede ver en la sección § 4 (2) de la Ley alemana de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017).

[1211] Cfr. (Sarmiento, 2008).

y reglamentarias; en las normas técnicas que hayan sido establecidas por la Comisión Europea, por su valor de presunción de cumplimiento de los requisitos legales[1212]; en las normas que eventualmente haya establecido el propio organismo de supervisión u otro organismo nacional, caso que en la ley nacional se haya previsto su valor presuntivo; las normas referenciadas –aun sin valor de presunción– por el organismo de supervisión; y en las directrices anteriormente dictadas por el organismo de supervisión, que, en la medida que suponen una interpretación de los requisitos legales, deben ser de publicación, como parte de las obligaciones de publicidad activa, al igual que las respuestas a consultas planteadas por los prestadores de servicios de confianza y otros particulares[1213], aunque el Anteproyecto no lo indique expresamente[1214].

No hace falta decir que, como es lógico, en la medida en que una sanción basada en una directriz sea anulada en sede judicial, por considerarse la interpretación del organismo de supervisión contraria a Derecho, dicha directriz no podrá seguir siendo aplicada, por lo cual las citadas Sentencias deberían también ser objeto de publicación.

7.2.2 La retirada de la cualificación

El artículo 17.4.g) del Reglamento eIDAS también prevé, entre las funciones del organismo del supervisor, la retirada de la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan, la cual se realizará en los términos previstos en el artículo 20 de Reglamento eIDAS[1215].

En este caso, dispone el artículo 20.3 del Reglamento eIDAS que "[c]uando el organismo de supervisión requiera a un prestador cualificado de servicios de confianza que corrija el incumplimiento de requisitos del presente Reglamento y este prestador no actúe en consecuencia, en su caso, en el plazo fijado por el organismo de supervisión, el organismo de supervisión, teniendo en cuenta en particular el alcance, la duración y las consecuencias de este incumplimiento, podrá retirar la cualificación al prestador o al servicio que este presta".

La retirada de la cualificación se configura como la principal consecuencia jurídica del incumplimiento de los requisitos del Reglamento eIDAS por parte de un prestador, y dado su carácter de autorización administrativa, de la misma se desprende que el prestador no podrá seguir ofreciendo el servicio cualificado, sin perjuicio de que pueda ofrecerlo en su modalidad no cualificada.

Dada la dicción literal del Reglamento eIDAS, en caso de que la ley nacional establezca requisitos adicionales o complementarios a los servicios cualificados de confianza tipificados en el Reglamento eIDAS, se deberá prever en dicha ley que el incumplimiento de los citados requisitos también será causa de eventual retirada de la cualificación[1216],

---

[1212] Cfr. el epígrafe 1.4.2 de este trabajo.

[1213] Así se dispone en el artículo 7.a) de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

[1214] Dado que dicha omisión no puede desplazar a la aplicación de la Ley 19/2013.

[1215] Aunque el artículo 17.4.g) del Reglamento se refiere también al artículo 21, el mismo sólo resulta aplicable a la concesión inicial de la cualificación, no a la retirada de la misma.

[1216] No es el caso del Anteproyecto español, pero sí de leyes como la alemana, como se desprende de la sección § 5 (2) de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por

dado que en otro caso se podría dar la circunstancia de que un prestador pudiera mantener la cualificación aun incumpliendo los requisitos nacionales[1217].

No es preciso resaltar la afectación extraordinariamente negativa que la retirada de la cualificación supone para el negocio del prestador de servicios de confianza –por ejemplo, en términos de su reputación y de la posible pérdida de valor en su marca en el mercado–, así como en sus clientes, en especial dado que el cambio de un servicio cualificado a un servicio sin cualificación implica la inaplicación de los efectos jurídicos, sustantivos o procesales, que se hayan establecido en relación con los correspondientes servicios o, de forma más precisa, con las pruebas electrónicas sustentadas en los mismos; nos estamos refiriendo a que una firma electrónica ya no goce del efecto directo de equivalencia con la firma escrita, o que un sello de tiempo ya no disfrute de la presunción de la fecha y hora, por citar sólo dos ejemplos.

Por ello, la potestad de retirada de la cualificación deviene la principal herramienta del organismo de supervisión en orden a incentivar a los prestadores al cumplimiento de los requisitos del Reglamento eIDAS, posiblemente más flexible y eficaz que la aplicación del régimen sancionador[1218], en el cual no se inserta, dado que la pérdida de la cualificación no tiene carácter sancionador.

Sin perjuicio de lo que se acaba de señalar, el ejercicio de esta potestad –que no puede considerarse absolutamente discrecional– deberá, en nuestra opinión, sustanciarse a través del correspondiente procedimiento administrativo formalizado[1219], dados los evidentes efectos perjudiciales que dicha actuación provocará en el prestador afectado, y, en particular –como menciona el propio artículo 20.3 del Reglamento eIDAS, que refiere a los parámetros de alcance, duración y consecuencias del incumplimiento– con aplicación del principio de proporcionalidad de la medida, no debiendo aplicarse en caso de todo incumplimiento, sino de aquellos incumplimientos que presenten una entidad suficiente, o que supongan riesgos para los usuarios, circunstancias que deben ser acreditadas, de la forma más objetiva suficiente por el organismo de supervisión, a los efectos de la ineludible motivación de la resolución que acuerde la retirada de la cualificación[1220].

En este sentido, se trata de un procedimiento que iniciará el órgano de supervisión, de

artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017), que extiende la aplicación de las medidas previstas en el artículo 17.4 del Reglamento eIDAS al cumplimiento de los requisitos nacionales, a todos los prestadores, con y sin cualificación.

[1217] Lo cual sólo podría corregirse mediante la aplicación del correspondiente régimen sancionador.

[1218] El artículo 17.2 del borrador de Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza indica que "[l]a revocación de la cualificación a un prestador o a un servicio mediante su retirada de la lista de confianza es independiente de la aplicación del régimen sancionador".

[1219] Resultando aplicable la regulación común contenida en la LPAC, inclusive la tramitación simplificada, por razón de interés público, que fácilmente se puede acreditar debido a los potentes efectos jurídicos en relación con la prueba electrónica que presentan los servicios cualificados de confianza.

[1220] Cfr. el artículo 35.1 de la LPAC, numerales a) e i), así como, eventualmente, numeral c).

oficio[1221] o por denuncia[1222], por lo que debe realizarse mención especial a la notificación[1223] de la correspondiente resolución de inicio del procedimiento, en la que se deberá indicar el supuesto incumplimiento, con al menos explicación de los indicios y argumentos jurídicos que sustentan este supuesto incumplimiento, y se concederá plazo para su corrección, así como para la realización de las alegaciones correspondientes.

Como en todo procedimiento, al objeto de evitar la indefensión del prestador cualificado, hay que entender que el mismo podrá intentar justificar la inexistencia del incumplimiento alegado, y que asimismo se deberá proceder a la correspondiente práctica de prueba, conforme a las reglas generales previstas en la LPAC, y las especialidades contenidas en el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza relativos a las actuaciones inspectoras, que ya analizamos con ocasión del procedimiento de concesión de la cualificación[1224].

También en la fase de instrucción, y a los efectos de la prueba, debe recordarse en este momento la posibilidad de que el organismo de supervisión acuda a las vías de colaboración con otros organismos de supervisión, al objeto de acreditar algún extremo concreto, que posiblemente se incorpore al procedimiento en forma de informe.

Procede, como no puede ser de otra forma, conceder trámite de audiencia previa a la resolución, para que el prestador pueda alegar lo que convenga a su derecho y, posteriormente, se dictará y notificará[1225] la oportuna resolución, siempre que el procedimiento no finalice –y en muchos casos sería así– mediante el cumplimiento por el prestador de las instrucciones del organismo de supervisión[1226].

Conforme a lo dispuesto en el artículo 20.3 del Reglamento eIDAS, una vez notificada la resolución administrativa acordando la retirada de la cualificación, que será inmediatamente ejecutiva[1227], el organismo de supervisión deberá "informar al organismo a que se refiere el artículo 22, apartado 3, a efectos de que se actualice la lista de confianza mencionada en el artículo 22, apartado 1", momento desde el que se entenderá materialmente ejecutada la resolución de retirada de la cualificación.

[1221] Dentro de esta posibilidad hay que incluir la petición de asistencia por parte de otro organismo de supervisión.

[1222] Por ejemplo, por parte de un usuario de un servicio de confianza que estime que el prestador ha incumplido sus obligaciones legales o contractuales.

[1223] Esta notificación normalmente será efectuada electrónicamente, dado que el prestador de servicios de confianza es, de forma habitual, una persona jurídica, pero en el caso de tratarse de una persona física –que de momento no se ha dado en España– la notificación deberá realizarse en papel, dado que no existe norma jurídica que imponga el medio de comunicación exclusivamente electrónica de los procedimientos administrativos de los prestadores de servicios de confianza con la Administración.

[1224] Cfr. el epígrafe 7.1.2.2 de este trabajo.

[1225] Conforme al mismo artículo 20.3 del Reglamento eIDAS, "[e]l organismo de supervisión comunicará al prestador cualificado de servicios de confianza la retirada de su cualificación o de la cualificación del servicio de que se trate", lo cual refuerza la exigencia de la notificación de la resolución.

[1226] Seguramente en este caso se podría acudir a una terminación convencional del procedimiento abierto, conforme al artículo 86 de la LPAC, en especial en caso de que se pacte el cumplimiento de instrucciones consensuadas con el organismo de supervisión, o a la declaración de caducidad, caso que el prestador simplemente decida adoptar las instrucciones inicialmente exigidas.

[1227] Dada la naturaleza no sancionadora de la retirada de la cualificación, a menos que la misma se suspenda, conforme al artículo 98 de la LPAC, será ejecutiva.

Finamente, frente a la resolución cabrá la presentación del correspondiente recurso administrativo, conforme al régimen general, que no presenta especialidades dignas de mención.

7.2.3 Otras medidas tendentes a garantizar la eficacia de la supervisión

Como acabamos de ver, en el caso de los prestadores cualificados de servicios de confianza, el organismo de supervisión dispone del mecanismo de la (amenaza de) retirada de la cualificación como herramienta para garantizar el cumplimiento de sus obligaciones por parte de estos prestadores.

En el caso de los prestadores de servicios de confianza sin cualificación, el artículo 17.3.b) del Reglamento eIDAS prevé que el organismo de supervisión tendrá la función de "adoptar medidas, en caso necesario, en relación con los prestadores no cualificados de servicios de confianza […] mediante actividades de supervisión posteriores".

Más allá del régimen sancionador, al que inmediatamente nos referiremos, el Reglamento eIDAS no prevé ninguna medida al respeto, por lo que las mismas deberían ser establecidas por la normativa nacional, ciertamente centradas en relación con las obligaciones que se imponen a estos prestadores, que son menores que en relación con los prestadores cualificados, pero no por ellos menos relevantes, incluyendo, como hemos estudiado anteriormente[1228], obligaciones relativas a la protección de datos, la accesibilidad y, en especial, la seguridad.

Dejando aparte la protección de datos, cuya normativa específica resulta suficiente para garantizar el cumplimiento, sin necesidad de que la legislación de servicios de confianza establezca nada al respecto, y de la accesibilidad, que, lamentablemente, casi no puede considerarse ni una verdadera obligación, en lo relativo a la seguridad podría ser conveniente establecer alguna medida de supervisión.

A título de ejemplo, la legislación alemana[1229] ha previsto, en relación con todos los prestadores, cualificados y sin cualificación, que el organismo de supervisión pueda imponer una prohibición de prestación del servicio, temporal, parcial o total, si aprecia que las medidas que ordene conforme al artículo 17.4.j) del Reglamento eIDAS no garantizan el cumplimiento, o si los hechos permiten presumir que el prestador no cumple con sus obligaciones, previstas en el Reglamento eIDAS o en la normativa nacional. Es cierto que la prohibición permanente y absoluta de operar se justifica, en la memoria explicativa de la Ley, mediante la conexión de los artículos 17.4.j) y 16 del Reglamento eIDAS, por lo que se podría considerar como una modalidad específica de sanción, no parece recibir el mismo tratamiento la prohibición temporal, aunque se podría reconducir al campo de las medidas cautelares para mayor seguridad jurídica.

[1228] Cfr. el epígrafe 6.1 de este trabajo.

[1229] Cfr. la sección § 4 (3) de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017).

7.3 EL RÉGIMEN ADMINISTRATIVO SANCIONADOR VINCULADO A LA PRESTACIÓN DE SERVICIOS DE CONFIANZA

Resulta habitual que en la regulación del ejercicio de las actividades económicas se establezca un régimen sancionador, al objeto de corregir las conductas que supongan infracción de las obligaciones y prohibiciones que se hayan establecido.

La prestación de servicios de confianza no es excepción a lo que se acaba de decir, y, al respecto, el artículo 16 del Reglamento eIDAS ordena que "los Estados miembros establecerán normas relativas a las sanciones aplicables a las infracciones del presente Reglamento", sanciones que deberán ser "eficaces, proporcionadas y disuasorias".

En cumplimiento de este mandato, que resulta novedoso en relación con la DFE –que no lo contenía– y ampliando el régimen ya establecido en la LFE y, anteriormente, en el RDLFE[1230], el Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza establece, en su título V, el régimen legal de infracciones y sanciones aplicable a la prestación de los servicios de confianza.

En primer lugar, el artículo 19.1 del Anteproyecto de Ley clasifica las infracciones del Reglamento eIDAS y de la propia Ley española en leves, graves y muy graves, modelo procedente de la LFE[1231], y recogido con carácter general en el artículo 27.1 de la LRJSP.

Conviene, antes de entrar en el análisis de las diferentes conductas potencialmente infractoras, al efecto de valorar la consecuencia sancionadora correspondiente, avanzar que, conforme al artículo 20.1 del Anteproyecto de Ley, "[p]or la comisión de infracciones recogidas en el artículo anterior, se impondrán al infractor las siguientes sanciones: a) Por la comisión de infracciones muy graves, una multa por importe de 150.001 hasta 300.000 euros. b) Por la comisión de infracciones graves, una multa por importe de 50.001 hasta 150.000 euros. c) Por la comisión de infracciones leves, una multa por importe de 5.000 hasta 50.000 euros", cantidades que podrán ser objeto de graduación en función de determinados criterios[1232] alineados con lo establecido en el

---

[1230] Para (Madrid Parra, 2001, pág. 227), la existencia de un régimen sancionador afecta negativamente al principio de libre competencia previsto en la normativa vigente, considerando que "resulta excesivo que haya obligaciones estrictamente jurídico-privadas que sean objeto de sanción administrativa. Parece que el funcionamiento del mercado (sin convertir a éste en axioma indiscutible) podría resolver la necesidad de eficiencia y los conflictos de interés en el ámbito de las relaciones jurídico-privadas sin necesidad de intervención administrativa", remitiendo al resarcimiento de los daños y perjuicios derivados del incumplimiento de las obligaciones de los prestadores, al ser "cuestiones que afectan fundamentalmente a intereses jurídico-privados", a lo que añade que "el incumplimiento en dichas materias, más que constituir el supuesto de hecho de una infracción administrativa sujeta al Derecho Administrativo sancionador, debe ser objeto de composición de intereses en el ámbito jurídico-privado", posición que no comparto, por los motivos que he expuesto en el epígrafe 1.3.2 de este trabajo.

[1231] Cfr. el artículo 31.1 de la LFE, cuya única diferencia es, lógicamente, no referirse al Reglamento eIDAS, que no existía.

[1232] Estos criterios se recogen en el artículo 20.2 del Anteproyecto de Ley, y son los siguientes: "a) El grado de culpabilidad o la existencia de intencionalidad. b) La continuidad o persistencia en la conducta infractora. c) La naturaleza y cuantía de los perjuicios causados. d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa. e) Volumen de la facturación del prestador responsable. f) Número de personas afectadas por la infracción. g) Gravedad del riesgo generado por la conducta o persistencia del mismo. h) Las acciones realizadas por el prestador encaminadas a paliar los efectos o consecuencias de la infracción".

artículo 29.3 de la LPAC.

Nótese que, con respecto a la LFE, el importe máximo de la sanción por infracción muy grave se reduce de 600.000 a 300.000 euros, pero que, en cambio, se eleva el importe mínimo de la sanción por infracción grave desde 30.001 a 50.001 euros; y que asimismo se establece un importe mínimo de 5.000 euros por la comisión de una infracción leve, elevándose también el máximo hasta 50.000 euros. Como se verá del análisis del catálogo de infracciones, ello implica realmente un incremento de la presión sancionadora, y no al contrario.

Mientras que, en el caso de las infracciones leves y graves, se contiene un catálogo de conductas concretas, en el caso de las infracciones muy graves, las mismas se caracterizan a partir de una infracción grave "cuando, como consecuencia de ella, se hayan causado daños graves constatables a usuarios concretos o la seguridad de los servicios de confianza se haya visto gravemente afectada", conforme dispone el apartado 2 del citado artículo. Se trata de un enfoque ya contenido en el artículo 31.2 de la LFE para la expedición de certificados reconocidos, debiéndose notar que en el mismo artículo también se consideraba infracción muy grave "[l]a expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor", conducta que ha pasado a ser infracción grave.

La dificultad que plantea este enfoque, tanto en la LFE como en el Anteproyecto de Ley, es el establecimiento de criterios que permitan determinar, de la forma más objetiva posible, qué se considera un daño grave a un usuario concreto, o una afectación grave a la seguridad de los servicios de confianza.

Un posible problema que plantea este enfoque es la cualificación de la gravedad de un daño con respecto a un usuario concreto, ya que una pérdida patrimonial –derivada, claro, de una conducta que se pueda considerar, al menos, como una infracción grave– puede ser económicamente poco grave para una persona de renta económica alta, pero muy gravosa para una persona de renta baja. El principio de seguridad jurídica exige la previsibilidad de las consecuencias de las conductas en que pueda eventualmente incurrir el prestador, algo que no ocurriría en el caso descrito, motivo por el que cabe insistir en la necesidad de objetivar la gravedad, dado que eleva la categoría de infracción de grave a muy grave.

Por otra parte, podría perfectamente darse el caso de que la afectación grave a la seguridad de los servicios de confianza se produzca con independencia total de la actuación o falta de actuación del prestador del servicio, como por ejemplo en el caso del descubrimiento de una vulnerabilidad a un algoritmo empleado en el servicio de confianza que haya sido implementado en los equipos criptográficos del prestador, que se encuentran certificados como seguros, y que resulta indetectable para el prestador hasta que se publica la misma, como ha sucedido en el caso conocido como ROCA[1233], que permitía obtener los datos de creación de firma electrónica cualificada a partir de los datos de verificación de firma electrónica.

Parece excesivo considerar, en estos casos, que el prestador haya cometido infracción

[1233] ROCA es el acrónimo inglés de la vulnerabilidad conocida como el Retorno del Ataque de Coppersmith. Cfr. https://crocs.fi.muni.cz/public/papers/rsa_ccs17 y (Nemec, Sys, Svenda, Klinec, & Matyas, 2017).

alguna, al menos antes de que la vulnerabilidad sea conocida, porque desde ese momento sí que deberá actuar diligentemente para resolver el problema de seguridad. De otro modo, estaríamos objetivando el modelo de responsabilidad de corte subjetivo, aunque incorpore un elevado nivel de diligencia. Y lo estamos haciendo a los efectos de imponer una sanción pecuniaria que, en la banda baja, parte de 150.001 euros, algo que podría ser disuasorio, desde luego, pero no en relación con la posible comisión de la infracción, sino con respecto a la prestación del servicio por parte de prestadores en España, en especial si en otros Estados de la Unión Europea se establecen modelos con menores cantidades.

Antes de entrar en el catálogo de conductas que se consideran infracción, es preciso indicar que algunas conductas podrían encontrarse también tipificadas en otras normas. Así sucede, en especial, en los casos de la protección de los datos de carácter personal o de la accesibilidad, que serán tipificadas en su propia normativa, y que pueden resultar en una doble sanción por concurso medial de infracciones, en una afectación clara al principio *non bis in ídem*, recogido actualmente –en materia de potestad sancionadora– en el artículo 29.5, en cuya virtud "[c]uando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida".

Esto no sucede en todos los casos, por supuesto, pero resulta importante porque, como ya hemos analizado[1234], los prestadores de servicios de confianza tratan en muchos casos con datos de carácter personal, de modo que una conducta podría ser considerada infracción en la legislación de servicios de confianza y en la de protección de datos, como por ejemplo en el caso de divulgación de los datos de creación de firma electrónica, que son indudablemente datos de carácter personal.

El apartado 3 del artículo 19 del Anteproyecto de Ley contiene el catálogo de infracciones graves, que analizamos a continuación. En primer lugar, veremos las infracciones que pueden cometer todos los prestadores, con independencia de los servicios que presten, y posteriormente analizaremos las infracciones relativas a servicios de confianza concretos.

En primer lugar, conforme al numeral a) del artículo 19.3 del Anteproyecto de Ley, constituye infracción grave "[l]a resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley", previsión claramente orientada a garantizar la eficacia de la inspección[1235], a la que nos hemos referido anteriormente como potestad asociada al contenido de la supervisión[1236], y que no merece mayor comentario que diferenciar esta conducta de la negativa a la colaboración que, como veremos inmediatamente, es tipificada como infracción leve.

En segundo lugar, también se considera infracción grave, a tenor del numeral b) del artículo 19.3 del Anteproyecto de Ley, "[a]ctuar en el mercado como prestador cualificado de servicios de confianza, ofrecer servicios de confianza como cualificados o utilizar la etiqueta de confianza «UE» como prestador de servicios de confianza cualificados sin haber obtenido la cualificación de los citados servicios", previsión que

[1234] Cfr. el epígrafe 6.1.1 de este trabajo.

[1235] Esta conducta ya se encontraba prevista como infracción grave en el artículo 31.3.f) de la LFE.

[1236] Cfr. el epígrafe 7.2.1 de este trabajo.

resulta novedosa con respecto a la LFE[1237] y que cabe entender absolutamente razonable en atención a los efectos jurídicos que se otorgan a los servicios de confianza, muy especialmente desde la óptica de la presunción de autenticidad que reciben, y que es determinante en sede procesal para invertir la carga de la prueba.

El tipo se integra por tres conductas diferentes, relacionadas entre ellas por la confusión que generan en los usuarios de los servicios, que creen disponer de pruebas electrónicas con una eficacia que, en realidad, no es tal; lo cual defrauda la confianza que se deposita en las mismas y, por tanto, en los procesos que las incorporan.

La primera conducta sería aquella en que un prestador, sin cualificación, se presenta como un prestador cualificado en infracción de lo establecido en los artículos 21 y 22 del Reglamento eIDAS, lo que sucederá en el caso de que no tenga ningún servicio cualificado. La segunda conducta podrá darse especialmente cuando un prestador cualificado para un servicio concreto ofrezca otro servicio como si fuera cualificado, como por ejemplo si se encuentra cualificado para expedir certificados cualificados, pero presenta su servicio de entrega electrónica certificada como cualificado, dado que ello supone, de nuevo, la infracción de lo establecido en los artículos 21 y 22 del Reglamento eIDAS. Finalmente, la tercera conducta resulta instrumental con respecto a las dos primeras, dado que el uso de la etiqueta en cuestión es el medio habitual de presentar un servicio como cualificado, por lo que su utilización irregular constituye una infracción del artículo 23 del Reglamento eIDAS.

En tercer lugar, el numeral d) del artículo 19.3 del Anteproyecto de Ley considera como infracción grave "[n]o proteger adecuadamente los datos de creación de firma, de sello o de autenticación de sitio web cuya gestión se le haya encomendado en la forma establecida en el artículo 9.1 b)", conducta encuadrable en las relativas a la ausencia de las necesarias medidas de seguridad por cualquier prestador que ofrezca esta posibilidad, cuya tipificación específica parece muestra de la preocupación que le causa al legislador la misma.

En cuarto lugar, determina el numeral e) del artículo 19.3 del Anteproyecto de Ley, que constituye infracción grave "[n]o notificar, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, al Ministerio de Energía, Turismo y Agenda Digital[1238] cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado, salvo que sólo afecte a los datos personales tratados por el prestador, o no ampliar la información notificada, según lo dispuesto en el artículo 14.3", conducta que se correspondería con el incumplimiento de la obligación prevista en el artículo 19.2 del Reglamento eIDAS, que ya hemos estudiado anteriormente[1239], aunque no coinciden los destinatarios de dichas notificaciones.

En efecto, el artículo 19.2 del Reglamento eIDAS ordena que la notificación se dirija también, "en caso pertinente, a otros organismos relevantes, como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos" y, en cambio, conforme al artículo 19.3.e) del Anteproyecto de Ley precisamente

---

[1237] Lógicamente, dado que en la LFE el modelo era de supervisión *a posteriori*, sin necesidad de obtener ningún reconocimiento o licencia previos para el acceso al mercado.

[1238] En la actualidad, es el Ministerio de Economía y Empresa.

[1239] Cfr. el epígrafe 6.1.3 de este trabajo.

no tipifica como infracción el no comunicar al órgano de supervisión la incidencia cuando la misma se refiera de forma exclusiva a los datos personales, seguramente para evitar el concurso de infracciones a que antes nos hemos referido. La ausencia de notificación, cuando únicamente afecte a datos de carácter personal, podrá ser considerada infracción por la normativa de protección de datos –significativamente, el nuevo RGPD– y sancionada conforme a la misma, pudiendo suponer un monto superior al previsto para los servicios de confianza.

Diferente sería el caso de la ausencia de notificación de incidencias al "organismo nacional competente en materia de seguridad de la información", que aun constituyendo una infracción de la obligación contenida en el artículo 19.2 del Reglamento eIDAS, tampoco se tipifica como infracción. Quizá ello sea así porque no es claro que en España exista actualmente dicho organismo nacional, sin perjuicio de las competencias del Centro Criptológico Nacional al amparo del Real Decreto 421/2004, de 12 de marzo.

En quinto lugar, el numeral f) del artículo 19.3 del Anteproyecto de Ley tipifica como infracción grave, "[c]uando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, no notificar también a la persona física o jurídica, sin demora indebida, la violación de seguridad o la pérdida de integridad", de nuevo en atención a que dicha conducta supone una infracción de la obligación prevista en el artículo 19.2 del Reglamento eIDAS.

En ambos casos, y como ya se dijo con ocasión del análisis de esta obligación, resultará clave poder determinar qué constituye un impacto significativo, en especial en el caso de un servicio no cualificado, dado que la cuantía mínima de la sanción asciende a la importante cantidad de 50.001 euros, asumiendo que se aplique lo previsto en el artículo 29.5 de la LRJSP, porque en caso contrario nos encontraremos ante una sanción mínima del doble.

En sexto lugar, y también en relación con la seguridad del sistema, el numeral i) del artículo 19.3 del Anteproyecto de Ley considera infracción grave "[l]a demostración de una notoria falta de interés en la resolución de los incidentes de seguridad en los productos, redes y sistemas de información", conducta que en especial se podrá dar frente a los requerimientos realizados por el órgano de supervisión derivados de una previa notificación de dicha incidencia.

En séptimo lugar, el numeral g) del artículo 19.3 del Anteproyecto de Ley considera infracción grave "[e]n caso de prestadores cualificados de servicios de confianza, el incumplimiento de alguna de las obligaciones establecidas en los artículos 24.2, letras b), c), d), e), f), g), h), y k) […] del Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, con las precisiones establecidas, en su caso, por esta ley"; esto es, prácticamente todas las obligaciones comunes que les impone el Reglamento eIDAS como tales prestadores, y a las que nos hemos referido en su momento[1240], quedando sólo exceptuadas las obligaciones de informar al órgano de supervisión de los cambios que realicen en la prestación del servicio, y de su intención de cesar en la actividad, así como en la disposición de un plan de cese.

En octavo lugar, y ya en relación con el servicio de expedición de certificados, el numeral c) del artículo 19.3 del Anteproyecto de Ley considera infracción grave, la conducta del prestador que expida certificados consistente en "almacenar o copiar, por sí o a través de

[1240] Cfr. el epígrafe 6.2 de este trabajo.

un tercero, los datos de creación de firma o sello de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante o del creador del sello"; tipificación que persigue que el prestador de servicios de expedición de certificados que genera las claves de firma o sello no pueda almacenarlas ni copiarlas excepto en caso de gestión de las mismas por cuenta del titular de las mismas, con independencia de que se trata de un prestador cualificado o no.

Se trata de una redacción que resulta criticable, porque el Reglamento eIDAS y el Anteproyecto de Ley, como ya sabemos[1241], permiten que la generación y gestión de datos de creación de firma electrónica cualificada o de sello electrónico cualificado pueda correr a cargo de cualquier prestador de servicios de confianza cualificado, y lo mismo puede ocurrir con la firma electrónica avanzada o el sello electrónico avanzado – donde ni siquiera es precisa la condición de emplear un prestador cualificado –, por lo que se debería haber extendido la posibilidad de comisión de esta infracción a cualquier persona que generase estas claves.

De otro modo, simplemente debe entenderse que el almacenamiento o copiado de claves por cualquier persona diferente del prestador del servicio que expidió el certificado, o de un tercero que actúe por su cuenta, no será ninguna infracción.

En noveno lugar, también en relación con la expedición de certificados cualificados, el ya analizado numeral g) del artículo 19.3 del Anteproyecto de Ley recoge como infracción grave "el incumplimiento de alguna de las obligaciones establecidas en los artículos […] 24.3 y 24.4 del Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, con las precisiones establecidas, en su caso, por esta ley", que ya conocemos[1242], mientras que el numeral h) del mismo artículo 19.3 del Anteproyecto de Ley considera infracción grave "[l]a expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado, o al poder de representación de quien lo solicita en su nombre señaladas en el Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, y en esta ley, cuando ello afecte a la mayoría de los certificados cualificados expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor"[1243].

Por su parte, el apartado 4 del artículo 19 del Anteproyecto de Ley contiene el catálogo de infracciones leves, que analizamos a continuación. En primer lugar, veremos las infracciones que pueden cometer todos los prestadores, con independencia de los servicios que presten, y posteriormente analizaremos las infracciones relativas a prestadores y servicios de confianza concretos.

Constituyen infracción leve, con carácter general, las conductas consistentes en "[n]o publicar información veraz y acorde con esta ley y el Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014" (numeral a) del artículo 19.4 del Anteproyecto de Ley), infracción de dicción muy amplia que podría resultar problemática porque podría entrar en concurso con, por ejemplo, la normativa de consumo, aunque no en todos los casos ésta última resultará aplicable, debiéndonos

[1241] Cfr. el epígrafe 4.1.2 de este trabajo.

[1242] Cfr. el epígrafe 2.1.2.3 de este trabajo.

[1243] Cfr. el epígrafe 2.1.2.2 de este trabajo.

remitir a lo que en su momento dijimos en relación con esta cuestión[1244]; en "[n]o comunicar el inicio de actividad, su modificación o cese por los prestadores de servicios no cualificados en el plazo establecido en el artículo 13" (numeral b) del artículo 19.4 del Anteproyecto de Ley), correlato de la obligación a la que en su momento nos hemos referido[1245], y en "[l]a ausencia de contestación a requerimientos de información por parte del Ministerio de Energía, Turismo y Agenda Digital[1246], por dos veces" (numeral g) del artículo 19.4 del Anteproyecto de Ley), conductas que se extienden a todos los prestadores a los efectos de facilitar su control por parte del órgano de supervisión en relación con todos ellos, que requieren de su colaboración[1247].

En segundo lugar, también constituye infracción leve "[e]l incumplimiento por los prestadores cualificados de servicios de confianza de alguna de las obligaciones establecidas en el artículo 24.2, letras a) e i) del Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014" (numeral c) del artículo 19.4 del Anteproyecto de Ley), así como "[e]l incumplimiento por los prestadores cualificados de servicios de confianza de su obligación de remitir un informe anual de actividad al Ministerio de Energía, Turismo y Agenda Digital antes del 1 de febrero de cada año" (numeral f) del artículo 19.4 del Anteproyecto de Ley).

Se trata de conductas reprochables a prestadores cualificados, pero que el legislador no considera tan graves como en otros casos anteriormente analizados. En el primer caso, sin embargo, aunque en efecto parece que no informar acerca de cualquier cambio en la prestación del servicio cualificado no tiene porqué ser una conducta especialmente grave, en cambio sorprende que no informar acerca de la intención de cesar en la actividad (artículo 24.2.a) *in fine* del Reglamento eIDAS) no se considere particularmente grave; y más aún llama la atención que tampoco se considere grave no disponer del plan de cese en el servicio, a tenor de la relevancia que esta circunstancia tiene en relación con el mantenimiento del valor de las pruebas electrónicas, como ya sabemos[1248].

Menos gravosa parece, por otra parte, que el prestador cualificado deje de presentar su informe de actividades anuales al órgano de supervisión[1249], dado el nulo impacto que dicha conducta produce sobre la prueba electrónica.

En tercer lugar, se tipifican como infracción leve dos conductas específicas del servicio de expedición de certificados cualificados, como son "[n]o colaborar con otros prestadores cualificados para determinar la fecha de la última personación de la persona física firmante o solicitante del sello o de empleo de un medio equivalente de identificación aceptado, cuando su colaboración sea necesaria" (numeral d) del artículo 19.4 del Anteproyecto) y "[e]n caso de prestadores que expidan certificados cualificados de sello electrónico, no registrar la información a la que se refiere el artículo 9.3.a)" (numeral e) del artículo 19.4 del Anteproyecto); esto es, "la información que permita

---

[1244] Cfr. el epígrafe 6.1.4 de este trabajo.

[1245] Cfr. el epígrafe 7.1.3 de este trabajo.

[1246] En la actualidad, el Ministerio de Economía y Empresa.

[1247] Cfr. el epígrafe 7.2.1 de este trabajo.

[1248] Cfr. el epígrafe 6.2.8 de este trabajo.

[1249] Cfr. el epígrafe 7.2.1 de este trabajo.

determinar la identidad de la persona física a la que se hayan entregado los citados certificados, para su identificación en procedimientos judiciales o administrativos", correlativas de las obligaciones a que ya nos hemos referido[1250], y que no exigen mayor comentario.

Como reflexión general, y en atención al número de conductas que se tipifican como infracción grave –que pueden pasar a ser muy graves en función de los parámetros que ya conocemos– y de la cuantía de la correspondiente sanción, podemos considerar que nos encontramos ante un régimen sancionador ciertamente duro, dado que la mayoría de infracciones llevan aparejada multa de entre 50.001 euros y 150.000 euros, en función de la aplicación de los criterios de graduación, en especial si se compara con la normativa de otros Estados miembros.

Así, la ley alemana[1251] establece sanciones máximas de 20.000 euros en relación con todas las infracciones del Reglamento eIDAS y de las normas contenidas en la propia ley, excepto en cuatro casos[1252], en que se eleva al máximo de 100.000 euros.

Por su parte, la ley austríaca[1253] impone sanciones máximas de entre 10.000 y 20.000 euros, en función de la infracción, con la excepción de una sanción máxima de 37.000 euros reservada a la infracción consistente en no notificar cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes, y sólo en caso de que el prestador sea cualificado.

Como nota curiosa, la ley austríaca tipifica como infracción que cualquier persona haga un uso indebido de los datos de creación de firma electrónica o sello electrónico sin el conocimiento o contra la voluntad del firmante o creador de sellos, conducta que lleva aparejada la sanción de multa de hasta 5.000 euros.

La ley belga adopta un enfoque diferente, al sancionar penalmente, y no por la vía administrativa, determinadas conductas graves[1254], con la pena de nivel 5; esto es, multa de 250 a 100.000 euros y prisión de un mes a un año, o una sola de ellas[1255].

[1250] Cfr. el epígrafe 2.1.2.2 de este trabajo.

[1251] Cfr. la sección § 19 (3) de la Ley de Servicios de Confianza – *Vertrauensdienstegesetz (VDG)*, promulgada por artículo 1 de la Ley para implementar el Reglamento eIDAS (*eIDAS-Durchführungsgesetz*), de 18 de julio de 2017.

[1252] Incluyendo no disponer de aseguramiento, o que el mismo sea insuficiente, no emplear o emplear incorrectamente sistemas o productos fiables, no tomar medidas adecuadas contra la falsificación y el robo de datos, o no hacerlo en el plazo adecuado, o no registrar la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza.

[1253] Cfr. la sección § 16 (2) y (3) de la Ley Federal sobre Firmas Electrónicas y Servicios de Confianza para Transacciones Electrónicas – *Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)*, promulgada por artículo 1 de la Ley Federal de 8 de julio de 2016.

[1254] Se trata de la actuación como prestador cualificado sin estar inscrito en la Lista de Confianza, dar a entender que se ofrece un servicio cualificado que no cumpla los requisitos previstos en el Reglamento eIDAS o en la legislación nacional, dar a entender que un servicio de tiempo electrónico, cualificado o no, confiere fecha cierta, o no poder acreditar –el titular de un sello electrónico cualificado de persona jurídica– qué persona física hace uso del mismo.

[1255] Cfr. el artículo XV.123, en relación con el artículo XV.70, del *Code de Droit Économique, artículo 123*

La legislación francesa no estableció, ni aún ha establecido[1256], un régimen de infracciones y sanciones general relativo a la prestación de servicios de confianza, con la única excepción del servicio de entrega electrónica certificada, en cuyo caso se tipifica la conducta consistente en ofrecer o prestar el servicio cuando no cumpla las condiciones legalmente establecidas, cuando pueda inducir al remitente o al destinatario a error acerca de los efectos jurídicos del envío, infracción que se sanciona con multa fija de 50.000 euros[1257]; cuantía que podría ser indicativa de una futura propuesta de regulación de corte más general.

También el derecho portugués[1258] prevé sanciones de cuantía relativamente moderada, de entre 1.500 euros y 3.740,98 euros, en caso de personas física, o 15.000 euros y 44.981,81 euros, en caso de persona jurídicas, todo ello frente a las infracciones de mayor gravedad; y reducidas a la mitad en caso de negligencia.

Y en el caso de la legislación del Reino Unido[1259], la sanción se limita, por cualquier infracción, a multa de cuantía fija de £ 1000, novedad con respecto a la normativa anterior[1260] al Reglamento eIDAS, que simplemente no preveía sanciones.

En cambio, el derecho italiano ha pasado, de no prever sanción alguna por la infracción de las obligaciones de los prestadores de servicios de certificación, a establecer un régimen con importantes sanciones, incluyendo multa de entre 40.000 y 400.000 euros en relación con cualquier obligación prevista para los prestadores de servicios de confianza en el Reglamento eIDAS o en la legislación nacional, en función de la gravedad de la infracción y a la entidad del daño causado[1261].

---

incorporado por el artículo 28 de la Loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique ; 21 juillet 2016.

[1256] No lo hizo la *Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, ni tampoco el *Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique*, hoy derogado por *Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique*, que tampoco ha establecido régimen sancionador general alguno, ni tampoco lo ha hecho la *Ordonnance n° 2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques*.

[1257] Cfr. el artículo 101 del *Code des postes et des communications électroniques, incorporado por artículo 93 de la Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1)*.

[1258] Cfr. el artículo 36.º-B del *Decreto-Lei n.º 290-D/99*, de 2 de agosto, incorporado por *Decreto-Lei n.º 88/2009*, de 9 de abril.

[1259] Cfr. *The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016*, de 1 de julio.

[1260] Cfr. *The Electronic Signatures Regulations 2002*, de 14 de febrero.

[1261] Cfr. el artículo 32-bis del *Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale*, modificado por artículo 31 del *Decreto legislativo 13 dicembre 2017, n. 217, Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*. Resulta

En este sentido, se debe considerar grave la infracción que pueda afectar a los derechos e intereses de una pluralidad de usuarios o que se encuentren relacionadas con carencias significativas de infraestructura o de proceso del prestador en cuestión, en cuyo caso, además de la multa, se puede sancionar al prestador con la prohibición de cualificarse de nuevo durante un plazo máximo de dos años.

Como se puede ver, el régimen español es de los más exigentes de nuestro entorno, algo que en cierto modo podría perjudicar a la industria española, al resultar más atractivo instalarse en Estados vecinos, con un menor riesgo económicos, algo que puede verse potenciado en atención a la libre circulación de los servicios de confianza[1262].

notable el hecho de que el Decreto legislativo de 26 de agosto de 2016 hubiera previsto multas de entre 4.000 y 40.000 euros, que posteriormente se multiplican por diez.

[1262] Cfr. el epígrafe 1.3.2 de este trabajo.

CONCLUSIONES

PRIMERA. La institucionalización jurídica de la acreditación de la actuación electrónica responde a un enfoque funcionalista, con al menos dos regímenes jurídicos diferenciados

El largo proceso de juridificación de los mecanismos y servicios de seguridad empleados para la autenticación, la integridad y el no-repudio de las comunicaciones electrónicas y de los documentos electrónicos ha conducido a la aparición de una colección de instituciones jurídicas orientadas a la acreditación de la actuación electrónica de las personas, así como de otros hechos acontecidos electrónicamente, y más en concreto referidas a la identificación, la atribución de documentos y mensajes, el tiempo o la comunicación.

Esta juridificación, sin embargo, no ha dado lugar a un régimen jurídico uniforme en todos los casos, sino que debemos distinguir entre la categoría, más amplia, de los servicios de confianza, y la categoría, más estricta, de sistemas de identificación electrónica.

Se trata de una distinción que no se encuentra justificada en criterios objetivos o técnicos, sino más bien de corte político, en el sentido de que los servicios de confianza se encuentran privatizados, mientras que los Estados no parecen estar, al menos de momento, dispuestos a admitir esta posibilidad con carácter general en el caso de los sistemas de identificación. Estos servicios de identificación se consideran servicios públicos, frecuentemente en sentido estricto y con reserva de actividad, como sucede en el caso de los documentos electrónicos de identidad expedidos por las autoridades.

La noción de que nos referimos a verdaderas instituciones jurídicas deriva precisamente del proceso de conceptualización jurídica que ha llevado desde su consideración como hechos brutos hasta la de hechos institucionales y, más en concreto, de tipo jurídico.

En efecto, el hecho bruto de la producción de una transformada matemática denominada firma digital se puede corresponder con el hecho jurídico, institucionalizado por el legislador, de la firma electrónica avanzada, pero también con el del sello electrónico avanzado, diferenciándose únicamente en función de la persona titular, y recibiendo efectos diferenciados. Por otra parte, el uso de la firma digital por una persona física o jurídica también ha sido institucionalizado alrededor del concepto de identificación electrónica, con sus propios efectos jurídicos, cuando se emplea para el propósito estricto de la comprobación de una identidad digital personal.

Es necesario, por tanto, concluir que los mismos mecanismos y servicios de seguridad de las TIC han dado lugar a instituciones jurídicas diferentes, en atención a la finalidad para que las mismas se utilizan.

En atención a esta finalidad de uso, del análisis del Reglamento eIDAS se deduce que se trata de instituciones que vienen a ser consideradas análogas a determinados hechos brutos, en función del caso, pero que de ello no se desprende necesariamente la equivalencia funcional con un concreto hecho institucional o jurídico, en especial cuando dicho hecho jurídico se corresponde con un acto jurídico.

Por este motivo, el Reglamento eIDAS viene a ser una base fundamental, pero

incompleta, de la experiencia jurídica en relación con estas instituciones. En el nivel nacional, sin embargo, los Estados miembros podrán moldear ulteriormente estas instituciones, de considerarlo necesario o conveniente, estableciendo los requisitos o efectos jurídicos oportunos.

SEGUNDA. La firma electrónica responde plenamente al principio de equivalencia funcional

En el Reglamento eIDAS, una firma electrónica (con independencia de que sea simple, avanzada o cualificada) se considera análoga al hecho bruto en que consiste el trazo de una firma manuscrita, por lo que se considerará también legalmente equivalente a alguno de los hechos jurídicos de firma que puedan existir en un ordenamiento jurídico (principio de equivalencia funcional), si bien se deberá investigar cuál, en cada caso concreto, y verificar si sirve a dicho efecto.

Esto es así porque el Reglamento eIDAS exige, como condición inexcusable, en el plano ontológico, para que un conjunto de datos sea considerado como firma electrónica que el mismo se utilice "para firmar" (y no para otra cosa), pero no armoniza la caracterización jurídica de esa firma (determinar cuáles son los efectos de la firma manuscrita, ni cuándo es exigible la misma), cuestión que, por tanto, queda en manos del derecho nacional.

Aunque esto no es inicialmente evidente, resulta fácil constatar que no todas las firmas manuscritas (hechos brutos) son igualmente relevantes para el Derecho, de modo que algunas firmas manuscritas conformarán el hecho jurídico de acreditar la atribución de una comunicación postal, mientras que otras pasarán a conformar el hecho institucional que conocemos como acto jurídico, dado que acreditarán una verdadera declaración de voluntad negocial o administrativa. Para comprender el sentido de esta institución, es imprescindible, por tanto, partir de que la firma manuscrita tiene diversos efectos jurídicos potenciales, pero también de que podría no tener, en función del caso, ningún efecto jurídico.

Y, como no puede ser de otra forma, ello se traslada a la firma electrónica, lo que se demuestra en la posibilidad de crear una firma electrónica cualificada en relación con cualquier objeto (como podría ser un mensaje de correo electrónico), sin que dicha firma constituya, entonces, acto jurídico alguno, aunque sí pueda conformar un hecho jurídico probatoriamente relevante.

Si esto es así, realmente el único efecto jurídico de la firma electrónica debe y puede ser el mismo que hubiera tenido la firma manuscrita a la que sustituye, simplemente porque, como hecho jurídico, no tiene una significación propia, diferente de la de la firma a que sustituye. Por ello, la institución en que consiste la firma electrónica es una abstracción que únicamente responde al principio de equivalencia funcional.

Diferente del caso anterior es el uso de una firma digital (hecho bruto) para una finalidad diferente a la de firmar, porque en este caso simplemente dicha firma digital no constituye el hecho jurídico de ser una firma electrónica, por no cumplir con el elemento esencial de su definición. Aquí podemos ver netamente el tránsito entre el mundo tecnológico y el jurídico, algo que no siempre resulta evidente.

La crítica a este enfoque, que es el adoptado por el Reglamento eIDAS, es que remite a cada ordenamiento nacional la determinación final de los efectos de la firma electrónica, en lugar de establecer un efecto jurídico armonizado, pero a mi juicio es la solución más

correcta y apropiada al principio de equivalencia funcional, universalmente entendido, porque de otro modo se debe restringir el alcance del propio principio de equivalencia funcional, para que el mismo se refiera sólo a las firmas que sirven para la realización de actos jurídicos.

En mi opinión, resulta más correcto un procedimiento de "dos pasos", en el que se garantice la equivalencia entre el correspondiente mecanismo tecnológico y el hecho jurídico de la firma (primer paso), y después se diluciden los efectos jurídicos concretos de esa firma electrónica, en función de los de la firma manuscrita (un concreto hecho jurídico, que normalmente será un acto jurídico) a los que ha sustituido (segundo paso).

TERCERA. Las restantes instituciones no responden al principio de equivalencia funcional, sino que reciben efectos jurídicos autónomos

Mejor se percibe esta noción de analogía entre mecanismo de seguridad y hecho bruto cuando nos referimos a otras instituciones previstas en el Reglamento eIDAS, en relación con las cuales se establece un efecto jurídico, pero sin emplearse el principio de equivalencia funcional.

En estos casos, el efecto jurídico asociado por el Reglamento eIDAS a la institución es autónomo, no referido a una institución preexistente en el mundo físico, por lo que se observa un total desacoplamiento entre ambos, el cual podrá ser, en su caso, corregido por el legislador nacional acudiendo al principio de equivalencia funcional, o estableciendo otro tipo de relación *ex novo*.

Así se ve, por ejemplo, en el sello electrónico de persona jurídica, en relación con el cual se establece el efecto jurídico de la atribución del origen de los datos y de la integridad de los mismos, permitiendo por tanto acreditar que un documento concreto ha sido producido por dicha persona jurídica.

Nos encontramos ante un indudable hecho jurídico, conformado a partir del hecho bruto subyacente que es la firma digital producida por el sistema informático bajo el control de dicha entidad, pero el mismo no es equivalente a ninguna otra institución (ningún otro hecho jurídico) previsto en el Reglamento eIDAS, lo que va a generar dudas acerca de la posibilidad de acudir a esta institución como fuente de prueba electrónica para un caso concreto.

Algo parecido ocurre con el sello de tiempo electrónico, institución que acredita la vinculación de unos datos a un instante temporal concreto y, por tanto, su existencia en dicho momento. Como en el caso anterior, el Reglamento no declara la equivalencia de este hecho jurídico con ningún otro, por lo que se deberá valorar el alcance de su valor jurídico a la luz de lo que establezcan otras normas, posiblemente en el nivel nacional.

En este sentido, y como ha especificado la legislación belga, el prestador de servicios que expide sellos de tiempo electrónico no puede dar a entender que dichos sellos constituyen fecha cierta de un acto jurídico, en el sentido que sucede, por ejemplo, con la intervención de fedatario público en el otorgamiento de un documento público, dado que no resulta posible determinar el momento en que se produjo la declaración, sino únicamente que el documento que contiene dicha declaración existe en la fecha del sello de tiempo. Sin embargo, posiblemente sería diferente en caso de uso de dos sellos de tiempo, uno sobre el contenido y otro sobre la firma electrónica, separados por sólo un segundo, algo que se acercaría mucho a una fecha cierta jurídicamente hablando.

Y también encontramos la misma situación en relación con las fuentes de prueba electrónica generadas por el servicio de entrega electrónica certificada, relacionadas con la gestión de los datos transmitidos, incluido el envío y la recepción de los datos. De nuevo, aunque el Reglamento eIDAS se establece un efecto jurídico para este servicio, que constituye un indudable hecho jurídico (sustentado en las diferentes evidencias técnicas, que serían el correlativo hecho bruto), se trata de un efecto jurídico autónomo, que no se predica en relación con otros hechos jurídicos.

Más en concreto, la entrega electrónica no tiene, en el Reglamento eIDAS, equivalencia con el envío postal certificado, por lo que no puede darse por supuesto que podrá acudirse a la entrega electrónica certificada en aquellos casos en que por exigencia legal deba emplearse un envío postal, dada la inexistencia de relación entre ambas instituciones.

Y aún se percibe más esta noción de equiparación entre institución y hecho bruto en un último grupo de casos, formado por las fuentes de prueba electrónica generadas en los servicios de validación y conservación de firma electrónica o sello electrónico, como por ejemplo sucede con el informe de validación o con las pruebas de existencia de un objeto de firma digital en un momento concreto del tiempo.

Aunque en estos casos no se establece efecto jurídico alguno, ello no implica que dichas fuentes de prueba electrónica no acrediten la existencia de un hecho bruto a los efectos de un hecho jurídicamente relevante. En efecto, aun cuando nada se diga en el Reglamento eIDAS acerca de un hipotético efecto jurídico de la validación cualificada de la firma electrónica cualificada, de ello no se desprende que no tenga un efecto jurídico inherente, que es el hecho bruto de haberse comprobado la corrección de dicha firma electrónica, algo que puede conformar el hecho jurídico de la conducta diligente del receptor de dicha firma electrónica cualificada.

CUARTA. Aunque la institucionalización de la identificación electrónica en el Reglamento eIDAS se ha producido para el ámbito de la administración electrónica, podría evolucionar para ser admitida en otros sectores

Algo diferente de los casos anteriores es el tratamiento de la identificación electrónica, que en el Reglamento eIDAS se juridifica sólo al efecto de extender los sistemas previamente existentes en los Estados miembros de modo que puedan ser empleados en la operativa transfronteriza con las entidades del sector público.

En este caso, la institución se define a efectos referenciales en relación con los sistemas que realmente existen en los Estados miembros, dado que el único efecto jurídico asociado a los mismos, una vez "reconocidos" conforme al Reglamento eIDAS, será precisamente el mandato de ser admitidos para el acceso a los servicios públicos.

A pesar de que lo que se acaba de decir, es verdad que los sistemas de identificación electrónica notificados conforme al Reglamento pasan a gozar de un mayor alcance, que es precisamente el del territorio de la Unión, por lo que pueden considerarse institucionalmente diferentes al momento previo al reconocimiento, algo que deriva de su sumisión a las reglas del Reglamento eIDAS.

En cualquier caso, el régimen legal de la autenticación transfronteriza en el Reglamento eIDAS es excesivamente limitado, dado que sólo se refiere a sistemas empleados para el acceso a servicios públicos en sede nacional que el Estado en relación con los cuales el

Estado miembro pretenda la extensión de su uso al acceso a servicios públicos prestados por entidades en otros Estados miembros.

Lo que se acaba de decir debe entenderse, sin embargo, sin perjuicio de que el certificado electrónico de firma electrónica de persona física y de sello electrónico de persona jurídica también constituye una institución de identificación electrónica, puesto que su función legal es precisamente confirmar la identidad, por lo que el uso de un certificado en un proceso de autenticación constituye una fuente de prueba electrónica de dicho hecho. Normalmente encontraremos la habilitación del uso de los certificados para este uso en la normativa sectorial, como se puede constatar, por ejemplo, en la legislación española reguladora del procedimiento administrativo.

Sería preciso evolucionar este sistema para que se pudiera aplicar a sistemas de identificación a efectos de su uso también, o incluso exclusivamente, para el acceso a servicios privados. La propuesta de admitir estos medios, por ejemplo, para el alta de nuevos clientes a efectos de prevención del banqueo de capitales constituye una posibilidad prometedora a estos efectos.

QUINTA. La legislación nacional previsiblemente establecerá otros efectos a las instituciones de acreditación de la actuación electrónica tipificadas en el Reglamento eIDAS, generando una mayor fragmentación del Mercado Único Digital

Las limitaciones que derivan de la caracterización de las instituciones de acreditación de la actuación electrónica en el Reglamento eIDAS pueden ser superadas mediante diversas vías, que incluyen el juego de la autonomía de la voluntad de las partes, cuando nos movamos en el espacio en que la misma opera libremente o, alternativamente, cuando interviene el legislador, intervención que puede producirse tanto en el nivel de la Unión Europea como en el nivel nacional.

Además, esta intervención de la legislación sectorial puede sustentarse en la aplicación del principio de equivalencia funcional o innovar el ordenamiento jurídico.

En este sentido, la posibilidad de emplear el sello electrónico en aquellos casos donde se requeriría la firma electrónica de un apoderado de la empresa, prevista por la legislación belga, constituye buen ejemplo de norma nacional que acude al principio de equivalencia funcional para conectar el hecho jurídico en que consiste el sello y el hecho jurídico de la representación.

En cambio, la exigencia de emplear un sello electrónico para que un operador de servicios de pago se autentique frente a otro de forma previa al intercambio de datos de usuarios de estos servicios, que ha sido impuesta por la Norma Técnica de Regulación aprobada por la Comisión Europea constituye un ejemplo de innovación en el plano de la Unión, ya que se trata de una situación que no tiene correlato en el mundo del soporte papel, simplemente porque es un proceso de negocio nuevo, y que únicamente existe en el entorno digital.

Por lo que se refiere a la entrega electrónica certificada, por ejemplo, la legislación francesa la ha equiparado al envío postal certificado, siempre que se cumplan determinadas condiciones, habilitando, además, su uso para el registro administrativo de documentos (como en el caso del, en España, denominado “correo administrativo”) y para la práctica de notificaciones electrónicas, camino que siguen Estados como Bélgica,

Alemania o Italia.

Las instituciones que acreditan la actuación electrónica no encuentran toda su regulación en el Reglamento eIDAS, que ha apostado por un enfoque de mínima armonización, limitado a los elementos fundamentales que conforman dichas instituciones, al objeto de que las mismas sirvan como bloques de construcción del Mercado Único Digital, como si fuera un juego de piezas cuyas combinaciones aportan confianza a los procesos en que las mismas se integran.

De esta forma, el uso de estas instituciones aporta una cierta fehaciencia a cualquier proceso, como pueda ser la contratación o el procedimiento administrativo.

Aunque este enfoque puede ser objeto de valoración positiva, en especial desde la compresión de la enorme dificultad que enfrenta cualquier proceso de armonización, que conduce a un mayor protagonismo de la interoperabilidad, el mismo conlleva una estructuración de la normativa en los dos niveles ya aludidos, con un núcleo armonizado en el nivel de la Unión, referido a los elementos que configuran cada institución, y ulteriores normas relativas al uso de estas instituciones en los diferentes ámbitos, normas sectoriales que pueden producirse indistintamente en el nivel de la Unión o en el de los Estados miembros.

Así ha sucedido, con especial intensidad, en el caso de la regulación del uso de estas instituciones en el sector de la administración electrónica, si bien hemos empezado a asistir a la aparición de normas para relaciones estrictamente privadas en las que también se regula este uso. Todo apunta que se trata de un fenómeno que irá en incremento en el futuro.

El problema que plantea que la legislación nacional establezca estos efectos es que conduce a una mayor fragmentación del Mercado Único Digital, por lo que cabe imaginar que en el futuro se produzca una mayor armonización de estas instituciones, así como a que la regulación de su uso sectorial se produzca directamente en el nivel de la Unión Europea.

SEXTA. La legislación nacional regulará nuevas instituciones de acreditación de la actuación electrónica, erigiendo nuevas barreras al Mercado Único Digital

El Reglamento eIDAS no ha agotado, por decisión expresa del legislador, el elenco de instituciones de acreditación de la actuación electrónica, permitiendo a los Estados miembros el mantenimiento o creación de otros servicios de confianza.

Esta opción ha de ser también valorada positivamente, ya que la experiencia demuestra que los Estados miembros son los laboratorios donde se crean estas instituciones, que posteriormente son armonizadas e incorporadas al acervo comunitario. Así sucedió inicialmente con la firma electrónica, y de nuevo ha ocurrido con los sellos electrónicos, los sellos de tiempo electrónico, o la entrega electrónica certificada.

Pero ello es nuevamente motivo de heterogeneidad y fragmentación en un Mercado Digital que se pretende único. Diversas legislaciones han regulado ya el archivo electrónico, como institución basada en el correspondiente servicio de confianza, al que se asocia el efecto jurídico de presumir la correcta conservación, incluso en el caso de la digitalización sustitutiva de documentos originales en soporte papel.

Es previsible que, en el futuro, estas instituciones se incorporen a la regulación armonizada en el nivel de la Unión, pero mientras esto no suceda se mantienen diferencias importantes en la gestión de documentos en sustento de procesos de negocio que pueden afectar a la competitividad de unas empresas que aspiran a operar en todo el territorio de la Unión.

En este sentido, resulta criticable que una empresa belga vaya a estar en situación de archivar electrónicamente la documentación en papel que reciba de sus clientes españoles, cuando una empresa española no podría hacerlo sin asumir el riesgo de que sus copias no se consideren auténticas; aunque es cierto que, al no tratarse de instituciones armonizadas, los efectos jurídicos quedan naturalmente limitados a dicho Estado, por lo que la posibilidad efectiva de uso de estas instituciones en las operaciones transfronterizas dependerán de la capacidad de sujetar el contrato a la legislación y, lo que es más importante, a la competencia judicial de dicho Estado.

El panorama global es, como se puede ver, el de un sistema complejo, fragmentario y, lo que es más importante, en construcción, que no parece aun suficientemente maduro para los ambiciosos objetivos del Mercado Único Digital, pero que seguramente es el sistema que, desde una óptica realista, se puede tener en la actual Unión Europea, y que ofrece significativas oportunidades en orden a la transformación digital de los procesos de negocio.

SÉPTIMA. La exigencia de un servicio cualificado impide la neutralidad tecnológica de las instituciones de acreditación de la actuación electrónica

El modelo del Reglamento eIDAS presenta la importante limitación de exigir, necesariamente, la intervención de un prestador de servicios en relación con las fuentes de prueba que reciben efectos jurídicos reforzados, puesto que sólo en estos casos es posible crear una fuente de prueba electrónica cualificada.

Esta opción del legislador deja fuera de la cualificación diversas posibilidades tecnológicas, como las tecnologías de registro distribuido y, más en concreto, de cadenas de bloques, en las que no interviene un prestador centralizado, sino una colección de nodos de infraestructura que replica la información de forma que la misma no puede ser arbitrariamente eliminada por una o ambas partes en la transacción.

La cualificación es, en algunos casos, excesivamente concreta, como sucede en el caso de la firma electrónica cualificada y en el sello electrónico cualificado, demostrando una fuerte dependencia de la tecnología de clave pública, lo que de nuevo conduce a la intervención de un prestador de servicios, lo que afecta a la necesaria neutralidad tecnológica, que se limita a muy pocos aspectos del sistema, tremendamente constreñido por los estándares de la infraestructura de clave pública.

En efecto, la cualificación debería ser más abstracta, de modo que se puedan cualificar cualesquiera firmas electrónicas o sellos electrónicos u otras instituciones de acreditación de la actuación electrónica que no se basen en el uso de claves criptográficas, como por ejemplo la firma manuscrita capturada electrónicamente. Se trata, ésta, de una tecnología que ha puesto de manifiesto las limitaciones lógicas del Reglamento eIDAS, el cual no permite considerar que una firma manuscrita capturada electrónicamente como firma electrónica cualificada. Dado que el efecto jurídico, como sabemos, de una firma

electrónica cualificada es resultar equivalente a la firma manuscrita, resulta sorprendente que una firma manuscrita capturada electrónicamente no reciba el efecto jurídico de ser equivalente a sí misma, una verdadera paradoja que en mi opinión ha puesto el sistema en evidencia.

Para extender este sistema a cualesquiera tecnologías, debería poder ser objeto de cualificación cualquier fuente electrónica de prueba en la que no haya intervenido, directa o indirectamente, un prestador de servicio, algo que con el modelo regulatorio actual simplemente no es posible, porque esta cualificación sólo sirve para adjetivar aquellas tecnologías que, por sus condiciones técnicas y previa la oportuna comprobación por la Administración, pueden obtener el efecto jurídico reforzado correspondiente.

OCTAVA. La intervención reforzada del Derecho público en las instituciones de acreditación de la actuación electrónica responde a razones imperiosas de interés general, pero también debe existir, con menor intensidad, aun cuando no dispongan de cualificación

Desde la óptica del actual modelo de intervención necesaria de un prestador de servicios de confianza, la apuesta por un modelo regulatorio de control público previo, en forma de autorización, debe ser objeto de valoración positiva, ya que resulta apropiada en relación con las instituciones de acreditación cualificada de la actuación electrónica, dada la afectación potencial a la tutela judicial efectiva de las partes, como manifestación del principio más general de seguridad jurídica, ambos recogidos en la Constitución.

Nos encontramos ante el primer caso de servicio de la sociedad de la información o servicio digital, como últimamente es también denominado por el legislador de la Unión, que se sujeta a autorización previa, dado que hasta este momento todos los regímenes de autorización (como, por ejemplo, la prestación de servicios financieros a través de Internet) existían previamente y simplemente se extendieron a las mismas actividades realizadas por medios electrónicos.

La novedad es que los servicios de confianza no se sujetan a autorización porque dicho régimen fuera preexistente y, por tanto, también deba aplicarse cuando la actividad se realiza por medios electrónicos, sino por los efectos que los mismos pueden producir a valores constitucionalmente protegidos.

El establecimiento de determinados efectos jurídicos a las diferentes instituciones jurídicas de acreditación de la actuación electrónica, en especial las presunciones de autenticidad, justifica sobradamente en mi opinión el régimen reforzado de intervención administrativa al que nos estamos refiriendo, y del que se desprende una íntima conexión entre el valor y eficacia de estas fuentes de prueba electrónica y el Derecho administrativo, que el legislador gradúa en función de la eficacia que en cada caso otorga a las mismas.

De este modo, podemos afirmar el absoluto protagonismo del Derecho administrativo en relación con la "fehaciencia" de las fuentes de prueba electrónica, pero con base en un modelo basado en la exigencia de condiciones técnicas y de seguridad, y no en la intervención de un funcionario público. Ello ha intensificado el debate acerca de las funciones que deben quedar reservadas a la fe pública, discusión en la que el Reglamento eIDAS o la normativa que lo complementa prudentemente no entra, manteniendo el principio de intangibilidad de los requisitos de forma, algo, en mi opinión, muy correcto.

De otro lado, aunque las instituciones de acreditación de la actuación electrónica que se sustentan en los servicios de confianza sin cualificación no gozan de un efecto jurídico reforzado, también en estos casos existen valores en juego que resulta necesario proteger, muy significativamente cuando dichos servicios de prestan al público, siendo adquiridos por consumidores, o cuando son empleados en el entorno laboral.

Por este motivo, debe ser objeto de valoración positiva la existencia de un régimen de supervisión y control menos riguroso, que opera *a posteriori*, en relación con los prestadores de servicios sin cualificación.

Ello es especialmente relevante, además, en aquellos casos en que la normativa sectorial admite de forma expresa el uso de estas fuentes de prueba sin cualificación, como sucede con la admisión de la firma electrónica avanzada en el procedimiento administrativo electrónico, caso de la legislación española, o cuando se acude a la autonomía de voluntad de las partes.

En este sentido, el análisis del uso de la firma electrónica en el procedimiento administrativo español, no exento de vacilaciones, ha mostrado de forma constante la apuesta por el uso de sistemas de firma electrónica con y sin cualificación, apostándose en un primer momento por la firma electrónica avanzada basada en certificado –como alternativa a la firma electrónica cualificada– y, en el momento actual, también por la firma electrónica no criptográfica. Al amparo de un enfoque basado en el análisis de riesgos, se autoriza el uso de los diferentes sistemas de firma y de sello electrónico, tanto a los interesados como a las Administraciones Públicas, y que resulta muy correcto desde el punto de vista del principio de neutralidad tecnológica.

NOVENA. El modelo regulatorio de los servicios cualificados de confianza otorga un excesivo protagonismo a las normas técnicas, que sin embargo no garantizan un nivel de protección suficiente

En el modelo regulatorio de los servicios de confianza se aprecia un complejo sistema de reparto competencial, que puede generar tensiones entre los diferentes centros de poder, público y privado, que participan en el mismo.

Significativamente, y siguiendo la técnica del reenvío indirecto, la Comisión Europea es facultada para el establecimiento, mediante actos de ejecución, de una gran cantidad de normas técnicas, que deben ser producidas por los organismos de normalización –esto es, por la industria–, de modo que, de ser estas normas adoptadas por la Comisión, su cumplimiento implica automáticamente la presunción de cumplimiento de los correspondientes requisitos jurídicos por parte de los prestadores que voluntariamente se adhieran a las mismas, presunción que vincula a los organismos nacionales de supervisión, por lo que su establecimiento se anticipa sujeto a una fuerte resistencia por parte de éstos.

Este modelo regulatorio concede, en efecto, un especial protagonismo a las normas técnicas, que vienen a ocupar el espacio tradicionalmente reservado a los reglamentos dictados en desarrollo de los requisitos legalmente establecidos, creando importantes espacios de autorregulación regulada, que en el caso de los servicios de confianza deben ser aplicados de forma prudente y contenida, de nuevo en atención a los intereses en juego, especialmente en aquellos casos en que potencialmente se puede afectar a la tutela judicial efectiva.

Quizá por ello, una parte del sistema se ha sujetado a verdaderos reglamentos técnicos, como es el caso de la seguridad de los prestadores y de los dispositivos de creación de firma electrónica cualificada y de sello electrónico cualificado. En el caso de estos dispositivos, los prestadores que los adquieren y, en su caso, operan, no son libres de emplear cualquier tecnología que les parezca adecuada, sino que deben obligatoriamente emplear productos previamente certificados conforme a la norma establecida por la Comisión Europea, o determinados equivalentes avalados por los Estados miembros en condiciones bastante restringidas.

Esta medida debe ser objeto de valoración positiva, puesto que constituye la mayor expresión de intervención administrativa en el plano de la seguridad que deben ofrecer los dispositivos que permiten la creación de fuentes de prueba electrónica fehaciente, pero debemos denunciar que se trata de una medida insuficiente, dado que estos dispositivos sólo cubren una parte del sistema en que se crea la firma electrónica cualificada, y pueden operar a partir de un documento diferente al que se mostró (si es que se mostró) al firmante, abriendo la puerta –y así consta en las normas técnicas– a la posibilidad de firmas electrónicas cualificadas y, por tanto, auténticas, producidas sobre documentos, también auténticos, pero que el firmante jamás conoció.

Ahora bien, si esto es así, como de hecho es, en mi opinión hay que ser extremadamente prudente al establecer presunciones legales en favor de estas instituciones, para evitar potenciales daños a los interesados. En el caso expuesto, una inversión de la carga de prueba sólo debería referirse al hecho de que una firma electrónica cualificada es atribuible al interesado, pero nada más. Por ello, en el caso de que el documento haya sido mostrado por la otra parte al firmante, en su página web, y posteriormente haya remitido al firmante el resumen criptográfico del mismo para que el firmante proceda a la creación de la firma electrónica cualificada, la carga de la prueba de que la firma electrónica cualificada corresponde al documento no debe ser objeto de inversión, porque resultaría imposible para el firmante levantar dicha carga invertida.

Nos encontramos ante una excelente muestra de los límites del sistema, al menos en su configuración actual, que exige de la aplicación de elementos adicionales para disponer de una prueba plenamente eficaz, cuando ello resulte necesario en función de los riesgos asociados a cada proceso, en cada ámbito sectorial concreto, pues las necesidades probatorias son diversas en el comercio electrónico, la administración electrónica, etc.

Existen diversas soluciones posibles para la problemática que se acaba de exponer, incluyendo una futura modificación legal, que extienda el ámbito de la certificación de producto a todo el sistema de creación de firma electrónica; la inclusión de estos requisitos en los reglamentos técnicos obligatorios, aunque esta segunda posibilidad podría conducir a la anulación del acto de establecimiento de la norma, por ser considerado ilegal; o, finalmente, acudir a los denominados “terceros de confianza”, pero siempre que los mismos actúen por interposición, dado que en este caso generan fuente de prueba electrónica de lo que se mostró al firmante en el momento de firma, a cuyo efecto expiden la correspondiente certificación (privada) acreditativa.

DÉCIMA. El Reglamento eIDAS apuesta por un régimen administrativo de acceso y permanencia en el mercado parcialmente privatizado, basado en la evaluación técnica independiente basada en normas técnicas

Respecto al acceso y la permanencia en la actividad en relación con los servicios cualificados de confianza, resulta especialmente novedoso que el Reglamento eIDAS exija la previa evaluación de la conformidad de los mismos con los requisitos legales. Se trata de un procedimiento a cargo de un organismo competente técnicamente, y que normalmente se realizará acudiendo a las correspondientes normas técnicas, inclusive cuando las mismas sean voluntarias; motivo por el cual se puede constatar la importancia de tales normas, en especial el caso de que las mismas gocen del valor de presunción de cumplimiento de requisitos legales.

En definitiva, el Reglamento eIDAS ha configurado un procedimiento autorizatorio que exige un doble control, puesto que el órgano de supervisión no podrá conceder la cualificación sin el previo informe favorable del organismo de evaluación de la conformidad, y que además abarata los costes del procedimiento para la Administración, tanto en la concesión de la cualificación como en el mantenimiento de la misma, mediante la obligación de la evaluación periódica.

Se trata un sistema que cabe entender razonable, dada la complejidad técnica de la materia en cuestión, cuya aplicación a servicios digitales resulta ciertamente novedosa, y que además incrementa el nivel de confianza entre los Estados miembros de la Unión, a efectos del reconocimiento del uso y/o de la eficacia transfronterizos de las correspondientes instituciones, y en la oferta transfronteriza de servicios de confianza.

Sin embargo, el sistema también presenta algunas deficiencias, como la dificultad de obtener la cualificación de un servicio cuando no existe una norma técnica, algo que no es imposible, pero que es difícil porque el organismo de evaluación debe entonces seleccionar un conjunto de criterios para dicha evaluación que quizá el órgano de supervisión no considere razonable, y también porque dicho organismo de evaluación debe ser acreditado por el organismo nacional de acreditación, o incluso cuando un prestador quiera evaluar su servicio con normas diferentes a las más utilizadas en el mercado.

No menos novedoso resulta el mecanismo diseñado en el Reglamento eIDAS para la publicidad de la cualificación de los servicios de confianza, quizá el primero que se realiza exclusivamente en forma electrónica, mediante su publicación empleando una sintaxis informática diseñada de forma exclusiva para que las aplicaciones informáticas puedan tomar decisiones automatizadas acerca de la cualificación. Por este motivo, el inicio de la prestación de servicios cualificados se autoriza únicamente desde el momento en que la información del prestador y de sus servicios se publica en dicha lista.

Se trata de un mecanismo que hay que valorar de forma muy positiva, dado que persigue de forma primaria el suministro, de forma normalizada, de la información mínima que se precisa para poder comprobar si una fuente de prueba goza de la cualificación, y facilitando enormemente la interoperabilidad de los procesos que incorporen este mecanismo; pero que no resulta particularmente útil como herramienta de difusión general de la información de los diferentes servicios ofrecidos, lo que facilitaría la transparencia en el mercado, por lo que sería deseable, en el futuro, su modificación.

UNDÉCIMA. La existencia de un estatuto legal generalmente aplicable a todos los servicios de confianza permite la ordenación de un mercado más amplio de instituciones fiables para la acreditación de la actuación

electrónica

El Reglamento eIDAS aporta un marco genérico de obligaciones y requisitos que deben cumplir los prestadores y los servicios que prestan, con un contenido mínimo común, que es ampliado de forma muy importante en el caso de aquéllos que sean objeto de cualificación.

En este punto, la novedosa aportación del Reglamento eIDAS consiste en haber establecido un estatuto general para la prestación de cualquier servicio de confianza, partiendo del que previamente existía para los prestadores que expedían certificados, tanto en el nivel de la Unión como en el de los Estados miembros. Este estatuto contenido en el Reglamento eIDAS constituye el mínimo armonizado en la Unión, por lo que sustenta la prestación transfronteriza de los servicios de confianza, con independencia de las obligaciones y requisitos adicionales que se puedan establecer por la legislación nacional sólo a los prestadores establecidos en el correspondiente Estado miembro, pero no a los que operan desde otros Estados miembros.

Como consecuencia de lo que se acaba de señalar, los Estados miembros pueden tener un menor incentivo para establecer un elevado nivel de obligaciones y requisitos adicionales a los prestadores de servicios de confianza establecidos en su territorio, en especial porque resta su competitividad frente a prestadores establecidos en Estados más permisivos, algo que viene parcialmente contenido por barreras específicas de la Unión Europea que afectan a la oferta global de servicios, significativamente la diversidad lingüística.

La valoración de este estatuto general para la prestación de servicios de confianza debe ser, en general, positiva, porque a mi juicio establece un marco equilibrado de control atendiendo a los potentes efectos jurídicos de los servicios de confianza cualificados, pero también a la necesidad general de mantener unos niveles de seguridad mínimos que permitan aportar confianza a las transacciones, incluso en el caso de servicios sin cualificación.

Esta novedad es también positiva porque permite el encaje en el nivel de la Unión Europea de futuros servicios de confianza, inicialmente definidos en la legislación nacional, ampliando horizontalmente el mercado de servicios disponibles. Así, cuando la legislación belga define el servicio de confianza, sólo aplicable en sede nacional, parte de la aplicación del estatuto general de prestación de servicios de confianza, extendiéndolo únicamente en lo necesario para dicho servicio de confianza, por lo que su futura armonización europea será más asequible.

DUODÉCIMA. Sin embargo, la configuración en sede nacional de la supervisión y del régimen sancionador podría afectar negativamente a la competitividad de los prestadores de servicios de confianza que actúan en este mercado

Desde el punto de vista de la supervisión, una de las cuestiones más notables del modelo reforzado de los servicios de confianza es la posibilidad de la retirada de la cualificación en caso de que el órgano de supervisión considere que el prestador no cumple las exigencias legales, medida que no tiene carácter sancionador, pero cuya afectación negativa al prestador queda fuera de toda duda, y que, por tanto, debe reservarse a casos muy justificados, y en los que no existan medidas más proporcionadas.

En efecto, esta posibilidad, combinada con las instrucciones y recomendaciones que puede emitir el órgano de supervisión conforme a la norma nacional, le confiere, en la práctica, un extraordinario poder que, por supuesto, queda sujeto a control judicial posterior, pero que sin duda le va a permitir moldear el funcionamiento de los prestadores actuando en este mercado. De nuevo se hacer preciso de la necesidad de hacer un uso lo más estricto y correcto de esta potestad, debido a los efectos negativos que puede producir.

Dado que, conforme al mandato del Reglamento eIDAS, en el nivel nacional se debe establecer un régimen sancionador que garantice el cumplimiento de las exigencias relativa a los prestadores y los servicios que prestan, podemos también observar diferencias entre los diferentes Estados miembros.

La combinación de estos tres elementos conduce a que el marco legal sea más o menos atractivo para los prestadores, en el momento de decidir en qué Estado se instalan, pero también se traslada de forma directa a la competitividad de los prestadores que decidan mantenerse en un Estado más rigorista que otro, dado el diferente coste que les supone el cumplimiento. Por ello, las divergencias en los niveles de exigencia afectan a la competencia efectiva en el mercado de la Unión Europea.

En relación con esta cuestión, el análisis del marco español denota que nos encontramos ante un marco comparativamente muy duro, tanto en número de infracciones como en cuantías económicas en caso de sanción, muy por encima de la mayoría de Estados miembros de la Unión que ya han establecido este régimen, algo que puede hacer pensar en su falta de proporción, especialmente a tenor de los controles previos y continuados a lo largo de la supervisión, que deberían reducir significativamente la necesidad de imponer grandes sanciones.

Así pues, del análisis realizado se puede concluir que, dentro de las lógicas diferencias que se van a presentar entre los diferentes Estados miembros, el marco español no es atractivo para instalarse o competir como prestador en un mercado de alcance europeo, por lo que sería conveniente ajustar la propuesta legislativa, aún pendiente del inicio de su tramitación parlamentaria, para hacerla menos rigorista.

REFLEXIÓN FINAL. ¿Hemos regulado un modelo que ya ha quedado obsoleto?

En definitiva, hay que reconocer que nos encontramos en un interesante momento, en el que disponemos de un marco normativo bastante completo, con un nivel de armonización que, aunque escaso, resulta suficiente para la incorporación de estas instituciones a los procesos de negocio, mediante el consumo de servicios de confianza, cualificados o no, en función de las necesidades.

Este marco legal supone un verdadero incentivo a la adopción de las instituciones cualificadas para la acreditación de la actuación personal, dado que reciben efectos jurídicos bien definidos y reforzados mediante presunciones legales, lo que permite intuir que su uso se extienda en el futuro. Sin embargo, podría repetirse el fracaso de la firma electrónica reconocida, y ocurrir que, incluso a pesar de estos incentivos, estas modalidades cualificadas de las instituciones a que nos estamos refiriendo no sean adoptadas socialmente, excepto, claro está, en caso de exigencia legal imperativa.

Esta falta de adopción social podría derivarse de la excesiva dependencia que presenta

todo el modelo de determinadas tecnologías y de la necesaria intervención de prestadores de servicios, algo especialmente relevante en un momento histórico en el que la innovación tecnológica está planteando sistemas que podrían aportar un nivel equivalente de fehaciencia sin la intervención de prestadores.

La gran pregunta, hoy, es si las tecnologías de registro distribuido y de cadenas de bloques eliminará la necesidad de los terceros prestadores de servicios de confianza, como ha sucedido ya con el dinero electrónico. Si ello sucede, indudablemente se deberá adoptar un modelo regulatorio radicalmente nuevo, algo que en mi opinión se debería abordar de forma proactiva, en lugar de esperar a que ello resulte ineludible.

NORMATIVA CITADA

NORMATIVA JURÍDICA

Naciones Unidas

- Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996), junto con su nuevo artículo 5 bis aprobado en 1998.
- Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001).

Unión Europea

- Tratado de Funcionamiento de la Unión Europea.
- Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998 por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas.
- Decisión 1720/1999/CE del Parlamento Europeo y del Consejo de 12 de julio de 1999 por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA).
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
- Decisión 2000/709/CE de la Comisión, de 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica.
- Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.
- Decisión Nº 2045/2002/CE del Parlamento Europeo y del Consejo, de 21 de octubre de 2002, por la que se modifica la Decisión Nº 1720/1999/CE por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA), así como el acceso a las mismas.
- Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC).
- Reglamento (CE) Nº 885/2004 del Consejo, de 26 de abril de 2004, por el que se

adaptan el Reglamento (CE) Nº 2003/2003 del Parlamento Europeo y del Consejo, los Reglamentos (CE) Nº 1334/2000, (CE) Nº 2157/2001, (CE) Nº 152/2002, (CE) Nº 1499/2002, (CE) Nº 1500/2003 y (CE) Nº 1798/2003 del Consejo, las Decisiones Nº 1719/1999/CE, Nº 1720/1999/CE, Nº 253/2000/CE, Nº 508/2000/CE, Nº 1031/2000/CE, Nº 163/2001/CE, Nº 2235/2002/CE y Nº 291/2003/CE del Parlamento Europeo y del Consejo, y las Decisiones 1999/382/CE, 2000/821/CE, 2003/17/CE y 2003/893/CE del Consejo, en los ámbitos de la libre circulación de mercancías, el derecho de sociedades, la agricultura, la fiscalidad, la educación y la formación, la cultura y la política audiovisual y las relaciones exteriores, como consecuencia de la adhesión de la República Checa, Estonia, Chipre, Letonia, Lituania, Hungría, Malta, Polonia, Eslovenia y Eslovaquia.

- Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido.
- Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior.
- Reglamento (CE) Nº 1896/2006 del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 por el que se establece un proceso monitorio europeo.
- Decisión Nº 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos.
- Reglamento (CE) Nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I).
- Decisión Nº 922/2009/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas (ISA) (Texto pertinente a efectos del EEE).
- Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de las ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior [notificada con el número C(2009) 7806].
- Directiva 2010/45/UE del Consejo, de 13 de julio de 2010, por la que se modifica la Directiva 2006/112/CE relativa al sistema común del impuesto sobre el valor añadido, en lo que respecta a las normas de facturación.
- Reglamento (UE) Nº 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión Nº 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión.
- Reglamento (UE) Nº 182/2011 del Parlamento Europeo y del Consejo de 16 de febrero de 2011 por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión.
- Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

- Reglamento (UE) Nº 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión Nº 1673/2006/CE del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE).
- Propuesta de Directiva del Parlamento Europeo y del Consejo, de 9 de abril de 2014, relativa a las sociedades unipersonales privadas de responsabilidad limitada (COM/2014/0212 final).
- Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE.
- Directiva 2014/55/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la facturación electrónica en la contratación pública.
- Recomendación 2014/478/UE de la Comisión, de 14 de julio de 2014, relativa a principios para la protección de los consumidores y los usuarios de servicios de juego en línea y la prevención del juego en línea entre los menores
- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Texto pertinente a efectos del EEE).
- Propuesta de modificación de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.
- Decisión de Ejecución (UE) 2015/296 de la Comisión, de 24 de febrero de 2015, por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al artículo 12, apartado 7, del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Texto pertinente a efectos del EEE).
- Reglamento de Ejecución (UE) 2015/806 de la Comisión, de 22 de mayo de 2015, por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados.
- Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.
- Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Texto pertinente a efectos del EEE).

- Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Texto pertinente a efectos del EEE).
- Decisión de Ejecución (UE) 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.
- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.
- Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Texto pertinente a efectos del EEE).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Reglamento (UE) 2017/1128 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, relativo a la portabilidad transfronteriza de los servicios de contenidos en línea en el mercado interior.
- Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros.

España

- Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.
- Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.

- Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil.
- Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.
- Resolución de 21 de octubre de 1999, del Congreso de los Diputados, por la que se ordena la publicación del acuerdo de convalidación del Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.
- Real Decreto 1829/1999, de 3 de diciembre, por el que se aprueba el Reglamento por el que se regula la prestación de los servicios postales.
- Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.
- Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Orden HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.
- Instrucción de 13 de junio de 2003, de la Dirección General de los Registros y del Notariado, complementaria de la Instrucción de 30 de diciembre de 1999, sobre presentación de las cuentas anuales en los Registros Mercantiles mediante procedimientos telemáticos.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Decreto 96/2004, de 20 de enero, por el que se regula la utilización de los medios electrónicos, informáticos y telemáticos en la contratación de la Generalitat de Cataluña.
- Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
- Orden EHA/3256/2004, de 30 de septiembre, por la que se establecen los términos en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 35.4 de la Ley General Tributaria.
- Ley 24/2005, de 18 de noviembre, de reformas para el impulso a la productividad.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior.
- Real Decreto 919/2006, de 28 de julio, por el que se aprueba el Reglamento técnico de distribución y utilización de combustibles gaseosos.

- Ley 32/2006, de 18 de octubre, reguladora de la subcontratación en el Sector de la Construcción.
- Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.
- Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Orden JUS/206/2009, de 28 de enero, por la que se aprueban nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación.
- Real Decreto 1586/2009, de 16 de octubre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Orden CUL/3410/2009, de 14 de diciembre de 2009, que regula el Registro Electrónico del Ministerio de Cultura.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Orden TIN/790/2010, de 24 de marzo, por la que se regula el envío por las empresas de los datos del certificado de empresa al Servicio Público de Empleo Estatal por medios electrónicos.
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Orden EHA/2219/2010, de 29 de julio, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en la sede electrónica de la Dirección General del Catastro.
- Orden INT/3022/2010, de 23 de noviembre, por la que se regula el Tablón Edictal de Sanciones de Tráfico.
- Resolución de 4 de febrero de 2011, de la Presidencia de la Agencia Estatal de Administración Tributaria, sobre uso de código seguro de verificación y por la que se crean sellos electrónicos del organismo.
- Orden CUL/1132/2011, de 28 de abril, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en el Registro Electrónico del Ministerio de Cultura y se modifica la Orden CUL/3410/2009, de 14 de diciembre de 2009, que regula el Registro Electrónico del Ministerio de Cultura.
- Orden JUS/1207/2011, de 4 de mayo, por la que se crea y regula el Registro Electrónico de Apostillas del Ministerio de Justicia y se regula el procedimiento de emisión de apostillas en soporte papel y electrónico.
- Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
- Ley 20/2011, de 21 de julio, del Registro Civil.
- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
- Resolución de 17 de noviembre de 2011, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Agencia Estatal de Administración Tributaria.
- Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos.
- Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.
- Orden FOM/2159/2013, de 31 de octubre, por la que se regula el sistema de código seguro de verificación de documentos electrónicos del Ministerio de Fomento.
- Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Orden HAP/2194/2013, de 22 de noviembre, por la que se regulan los

procedimientos y las condiciones generales para la presentación de determinadas autoliquidaciones, declaraciones informativas, declaraciones censales, comunicaciones y solicitudes de devolución, de naturaleza tributaria.

- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.
- Orden HAP/455/2014, de 20 de marzo, por la que se aprueban los modelos de declaración del Impuesto sobre la Renta de las Personas Físicas y del Impuesto sobre el Patrimonio, ejercicio 2013, se determinan el lugar, forma y plazos de presentación de los mismos, se establecen los procedimientos de obtención o puesta a disposición, modificación y confirmación del borrador de declaración del Impuesto sobre la Renta de las Personas Físicas, y se determinan las condiciones generales y el procedimiento para la presentación de ambos por medios telemáticos o telefónicos.
- Ley 3/2014, de 27 de marzo, dictada con el fin de transponer al derecho interno la Directiva 2011/83/UE, del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Orden HAP/800/2014, de 9 de mayo, por la que se establecen normas específicas sobre sistemas de identificación y autenticación por medios electrónicos con la Agencia Estatal de Administración Tributaria.
- Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Resolución de 4 de junio de 2014, del Instituto Nacional de la Seguridad Social, por la que se aprueban sistemas de identificación y autenticación de los ciudadanos para relacionarse electrónicamente con el Instituto Nacional de la Seguridad Social.
- Resolución de 24 de julio de 2014, de la Tesorería General de la Seguridad Social, por la que se aprueba el sistema de identificación, autenticación y firma electrónica, para relacionarse electrónicamente con la Tesorería General de la Seguridad Social.
- Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa.
- Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.
- Orden DEF/2594/2014, de 16 de diciembre, por la que se establece el sistema de

utilización del código seguro de verificación de documentos electrónicos del Ministerio de Defensa.

- Ley 7/2014, de 22 de diciembre, de Medidas Fiscales, de Gestión Administrativa y Financiera, y de Organización de la Generalitat (Valenciana).
- Real Decreto 22/2015, de 23 de enero, por el que se establecen los requisitos de expedición del Suplemento Europeo a los títulos regulados en el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales y se modifica el Real Decreto 1027/2011, de 15 de julio, por el que se establece el Marco Español de Cualificaciones para la Educación Superior.
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Orden INT/665/2015, de 27 de marzo, por la que se modifica la Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior.
- Decreto 31/2015, de 14 de mayo, por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de Cantabria.
- Real Decreto 414/2015, de 29 de mayo, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 668/2015, de 17 de julio, por el que se modifica el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Orden HAP/2553/2015, de 25 de noviembre, por la que se modifica la Orden EHA/2219/2010, de 29 de julio, por la que se aprueba el sistema de firma electrónica de clave concertada para actuaciones en la sede electrónica de la Dirección General del Catastro.
- Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve.
- Resolución de 16 de diciembre de 2015, de la Confederación Hidrográfica del Guadalquivir, sobre el uso del sistema de código seguro de verificación.
- Orden HAP/365/2016, de 17 de marzo, por la que se aprueban los modelos de declaración del Impuesto sobre la Renta de las Personas Físicas y del Impuesto sobre el Patrimonio, ejercicio 2015, se determinan el lugar, forma y plazos de

presentación de los mismos, se establecen los procedimientos de obtención, modificación, confirmación y presentación del borrador de declaración del Impuesto sobre la Renta de las Personas Físicas, se determinan las condiciones generales y el procedimiento para la presentación de ambos por medios telemáticos o telefónicos y se modifica otra normativa tributaria.

- Resolución de 20 de mayo de 2016, del Servicio Español para la Internacionalización de la Educación, sobre el uso del sistema de código seguro de verificación de este Organismo.
- Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.
- Orden HFP/255/2017, de 21 de marzo, por la que se aprueban los modelos de declaración del Impuesto sobre la Renta de las Personas Físicas y del Impuesto sobre el Patrimonio, ejercicio 2016, se determinan el lugar, forma y plazos de presentación de los mismos, se establecen los procedimientos de obtención, modificación, confirmación y presentación del borrador de declaración del Impuesto sobre la Renta de las Personas Físicas, se determinan las condiciones generales y el procedimiento para la presentación de ambos por medios telemáticos o telefónicos y por la que se modifica la Orden HAP/2194/2013, de 22 de noviembre, por la que se regulan los procedimientos y las condiciones generales para la presentación de determinadas autoliquidaciones, declaraciones informativas, declaraciones censales, comunicaciones y solicitudes de devolución, de naturaleza tributaria.
- Orden JUS/471/2017, de 19 de mayo, por la que se aprueban los nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación.
- Decreto 42/2017, de 22 de junio, por el que se regula el Régimen Jurídico de la Autorización y Uso de la firma electrónica de autoridades y empleados públicos de la Administración de la Comunidad Autónoma de Cantabria y su Sector Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Proyecto de Decreto por el que se regula el régimen jurídico de la Administración de la Comunidad Autónoma de Cantabria en el uso de medios electrónicos en su actividad administrativa y sus relaciones con los ciudadanos.
- Anteproyecto de Ley por la que se modifica la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, de noviembre de 2017.
- Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.
- Orden JUS/319/2018, de 21 de marzo, por la que se aprueban los nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación.

- Real Decreto 355/2018, de 6 de junio, por el que se reestructuran los departamentos ministeriales.

Alemania

- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturegesetz – SigG), promulgada por artículo 1 de la Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, de 1 de mayo de 2001.
- Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), de 16 de noviembre de 2001.
- Vertrauensdienstegesetz (VDG), promulgada por artículo 1 de la eIDAS-Durchführungsgesetz, de 18 de julio de 2017.
- Zivilprozessordnung (ZPO).

Austria

- Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur-und Vertrauensdienstegesetz – SVG), promulgada por artículo 1 de la Ley Federal de 8 de julio de 2016.

Bélgica

- Code Civil.
- Code de droit économique.
- Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ; 9 juillet 2001.
- Loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire ; 20 octobre 2000.
- Loi portant insertion du Livre XII, "Droit de l'économie électronique" dans le Code de droit économique, portant insertion des définitions propres au Livre XII et des dispositions d'application de la loi propres au Livre XII, dans les Livres I et XV du Code de droit économique ; 15 décembre 2003.
- Loi portant insertion du livre VII "Services de paiement et de crédit" dans le Code de droit économique, portant insertion des définitions propres au livre VII et des peines relatives aux infractions au livre VII, dans les livres I et XV du Code de droit économique, et portant diverses autres dispositions ; 19 avril 2014.
- Loi modifiant le Code de droit économique et portant diverses autres dispositions modificatives ; 26 octobre 2015.
- Loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique ; 21 juillet 2016.

- Arrêté royal fixant l'entrée en vigueur de la loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII "Droit de l'économie électronique" du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique ; 14 septembre 2016.
- Loi portant dispositions diverses en matière d'économie ; 18 avril 2017.

Francia

- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
- Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat.
- Arrêté du 20 avril 2011 relatif à la reconnaissance de la qualification des prestataires de services d'horodatage électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
- Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.
- Décret n° 2016-1278 du 29 septembre 2016 portant coordination des textes réglementaires avec l'ordonnance n° 2016-131 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
- Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil.
- Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique.
- Ordonnance n° 2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques.

Italia

- Regio Decreto 16 marzo 1942, n. 262. Approvazione del testo del Codice civile.

- Decreto del Presidente della Repubblica 2 marzo 2004, n. 117. Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3.
- Decreto legislativo 7 marzo 2005, n. 82. Codice dell'amministrazione digitale.
- Decreto legislativo 4 aprile 2006, n. 159. Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.
- Decreto legislativo 21 novembre 2007, n. 231, Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione.
- Decreto del Presidente del Consiglio dei Ministri 24 maggio 2010. Regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al D.P.R. n. 851 del 1967 rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 88, del decreto legislativo n. 82.
- Decreto legislativo 30 dicembre 2010, n. 235. Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
- Decreto-legge 18 ottobre 2012, n. 179. Ulteriori misure urgenti per la crescita del Paese.
- Decreto legislativo 26 agosto 2016, n. 179. Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.
- Decreto legislativo 25 maggio 2017, n. 90, Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006.
- Decreto legislativo 13 dicembre 2017, n. 217. Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.

Portugal

- Decreto-Lei n.º 290-D/99, de 2 de agosto, modificado por Decretos-Leis n.os 62/2003, de 3 de Abril, 165/2004, de 7 de Junho, 116-A/2006, de 16 de Junho e n.º 88/2009, de 9 de Abril.

Reino Unido

- The Electronic Signatures Regulations 2002, de 14 de febrero.
- The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, de 1 de julio.

NORMATIVA TÉCNICA

European Telecommunication Standards Institute – Instituto Europeo de Normas de Telecomunicación (ETSI)

- ETSI EN 301 549 V1.1.2 (2015-04). Accessibility requirements suitable for public procurement of ICT products and services in Europe.
- ETSI EN 319 102-1 V1.1.1 (2016-05). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.
- ETSI EN 319 122-1 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.
- ETSI EN 319 122-2 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures.
- ETSI EN 319 132-1 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.
- ETSI EN 319 132-2 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures.
- ETSI EN 319 142-1 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.
- ETSI EN 319 142-2 V1.1.1 (2016-04). Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles.
- ETSI EN 319 401 v2.2.1 (2018-04). Electronic signatures and infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 403 V2.2.2 (2015-08). Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI EN 319 411-1 V1.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2 V2.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2 V2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3 V1.1.1 (2016-02). Electronic Signatures and Infrastructures

(ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

- ETSI EN 319 412-4 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ETSI EN 319 412-5 V2.2.1 (2017-11). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- ETSI EN 319 421 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI TS 101 456 (2007-05). Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 533-1 V1.3.1 (2012-04). Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management.
- ETSI TS 102 158 V1.1.1 (2003-10). Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates.
- ETSI TS 102 176-1 V2.1.1 (2011-07). Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 176-2 V1.2.1 (2005-07). Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices.
- ETSI TS 102 640-1 V2.2.1 (2011-09). Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture.
- ETSI TS 103 171 V2.1.1 (2012-03). Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.
- ETSI TS 103 172 V2.2.2 (2013-04). Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.
- ETSI TS 103 173 V2.2.1 (2013-04). Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile.
- ETSI TS 103 174 V2.2.1 (2013-06). Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile.
- ETSI TS 119 312 V1.2.1 (2017-05). Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ETSI TS 119 612 V2.1.1 (2015-07). Electronic Signatures and Infrastructures (ESI); Trusted Lists.

European Committee for Standardization – Comité Europeo de Normalización (CEN)

- CEN EN 419 211-1:2014 – Protection profiles for secure signature creation device – Part 1: Overview.
- CEN EN 419 211-2:2013 – Protection profiles for secure signature creation device – Part 2: Device with key generation.
- CEN EN 419 211-3:2013 – Protection profiles for secure signature creation device – Part 3: Device with key import
- CEN EN 419 211-4:2013 – Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application.
- CEN EN 419 211-5:2013 – Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted channel to signature creation application.
- CEN EN 419 211-6:2014 – Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted channel to signature creation application.
- CEN EN 419 212-1:2014 – Application Interface for smart cards used as Secure Signature Creation Devices – Part 1: Basic services.
- CEN EN 419 212-2:2014 – Application Interface for smart cards used as Secure Signature Creation Devices – Part 2: Additional services.
- CEN/TS 419 221-1:2016 – Protection Profiles for TSP cryptographic modules - Part 1: Overview.
- CEN/TS 419 221-2:2016 – Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup.
- CEN/TS 419 221-3:2016 – Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services.
- CEN/TS 419 221-4:2016 – Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup.
- CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.
- CEN EN 419 241-1 – Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.
- CEN EN 419 241-2 – Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing.
- CEN EN 419 241-3 – Trustworthy Systems Supporting Server Signing – Part 3: Protection profile for Signature Activation Data management and Signature Activation Protocol (PP-SAD+SAP).

ÍNDICE DE ILUSTRACIONES

BIBLIOGRAFÍA

Aavik, G., & Krimmer, R. (2016). Integrating Digital Migrants: Solutions for Cross-Border Identification from E-Residency to eIDAS. A Case Study from Estonia. In H. J. Scholl, O. Glassey, M. Jansenn, B. Klievink, I. Lindgren, P. Parycek, . . . D. Sá Soares (Ed.), *Electronic Government. 15th IFIP WG 8.5 International Conference, EGOV 2016, Guimarães, Portugal, September 5-8, 2016, Proceedings. LNCS 9820*, pp. 151-163. Springer.

Abogacía General del Estado. (2013). *Anales de la Abogacía General del Estado 2012*. Agencia Boletín Oficial del Estado.

Adams, C., & Lloyd, S. (2003). *Understanding PKI: Concepts, Standards, and Deployment Considerations* (Second ed.). Addison-Wesley Professional.

Agence nationale de la sécurité des systèmes d'information. (2017, javier 3). Services de conservation qualifiés des signatures et des cachets électroniques qualifiés. Critères d'évaluation de la conformité au règlement eIDAS.

Agence nationale de la sécurité des systèmes d'information. (2017, javier 3). Services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés. Critères d'évaluation de la conformité au règlement eIDAS.

Alamillo Domingo, I. (2010a). Identidad electrónica, robo de identidad y protección de datos personales en la red. En *Robo de identidad y protección de datos* (Primera ed., págs. 17-34). Cizur Menor, Navarra, España: Aranzadi.

Alamillo Domingo, I. (2010b). La identidad electrónica en la red. En A. Rallo Lombarte, & R. Martínez Martínez (Edits.), *Derecho y Redes Sociales* (Primera ed., págs. 37-54). Cizur Menor, Navarra, España: Aranzadi.

Alamillo Domingo, I. (2012). *Las políticas de firma electrónica en la Administración Pública.* Recuperado el 15 de septiembre de 2014, de http://hdl.handle.net/2072/217067

Alamillo Domingo, I. (2017). Innovación y seguridad en la contratación pública. Especial referencia a la presentación y recepción electrónica de ofertas. En C. Campos Acuña (Ed.), *La nueva contratación pública en el ámbito local.* Wolters Kluwer.

Alamillo Domingo, I., & Cuenca León, N. (2014). 10 años de firma electrónica reconocida: ¿ha tenido algún impacto significativo en la e-Administración? En J. Balcells Padullés, A. Cerrillo i Martínez, M. Peguera Poch, I. Peña López, M. J. Pifarré de Moner, & M. Vilasau Solana (Ed.), *Internet, Derecho y Política. Una decada de transformaciones. Actas del X Congreso Internacional Internet, Derecho y Política* (págs. 657-672). Barcelona: Huygens.

Alamillo Domingo, I., & Urios Aparisi, X. (2004). Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica. *Revista de la Contratación Electrónica*(46).

Alamillo Domingo, I., & Urios Aparisi, X. (2010). El nuevo régimen legal de gestión de la identidad y firma electrónica por las Administraciones Públicas. En L. Cotino Hueso, & J. Valero Torrijos (Edits.), *Administración electrónica. La Ley 11/2007,*

de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y los retos jurídicos del e-gobierno en España (1ª ed., págs. 657-708). Valencia, España: Tirant lo blanch.

Alamillo Domingo, I., & Urios Aparisi, X. (2011). *La actuación administrativa automatizada en el ámbito de las Administraciones Públicas. Análisis jurídico y metodológico para la construcción y la explotación de trámites automáticos* (1ª ed.). Barcelona, España: Escola d'Administració Pública de Catalunya. Obtenido de http://eapc.gencat.cat/web/.content/home/publicacions/col_leccio_estudis_de_recerca_digital/3_actuacio_administrativa_automatitzada/alamillo_urios_castellano.pdf

Alonso Ureba, A., & Alcover Garau, G. (2000). La firma electrónica. En *Derecho de Internet. Contratación electrónica y firma digital* (págs. 175-206). Cizur Menor, Navarra, España: Aranzadi.

Alvestrand, H. T. (2004). *Request for Comments 3935 / Best Current Practice 95. A Mission Statement for the IETF*. IETF.

Anderson, R., & Moore, T. (2007). *Information Security Economics – and Beyond.* Retrieved from http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf

Anguiano Jiménez, J. (09 de 10 de 2015). *Sobre la emisión de declaraciones de voluntad mediante el uso de firmas digitalizadas.* Obtenido de El Derecho.com: http://www.elderecho.com/tribuna/www-elderecho-com/emision-declaraciones-voluntad-firmas-digitalizadas_11_870430001.html

Anguiano Jiménez, J. M. (2016). La prueba electrónica en la banca digital; el soporte duradero. En *El crédito al consumo y la sociedad digital* (Primera ed., págs. 127-148). Madrid, España: Asociación Nacional de Establecimientos Financieros de Crédito.

Atzeni, A., & Lioy, A. (2011). *STORK. D2.4 – Mapping of the national authentication levels of the new Member States to the STORK QAA levels.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1876

Baier, D., Bertocci, V., Brown, K., Pace, E., & Woloski, M. (2010). *A guide to claims-based identity and access control.* Redmon, Washington, USA: Microsoft.

Baldwin, A., Shiu, S., & Cassasa Mont, M. (2002). Trust Services: A framework for service-based solutions. *Proceedings of the 26 th Annual International Computer Software and Applications Conference (COMPSAC'02)* (pp. 507-513). IEEE.

Ballbé, M., & Martínez, R. (2003). *Soberanía dual y constitución integradora. La reciente doctrina federal de la Corte Suprema norteamericana.* Barcelona: Ariel Derecho.

Ballbé, M., & Padrós, C. (1997). *Estado competitivo y armonización europea.* Barcelona: Editorial Ariel.

Barrat Esteve, J. (2010). En defensa del anonimato. A propósito de la protección de los datos personales en la actividad estadística. En L. Cotino Hueso, & J. Valero Torrijos, *Administración electrónica: la Ley/2007, de 22 de junio, de acceso*

electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España (Primera ed., págs. 819-830). Valencia, España: Tirant lo Blanch.

Bashir, M., & Kempf, J. (2009). Bio-Inspired Reference Level Assigned DTW for Person Identification Using Handwritten Signatures. In J. Fierrez, J. Ortega-Garcia, A. Esposito, A. Drygajlo, & M. Faundez-Zanuy (Ed.), *Biometric ID Management and Multimodal Communication. BioID 2009* (pp. 200-206). Berlin: Springer.

Bauzá Martorell, F. J. (2002). *Procedimiento administrativo electrónico.* Granada: Comares.

Bauzá Martorell, F. J. (2016). Identificación, autenticación y actuación automatizada de las Administraciones Públicas. En E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Edits.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Primera ed., págs. 769-794). Valencia: Tirant lo Blanch.

Beltrán de Felipe, M. (2010). ¿Qué es el derecho a la identidad? En *Robo de identidad y protección de datos* (págs. 35-64). Cizur Menor, Navarra, España: Aranzadi.

Bierekoven, C., Bazin, P., & Kozlowski, T. (2004). Electronic signatures in German, French and Polish law perspective. *Digital evidence and electronic signature law review, 1*, 7-13. doi:http://dx.doi.org/10.14296/deeslr.v1i0.1719

Blanquer, D. (2006). *Hechos, ficciones, pruebas y presunciones en el Derecho Administrativo. "Taking facts seriously"* (Primera ed.). Valencia, España: Tirant lo Blanch.

Bocanegra Sierra, R., & García Luengo, J. (Septiembre-diciembre de 2008). Los actos administrativos transnacionales. *Revista de Administración Pública*(177), 9-29.

Boer, A. (2009). *Legal theory, sources of law and the semantic web.* Amsterdam: IOS Press. doi:10.3233/978-1-60750-003-2-i

Boix Palop, A. (2010). Previsiones en materia de neutralidad tecnológica y acceso a los servicios de la Administración. En L. Cotino Hueso, & J. Valero Torrijos (Edits.), *Administración electrónica: la Ley/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España* (1ª ed., págs. 305-324). Valencia: Tirant lo blanch.

Borges, G. (2012, 09 05). The Draft Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM (2012) 238. *Presentation at the Workshop on Electronic Identification and Trust Services*. Brussels.

Brennen, A. (2008, 01 24). *The Keysigning Party HOWTO*. Retrieved 08 17, 2015, from http://www.cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html

Brugger, J., & Fraefel, M. (2013). *STORK 2.0. D.7.3 Business Plans - Consolidated Report & Recommendations.* STORK 2.0 Consortium. Retrieved from https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=40:d731-business-plans-consolidated-report-a-recommendations&Itemid=177

Brugger, J., Fraefel, M., Meerbergen, P., Van der Donckt, C., Riedl, R., & Sánchez, J.

(2014). *STORK 2.0. D.7.2 Service Design and Pricing - Consolidated Report & Open Questions.* STORK 2.0 Consortium. Retrieved from https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=39:d72-service-design-and-pricing-consolidated-report-a-open-questions&Itemid=177

Buchmann, N., Rathgeb, C., Baier, H., & Busch, C. (2014). Towards Electronic Identification and Trusted Services for Biometric Authenticated Transactions in the Single Euro Payments Area. In B. Preneel, & D. Ikonomou, *Privacy Technologies and Policy. Second Annual Privacy Forum, APF 2014, Athens, Greece, May 20-21, 2014. Proceedings* (pp. 172-190). Springer International Publishing. doi:10.1007/978-3-319-06749-0_12

CA/Browser Forum. (2017a). *Guidelines For The Issuance And Management Of Extended Validation Certificates v1.6.2.* Retrieved from https://cabforum.org/extended-validation/

CA/Browser Forum. (2017b). *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates v1.4.9.* Retrieved from https://cabforum.org/baseline-requirements-documents/

Cámara Largo, A. (2013). La firma de contratos en pizarra digital como firma manuscrita. *Actualidad Jurídica Uría Menéndez*(34), 89-92.

Campos Acuña, C. (Mayo de 2018). Las funciones electrónicas de los Secretarios en el Real Decreto 128/2018, de 16 de marzo. *El Consultor de los Ayuntamientos*(5), 58. Obtenido de El Consultor de los Ayuntamientos: http://elconsultor.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMzUwsTQ7Wy1KLizPw8WyMDQwsDE0NjkEBmWqVLfnJIZUGqbVpiTnEqANbJnyA1AAAAWKE

Caprioli, É. (2014). *Signature électronique et dématérialisation. Droit et pratiques.* Paris, France: LexisNexis .

Carrillo Donaire, J. A. (2016). Actuación de los ciudadanos. En E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Edits.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Primera ed., págs. 581-593). Valencia, España: Tirant lo Blanch.

Cerrillo i Martínez, A. (2010). Cooperación entre Administraciones públicas para el impulso de la Administración electrónica. En E. Gamero Casado, & J. Valero Torrijos (Edits.), *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos* (Tercera ed., págs. 757-810). Cizur Menor, Navarra, España: Aranzadi.

Chou, E. Y. (2015). What's in a name? The toll e-signatures take on individual honesty. *Journal of Experimental Social Psychology*(61), 84-95.

Clowes, N., & Brathwait, L. (2009). *STORK. D4.2 Final report on eID process flows.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=952

Coello de Portugal Martínez del Peral, I. (2003). Contratos, convenios y firma electrónica. In VVAA, *Firma digital y Administraciones Públicas* (pp. 99-106). Madrid:

Instituto Nacional de Administración Pública.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, T. (2008). *Request for Comments 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* IETF.

Cotino Hueso, L. (2010). El derecho a relacionarse electrónicamente con las Administraciones y el estatuto del ciudadano e-administrado en la Ley 11/2007 y la normativa de desarrollo. In E. Gamero Casado, & J. Valero Torrijos (Eds.), *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos* (Tercera ed., pp. 177-342). Cizur Menor, Navarra, España: Aranzadi.

Cotino Hueso, L. (2017). Capítulo VI. El derecho y deber de relacionarse por medios electrónicos (art. 14 LPAC). Asistencia en el uso de medios electrónicos a los interesados (art. 12 LPAC). In E. Gamero Casado, S. Fernández Ramon, & J. Valero Torrijos (Eds.), *Tratado de procedimiento administrativo común régimen jurídico básico del sector público* (Vol. Tomo I, pp. 476-531). Valencia: tirant lo blanch.

Cotino Hueso, L., & Montesinos García, A. (2012). Derechos de los ciudadanos y los profesionales en las relaciones electrónicas con la Administración de Justicia. In E. Gamero Casado, & J. Valero Torrijos, *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio.* Cizur Menor: Thompson Reuters Aranzadi.

Couto Calviño, R. (2007). Reflexiones acerca de la firma electrónica y el nuevo mercado de servicios de certificación. *Revista de Contratación Electrónica*(83), 3-37.

Cruz Rivero, D. (2005). Análisis de los antecedentes del concepto de firma electrónica como equivalente a la firma manuscrita. *Revista de Contratación Electrónica*(60), 3-122.

Darnaculleta Gardella, M. M. (Enero-abril de 2016). El Derecho Administrativo Global: ¿Un nuevo concepto clave del Derecho Administrativo? *Revista de Administración Pública*(199), 11-50.

Davara Rodríguez, M. Á. (1996). *De las autopistas de la información a la sociedad virtual.* Elcano, Navarra, España: Aranzadi SA.

De Miguel Asensio, P. A. (2015). *Derecho privado de Internet* (Quinta ed.). Cizur Menor, Navarra, España: Aranzadi.

De Urbano Castrillo, E. (2009). *La valoración de la prueba electrónica.* Valencia: Tirant lo Blanch.

Delgado García, A., & Oliver Cuello, R. (2007). La actuación administrativa automatizada. Algunas experiencias en el ámbito tributario. *Revista Catalana de Dret Públic*(35).

Delos, O., & Lacroix, S. (2010a). *Study on Cross-Border Interoperability of eSignatures (CROBIES). "Trusted Lists". Implementer's Guide.* Tournai: SEALED.

Delos, O., Lacroix, S., & Graux, H. (2010). *Study on Cross-Border Interoperability of eSignatures (CROBIES). Framework for Secure Signature Creation Devices cross-border recognition.* Tournai: SEALED.

Díaz-Romeral Gómez, A. (2011). La sede electrónica: eje vertebrador del derecho de los ciudadanos a la información, participación y a relacionarse por medios electrónicos con las Administraciones Públicas. In J. Piñar Mañas (Ed.), *Administración electrónica y ciudadanos* (pp. 379-406). Cizur Menor, Navarra, España: Editorial Aranzadi SA.

Dimitriadis, S., & Kyrezis, N. (2010, August). Linking trust to use intention for technology-enabled bank channels: The role of trusting intentions. *Psychology and Marketing, 27*(8), 799-820. doi:10.1002/mar.20358

Dumortier, J. (2004). Legal Status of Qualified Electronic Signatures in Europe. In P. Sachar, N. Polhmann, & H. Reimer (Ed.), *ISSE 2004 — Securing Electronic Business Processes. Highlights of the Information Security Solutions Europe 2004 Conference* (pp. 281-289). Wiesbaden: Vieweg+Teubner Verlag.

Dumortier, J. (2016, July 1). *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation).* Retrieved from SSRN: https://ssrn.com/abstract=2855484

Dumortier, J., & Vandezande, N. (2012a, September 26). *Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. ICRI Research Paper 9.* Retrieved from SSRN: https://ssrn.com/abstract=2152583

Dumortier, J., & Vandezande, N. (2012b, October). Trust in the proposed EU regulation on trust services? *Computer Law & Security Review, 28*(5), 568-576. doi:10.1016/j.clsr.2012.07.010

Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., & Van Eecke, P. (2003). *The legal and Market Aspects of Electronic Signatures: Legal and market aspects of the application of Directive 1999/93/EC and practical applications of efectronic signatures in the Member States, the EEA, the Candidate and the Accession countries.* Interdisciplinary centre for Law and Information Technology, Katholieke Universiteit Leuven. Retrieved from http://skilriki.is/media/skjol/electronic_sig_report.pdf

Eertink, H., Hulsebosch, B., & Lenzini, G. (2008). *STORK. D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=579

Elías Baturones, J. (2008). *La prueba de documentos electrónicos en los Tribunales de Justicia* (Vol. 574). Valencia: Tirant lo blanch.

Esteve Pardo, J. (2010). Transparencia y legitimidad en las decisiones pública adoptadas en entornos de complejidad científica. En R. García Macho (Ed.), *Derecho administrativo de la información y administración transparente.* Madrid: Marcial Pons.

Esteve Pardo, J. (2015). La administración garante. Una aproximación. *Revista de Administración Pública*(197), 11-39.

European Commission. (2005). *Signposts toward eGovernment 2010.* Luxembourg: Office for Official Publications of the European Communities.

European Commission. Directorate-General Enterprise. (2004). *Interchange of Data between Administrations (IDA). Authentication Policy. Basic Policy for establishing the appropriate authentication mechanisms in sectoral networks and projects.* Retrieved from http://ec.europa.eu/idabc/en/document/3532/5585.html

European Commission. Directorate-General for Informatics. (2003). *Electronic interchange of data between administrations (IDA). The Horizontal Actions and Measures (HAM) 2003 Work Programme.* Retrieved from http://ec.europa.eu/idabc/en/document/2548/3.html

European Commission. Information Society and Media Directorate-General. eGovernment Unit. (2006). *A Roadmap for a pan-European eIDM Framework by 2010, v1.0.*

European Union. (2011). *European Interoperability Framework (EIF). Towards Interoperability for European Public Services.* Luxembourg: Publications Office of the European Union.

Farrell, S., Housley, R., & Turner, S. (2010). *Request for Comments 5755. An Internet Attribute Certificate Profile for Authorization.* IETF.

Feliú Rey, M. I. (1999). Artículo 5.º Requisitos de incorporación. En I. Arroyo Martínez, & J. Miquel Rodríguez (Edits.), *Comentarios a la Ley sobre Condiciones Generales de la Contratación* (Primera ed., págs. 54-62). Madrid, España: Tecnos.

Fondevila Antolín, J. (2016). Seguridad en la utilización de medios electrónicos. El Esquema Nacional de Seguridad. En E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Edits.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Primera ed., págs. 598-674). Valencia, España: Tirant lo Blanch.

Ford, W., & Baum, M. S. (1997). *Secure electronic commerce: Building the infrastructure for sigital signatures and encryption.* Upper Saddle River, New Jersey, USA: Prentice-Hall.

Fraenkel, B. (1992). *La signature. Genèse d'un signe.* Paris, France: Gallimard.

Fraenkel, B. (2008). La signature: du signe à l'acte. *Sociétés & Représentations*(25), 15-23.

Fraenkel, B., & Pontille, D. (2006). La signature au temps de l'électronique. *Politix*(74), 103-121.

Fundación Telefónica. (2015). *La Sociedad de la Información en España 2014_ siE[14.* Ariel. Retrieved from http://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/?itempubli=323

Galindo, F. (1998). *Derecho e Informática* (Primera ed.). Las Rozas, Madrid, España: La Ley-Actualidad.

Gamero Casado, E. (2009). Interoperabilidad y Administración electrónica: conéctense, por favor. *Revista de Administración Pública*(179), 291-332.

Gamero Casado, E. (2015). *Desafíos del derecho administrativo ante un mundo en disrupción* (Primera ed.). Granada, España: Comares.

Gamero Casado, E. (2016). Funcionamiento electrónico del sector público. En F. López Menudo (Ed.), *Innovaciones en el procedimiento administrativo común y el régimen jurídico del sector público* (Primera ed., págs. 83-113). Sevilla, España: Universidad de Sevilla.

Gamero Casado, E. (2016). Panorámica de la administración electrónica en la nueva legislación administrativa básica. *Revista Española de Derecho Administrativo*(175), 15-27.

Gamero Casado, E. (2018). ¿El «retorno» al derecho administrativo?: manifestaciones en las leyes de procedimiento, régimen jurídico y contratos del sector público. *Revista Española de Derecho Administrativo*(189).

García de Enterría, E., & Fernández, T. R. (2008). *Curso de derecho administrativo. II* (Undécima ed.). Madrid: Civitas.

García Mas, F. (2010). Especial consideración del documento electrónico en el art. 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica: la modificación de la Ley 56/2007. *Actualidad Civil*(10).

García Mas, F. J. (2017). De nuevo con la firma electrónica y otras cuestiones: Reglamento UE núm. 910/2014 de 23 de julio de 2014. *Revista Jurídica del Notariado*(102-103), 113-188.

García Medina, J. (1995). *Teoría integral del Derecho en el pensamiento de Miguel Reale.* Valladolid, España: Grapheus.

Garfinkel, S., & Spafford, G. (1999). *Seguridad y comercio en el Web.* México D.F.: McGraw-Hill.

Gjøsteen, K. (2008). Weaknesses in BankID, a PKI-Substitute Deployed by Norwegian Banks. In S. F. Mjølsnes, S. Mauw, & S. K. Katsikas, *Public Key Infrastructure. 5th European PKI Workshop: Theory and Practice, EuroPKI 2008 Trondheim, Norway, June 16-17, 2008 Proceedings* (pp. 196-206). Springer Berlin Heidelberg. doi:10.1007/978-3-540-69485-4_14

Gobert, D. (2015, Février). *Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : analyse approfondie.* Récupéré sur http://www.droit-technologie.org

Gobert, D. (2016, Octobre). *La loi belge du 21 julliet 2016 mettant en œvre le règlement européen eIDAS et le complétant avec des règles sur l'archivage électronique: analyse approfondie.* Récupéré sur http://www.droit-technologie.org

Gómez Puente, M. (2011). El impulso de la sociedad de la información. La administración electrónica en el marco europeo y estatal. En *Administración electrónica y ciudadanos* (Primera ed., págs. 53-117). Cizur Menor, Navarra, España: Aranzadi.

González Pérez, J., & González Navarro, F. (2012). *Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común* (Quinta ed.). Cizur Menor, Navarra, España: Aranzadi.

Graux, H. (2011). Rethinking the e-Signatures Directive: On laws, trust services and the digital single market. *Digital Evidence and Electronic Signature Law Review*(8), 9-24.

Graux, H., & Majava, J. (2007). *eID Interoperability for PEGS. Proposal for a multi-*

level authentication mechanism and a mapping of existing authentication mechanisms. European Communities. Retrieved from http://ec.europa.eu/idabc/en/document/6484/5938/

Graux, H., & Majava, J. (2007). *eID Interoperability for PEGS. Summary of existing national and other authentication schemes.* European Communities. Retrieved from http://ec.europa.eu/idabc/en/document/6484/5938/

Graux, H., Majava, J., & Meyvis, E. (2009). *Study on eID Interoperability for PEGS: Update of Country Profiles. Analysis & assessment report.* Retrieved from http://ec.europa.eu/idabc/en/document/6484/5938/

Gruber, C., Hook, C., Kempf, J., Scharfenberg, G., & Sick, B. (2006). A Flexible Architecture for Online Signature Verification Based on a Novel Biometric Pen. *2006 IEEE Mountain Workshop on Adaptive and Learning Systems* (pp. 110-115). Logan: IEEE. doi:10.1109/SMCALS.2006.250700

Gudín Rodríguez-Magariños, A. (2010). La diligencia de cotejo de los documentos electrónicos. *Revista General de Derecho Procesal*(22), 1-25.

HageI III, J., & Armstrong, A. G. (1999). *Net Gain. Negocios rentables a través de Internet.* Barcelona: Paidós.

Heichlinger, A., & Gallego, P. (2010). A new e-ID card and online authentication in Spain. *Identity in the Information Society, 3*(1), 43-64. doi:10.1007/s12394-010-0041-3

Heppe, J. (2010). *STORK. D4.3 Updated Report on eID Process Flows.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1875

Heppe, J., Berbecaru, D., Jorquera, E., Schiavo, M., Johnston, A., Lioy, A., . . . Bauer, W. (2011). *STORK. D5.7.3 Functional Design for PEPS, MW models and interoperability.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1874

Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., de Fuentes, J. M., & Ramos, B. (2013, May). A taxonomy and survey of attacks on digital signatures. *Computers & Security, 34*, 67-112. doi:10.1016/j.cose.2012.11.009

Hoffman, P. (1999). *Request for Comments 2634. Enhanced Security Services for S/MIME.*

Hoffman, P., & Schneier, B. (2005). *Request for Comments 4270. Attacks on Cryptographic Hashes in Internet Protocols.* IETF.

Hoogstraaten, H., Prins, R., Niggebrugge, D., Heppener, D., Groenewegen, F., Wettinck, J., . . . Hu, Y. Z. (2012). *Black Tulip. Report of the investigation into the DigiNotar Certificate Authority breach.* Fox IT.

Housley, R. (2005). *Request for Comments 4073. Protecting Multiple Contents with the Cryptographic Message Syntax (CMS).* IETF.

Housley, R. (2005). *Request for Comments 4108. Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages.* IETF.

Housley, R., Ashmore, S., & Wallace, C. (2010). *Request for Comments 5914. Trust Anchor Format.* IETF.

Housley, R., Ashmore, S., & Wallace, C. (2010). *Request for Comments 5934. Trust Anchor Management Protocol (TAMP).* IETF.

Huerta Viesca, M., & Rodríguez Ruiz de Villa, D. (2001). *Los Prestadoresde Servicios de Certificación en la Contratación Electróica* (Primera ed.). Elcano, Navarra, España: Aranzadi.

Hulsebosch, B., Lenzini, G., & Eertink, H. (2009). *STORK. D2.3 - Quality authenticator scheme.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577

IBM. (n.d.). *Guía del usuario de Tívoli Risk Manager. Certificados digitales.* Retrieved 08 19, 2015, from https://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/es_ES/HTML/user276.htm#HDRDIGICERTS

Illescas Ortíz, R. (2001). *Derecho de la contratación electrónica.* Madrid, España: Civitas Ediciones.

ISO. (2008). *International Standard 32000-1. Document management - Portable document format - Part 1: PDF 1.7.*

Izquierdo Carrasco, M. (2000). *La seguridad de los productos industriales. Régimen jurídico-administrativo y protección de los consumidores* (Primera ed.). Madrid, España: Marcial Pons.

Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. *Computer Law & Security Review*(32), 91-110.

Khatchatourov, A., Laurent, M., & Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption. In E. Tambouris, M. Janssen, H. J. Scholl, M. A. Wimmer, K. Tarabanis, M. Gascó, . . . P. Parycek, *Electronic Government. 14th IFIP WG 8.5 International Conference, EGOV 2015, Thessaloniki, Greece, August 30 -- September 2, 2015, Proceedings* (pp. 273-290). Springer International Publishing. doi:10.1007/978-3-319-22479-4_21

Krawczyk, P. (2010). When the EU qualified electronic signature becomes an information services preventer. *Digital evidence and electronic signature law review, 7*, 7-18.

Leitold, H. (2010). Challenges of eID Interoperability: The STORK Project. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang, *Privacy and Identity Management for Life. 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010* (pp. 144-150). Springer-Verlag Berlin Heidelberg.

Leitold, H., & Zwatterndorfer, B. (2010). STORK: Architecture, Implementation and Pilots. *ISSE 2010 Securing Electronic Business Processes* (pp. 131-142). Vieweg+Teubner.

Leitold, H., Lioy, A., & Ribeiro, C. (2014). STORK 2.0: Breaking New Grounds on eID and Mandates. *Proceedings of ID World International Congress.* Retrieved from https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=81827

Linares Gil, M. I. (2004). Los interesados en el procedimiento: la problemática de las personas jurídicas. In VVAA, *Administración electrónica y procedimiento administrativo* (pp. 455-485). Madrid: Ministerio de Economía.

Linares Gil, M. I. (2010). Identificación y autenticación de las Administraciones Públicas. In E. Gamero Casado, & J. Valero Torrijos (Eds.), *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos* (Tercera ed., pp. 415-462). Cizur Menor, Navarra, España: Aranzadi.

Linares Gil, M. I. (2012). Identificación electrónica de los órganos judiciales y autenticación del ejercicio de su competencia. En E. Gamero Casado, & J. Valero Torrijos (Edits.), *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio* (Primera ed., págs. 477-502). Cizur Menor, Navarra, España: Aranzadi.

Linde Paniagua, E. (2008). Notas sobre el objeto, ámbito y reglas de aplicación de la Directiva relativa a los servicios en el mercado interior. *Revista de Derecho de la Unión Europea*(14), 35-46.

López, M. (2014, 12 11). *Los 6 ataques de seguridad más famosos de 2014.* Retrieved 08 08, 2015, from panda mediacenter: http://www.pandasecurity.com/spain/mediacenter/seguridad/los-6-ataques-de-seguridad-mas-famosos-de-2014/

Lusoli, W., Maghiros, I., & Bacigalupo, M. (2008). eID policy in a turbulent environment: is there a need for a new regulatory framework? *Identity in the Information Society, 1*(1), 173-187. doi:10.1007/s12394-009-0011-9

MacCormick, N. (1998). Norms, institutions, and institutional facts. *Law and Philosophy*(7), 301-345.

Madrid Parra, A. (2001). Aspectos jurídicos de la identificación en el comercio electrónico. En R. Illescas Ortiz, & I. Ramos Herranz (Edits.), *Derecho del comercio electrónico* (Primera ed., págs. 185-250). Las Rozas, Madrid, España: La Ley-Actualidad.

Majava, J., Biasiol, A., & van der Maren, A. (2007). *eID Interoperability for PEGS. Report on comparison and assessment of eID management solutions interoperability.* European Communities. Retrieved from http://ec.europa.eu/idabc/en/document/6484/5938/

Martín Delgado, I. (2009, Septiembre-Diciembre). Naturaleza, concepto y régimen jurídico de la actuación jurídica automatizada. *Revista de Administración Pública*(180), 353-386.

Martín Delgado, I. (2010). Identificación y autenticación de los ciudadanos. In E. Gamero Casado, & J. Valero Torrijos (Eds.), *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos* (Tercera ed., pp. 463-536). Cizur Menor, Navarra, España: Aranzadi.

Martín Delgado, I. (2012). Identificación electrónica de ciudadanos y profesionales en el ámbito de la justicia. In E. Gamero Casado, & J. Valero Torrijos (Eds.), *Las Tecnologías de la Información y la Comunicación en la Administración de*

Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio. Aranzadi Thomson Reuters.

Martin, A. K., van Brakel, R. E., & Bernhard, D. J. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*(6(3)), 213-232.

Martínez Gutiérrez, R. (2009). *Administración Pública electrónica.* Cizur Menor: Civitas Thomson Reuters.

Martínez Gutiérrez, R. (2011). Identificación y autenticación: DNI electrónico y firma electrónica. In J. L. Piñar Mañas (Ed.), *Administración electrónica y ciudadanos* (Primera ed., pp. 407-454). Cizur Menor, Navarra, España: Aranzadi.

Martínez Gutiérrez, R. (2015). *La contratación pública electrónica: Análisis y propuesta de transposición de las Directivas Comunitarias de 2014.* Valencia: Tirant lo blanch.

Martínez Gutiérrez, R. (2016a). *El régimen jurídico del nuevo procedimiento administrativo común* (1ª ed.). Cizur Menor, Navarra, España: Editorial Aranzadi SAU.

Martínez Gutiérrez, R. (2016b). Relaciones interadministrativas por medios electrónicos. Interoperabilidad. En E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Edits.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Primera ed., Vol. II, págs. 2891-2932). Valencia, España: Tirant lo Blanch.

Martínez Martínez, R. (2010). Protección de datos personas y redes sociales: un cambio de paradigma. In A. Rallo Lombarte, & R. Martínez Martínez (Eds.), *Derecho y redes sociales.* Cizur Menor, Navarra, España: Editorial Aranzadi.

Martínez Nadal, A. (1998). *Comercio electrónico, firma digital y autoridades de certificación.* Madrid, España: Civitas.

Martínez Nadal, A. (2001). *La Ley de firma electrónica* (Segunda ed.). Madrid: Civitas.

Martínez Nadal, A. (2009). *Comentarios a la Ley 59/2003 de firma electrónica* (Segunda ed.). Cizur Menor: Civitas Thompson Reuters.

Martínez Quirante, R. (2002). *Armas: ¿Libertad americana o prevenció europea?* (Primera ed.). L'Hospitalet de Llobregat, Barcelona, España: Ariel.

Mason, S. (2017). *Electronic Signatures in Law* (Fouth ed.). London, United Kingdom: University of London. doi:10.14296/117.9781911507017

Mateti, P. (2013). *Cryptography in Internet Security.* Retrieved 08 15, 2015, from http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/Cryptography/

Merchán Murillo, A. (2012). La firma electrónica: Problemas en su reconocimiento transfronterizo. *Revista de Contratación Electrónica*(117), 3-29.

Merchán Murillo, A. (2016). *Firma electrónica: Funciones y problemática (Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica)* (Primera ed.). Cizur Menor, Navarra, España: Aranzadi.

Merchán Murillo, A. (2018). Servicios de identificación electrónica dentro de la e-

Administración. *Revista General de Derecho Administrativo*(47), 1-25.

Miguez Macho, L. (2004). *Los servicios públics y el régimen jurídico de los usuarios.* Cedecs.

Moles Plaza, R. J. (2001). *Derecho y calidad. El régimen jurídico de la normalización técnica.* Barcelona: Ariel.

Moles Plaza, R. J. (2004). *Derecho y control en Internet. La regulabilidad de Internet.* Barcelona: Ariel.

Montero Aroca, J. (2007). *La prueba en el proceso civil.* Madrid: Thomson Civitas.

Mora Ruiz, M. (2016). Principios de intervención de las Administraciones Públicas y títulos habilitantes para el desarrollo de una actividad. En E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Edits.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Primera ed., págs. 1091-1153). Valencia, España: Tirant lo Blanch.

Morant, J. L., Ribagorda, A., & Sancho, J. (1994). *Seguridad y protección de la información.* Madrid, Madrid, España: Centro de Estudios Ramón Areces SA.

Munar i Pascual, E. (2003). Firma electrónica, certificados y entidades de certificación: Análisis comparativo de las regulaciones autonómicas sobre la firma electrónica. *Revista de la Contratación Electrónica*(43), 61-87.

Muñoz Machado, S. (2000). *La regulación de la red. Poder y Derecho en Internet* (Primera ed.). Madrid: Taurus.

Muñoz Soro, J. F. (2003). *Decisión jurídica y sistemas de información* (Primera ed.). Madrid, España: Fundación Beneficentia et Peritia Iuris. Colegio de Registradores de la Propiedad y Mercantiles de España.

Muñoz Soro, J. F. (2017). Aspectos jurídicos de la custodia de documentos electrónicos. *Ibersid: revista de sistemas de información y documentación, 11*(2), 35-40.

Nakamoto, S. (2008, October 31). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. *24th ACM Conference on Computer and Communications Security CCS'17* (pp. 1631-2648). Dallas: ACM. doi:http://dx.doi.org/10.1145/3133956.3133969

Nieva Fenoll, J. (2009). Práctica y valoración de la prueba documental multimedia. *Actualidad Civil*(17).

Nualart Mercadé, R. (2008). iArxiu: un servicio de custodia y preservación a largo plazo de documentos electrónicos. In VVAA, *El documento electrónico: aspectos jurídicos, tecnológicos y archivísticos* (pp. 177-214). Castelló de la Plana: Publicacions de la Universitat Jaume I.

Olnes, J. (2001). A Taxonomy for Trusted Services. In B. Schmid, K. Stanoevska Slabeva, & V. Tschammer (Eds.), *Towards the E-Society: E-Commerce, E-Business, and E-Government* (Vol. 74, pp. 31-44). Kluwer Academic Publishers.

Ormazábal Sanchez, G. (Septiembre de 2002). Firma electrónica y valor probatorio ante las reformas proyectadas en la LSSI y en el borrador de APLFE. *Revista de*

Contratación Electrónica(30), 83-110.

Ortega Díaz, J. (2008). *La firma y el contrato de certificación electrónicos* (Primera ed.). Cizur Menor: Thomson Aranzadi.

Palomar Olmeda, A. (2014). La Administración ante los nuevos títulos habilitantes: facultades de supervisión, control, inspección y suspensión de las actividades. En A. Palomar Olmeda, & R. Terol Gómez (Edits.), *El nuevo marco de ejercicio de las actividades económicas* (Primera ed., págs. 137-184). Cizur Menor, Navarra, España: Aranzadi.

Pelletan, J. (2017). *Sociétés sécuritaires ou sociétés de confiance.* Paris, France: L'Harmattan.

Peña, J., & Alamillo Domingo, I. (2014). La identidad digital en procesos de democracia electrónica. La desastrosa experiencia de la firma electrónica basada en certificados, en MiFirma.com. En J. Balcells Padullés, A. Cerrillo i Martínez, M. Peguera Poch, I. Peña López, M. J. Pifarré de Moner, & M. Vilasau Solana (Ed.), *Internet, Derecho y Política. Una decada de transformaciones. Actas del X Congreso Internacional Internet, Derecho y Política* (págs. 767-776). Barcelona: Huygens.

Pérez Pereira, M. (2009). *Firma Electrónica: Contratos y Responsabilidad Civil* (Primera ed.). Cizur Menor, Navarra, España: Aranzadi.

Piñar Mañas, J. L. (2011). Revolución tecnológica y nueva administración. In J. L. Piñar Mañas (Ed.), *Administración electrónica y ciudadanos* (Primera ed., pp. 25-52). Cizur Menor, Navarra, España: Aranzadi.

Polanksi, P. (2015). Towards the single digital market for e-identification and trust services. *Computer law & security review*(31), 773-781.

Polk, T., Chen, L., Turner, S., & Hoffman, P. (2011). *Request for Comments 6194. Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms.* IETF.

Popov, A. (2015). *Request for Comments 7465. Prohibiting RC4 Cipher Suites.* IETF.

Posch, R. (2017). Digital sovereignty and IT-security for a prosperous society. *Informatics in the Future. Proceedings of the 11th European Computer Science Summit (ECSS 2015), Vienna, October 2015* (pp. 77-86). Cham: Springer.

Punzón Moraleda, J., & Sánchez Rodríguez, F. (2008). Reflexiones en torno al documento electrónico y la firma electrónica. *Diario La Ley*(6985-6987).

Purves, J. (2009). *STORK. D6.1.1 Cross Border Authentication for Electronic Services - Functional Specification.* STORK-eID Consortium. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=964

Ramsdell, B., & Turner, S. (2010). *Request for Comments 5751. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2. Message Specification.* IETF.

Reed, D. (2003). *Applying the OSI sevel layer network model to information security.* Paper, SANS Institute. Retrieved 08 07, 2015, from http://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-

security-1309

Rego Blanco, M. (2014). Sobre la simplificación administrativa y la perversión de las solicitudes generadas electrónicamente que neutralizan la reducción de cargas administrativas. En J. Balcells Padullés, A. Cerrillo i Martínez, M. Peguera Poch, I. Peña López, M. Pifarré de Moner, & M. Vilasau Solana (Edits.), *Actas del X Congreso Internacional Internet, Derecho y Política. Barcelona, 3-4 julio de 2014* (págs. 601-616). Barcelona: Editorial Huygens.

Rego Blanco, M. (2017). Capítulo XV. La presentación de solicitudes, escritos y documentos ante las Administraciones Públicas. En E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Edits.), *Tratado de procedimiento administrativo comun y régimen jurídico del sector público* (Vol. Tomo I, págs. 998-1055). Valencia: tirant lo blanch.

Richards, J. R. (1999). The Utah Digital Signature Act As "Model" Legislation: A Critical Analysis. *The John Marshall Journal of Information Technology & Privacy Law, 17*, 873-907.

Rico Carrillo, M. (2015). El Reglamento europeo sobre identificación y servicios de confianza electrónicos. *Revista General de Derecho Europeo*(35), 1-24.

Rodríguez Adrados, A. (2000). La firma electrónica. En *Notariado y contratación electrónica* (Primera ed., págs. 375-404). Madrid, España: Consejo General del Notariado.

Rodríguez Ayuso, J. F. (2018). *Impacto de la nueva regulación europea sobre identificación electrónica y servicios de confianza en el ámbito de la contratación privada dotada de firma electrónica.* Alma Mater Studiorum - Università di Bologna, Bologna.

Roig Batalla, A. (2007). El anonimato y los límites a la libertad en internet. En L. Cotino Hueso (Ed.), *Libertad en Internet. La red y las libertades de expresión e información* (Primera ed., págs. 321-354). Valencia, España: Tirant lo Blanch.

Roβnagel, H. (2006). On diffusion and confusion - Why electronic signatures have failed. In S. Fischer-Hübner, S. Furnell, & C. Lambrinoudakis (Eds.), *Trust and Privacy in Digital Business. 3rd International Conference on Trust and Privacy in Digital Business, TrustBus 2006* (Vol. LNCS 4083, pp. 71-80). Springer.

Rundle, M., Blakley, B., Broberg, J., Nadalin, A., Olds, D., Ruddy, M., . . . Trevithick, P. (2007). At a crossroads: "personhood" and digital identity in the information society. STI Working Paper 2007/07. Organisation for Economic Co-operation and Development. Retrieved from http://www.oecd.org/sti/working-papers

Sarmiento, D. (2008). *El soft law administrativo. Un estudio de los efectos jurídicos de las normas no vinculantes de la Administración.* Cizur Menor: Aranzadi.

Sarwat, R. (2010). *DNI-e. Tecología y usos* (Primera ed.). Móstoles, Madrid, España: Informática64.

Schaad, J. (2007). *Request for Comments 5035. Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility.*

Segarra Tormo, S. (2004). Utilización de la firma electrónica en la Administración española I: La Agencia Estatal de Administración Tributaria. En *Administración*

electrónica y procedimiento administrativo (Primera ed., págs. 91-118). Madrid, España: Ministerio de Economía.

SOG-IS Crypto Working Group. (2016). *SOG-IS Crypto Evaluation Scheme. Agreed Cryptographic Mechanisms.* Retrieved from https://www.sogis.org/es/supporting_doc_es.html

Sorge, C. (2014). The legal classification of identity-based signatures. *Computer Law & Security Review*(30), 126-136.

Srivastava, A. (2011, November). Resistance to change: Six reasons why businesses don't use e-signatures. *Electronic Commerce Research, 11*(4), 357-382. doi:10.1007/s10660-011-9082-4

Statista. (2015). *Leading social networks worldwide as of August 2015, ranked by number of active users (in millions).* Retrieved 08 10, 2015, from http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Statista. (2015). *Number of social network users worldwide from 2010 to 2018 (in billions).* Retrieved 08 10, 2015, from http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

STORK 2.0 Consortium. (2013). *STORK 2.0. D4.2 First version of Functional Design.* Retrieved from https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=23:d42-first-version-of-functional-design&Itemid=174

STORK 2.0 Consortium. (2015). *STORK 2.0. D4.8 Final version of process flows.* Retrieved from https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=56:d48-final-version-of-process-flows&Itemid=174

STORK-eID Consortium. (2011). *Secure Electronic Identity Across Europe. STORK Fact Sheet.* Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=60&act=streamDocument&did=1831

Sui, J., & Stinton, D. R. (2008). A Critical Analysis and Improvement of AACS Drive-Host Authentication. In Y. Mu, W. Susilo, & J. Seberri (Eds.), *Information security and privacy. 13th Australasian Conference, ACISP 2008. Wollongong, Australia, July 7-9, 2008. Proceedings* (pp. 37-52). Springer Berlin Heidelberg. doi:10.1007/978-3-540-70500-0_4

Swan, M. (2016). Blockchain Temporality: Smart Contract Time Specifiability with Blocktime. In J. Alferes, L. Bertossi, G. Governatori, P. Fodor, & D. Roman (Ed.), *Rule Technologies. Research, Tools, and Applications. RuleML 2016. Lecture Notes in Computer Science, vol 9718* (pp. 184-196). Cham: Springer. doi:10.1007/978-3-319-42019-6_12

Turner, S., & Chen, L. (2011). *Request for Comments 6151. Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms.* IETF.

Urios Aparisi, X. (2012). Los cuerpos jurídicos autonómicos y la administración

electrónica de la Justicia. En E. Gamero Casado, & J. Valero Torrijos (Edits.), *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio* (Primera ed., págs. 895-924). Cizur Menor, Navarra, España: Aranzadi.

Valero Torrijos, J. (2007). *El régimen jurídico de la e-Administración: El uso de medios informáticos y telemáticos en el procedimiento administrativo común.* Granada: Comares.

Valero Torrijos, J. (2010). El alcance de la protección constitucional del ciudadano frente al uso de medios electrónicos por las Administraciones Públicas (Especial referencia a las implicaciones para la protección de datos personales de la Ley 11/2007...). En L. Cotino Hueso, & J. Valero Torrijos (Edits.), *Administración electrónica. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y los retos jurídicos del e-gobierno en España.* Valencia: Tirant lo Blanch.

Valero Torrijos, J. (2012). La Administración Pública en la Nube. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica. En R. Martínez Martínez (Ed.), *Derecho y Cloud computing.* Cizur Menor: Thomson Civitas.

Valero Torrijos, J. (2013). *Derecho, innovación y administración electrónica.* Sevilla: Global Law Press - Editorial Derecho Global.

Valero Torrijos, J. (2016). Los órganos administrativos. En E. Gamero Casado, S. Fernández Ramos, & J. Valero Torrijos (Edits.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público* (Primera ed., págs. 2705-2755). Valencia, España: Tirant lo Blanch.

von Ahn, L., Maurer, B., McMillen, C., Abraham, D., & Blum, M. (2008, 09 12). reCAPTCHA: Human-Based Character Recognition via Web Security Measures. *Science*, 1465-1468. Retrieved from http://www.sciencemag.org

Windley, P. J. (2005). *Digital identity.* Sebastopol, California, USA: O'Reilly Media.

Yee, P. E. (2013). *Request for Comments 6818. Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* IETF.

ANEXOS TÉCNICOS

ANEXO A. LOS MECANISMOS Y SERVICIOS DE SEGURIDAD DE LAS TIC PARA LA ACREDITACIÓN DE LA ACTUACIÓN ELECTRÓNICA

A.1 La criptografía como base tecnológica de los mecanismos y servicios de seguridad

La criptografía es la base tecnológica que fundamenta los mecanismos y servicios de las TIC empleados para la acreditación de la actuación, de modo análogo a cómo la tecnología de la tinta y el papel sustenta la prueba en que consiste una firma manuscrita, en relación con un texto escrito.

Por esta simple razón, la mayoría de pruebas electrónicas se basan en la criptografía, de modo que la normativa sobre el uso de algoritmos criptográficos tiene un reflejo jurídico en la legislación reguladora de las instituciones reguladoras de estas pruebas de la actuación electrónica, que lógicamente se traslada a los prestadores de servicios de confianza que las sustentan.

En el ámbito de la interconexión de los sistemas y, por tanto, con un enfoque orientado a la seguridad de las comunicaciones electrónicas[1263], la norma internacional ISO 7498-2:1989 (1ª ed.)[1264] define el servicio de seguridad como aquel prestado por una capa de un sistema abierto de comunicación, que garantiza la seguridad adecuada de los sistemas o de las transferencias de datos[1265].

Los servicios de seguridad existen para satisfacer los requisitos de las políticas de seguridad y los requerimientos de los usuarios; en ambos casos, la finalidad última consiste en proteger los activos de la organización de los peligros de todo tipo a que se puedan enfrentar[1266].

Los servicios de seguridad que, de uno u otro modo, sustentan la confianza en los procesos electrónicos incluyen la autenticación, la integridad de datos y el no rechazo; conformando la base tecnológica de las garantías de la actuación electrónica.

Los citados servicios se basan en técnicas de seguridad, incluyendo de forma particularmente relevante el uso de la criptografía como mecanismo técnico, a la que

---

[1263] Que ciertamente presenta necesidades y requisitos que pueden ser diferentes a los de la autenticación de documentos.

[1264] El título de la norma es Sistemas de procesamiento de la información – Interconexión de sistemas abiertos – Modelo básico de referencia – Parte 2: Arquitectura de seguridad. Se trata de una norma idéntica a la Recomendación X.800 (1991) de la ITU-T.

[1265] ISO 7498-2:1989, sección 3.3.51. También es frecuente referirse a procesos de seguridad, como término intercambiable con el de servicio de seguridad (por ejemplo, cfr. ISO 16609:2012, Servicios financieros – Requisitos para la autenticación de mensajes empleando técnicas simétricas.

[1266] Normalmente se va hablar de amenazas, para mitigar las cuales existen controles, entre los cuales, los servicios de seguridad de las tecnologías de la información y la comunicación.

introduciremos en este capítulo, y en el establecimiento de entornos de confianza, en especial en atención a la existencia de los denominados terceros de confianza.

Hay que notar que algunos de estos servicios de seguridad son también denominados objetivos de seguridad, como sucede, en concreto, con los tres servicios que presentamos en este anexo técnico, por su importancia. Además de la autenticación, de la integridad/autenticidad y del no rechazo, se suele incluir entre los objetivos de seguridad a la confidencialidad[1267], que también se basa en mecanismos técnicos eminentemente criptográficos.

La criptografía es una disciplina que incluye los principios, medios y métodos para la transformación de los datos con el fin de ocultar su contenido semántico, prevenir su uso no autorizado, o impedir su modificación no detectada[1268].

En general, nos referiremos a técnicas de protección de la información mediante el desorden de los elementos que la conforman, como la transposición o sustitución (*cryptós*) de las letras (*graphós*) de un documento, con el objetivo de hacerlo confidencial[1269]. La criptografía se diferencia de la esteganografía, que tiene por objetivo esconder la información (*esteganós*) entre las letras (*graphós*) de un documento[1270].

La aplicación de la criptografía a las tecnologías de la información y la comunicación se basa en algoritmos y claves correspondientes a las diferentes cifras, simétricas y asimétricas, que se utilizan como mecanismos de seguridad, para el cifrado, resumen, comprobación de mensaje o firma digital.

Una cifra[1271] es un algoritmo diseñado para proteger una información (sea una comunicación en tránsito o un documento más o menos perdurable) de forma que los terceros no autorizados no puedan acceder.

Las cifras se basan en el uso de claves para transponer[1272] o sustituir[1273] la posición de los signos alfabéticos y numéricos que componen el documento, operación que se denomina "cifrar"[1274], y que se define, en términos generales, como la transformación criptográfica de datos[1275].

La clave aporta la información necesaria para devolver el documento, ahora desordenado

---

[1267] Un ejemplo de servicio de seguridad de las TIC sería el control de acceso, que apoya el objetivo de seguridad de la confidencialidad.

[1268] Cfr. definición 2126278 de la norma ISO/IEC 2382:2015.

[1269] La criptografía se ha empleado desde tiempos remotos, siendo una de las primeras referencias bien conocidas la "clave del César".

[1270] Generalmente con el objetivo de poder trazar la autenticidad de la información, se incluye información oculta en la misma, a modos de marcas de agua.

[1271] El Diccionario de la Real Academia de la Lengua la define como la "escritura en que se usan signos, guarismos o letras convencionales, y que solo puede comprenderse conociendo la clave".

[1272] Cfr. definición 2126292 de la norma ISO/IEC 2382:2015.

[1273] Cfr. definición 2126293 de la norma ISO/IEC 2382:2015.

[1274] Atención al uso del incorrecto término "encriptar", muy generalizado, pero no recogido en el Diccionario de la Real Academia de la Lengua Española.

[1275] Definición 2126279 de la norma ISO/IEC 2382:2015.

y por tanto ininteligible, a su estado original, operación que se denomina "descifrar"[1276].

Las cifras pueden ser simétricas o asimétricas:

- La cifra simétrica[1277] utiliza una sola clave para cifrar y para descifrar y, en consecuencia, esta clave ha de ser conocida por el originador y por el destinatario de la transmisión o del documento confidencial.

  Las cifras simétricas son muy eficientes y permiten ejecutar operaciones con mucha velocidad, pero el descubrimiento de la clave (o del libro de claves, en su versión más sofisticada) compromete la seguridad de todas las informaciones protegidas con esta cifra.

- La cifra asimétrica[1278] utiliza dos claves, una para cifrar y otra para descifrar, de forma que ya no es necesario que el originador y el destinatario de la transmisión o del documento confidencial compartan ninguna clave.

  Las cifras asimétricas son muy seguras, pero no son tan eficientes computacionalmente como las cifras simétricas, y además incrementan de forma muy importante el volumen del objeto firmado.

A.1.1 Los algoritmos criptográficos

Los algoritmos que tienen por finalidad el tratamiento del secreto de la información se denominan criptográficos, e implementan el uso de cifras seguras en los servicios de seguridad de la TIC.

Un algoritmo criptográfico es una secuencia finita de reglas bien definidas para la solución de un problema, en este caso, orientado a la garantía de la seguridad de la TIC; conjuntamente con los datos, es la base del producto informático, formado habitualmente por un bien de equipo (hardware) y una aplicación o programa (software).

Los algoritmos criptográficos constituyen los mecanismos más importantes de los servicios de seguridad de las TIC y, por tanto, los mismos, y sus implementaciones en forma de programas, deben resultar confiables.

Uno de los principales inconvenientes de todos los algoritmos de cifrado es que, debido al tipo de problema matemático en el que se basan, cuya dificultad de resolución es precisamente lo que lo hace seguro – propiedad que se denomina "inviabilidad computacional" –, cuanto más tiempo transcurre desde su aplicación, mayor es la posibilidad de encontrar un algoritmo que produzca resultados fraudulentos, en especial debido al incremento progresivo de la capacidad de cálculo.

Por ejemplo, si nuestra clave secreta simétrica tiene 128 bits, existen aproximadamente 340 billones de cuatrillones de posibles claves[1279], por lo que en un ataque por fuerza

---

[1276] Cfr. definición 2126281 de la norma ISO/IEC 2382:2015, y atención al uso del también incorrecto término "desencriptar", igualmente generalizado, y tampoco recogido en el Diccionario de la Real Academia de la Lengua Española.

[1277] Cfr. la definición 2126290 de la norma ISO/IEC 2382:2015.

[1278] También denominada "de clave pública". Cfr. la definición 2126289 de la norma ISO/IEC 2382:2015.

[1279] 340.282.366.920.938.463.463.374.607.431.768.211.456 claves. Esto sería lo que habitualmente se conoce como "sixtillón", término que no aparece en el Diccionario de la Real Academia de la Lengua.

bruta el número de intentos que se debe realizar para descubrir la clave se considera computacionalmente inviable con la tecnología actual[1280].

En definitiva, ello implica que, por ejemplo, una firma digital creada hoy sea sólo segura mientras tanto el algoritmo como la clave empleada no hayan sido superados por la capacidad de cálculo de un atacante, entre otros retos; por lo que, en términos prácticos, se suelen marcar periodos de tiempo durante los cuales se considera seguro el empleo de una cifra, y transcurridos los mismos, resulta necesario aplicar medidas adicionales de protección a un testimonio de seguridad basado en criptografía, como una firma digital o un código de autenticación de mensaje.

No cabe decir que la seguridad de los algoritmos criptográficos es una de las principales preocupaciones del sector, por lo que la autorregulación establece normas muy concretas referidas al uso de los concretos algoritmos en cada protocolo y en cada momento del tiempo.

Por ejemplo, la especificación técnica IETF RFC 6151:2011 prohíbe el empleo del algoritmo de resumen MD5 en relación con la creación de firmas digitales[1281], aunque no en otros mecanismos de seguridad (Turner & Chen, 2011).

Por su parte, la especificación técnica IETF RFC 6194:2011 prohíbe el empleo del algoritmo de resumen SHA-0 en los protocolos de Internet, mientras que recomienda la sustitución del algoritmo de resumen SHA-1 por otros más robustos, como SHA-256, aunque no prohíbe el uso de SHA-1 debido al impacto que ello tendría en las infraestructuras de clave pública, empleadas en casi todos los protocolos de seguridad de Internet (Polk, Chen, Turner, & Hoffman, 2011).

Finalmente, y sin ánimo alguno de exhaustividad, la especificación técnica IETF RFC 7465:2015 prohíbe el uso del algoritmo simétrico RC4 en todas las versiones de TLS, debido a la existencia de debilidades demostradas académicamente que lo hacen vulnerable (Popov, 2015).

En todos estos casos, el autorregulador correspondiente[1282] toma una decisión indudablemente reguladora, con base en los descubrimientos publicados en instancias académicas o en otras instancias de autorregulación[1283], lo que aporta a dicha decisión una fuerte legitimación, así como un estándar aceptado que informa la actuación de todas las partes involucradas.

Veamos, a continuación, algunos de los algoritmos que se emplean en los servicios de seguridad de la TIC, dentro del ámbito de nuestro estudio[1284]: se trata de los algoritmos

---

[1280] Como indica (Mateti, 2013), el número de intentos para una clave de 128 bits sería aproximadamente de 170 billones de cuatrillones; sin embargo, recuerda que inviabilidad computacional no significa no computable, en el sentido de la teoría de la computabilidad, ni que no resulte posible diseñar ataques que encuentren la clave en un tiempo breve, empleando diversos tipos de técnicas, como, por ejemplo, de tipo heurístico.

[1281] Con base en las consideraciones previamente realizadas en (Hoffman & Schneier, 2005).

[1282] En relación con los protocolos y aplicaciones de Internet, nos referimos en gran medida al IETF, así como al W3C.

[1283] Como el NIST de los EEUU, que desde luego tiene un papel absolutamente relevante en materia de algoritmos criptográficos de amplia utilización.

[1284] No vamos a ver, en concreto, los algoritmos de cifrado, ya que los mismo se emplean para la

de resumen, de código de autenticación de mensaje y de firma digital.

A.1.1.1 Los algoritmos de resumen

El algoritmo de resumen permite obtener una versión reducida de un conjunto de datos, como por ejemplo un documento que hay que firmar digitalmente. De acuerdo con la norma internacional ISO/IEC 10118-1:2000 (2ª ed.)[1285], los algoritmos de resumen resultan aplicables a los servicios de autenticación, integridad y no rechazo[1286].

Este sistema se aplica de forma independiente o en combinación con otros algoritmos criptográficos, como los códigos de autenticación de mensaje o la firma digital, por razones de eficacia[1287], compatibilidad e integridad.

También en la generación de sellos de tiempo electrónicos se emplean resúmenes criptográficos, en concreto sobre los objetos digitales a proteger mediante los sellos de tiempo, de forma que estos resúmenes se incorporan a los sellos de tiempo electrónico, que se firman digitalmente para su seguridad.

Otras aplicaciones que requieren autenticación y/o integridad, pero no rechazo, también utilizan estos algoritmos de resumen. Por ejemplo, para la transmisión segura de una contraseña se envía el resumen criptográfico de la misma, en lugar de la contraseña en claro, permitiendo la autenticación sin revelar el secreto en cuestión.

El algoritmo de resumen perfecto debe garantizar una serie de condiciones[1288]:

- Debe ser unidireccional; esto es, dado un conjunto de datos, la posibilidad de encontrar un segundo conjunto de datos con el mismo hash debe requerir 2^L operaciones, donde L es el número de bits del resumen.
- Debe ser resistente a colisiones; esto es, la posibilidad de encontrar dos conjuntos de datos diferentes con el mismo resumen criptográfico debe requerir $2^{\frac{L}{2}}$ operaciones, donde L es el número de bits del algoritmo.

Es importante reseñar que existen diversos algoritmos de resumen criptográfico, incluyendo algoritmos de resumen basados en bloques de n-bits[1289], en funciones dedicadas[1290] y en aritmética modular[1291]; de entre los cuales se debe emplear el que corresponda en función de las necesidades, y dentro del marco de la autorregulación o

---

confidencialidad.

[1285] El título de la norma es Tecnología de la información – Técnicas de seguridad – Funciones de resumen – Parte 1: General, y se encuentra actualmente en revisión. La primera edición es de 1994.

[1286] Cfr. sección 1 de la norma.

[1287] La firma digital creada a partir de un mensaje breve es más corta que sobre un mensaje largo, y lógicamente requiere menor capacidad de cómputo.

[1288] Cfr. sección 3.5 de la norma internacional ISO/IEC 10118-1:2000, así como (Hoffman & Schneier, 2005).

[1289] Cfr. la norma internacional ISO/IEC 10118-2:2010 (3º ed.)

[1290] Cfr. la norma internacional ISO/IEC 10118-3:2004 (3ª ed.), modificada en 2006, que normaliza algoritmos como RIPEMD, SHA y WHIRLPOOL.

[1291] Cfr. la norma internacional ISO/IEC 10118-4:1998 (1ª ed.), que normaliza los algoritmos MASH. Existen correcciones y modificaciones en 2014.

legislativo que corresponda en cada caso.

A.1.1.2 Los algoritmos de código de autenticación de mensaje

Un código de autenticación de mensaje se define como una cadena de bits producida en función tanto de datos (ya sea de texto plano o texto cifrado) y una clave secreta, y que se adjunta a los datos con el fin de permitir la autenticación de datos[1292].

Dado que ambas partes comparten la clave secreta, este tipo de algoritmo sustenta autenticación de origen de datos entre ellas[1293], así como integridad, pero no el no rechazo entre ellas.

Es importante reseñar que existen diversos algoritmos de código de autenticación de mensaje, incluyendo algoritmos basados en cifras de bloque[1294], en funciones de resumen dedicadas[1295] y utilizando funciones de resumen universal [1296]; de entre los cuales se debe emplear el que corresponda en función de las necesidades, y dentro del marco de autorregulación o legislativo que corresponda en cada caso.

A.1.1.3 Los algoritmos de firma digital

Una firma digital se define, desde una óptica general, como los datos adjuntos a un mensaje que permiten al destinatario del mensaje verificar el origen del mismo[1297].

El algoritmo de firma digital se basa en una cifra asimétrica; es decir, formada por una clave privada y una clave pública, que permite "firmar" documentos con la clave privada y verificar la firma digital con la clave pública.

Criptográficamente, firmar digitalmente es generar un dato matemático asociado al objeto digital[1298] (como, por ejemplo, un documento electrónico), empleando una clave privada que sólo conoce el firmante, de la misma manera que en el mundo físico, firmar es producir personalmente un grafismo fijado al soporte material que contiene el documento. Por analogía entre ambos, se considera que la firma digital es un mecanismo apropiado para el no rechazo.

La firma digital ofrece también integridad, que nos permite determinar que un objeto digital no ha sido manipulado, así como la autenticación, que nos permite comprobar cuál ha sido la entidad que ha originado el documento.

[1292] Definición 2126391 de la norma internacional ISO/IEC 2382:2015.

[1293] Pero no frente a terceros, dado que un tercero no puede determinar cuál de las dos partes que poseen la clave ha generado el código de autenticación de mensaje.

[1294] Cfr. la norma internacional ISO/IEC 9797-1:2011 (2º ed.)

[1295] Cfr. la norma internacional ISO/IEC 9797-2:2011 (2ª ed.), que emplea los algoritmos de resumen normalizados en ISO/IEC 10118-3:2004 y su modificación de 2006.

[1296] Cfr. la norma internacional ISO/IEC 9797-3:2011 (1ª ed.), que emplea los algoritmos de resumen universal UMAC, Badger, Poly1305-AES y GMAC.

[1297] Definición 2126378 de la norma internacional ISO/IEC 2382:2015.

[1298] Típicamente, cifrando el resumen criptográfico del documento con la clave privada, lo que permite la "verificación" de la firma digital, mediante el descifrado del resumen y su comparación con un nuevo resumen del documento a comprobar.

El algoritmo de firma digital debe garantizar una serie de condiciones[1299]:

- Debe ser irreversible, en un doble sentido; en primer lugar, de la clave pública no se debe poder obtener una firma digital válida para ningún mensaje; en segundo lugar, a partir de una firma digital no se debe poder generar otra firma digital ni obtener la clave privada.
- La firma digital producida debe ser única para cada documento; es decir, no se debe poder encontrar dos mensajes diferentes para una misma firma digital, ni siquiera por parte del firmante.

Existen diversos algoritmos de firma digital, incluyendo mecanismos de firma[1300] basados en factorización de enteros[1301] o en logaritmos discretos[1302], así como de firma digital anónima[1303] – en los cuales ninguna entidad no autorizada, incluyendo al verificador de una firma digital, puede conocer la identidad del firmante, pero manteniéndose la característica de que sólo un firmante legítimo puede generar firmas digitales válidas[1304] –; de entre los cuales se debe emplear el que corresponda en función de las necesidades, y dentro del marco de autorregulación o legislativo que corresponda en cada caso.

En general, el algoritmo de firma digital funciona de forma conjunta con uno de resumen, por cuestiones de eficiencia computacional, como se puede ver en la Ilustración 19[1305], referido a las primitivas matemáticas de los correspondientes algoritmos[1306].

Normalmente será en la norma o especificación técnica que defina cada protocolo, servicio de seguridad o aplicación de firma digital donde se concreten los algoritmos de firma digital que se pueden o deben emplear en cada caso, dejando libertad a las partes para tomar la decisión que mejor consideren, excepto en aquellos casos donde exista una legislación imperativa que imponga sus propias reglas, como veremos sucede en algunos casos.

Por ejemplo, en las especificaciones técnicas IETF RFC 3370 y 5754 se indican, entre otros, los algoritmos de firma digital que se pueden emplear para la sintaxis de mensaje criptográfico (CMS), un formato empleado en aplicaciones como el correo electrónico seguro S/MIME o en la firma de documentos en PDF, y que veremos posteriormente con

---

[1299] Cfr. la norma internacional ISO/IEC 9796-2:2010, introducción.

[1300] Los mecanismos de firma digital se clasifican también en algoritmos con recuperación de mensajes y con apéndice.

[1301] Cfr. las normas internacionales ISO/IEC 9796-2:2010 y 14888-2:2008.

[1302] Cfr. las normas internacionales ISO/IEC 9796-3:2006 y 14888-3:2006.

[1303] Cfr. las normas internacionales ISO/IEC 20008-1:2013 y 20008-2:2013.

[1304] La norma internacional prevé cuatro casos de uso diferentes: a) un mecanismo que permite a una entidad autorizada conocer la identidad del firmante; b) un mecanismo que permite a una entidad autorizada comprobar que dos firmas son del mismo firmante, pero sin conocer su identidad; c) un mecanismo que involucra a las entidades autorizadas en los casos a) y b); y d) un mecanismo que no involucra a ninguna de las entidades autorizadas en los casos a) y b).

[1305] Wikimedia Commons, en http://es.wikipedia.org/wiki/Archivo:Firma_Digital.png.

[1306] En este gráfico se muestra la operativa de firma y verificación de firma empleando el algoritmo RSA_PKCS1_v1.5, un mecanismo de firma digital con apéndice basado en factorización de enteros. Se trata de uno de los algoritmos más empleados en las aplicaciones actuales. Cfr. RSA Laboratories PKCS#1 v2.2: RSA Cryptography Standard.

algo más de detalle, dado su indudable interés desde la óptica pericial informática.

A.1.2 Las claves criptográficas

Las claves criptográficas son los elementos numéricos que forman una cifra criptográfica, y que funcionan conjuntamente con los algoritmos criptográficos para generar firmas electrónicas y las formas de autenticación o para hacer confidencial un documento.

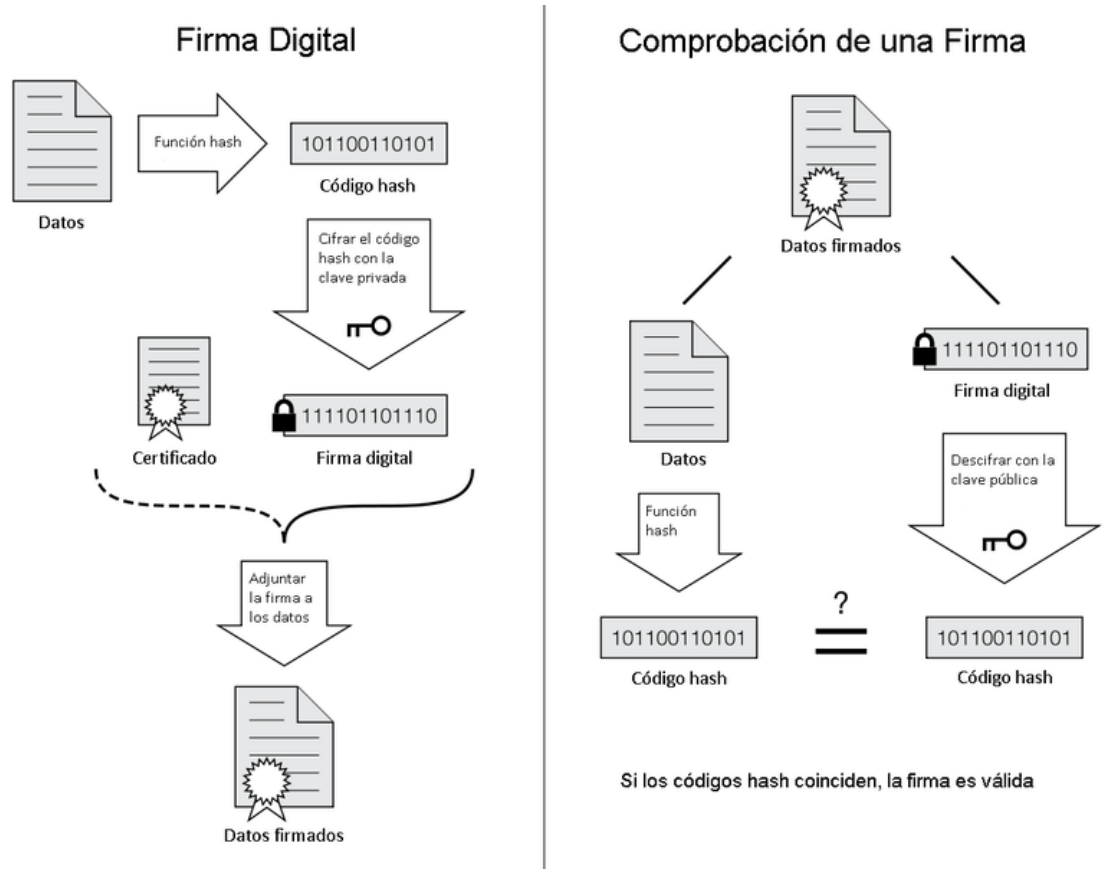


Ilustración 19. Firma digital con RSA PKCS#1-5

La clave criptográfica se define[1307] como la secuencia de símbolos que controla el funcionamiento de una transformación criptográfica (por ejemplo, cifrado, descifrado, criptográfica función de comprobación de cálculo, la generación de la firma, o de verificación de firma).

Por este motivo, las claves son elementos importantes y, eventualmente, críticos de los servicios de seguridad de las TIC en general, y de los mecanismos de firma digital en particular: conocer la clave de una persona implica adquirir la capacidad de autenticarse o firmar en nombre de otro, o de poder acceder a sus datos secretos.

A.1.2.1 Las parejas de claves criptográficas

Una clave criptográfica privada es un dato numérico, que forma parte de una cifra, y que debe ser secreto, porque sirve para autenticarse, firmar o acceder a datos confidenciales.

En las cifras asimétricas, las que se utilizan para la generación de la firma digital[1308],

[1307] Cfr. la norma internacional ISO/IEC 11770-1:2010.

[1308] Como veremos posteriormente, la firma digital es uno de los mecanismos que sustenta la firma o sello electrónicos avanzados (también en los reconocidos/cualificados).

existen dos claves, de las cuales una es privada y la otra pública. Los que firman digitalmente lo hacen con la clave privada, mientras que los terceros que reciben documentos firmados digitalmente los validan con la clave pública, que no es necesario sea secreta.

De hecho, la idea es que esta segunda clave sea lo más pública posible, motivo por el cual se suele certificar la clave pública, en asociación con los datos de identidad de la persona que posee la clave privada, para que se pueda librar esta clave pública certificada, habitualmente a través de aplicaciones y la red Internet, y que llegue a cualquier potencial destinatario de documentos firmados o sellados, como posteriormente veremos.

A.1.2.2 La correlación entre las claves criptográficas

La correlación entre claves criptográficas es el ligamen matemático que existe entre la clave privada y la clave pública, que permite utilizar una clave para hacer una acción (firmar, por ejemplo) y la otra clave para deshacerla (por tanto, en nuestro ejemplo, validando la firma).

Como es evidente, sin este ligamen, que es propio de las cifras asimétricas, el sistema no funcionaría. El ligamen, sin embargo, ha de permitir garantizar la seguridad del sistema, de forma que el conocimiento de la clave pública no suponga una amenaza para la clave privada (propiedad frecuentemente denominada irreversibilidad).

A.1.2.3 La longitud de las claves criptográficas

La longitud de la clave criptográfica es una propiedad de la clave que consiste en el límite superior del espacio numérico de la cifra, y que por tanto determina el número de combinaciones que debería probar un atacante que quisiera adivinar la clave y, por tanto, el grado teórico de inviabilidad computacional de la cifra[1309].

La longitud de la clave criptográfica se determina en bits, debiéndose emplear la que corresponda en función de las necesidades, y dentro del marco de la regulación que resulte aplicable en cada caso.

A título de ejemplo, en relación con el correo electrónico seguro S/MIME, la RFC 5751:2010 establece normas imperativas referidas a la longitud de las claves aceptables para este propósito en particular.

A.1.2.4 La gestión de las claves criptográficas

La gestión de claves se define como el conjunto de actuaciones de generación, registro, certificación, cancelación del registro, distribución, instalación, almacenamiento, archivo, revocación, derivación y destrucción de material de claves, de acuerdo con una política de seguridad concreta[1310].

La autorregulación de estas actuaciones, como es lógico, se completa mediante reglas específicas en función del tipo de claves a gestionar:

- En el caso de las claves simétricas, y entre otras, encontramos reglas[1311] aplicables

[1309] Por ello, su relación con el grado de confianza que podemos depositar en el sistema es total.

[1310] Sección 2.28 de la norma internacional ISO/IEC 11770-1:2010.

[1311] Cfr. la norma internacional ISO/IEC 11770-2:2008.

a mecanismos de establecimiento de claves punto a punto[1312], mecanismos que emplean centros de distribución de claves[1313] y centros de traducción de claves[1314], así como reglas[1315] aplicables a mecanismos de negociación de claves y transporte de claves secretas.

- En el caso de las claves asimétricas, y entre otras, encontramos reglas[1316] aplicables al transporte de claves públicas, así como al ciclo de vida general de la gestión de claves por parte de terceros de confianza[1317].

De una correcta gestión de claves depende, en realidad, toda la confianza en el sistema criptográfico en cuestión, por lo que se trata de una de las cuestiones en relación con la que se ha producido una completa autorregulación.

Anteriormente hemos visto que, en las cifras asimétricas, para crear una firma digital se emplea la clave privada, mientras que la clave pública se emplea para la verificación de la misma; y que por ello resulta esencial poder determinar a qué entidad (persona, dispositivo, etc.) pertenece una clave pública.

Asimismo, mediante una adecuada gestión de las claves, podemos asociar un par de claves a una entidad, de forma que podremos, en principio, asumir que las firmas digitales que sean verificables empleando una clave pública serán imputables a la entidad a la que hemos asociado la clave privada correspondiente.

Como se puede intuir, un reto importante para la extensión del uso de las firmas digitales viene dado por la necesidad de dar a conocer las claves públicas de las entidades que poseen las correspondientes claves privadas, por lo que los mecanismos de distribución y certificación de claves criptográficas públicas revisten gran importancia.

A.1.2.5 La distribución de claves públicas, en general

Existen muchas formas de distribuir claves públicas, en función de las circunstancias concretas. Por ejemplo, en la comunidad de usuarios de aplicaciones de firma digital basadas en el formato OpenPGP[1318] la distribución de claves se realiza mediante el intercambio directo de claves entre personas que se encuentran personalmente[1319].

Otra posibilidad para distribuir claves públicas es establecer directorios de claves de acceso público en Internet, donde las partes puedan conectarse para obtener las claves. Un ejemplo, referido al mismo protocolo OpenPGP anteriormente mencionado, es el

---

[1312] En este caso, se produce el establecimiento directo de claves entre las partes, sin la participación de un tercero de confianza.

[1313] Un tercero de confianza que se ocupa de generar o adquirir claves, y distribuirlas a las partes que se comunican, compartiendo una clave simétrica única con cada una de las partes, para dichos cometidos.

[1314] Un tercero de confianza que se ocupa a descifrar una clave que se generó y se cifró por una de las partes y se volvió a cifrar para entregarla a otra parte.

[1315] Cfr. la norma internacional ISO/IEC 11770-3:2015.

[1316] Cfr. la norma internacional ISO/IEC 11770-3:2015.

[1317] Cfr. la norma europea ETSI EN 319 411-1, así como los CAB Forum Baseline Requirements.

[1318] Cfr. la especificación técnica IETF RFC 4880.

[1319] En encuentros frecuentemente denominados “fiestas de firma de claves”; Cfr. (Brennen, 2008).

Directorio Global de PGP – Servicio de clave verificada[1320], al cual las personas pueden subir sus claves públicas para facilitar su recuperación por otras personas[1321].

Otro ejemplo de depósito de claves públicas lo podemos ver en la especificación técnica conocida como XKMS, del Consorcio W3C, que define protocolos para la distribución y el registro de claves públicas, para su uso con la sintaxis de firma digital XML, también del consorcio W3C.

En este caso, cuando se crea una firma digital en XML, se puede indicar el nombre de la clave pública que sirve para verificar la firma digital, así como a qué depósito debe acudir el receptor del documento firmado para obtener la clave pública, facilitando su distribución. Nótese que, en muchos casos, la clave que será objeto de registro habrá sido previamente certificada.

A.2 Los certificados de clave pública

Como el intercambio directo de claves entre personas no es un sistema que crezca fácilmente hasta cubrir a millones de personas, otra forma de distribuir claves es certificarlas – esencialmente, pedir que alguien en quien se confía la asocie digitalmente a su titular –, para lo cual existen diversos modelos.

En este sentido, la certificación de claves responde a la necesidad de establecer un cierto grado de confianza en el hecho de que una clave pública pertenece a una persona en concreto, sin tener que relacionarse directamente con dicha persona. Para ello, la clave pública debe ser obtenida de una fuente confiable, y constituye un importante testimonio de seguridad en soporte de los servicios de autenticación, integridad y no rechazo.

En el caso de OpenPGP, la confianza se basa en un sistema en el que cada clave pública de una persona es firmada por otras personas, con las que el usuario se ha encontrado en persona, o que disponen de claves firmadas por personas en las que el usuario confía, creando un sistema altamente descentralizado que permita confiar en que la clave es efectivamente de esa persona[1322].

Otra posibilidad es encargar una certificación de la clave pública, infalsificable[1323], a una autoridad de certificación, proceso alrededor del cual se ha establecido una potente autorregulación de la industria.

La Recomendación de la ITU-T X.509 constituye, desde finales de los años 80 del siglo pasado, la norma técnica de base[1324] para las denominadas infraestructuras de

---

[1320] Disponible en http://keyserver.pgp.com/

[1321] Este servicio incorpora una política de verificación de claves que advierte claramente acerca de las limitaciones de servicio respecto a la efectiva verificación de las claves, ya que el mismo esencialmente se basa en la remisión de una confirmación del correo electrónico de la persona que remite la clave para registro.

[1322] Este sistema se ha denominado como Web of Trust (telaraña de confianza).

[1323] El certificado es infalsificable porque está firmado digitalmente por la entidad que lo expide, como veremos.

[1324] El entonces denominado CCITT, Comité Consultivo Internacional Telegráfico y Telefónico, había aprobado, en noviembre de 1988, la Recomendación X.509 (inicialmente publicada en el Libro Azul, Fascículo VIII.8), que también sería publicada en 1990 como norma internacional ISO/IEC 9594-8, así como una segunda edición en 1993, y se estaba finalizando una tercera edición, que se publicaría en 1997.

certificación de clave pública (ICP o, en inglés, PKI) y, desde su edición de 1997, de certificación de atributos (a las que denomina de gestión de privilegios[1325], IGP o, en inglés, PMI); esto es, la base del complejo sistema técnico, jurídico, de seguridad y de organización que hoy ofrece soporte a los servicios de certificación y de firma digital[1326].

En general, la norma internacional define un marco de trabajo para los certificados, incluyendo la definición de los objetos de datos empleados para representar a dichos certificados, y de los mecanismos para informar acerca de los certificados que han perdido su validez, pero, como la propia norma indica, no define completamente estas infraestructuras, por lo que permite una base común a partir de la cual la industria autorregule diversos esquemas de uso, en función del caso.

Y, de hecho, así ha sucedido en los últimos años. Uno de los casos más relevantes consiste en la autorregulación realizada por el IETF[1327], mediante la constitución de un grupo de trabajo específico denominado PKIX[1328], de una colección de especificaciones técnicas para el uso de los certificados de clave pública (Cooper, y otros, 2008) y de atributos para la autorización (Farrell, Housley, & Turner, 2010), a partir de las cuales se ha creado, como veremos posteriormente, aún más autorregulación sectorial[1329].

Existe, por tanto, una multiplicidad de formatos técnicos de certificados, que se aplican a situaciones reales para producir diferentes tipos o clases de certificados, de acuerdo con perfiles personalizados de certificados y con políticas concretas de certificación[1330].

Esta Recomendación | Norma internacional regulaba el uso de técnicas de autenticación simple y autenticación fuerte basada en criptografía para el acceso al Directorio, pero permitiendo también su uso potencial para otras aplicaciones, y se ha convertido en la base de la infraestructura de clave pública. Por este motivo, a partir de la cuarta edición, del año 2000, se centra en la definición de un marco de trabajo para los certificados de clave pública y de atributos. La edición vigente, séptima, es del año 2012. Aunque existen diversas ediciones, se suele hablar del certificado X509 versión 3.

[1325] Se emplea este término de privilegio porque, en esta norma internacional emplea los certificados de atributos en el contexto de un servicio de control de acceso al Directorio; en este sentido, los atributos representan derechos de acceso; posteriormente, en otras normas o especificaciones técnicas se amplía la semántica de estos certificados, que pueden emplearse para incluir, por ejemplo, informaciones acerca de la capacidad de representación legal, para su uso en el contexto de una firma digital que deba producir efectos jurídicos; cfr. la especificación técnica ETSI TS 102 158 V1.1.1:2003.

[1326] Para una descripción técnica completa de las infraestructuras de clave pública, cfr. (Ford & Baum, 1997), y entre nosotros, desde una perspectiva eminentemente jurídica, (Martínez Nadal, 1998).

[1327] Internet Engineering Task Force, una comunidad internacional de diseñadores, operadores, fabricantes e investigadores sobre las redes, que desarrolla las principales especificaciones técnicas de Internet (Alvestrand, 2004).

[1328] El grupo de trabajo fue creado en octubre de 1995 con el objetivo de desarrollar estándares de Internet en soporte de las PKI basadas la Recomendación ITU-T X.509. Si bien inicialmente perseguía únicamente concretar cómo se debían emplear los certificados X.509 mediante perfiles de detalle técnico, posteriormente el grupo empezó a desarrollar iniciativas dirigidas a resolver la problemática propia de la PKI en Internet, que se han convertido en la principal línea de trabajo.

[1329] De nuevo se trata de un enfoque laxo, en el que no se persigue normalizar nada que no sea estrictamente necesario, ni mucho menos de establecer excesivos detalles, lo que permite la reutilización de los materiales por parte de otros esfuerzos de autorregulación. Cfr. (CA/Browser Forum, 2017b) y (CA/Browser Forum, 2017a)

[1330] Como veremos, estas políticas son un elemento importante de la autorregulación.

Desde la perspectiva de la autorregulación, los certificados digitales se pueden clasificar de acuerdo con diversos criterios, entre los cuales en función del objeto; en atención al propósito de uso de la clave; o de la entidad cuya clave se certifica.

A continuación, presentamos estas tipologías de certificados, dejando para más adelante otros aspectos de la autorregulación de los certificados, por razones metodológicas[1331].

A.2.1 Tipos de certificados, en función del objeto

En función del objeto, podemos diferenciar los certificados de clave pública de los certificados de atributos.

El certificado de clave pública, como su nombre indica, contiene la clave pública de una persona o entidad identificada en el propio certificado, que dispone de la clave privada correspondiente para su uso en el mecanismo o servicio de seguridad correspondiente; típicamente, firmar documentos, autenticarse ante terceros o descifrar documentos que hayan sido cifrados por terceros utilizando su clave pública.

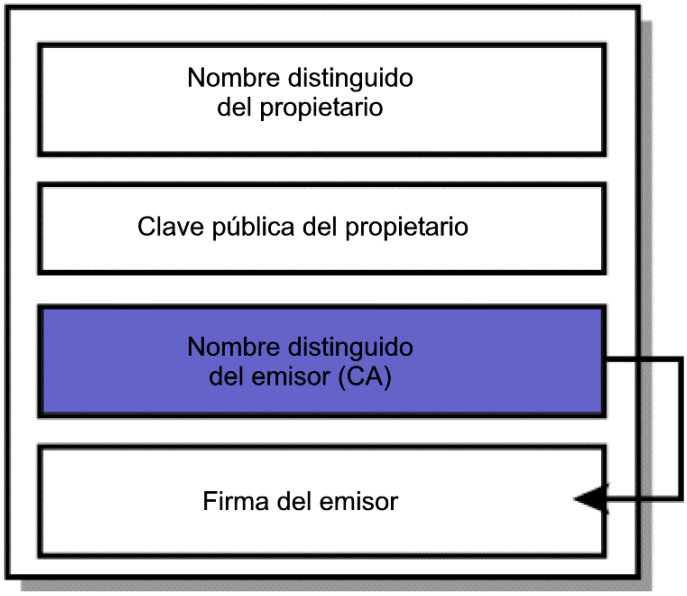


Ilustración 20. Diseño simplificado de un certificado digital (IBM)

Los certificados de atributos, por otra parte, no contienen ninguna clave pública, sino sencillamente la identificación de la persona – generalmente mediante una referencia a su certificado de clave pública – y un conjunto de atributos.

Estos certificados se utilizan para certificar información muy variable en el tiempo, o que no se desea o no se puede incluir en el certificado de clave pública[1332].

Habitualmente, el certificado de clave pública también contiene otras informaciones

[1331] En efecto, en este momento sólo nos interesa conocer acerca de la existencia de los certificados digitales, no todos los detalles acerca de su gestión, que será más interesante presentar posteriormente.

[1332] Los certificados de atributos precisamente fueron diseñados para poder certificar informaciones de efímera vida, incluso de minutos.

personales[1333], en cuyo caso, se suelen denominar certificados de clave pública con atributos o, sencillamente, certificados con atributos.

El certificado es un elemento de indudable valor probatorio en soporte de la firma digital, dado que en realidad contiene toda la información en la que confiamos, y que asumimos verídica; por lo que conviene presentar los contenidos más relevantes[1334] de un certificado de clave pública previstos en la autorregulación de las aplicaciones de Internet[1335], para lo cual emplearemos, a título de ejemplo, el certificado personal del autor de este trabajo:

- Un número de serie (campo `serialNumber`), que debe ser único para cada certificado expedido por una autoridad de certificación.
- El algoritmo de firma digital (campo `signature`) empleado por la autoridad de certificación para firmar el certificado.
- La identificación de la autoridad de certificación que expide el certificado (campos `issuer` e `issuerAltName`), mediante uno o varios nombres formados por una colección de atributos, que típicamente incluyen el país, el nombre de la organización o de alguna unidad organizativa o un nombre común.

  El nombre del emisor de este certificado es "CN = EC-IDCat; OU = Entitat publica de certificacio de ciutadans; OU = Vegeu https://www.catcert.net/verCIC-2 (c)03; OU = Serveis Publics de Certificacio ECV-2; L = Passatge de la Concepcio 11 08008 Barcelona; O = Agencia Catalana de Certificacio (NIF Q-0801176-I); C = ES".

  Este emisor indica, como nombre alternativo, la dirección de correo electrónico "ec_idcat@catcert.net".
- El periodo de validez del certificado (campo `validity`), que es el periodo durante el cual la autoridad de certificación que expide el certificado debe garantizar que mantendrá información sobre el estado – de revocación – del certificado[1336], y, por tanto, el periodo durante el que se puede confiar en el mismo.
- La identificación del sujeto[1337] para el que se expide el certificado (campos `subject` y `subjectAltName`), mediante un nombre formado por una colección de atributos, que típicamente incluyen el país, el nombre de la organización o de alguna unidad organizativa o un nombre común.

  Este certificado identifica al sujeto vinculado a la clave pública de la siguiente

---

[1333] Estos atributos pueden ser de lo más variado, y la práctica habitual – seguramente influida por la propia legislación – muestra como ejemplos como por ejemplo la inclusión de un cargo administrativo o la condición de profesional colegiado del titular del certificado, por ejemplo.

[1334] El certificado contiene también informaciones de carácter accesorio, que no presentaremos por no ser relevantes para nuestro análisis.

[1335] Cuyos aspectos básicos y comunes se contienen en (Cooper, y otros, 2008), modificada por (Yee, 2013).

[1336] Se trata de una norma de indudable contenido obligatorio, definida desde la perspectiva de la semántica de este campo.

[1337] Esta entidad puede ser una persona, una organización, un dispositivo técnico o un programa de informático, entre otros.

forma: “CN = IGNACIO ALAMILLO DOMINGO; SERIALNUMBER = 43714981P; G = IGNACIO; SN = ALAMILLO DOMINGO; OU = Serveis Publics de Certificacio CPIXSA-2; OU = Vegeu https://www.catcert.cat/veridCAT (c)03; C = ES”, y, como nombre alternativo, incluye una dirección de correo electrónico[1338].

- La información de clave pública del sujeto (campo `subjectKeyInfo`), así como, en su caso, los parámetros correspondientes.
- La autorización del uso de la clave (campos `keyUsage` y `extendedKeyUsage`), donde se determina, por ejemplo, si el certificado está pensado para ser empleado en el contexto de un servicio de no rechazo, o de autenticación, o confidencialidad, entre otros.
- La política de certificación aplicable (campo `certificatePolicy`), que regula el uso del certificado, apuntando a la página web de la autoridad de certificación donde se contiene dicha información.
- Uno o varios atributos adicionales del sujeto (campo `subjectDirectoryAttributes`), según convenga; como, por ejemplo, el Estado de nacionalidad o de residencia, entre otros muchos posibles.
- Información sobre dónde obtener información de estado de revocación del certificado (campos `crlDistributionPoints`, `freshestCRL` y `authorityInfoAccess`), útil para que los terceros puedan comprobar si el certificado es válido.

A continuación, se muestra la representación gráfica del certificado anteriormente presentado[1339]:

[1338] De esta forma, el certificado funciona conjuntamente con aplicaciones de correo electrónico seguro basadas en el protocolo S/MIME.

[1339] Tal y como el mismo se presenta en el sistema operativo Windows.

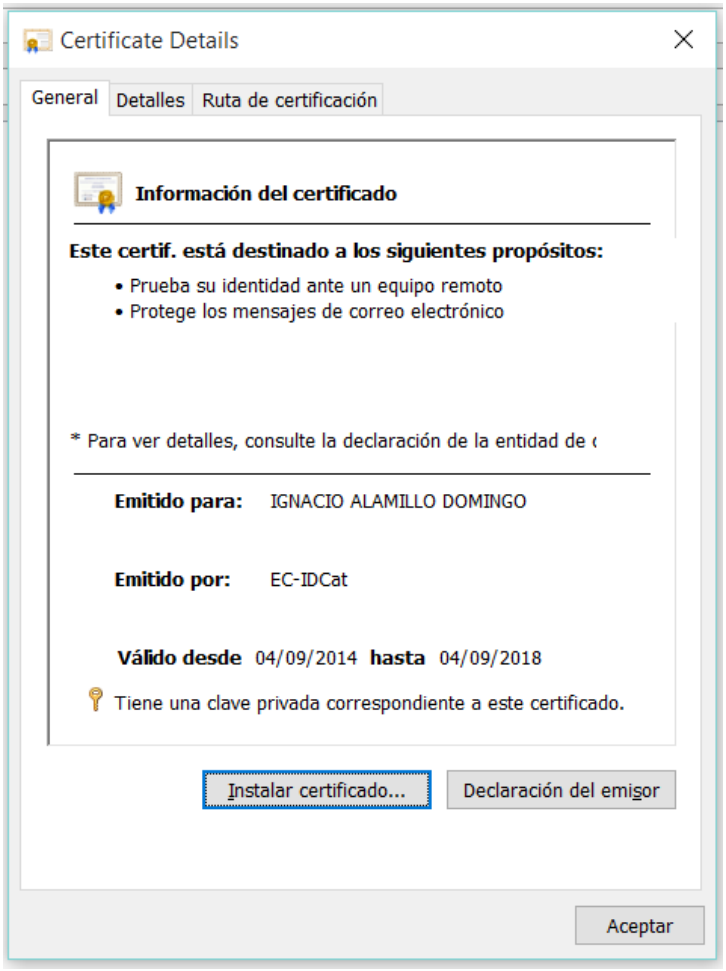


Ilustración 21. Certificado de firma digital de persona física (general)

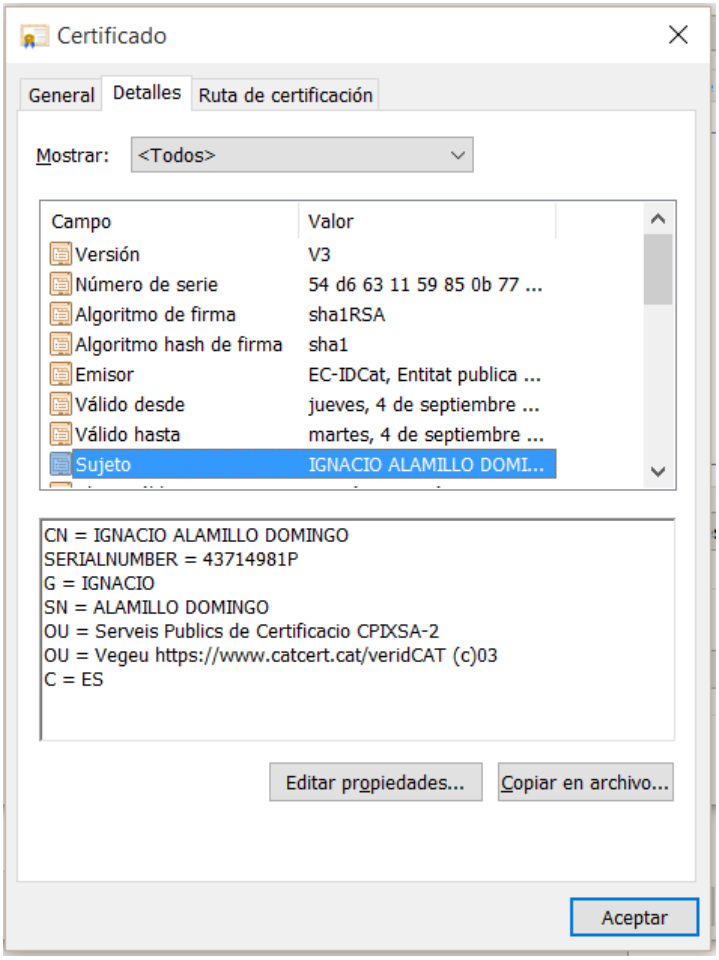


Ilustración 22. Certificado de firma digital de persona física (detalles)

A.2.2 Tipos de certificados, en función de la finalidad de uso

Los certificados de clave pública se han ido especializando en función de aquellas finalidades en relaciones con las que se prevé el uso de la clave.

En función de estas finalidades, especialmente cuando la misma entidad recibe diferentes certificados, se suele hablar de certificados de autenticación, certificados de firma digital y certificados de cifrado; distinción que se establece en atención al uso autorizado de la clave contenida en el certificado, como hemos visto anteriormente.

Sin embargo, existen muchos otros tipos de certificados previstos en diversas autorregulaciones, resultando muy destacables – por su extendido uso en la actualidad[1340] – los siguientes.

En primer lugar, encontramos los certificados de servidor seguro, para la autenticación de servidores de Internet, y el establecimiento de comunicaciones confidenciales con los mismos, empleando el protocolo TLS[1341].

[1340] No son los únicos ejemplos. Históricamente han existido algunas propuestas, hoy en desuso, como el protocolo Secure Electronic Transaction o Identrust, ambas nacidas en el ámbito de las entidades financieras.

[1341] En SSL/TLS se emplean mecanismos criptográficos para la autenticación de una (servidor web) o

Aunque el caso de uso más importante quizá sea el acceso a sitios web mediante HTTPS, realmente se pueden emplear para el acceso a otros tipos de servidores como, por ejemplo, servidores de ficheros (FTP), el acceso a los servidores para la obtención (POP3 o IMAP) y la remisión de correo electrónico (SMTP), etc.

En relación con estos certificados se ha producido una potente autorregulación de la industria, orientada a ofrecer una garantía suficiente de uno de los procesos de autenticación más relevantes y empleados en Internet, dado que se emplea para el aseguramiento del acceso a la mayoría de servicios de Internet.

En concreto, resulta necesario referirse a una asociación de la industria[1342] denominada CA/Browser Forum[1343], que ha publicado un conjunto de especificaciones que establecen los requisitos mínimos en relación con la gestión de los certificados digitales de servidor seguro[1344], con un enfoque muy fuerte en la verificación de la identidad del titular del servidor certificado, por lo que dichos certificados pueden ser reconocidos como de confianza por parte de los clientes informáticos de forma automática[1345].

En segundo lugar, tenemos los certificados de firma de código, que se emplean para la garantía de la integridad del código de las aplicaciones informáticas que deben ser objeto de distribución por Internet y de la identidad de la persona u organización que las distribuya, entre otros usos.

También en este caso se ha creado una importante autorregulación, en el CA/Browser Forum, en forma de requisitos mínimos para la gestión de este tipo de certificados[1346].

Fuera del ámbito de los protocolos de Internet, también encontramos tipos de certificado[1347] de muy amplia utilización, entre los que podemos destacar algunos

---

ambas partes (servidor y cliente web). SSL fue creado y publicado por la compañía privada Netscape Communications Inc y la versión 3.0 de la especificación, de 1996, fue publicada por IETF en la RFC 6101:2011, sin la categoría de norma de Internet y a exclusivos efectos informativos. TLS, que es la versión normalizada en IETF de SSL, y su sucesor a todos los efectos futuros, se encuentra definido y ampliamente regulado en las especificaciones técnicas del IETF 2246:1999 (TLS 1.0), RFC 3546:2003 (Extensiones de TLS 1.0), RFC 4346:2006 (TLS 1.1), RFC 4347:2006 (Datagram Transport Layer Security o DTLS 1.0), RFC 4366:2006 (extensiones de TLS 1.1), RFC 5246:2008 (TLS 1.2), RFC 5746:2010 (Extensión de indicación de renegociación de TLS), RFC 6176:2011 (Prohibición de uso de SSL 2.0), RFC 6347:2012 (DTLS 1.2), RFC 6520:2012 (Extensión Heartbeat a TLS y DTLS), RFC 7465:2015 (Prohibición de uso de los conjuntos de cifra RC4), RFC 7507:2015 (Prevención de ataques de degradación de protocolo) y RFC 7568:2015 (Obsolescencia de SSL 3.0), entre otras.

[1342] Formada por los principales fabricantes de clientes informáticos de acceso a web, como Apple, Google, Microsoft o Mozilla, y múltiples autoridades de certificación, entre las cuales las españolas Camerfirma, Firmaprofesional o ANF.

[1343] https://cabforum.org/

[1344] Principalmente, los documentos Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, versión 1.3.0, de 16 de abril de 2015; y Guidelines For The Issuance And Management Of Extended Validation Certificates, versión 1.5.6, de 25 de junio de 2015.

[1345] Este reconocimiento se basa en el hecho de que los fabricantes de clientes informáticos programan sus aplicaciones precisamente para ello, por lo que la eficacia de esta autorregulación para promover la confianza resulta extraordinaria – nótese que sin que la legislación juegue papel alguno en ello.

[1346] Cfr. el documento Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates, versión 1.3, de 16 de septiembre de 2014.

[1347] Estos certificados no suelen seguir el formato X.509 o la RFC 5280, sino que suelen tener su propio

ejemplos.

En primer término, podemos mencionar los certificados de tarjeta de pago con microchip, que se emplean para la autenticación de la tarjeta conforme a la autorregulación[1348] de las entidades financieras, canalizada a través de la organización EMV[1349].

En segundo término, resulta interesante el caso de los certificados de dispositivo para la protección de contenido digital, que se expiden a los productos – físicos o lógicos – de reproducción de vídeo de alta definición, como Bluray o HDD, para que los mismos estén identificados y puedan reproducir el contenido, que se encuentra cifrado.

Estos certificados se autorregulan en el marco de una entidad creada por la industria[1350], denominada Advanced Access Content System Licensing Administrator (AACS LA)[1351]. La autorregulación se contiene en las especificaciones técnicas producidas por dicha entidad[1352], que pueden emplearse en los términos establecidos por un contrato de licencia. Asimismo, el AACS LA actúa como autoridad de certificación de los correspondientes certificados, de forma exclusiva.

A.2.3 Tipos de certificados, en función de la entidad cuya clave se certifica

En toda infraestructura de clave pública se diferencia entre certificados de autoridad y certificados de usuario final.

El certificado de autoridad es un certificado de clave pública expedido a un componente técnico de una infraestructura de servicios de certificación, y que es empleado por el prestador de servicios para sus operaciones, como por ejemplo la expedición de los certificados a las entidades finales, de informaciones de estado de revocación, o de sellos de tiempo.

En el caso de la expedición de certificados, en general hay que partir de la existencia de un cierto número de autoridades de certificación, por diversas razones, entre las que se incluyen el hecho de que una sola autoridad de certificación difícilmente podría escalar para ofrecer un servicio único de alcance mundial; que dicha autoridad de certificación supondría un punto único de fallo del sistema; la necesidad de adecuar la práctica a las necesidades concretas de diferentes colectivos de usuarios; o simplemente intereses nacionales, estratégicos o comerciales.

En general, las autoridades de certificación se organizan en infraestructuras, donde una autoridad de certificación certifica a otras autoridades de certificación, que a su vez son las que expiden los certificados a los usuarios finales; lo cual permite confiar en un gran

---

formato, más

[1348] Cfr. el documento EMV Integrated Circuit Card Specifications for Payment Systems. Book 2. Security and Key Management, versión 4.3, de noviembre de 2011.

[1349] http://www.emvco.com/

[1350] Formada por IBM, Intel, Microsoft, Panasonic, Sony, Toshiba, The Walt Disney Company y Warner Bros.

[1351] http://www.aacsla.com/home

[1352] Principalmente, el documento Advanced Access Content System (AACS). Introduction and Common Cryptographic Elements Book, versión 0.953 final, de 26 de octubre de 2012. Para una revisión crítica de este sistema den autenticación, Cfr. (Sui & Stinton, 2008).

número de certificados, incluyendo los expedidos por nuestra autoridad de certificación, y otras autoridades de certificación que hayan sido certificadas para incorporarse a una infraestructura más grande, creando una cadena de certificación, como se puede ver en la siguiente ilustración:

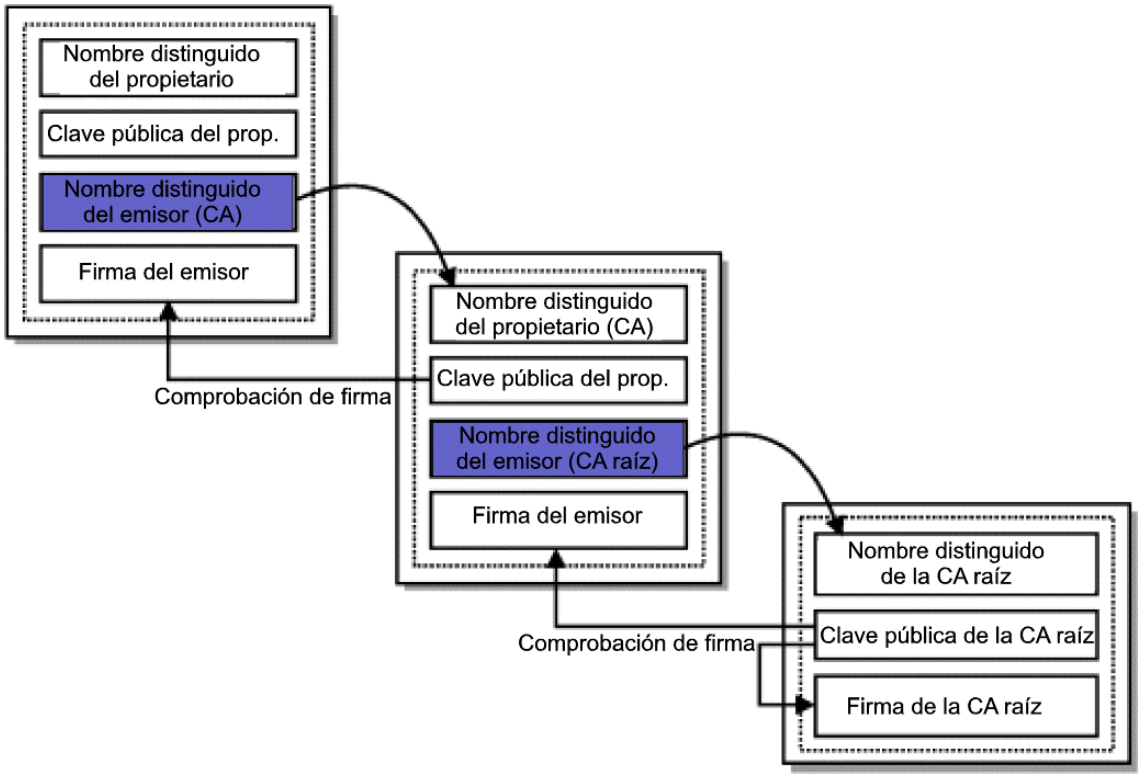


Ilustración 23. Cadena de confianza (IBM)

Los integrantes de una infraestructura de clave pública pueden ser componentes técnicos o entidades que cumplen un rol o prestan diferentes servicios, incluyendo las llamadas autoridades o entidades de certificación, de registro, de sellos de tiempo y de validación.

Las relaciones que se establecen entre estos sujetos determinan la topología de la infraestructura de claves públicas; es decir, la forma y el alcance del sistema de certificación. Por otra parte, las relaciones internas entre las autoridades de certificación y entre éstas y los usuarios determinan el modelo de confianza de la infraestructura de claves públicas.

Por su parte, el certificado de usuario final es todo aquel certificado, de clave pública o de atributos, expedido por una autoridad de certificación para usos diferentes a actuar como autoridad.

Como ya hemos anticipado, el concepto de usuario final es variable en función de la autorregulación, incluyendo personas, pero también organizaciones y, cada vez en más casos, dispositivos.

A.3 La autenticación

A.3.1 Concepto

En términos generales, y a los efectos que nos interesa, podemos definir la autenticación[1353] como el acto de verificar la identidad alegada por una entidad[1354], constituyendo un servicio básico de seguridad de las tecnologías de la información y la comunicación[1355]; un servicio con el que estamos más que familiarizados en nuestro día a día – ¡quién no está harto de gestionar decenas de contraseñas para redes, ordenadores y servicios de Internet!

Desde luego, la necesidad de este servicio de seguridad parece fuera de toda duda, y se encuentra muy ampliamente normalizado[1356] e implementado – con mayor o menor garantía – a pesar de lo cual resulta frecuente recibir noticia de casos del denominado "robo de identidad"[1357], por lo que cada vez resulta más importante implementar medios seguros de autenticación.

Entrando en algo más de detalle, la norma ISO 7498-2:1989 se refiere a este servicio de seguridad de "autenticación" diferenciando dos modalidades diferentes del servicio[1358]:

- Autenticación de entidad[1359], en la que se produce la verificación de que una entidad se corresponde con la entidad alegada; esto es, que dicha entidad es quien dice ser, bien en el inicio de una comunicación, o a lo largo de la misma. Este servicio permite confiar en que, en el momento de su uso, una entidad no está intentando suplantar a otra o reproducir, de forma no autorizada, una comunicación anterior.
- Autenticación de origen de datos[1360], en la que se produce la verificación de que

---

[1353] (Morant, Ribagorda, & Sancho, 1994, pág. 195) indican que la palabra autenticación, en su sentido más amplio, abarca excesivas posibilidades, dentro de las cuales cabrían todas las técnicas de reconocimiento de huellas digitales, fotografías, etc. y las técnicas que permiten la identificación de usuarios ante los equipos informáticos, por lo que emplean un concepto más restringido de autenticación, centrado en la autenticación de ficheros, mensajes, conjuntos de datos, etc.

[1354] Definición 2126251 de la norma internacional ISO/IEC 2382:2015 (1ª ed.), Tecnología de la información – Vocabulario.

[1355] Sin embargo, también veremos que existen mecanismos de autenticación, protocolos de autenticación y otros conceptos conexos que conviene tratar de forma apropiada para alcanzar una comprensión suficiente a los efectos del análisis de la regulación que realizaremos posteriormente. En este sentido, el servicio de autenticación se implementa mediante mecanismos y protocolos de autenticación.

[1356] Como muestra de la ingente cantidad de trabajos – en el nivel de autorregulación de la industria – existentes, resulta digno de mención que, sólo en ISO, existen 693 estándares en los que se contienen referencias a la autenticación.

[1357] Durante 2014 se ha informado acerca de múltiples casos, entre los cuales algunos donde se han comprometido millones de identificadores de cuentas de usuario, como en el caso de Gmail o Dropbox, como indica (López, 2014).

[1358] ISO/IEC 7498-2:1989, sección 5.2.1.

[1359] Cfr. la definición de autenticación de identidad contenida en el numeral 2126305 de la norma internacional ISO/IEC 2382:2015.

[1360] Cfr. las definiciones de autenticación de mensaje y de autenticación de datos contenidas en los

el origen de los datos recibidos se corresponde con el origen alegado; esto es, que los datos provienen de quien dicen provenir. En este caso, se puede confiar en que los datos provienen de una entidad determinada (aunque puede que no haya una garantía de quién sea esa entidad en realidad), pero no en que los datos no hayan sido duplicados o modificados.

Las dos modalidades son, en realidad, independientes y complementarias, al menos desde la perspectiva técnica, sin perjuicio de que en algunos casos se aplicarán de forma conjunta. También es interesante decir, en este momento, que de acuerdo con ISO 7498-2:1989, la integridad de los datos no forma parte del servicio de autenticación[1361].

Para el servicio de autenticación de entidad, se debe emplear un mecanismo de intercambio de autenticación. A este respecto, la norma ISO 7498-2:1989 identifica los tres siguientes: el uso de información de autenticación, como contraseñas y otras credenciales; el uso de técnicas criptográficas[1362]; y el uso de características y/o posesiones de la entidad.

La norma ISO 7498-2:1989 ofrece, en su sección A.4.6.1 algunas recomendaciones sobre la elección de estos mecanismos, en función de las circunstancias concretas del caso, que resulta interesante comentar en este momento:

- Cuando las entidades y los medios de comunicación resultan ambos confiables, la identificación de entidad se puede realizar mediante una contraseña.
- Cuando las entidades confían entre ellas, pero no en el medio de comunicación, se puede lograr protección frente a ataques activos mediante la combinación de contraseñas y cifrado, o mediante medios criptográficos.
- Cuando las entidades no confían entre ellas, ni en los medios de comunicación, se puede acudir el uso de servicios de no-rechazo, basados en firma digital y/o en notarización.

Para el servicio de autenticación de origen de datos, se debe emplear necesariamente algún tipo de mecanismo criptográfico, bien sea el cifrado o la firma digital, a los que nos referimos *infra*. En el caso del cifrado, se garantiza la autenticación del origen de los datos porque sólo la parte que tiene la correspondiente clave puede remitir los datos a través del canal cifrado, y no un tercero no autorizado. Algo parecido sucede con la firma digital, mecanismo que además ofrece integridad de datos, un servicio diferente de seguridad que presentaremos posteriormente.

Adicionalmente, la norma ISO 7498-2:1989 identifica que los servicios de autenticación de entidad y de origen de datos se deberían ofrecer en diversas capas del modelo conceptual de interconexión de sistemas abiertos[1363]:

---

numerales 2126252 y 2126390, respectivamente, de la norma internacional ISO/IEC 2382:2015.

[1361] A pesar de lo cual, es cierto – y así lo reconocen normas técnicas posteriores – que para que se pueda hablar de autenticación de origen de datos, es preciso también garantizar que los datos transmitidos no han sido modificados (cfr. ISO/IEC 10181-2, sección 5.1).

[1362] En particular, la firma digital es un mecanismo muy apropiado para la autenticación de entidad y para la autenticación de origen de datos, y además aporta integridad de datos.

[1363] Este modelo, conocido como OSI, se encuentra actualmente definido en la norma internacional ISO/IEC 7498-1:1994 (1ª ed.) – también publicada como Recomendación X.200 (1994) de la ITU-T –, y ofrece una

- En la capa 3 o de red, que es donde se contienen los medios funcionales y técnicos para las conexiones entre dispositivos dentro de una misma red.
- En la capa 4 o de transporte, que es donde se contienen los medios funcionales y técnicos para las conexiones entre dispositivos de diferentes redes.
- En la capa 7 o de aplicación, que es donde los usuarios interactúan directamente con las aplicaciones.

En el caso de la red Internet, que no sigue exactamente el mismo enfoque de capas que el modelo OSI, también se pueden considerar servicios de autenticación de entidad y de origen de datos en las capas del protocolo Internet (IP), de transporte (como, por ejemplo, TCP o UDP)[1364] y de aplicación[1365].

A título de ejemplo, cuando accedemos a una página web a través del protocolo HTTP, estamos en la capa 7 o de aplicación en el modelo OSI, o capa 4 en el modelo Internet, –la más frecuente para los usuarios humanos –, en la que se nos puede ofrecer un servicio de autenticación de entidad y de autenticación de origen de datos basado en el protocolo HTTPS[1366], de forma que podamos determinar, con cierto grado de confianza, qué persona física o jurídica es titular de la citada página web, algo que resulta de una importancia extraordinaria para evitar que entreguemos datos sensibles a un desconocido que haya suplantado la citada página web[1367].

---

base común para la coordinación del desarrollo de normas de interconexión de sistemas, al tiempo que permite la ubicación de las normas ya existentes en el modelo global de referencia. También identifica áreas para el desarrollo y la mejora de las normas y ofrece una referencia común para mantener la consistencia entre normas. A los efectos de la norma ISO/IEC 7498-1:1994, un sistema es un conjunto de uno o más ordenadores, así como el software, periféricos, terminales, operadores humanos, procesos físicos, medios de transferencia de información, etc. asociados, que forman un todo autónomo capaz de ejecutar procesamiento de información o intercambio de información. En esta norma, los diferentes subsistemas se agrupan en capas jerárquicas de funcionalidades, a los efectos de facilitar las comunicaciones. En cada capa se ofrecen determinadas capacidades de servicio, de forma que se facilita la interconexión (hoy seguramente hablaríamos de que se facilita la interoperabilidad). Para cada capacidad de servicio, se pueden definir componentes y protocolos, a los efectos de determinar el comportamiento de las entidades que se comunican. El modelo de referencia OSI contiene siete capas: la capa 1 o física; la capa 2 o de enlace de datos; la capa 3 o de red; la capa 4 o de transporte; la capa 5 o de sesión; la capa 6 o de presentación y la capa 7 o de aplicación.

[1364] Los protocolos de Internet y de transporte se encuentran actualmente definidos en la especificación técnica IETF 1122:1989 (Requisitos para hosts de Internet – capas de comunicación), y sus actualizaciones posteriores.

[1365] En el caso de Internet, la capa de aplicación se corresponde con las capas 5 a 7 del modelo OSI. Se encuentra definida en la especificación técnica IETF RFC 1123:1989 (Requisitos para hosts de Internet – aplicación y soporte), y sus actualizaciones posteriores.

[1366] El protocolo se denomina HTTP sobre SSL, y se encuentra definido en la especificación técnica del IETF RFC 2818:2000, actualizada por las RFC 5785:2010 y RFC 7230:2014. Aunque HTTPS funciona en la capa de aplicación, en realidad se basa en el protocolo Secure Sockets Layer (SSL) y su sucesor, denominado Transport Layer Security (TLS), que también funciona en la capa de aplicación.

[1367] Por ejemplo, cuando una persona suplanta una página web legítima con la finalidad de interceptar las comunicaciones del usuario para robarle datos sensibles, como datos de tarjetas de pago. Cfr. (Garfinkel & Spafford, 1999, págs. 14-16).

Ilustración 24. Autenticación con HTTPS, información básica

Cuando se accede a una web que implementa este protocolo de seguridad, en la parte inicial de la caja de introducción de la dirección de Internet a la que se accede aparece, remarcado en color verde, el nombre de la entidad titular de la dirección de la página web en cuestión. Así se ve en la Ilustración 24.

Este es el resultado de haberse realizado correctamente el mecanismo de autenticación en cuestión, que en este caso se basa en un mecanismo criptográfico donde interviene la clave pública de la entidad, certificada por una tercera parte, y que nuestro cliente web es capaz de procesar para identificar a la entidad[1368].

Si se hace clic en el citado nombre de la entidad, se obtiene información técnica adicional, como se puede ver en la Ilustración 25.

[1368] E inmediatamente, generar una clave simétrica que se utilizará, sólo en esta sesión, para cifrar todas las comunicaciones, garantizando la confidencialidad.

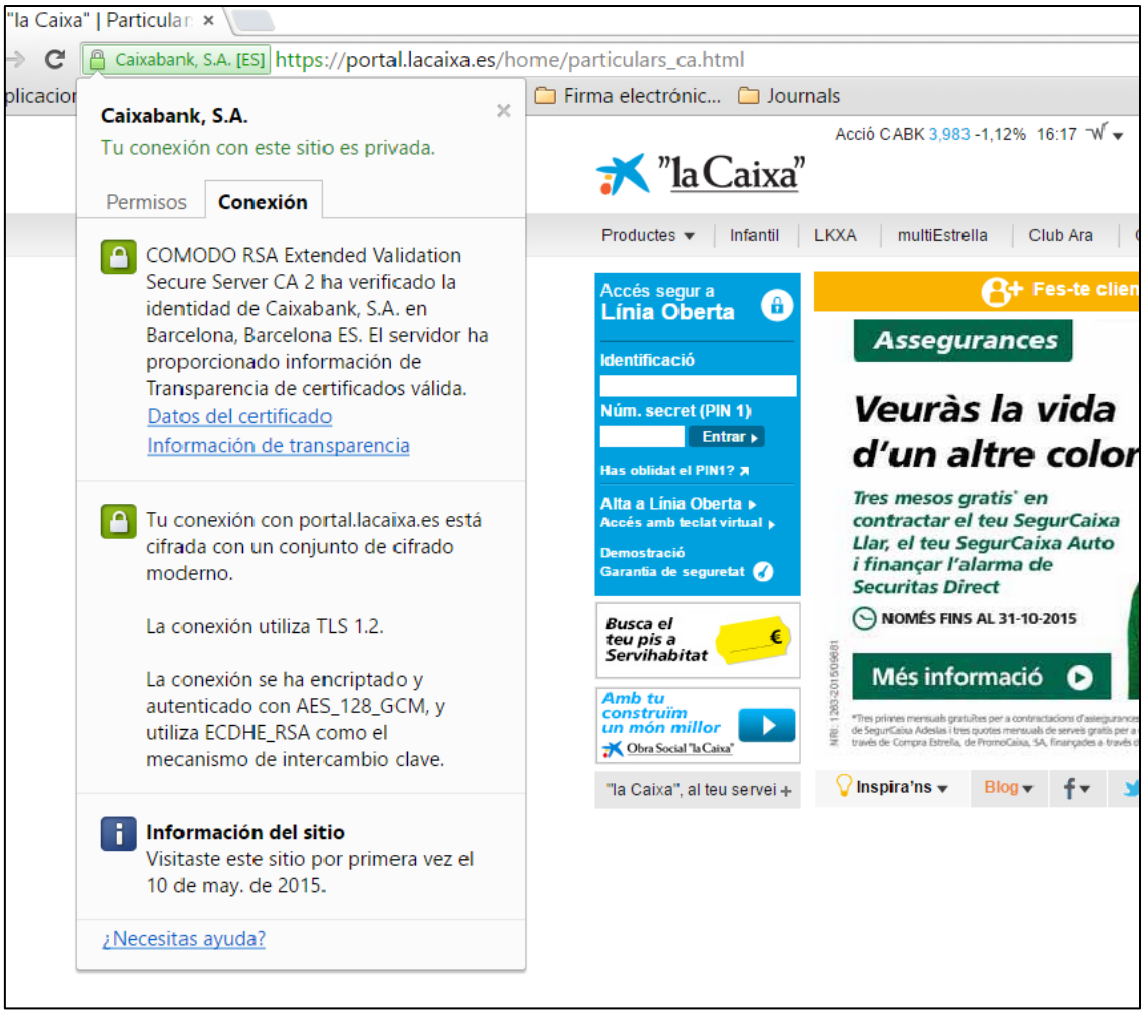


Ilustración 25. Autenticación con HTTPS, información adicional

En este caso, se nos informa de que una tercera entidad ha verificado, y avala, la identidad de la entidad en cuestión, así como de los mecanismos que se han empleado para la autenticación, que se basa en la firma digital de la entidad, que además se encuentra certificada por esta tercera entidad[1369].

Si queremos obtener información adicional, podemos seleccionar la opción de "Datos del certificado", y accederemos al certificado, donde se indica que este mecanismo garantiza la autenticación de la entidad, y se especifica exactamente la dirección avalada, lo que nos permite confiar en que realmente accedemos a esta entidad, y no a otra[1370].

De esta forma se ve en la Ilustración 26:

[1369] Como veremos más adelante, de acuerdo con una autorregulación detallada que se refiere al ciclo de vida de los certificados digitales.

[1370] Más adelante explicaremos por qué motivo podemos confiar en este certificado, primero desde una perspectiva técnica y, posteriormente, jurídica.

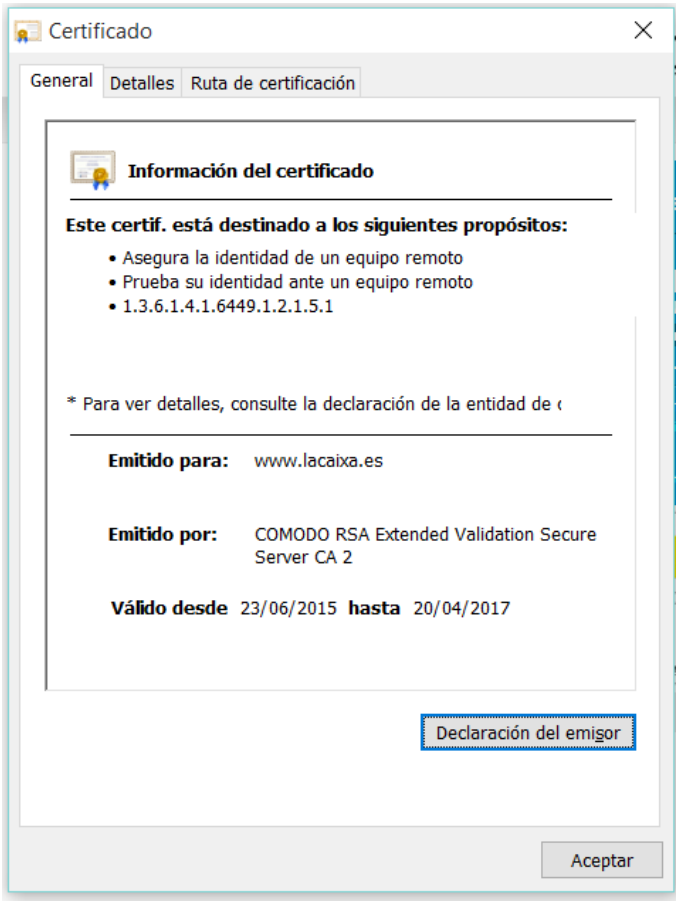


Ilustración 26. Certificado de autenticación de servidor HTTPS

Con esto hemos obtenido autenticación sólo de la entidad respecto a nosotros (autenticación unidireccional), pero también podemos autenticarnos nosotros frente a la entidad, introduciendo nuestro identificador y el número secreto (PIN1), suministrados previamente por la entidad (autenticación mutua o bilateral).

Otro ejemplo de procedimiento de autenticación es el que ocurre cuando nuestro ordenador o dispositivo se conecta a nuestra WiFi doméstica y se autentica empleando la dirección MAC para acceder y recibir una IP, en cuyo caso nos encontramos en la capa 2, igual que cuando empleamos una contraseña para el cifrado de la WiFi con WPA2, por ejemplo[1371].

Y si para acceder a la red del trabajo nos exigen implementar una red privada virtual basada en IPSec, entonces nos encontramos en la capa 3, ocurriendo un proceso bastante parecido al anteriormente visto.

Otro ejemplo de aplicación de Internet que implementa el servicio de autenticación es el

[1371] En ambos casos, es curioso notar que en ISO 7498-2:1989 indique que la autenticación de entidad y de origen de datos no se considere útil en las capas 1 y 2. Seguramente en este punto podemos observar como la evolución tecnológica ha convertido esta opinión en obsoleta. Como explica (Reed, 2003, pág. 25), con el advenimiento de la tecnología de redes inalámbricas aparecieron nuevos retos de seguridad que no existían en las redes cableadas, por lo que ha resultado preciso agregar servicios de autenticación y confidencialidad en la capa 2.

denominado correo electrónico seguro, o S/MIME, un protocolo adicional al correo electrónico de Internet que emplea criptografía[1372].

Y es que diferentes tipos de servicio requieren o utilizan, como se puede comprobar, diversos tipos de mecanismos de autenticación, en función de las necesidades y, lo que es más importante, de los riesgos, reales o percibidos[1373].

A.3.2 Un marco de trabajo autorregulado para la autenticación

Por su parte, la norma ISO/IEC 10181-2:1996 (1ª ed.)[1374], que regula de forma monográfica un marco de trabajo de seguridad[1375] referido a la autenticación, la define como "la provisión del aseguramiento de la identidad alegada de una entidad".

Esta norma relaciona, y aclara el uso de, los términos "identificación" y "autenticación", en el sentido de indicar que los servicios de autenticación se emplean para verificar las identidades alegadas por las entidades (de forma más precisa, las identificaciones diferenciadoras que las mismas poseen, y que les permiten ser reconocidas de forma unívoca).

Y en este punto es necesario traer a colación que esta norma reconoce de forma más explícita la existencia de múltiples identidades (o identificaciones diferenciadoras), como los nombres y apellidos, o los números de determinados documentos oficiales, y que las mismas pueden ser, o no, apropiadas para un contexto de seguridad concreto; y que las identidades siempre son alegadas, por lo que deberán ser verificadas con un nivel de garantía concreto.

En general, en estas normas técnicas se definen los servicios de autenticación como mecanismos – de diversa naturaleza técnica – en los que una entidad, denominada principal, se autentica frente a otra entidad, denominada verificador. Para ello, típicamente el principal deberá haber sido previamente identificado por el verificador, y podrá hacer uso del mecanismo técnico del que disponga para autenticarse a distancia, demostrando, por tanto, que es la misma entidad.

Como hemos anticipado anteriormente, los servicios de autenticación se emplean en diversos escenarios, y que en muchos de ellos las entidades que se autentican no son

---

[1372] El servicio de autenticación emplea un código de autenticación de mensaje (MAC).

[1373] Como ha dicho acertadamente (Davara Rodríguez, 1996, pág. 151), "las TIC proporcionan múltiples posibilidades de autenticación; no obstante, en el terreno de lo práctico, la necesidad ha llevado a que se utilicen estos documentos sin caer en la tentación de excesivos formalismos de seguridad", citando la Circular 6/1990 del Banco de España (que fue sustituida por la Circular 5/1996, que a su vez fue derogada por Circular 1/2007).

[1374] El título de la norma es Tecnología de la información – Interconexión de sistemas abiertos – Marcos de trabajo de seguridad para sistemas abiertos: Marco de trabajo de autenticación. Se trata de una norma idéntica a la Recomendación X.811 (1995) de la ITU-T

[1375] Un marco de trabajo de seguridad se refiere a elementos de datos y secuencias de operaciones empleados para la obtención de un servicio de seguridad, pero no a protocolos concretos, ni tampoco se preocupa de la metodología para la construcción de sistemas o mecanismos. El marco de trabajo constituye una base para la estandarización posterior de los servicios de seguridad, ofreciendo una terminología consistente y definiciones de interfaces de servicios genéricas y abstractas, describiendo el rango de mecanismos que se pueden emplear para ofrecer los servicios de seguridad, e identificando interdependencias entre los servicios y los mecanismos (cfr. ISO/IEC 10181-1:1996, sección 1).

personas, sino dispositivos electrónicos[1376], por lo que hay que realizar un cierto esfuerzo de adaptación de la terminología empleada en las normas, y en nuestro caso concreto, nos vamos a limitar a la autenticación de personas, que es la única que parece relevante a los efectos legales.

La norma ISO/IEC 10181-2:1996 es particularmente detallada en cuanto a los aspectos generales que sustentan la autenticación, la información de autenticación y las capacidades que se requieren para la autenticación, las características de los mecanismos de autenticación, los mecanismos de autenticación y las interacciones con otros servicios y mecanismos de autenticación, y concreta algunas cuestiones en relación con la autenticación de personas (a las que se refiere como usuarios humanos, en contraposición a los usuarios que representan procesos informáticos).

En el anexo A de la norma en cuestión se indica que la autenticación de las personas se basa en uno o más de los siguientes principios de autenticación[1377]:

- Algo que se conoce, como una contraseña, o un conjunto de contraseñas, o una contraseña de un solo uso.
- Algo que se posee, como un dispositivo físico o lógico, incluyendo recientemente el uso extendido de los terminales móviles.
- Alguna/s característica/s de la persona (principio generalmente conocido como "algo que se es" y al que usualmente se denomina como biometría), incluyendo la firma manuscrita, la huella digital, el patrón vocal o de retina, o el reconocimiento del tecleado dinámico.
- Aceptando la autenticación realizada por una tercera entidad.
- Uso de información contextual, como una dirección de origen de la comunicación, por ej. una dirección IP de Internet.

La norma ISO/IEC 10181-2:1996 clasifica los diferentes mecanismos de autenticación en función de las vulnerabilidades a las que se encuentran sometidas las informaciones empleadas para la autenticación – como la contraseña –, considerando las siguientes categorías[1378]:

- Clase 0: Desprotegida, como por ejemplo cuando se remite una contraseña en texto claro.
- Clase 1: Protegida frente a la divulgación, como por ejemplo cuando se remite un resumen criptográfico de la contraseña, o se genera una huella digital firmada con una clave privada.
- Clase 2: Protegida frente a la divulgación y la repetición frente a diferentes verificadores, que añade, a la protección de la clase 1, algún dato propio de cada

[1376] Por ejemplo, en ISO/IEC 10181-2:1996, se discute la autenticación de dispositivos de red, la autenticación de sistemas informáticos y la autenticación de aplicaciones (que es donde se produce la autenticación de personas o de procesos que actúan en su nombre).

[1377] Se trata de una lista que considera algunos de los mecanismos de autenticación de entidad que se contienen en ISO 7498-2:1989, resultando interesante que pasen de ser considerados mecanismos, para ser cualificados como principios.

[1378] Cfr. la sección 8.4 de la norma.

verificador, para evitar la reutilización de dicha información de autenticación.

- Clase 3: Protegida frente a la divulgación y la repetición frente al mismo verificador, como por ejemplo cuando se emplea sellado de tiempo o contador de operación.
- Clase 4: Protegida frente a la divulgación y la repetición frente al mismo o diferentes verificadores, que añade, a la protección de la clase 3, algún dato propio de cada verificador, para evitar la reutilización de dicha información de autenticación.

Como se puede fácilmente intuir, dependiendo de las circunstancias, se acudirá a un mecanismo con mayor o menor nivel de protección, sin que la norma en cuestión prescriba nada al respecto.

De particular interés resulta la identificación de las fases de proceso que se dan en relación con la autenticación[1379], incluyendo:

- Instalación de la autenticación, durante la que se definen las informaciones que se emplearan para la autenticación. Por ejemplo, se puede generar una contraseña nueva, o un par de claves de firma digital, o registrar una huella digital.
- Modificación de la información de autenticación. Por ejemplo, un cambio de contraseña.
- Distribución de la información de verificación de autenticación. Por ejemplo, se entrega una contraseña protegida al verificador, o un certificado de clave pública y su información de revocación, siempre para poder verificar una autenticación concreta.
- Adquisición, durante la cual se obtiene una credencial para poderse autenticar frente a la otra parte.
- Transferencia, durante la cual las partes se intercambian la información para la autenticación. Por ejemplo, cuando se remite una contraseña para demostrar la identidad.
- Verificación, durante la cual se comprueba la información de autenticación por parte del verificador, para corroborar la identidad del principal.
- Desactivación, durante la cual se suspende la posibilidad de autenticarse.
- Reactivación de una información de autenticación que había sido suspendida.
- Desinstalación, durante la cual se cancela definitivamente una información de autenticación.

Dado el carácter de marco de trabajo de esta norma, estas fases deben concretarse con bastante detalle para cada mecanismo y protocolo de autenticación, y ser completadas con previsiones organizativas por parte de cada entidad responsable de un servicio de autenticación (sea interno, dirigido sólo a los empleados para autenticarse frente a la compañía, o externo, dirigido a personas que incluso se podrán autenticar frente a terceras organizaciones).

Uno de los procesos que va a resultar particularmente relevante es la identificación del

[1379] Cfr. la Norma ISO/IEC 10181-2:1996, sección 5.4.

usuario a autenticarse. En efecto, podemos emplear un mecanismo técnico de autenticación muy robusto y seguro, pero si lo vinculamos con una persona concreta, ciertamente no sabremos quién se está autenticando.

Por su parte, y en un nivel más concreto en términos técnicos, la norma internacional ISO/IEC 9798, partes 1 a 6, establece un conjunto de mecanismos concretos de autenticación empleando diversas técnicas de seguridad, de forma alineada con las normas anteriormente indicadas. Se trata, en este caso, de concretar la colección de técnicas de seguridad que resultan apropiadas para cada caso concreto, incluyendo mecanismos que emplean algoritmos simétricos de cifrado – con y sin intervención de un tercero de confianza[1380]; mecanismos que emplean algoritmos de firma digital[1381]; mecanismos que emplean una función de comprobación criptográfica[1382]; mecanismos de conocimiento cero[1383] y mecanismos de transferencia manual de información[1384].

Nótese que sólo estas normas definen ¡hasta 27 mecanismos diferentes de autenticación!, que se van a emplear en múltiples protocolos para la autenticación.

Todos estos mecanismos, de acuerdo con ISO/IEC 9798-1:2010 (3ª ed.[1385]) se incardinan en dos grandes modelos de autenticación: de una parte, en un primer modelo en el que las partes que participan en el proceso de autenticación se comunican directamente, intercambiando las informaciones correspondientes, en función del mecanismo técnico aplicable; y de otra, en un segundo modelo en el que interviene necesariamente un tercero de confianza.

Como se puede ver, en las normas internacionales analizadas hasta este momento determinan aspectos bastante generales del servicio de autenticación y de sus mecanismos y protocolos asociados, pero no son en absoluto prescriptivas, algo que es plenamente lógico dado su carácter de marcos de trabajo de referencia general. Con independencia de realizar alguna recomendación general, dejan una libertad plena a las partes para autorregularse completamente.

Ello implica que podemos encontrarnos frente a una enorme variedad de mecanismos de autenticación, así como con diferentes prácticas referidas a los procesos de autenticación; en función de la combinación de mecanismos y práctica que se adopte en cada caso, podremos confiar en la autenticación en mayor o menor grado.

En este sentido, cada vez resulta más habitual emplear más de un mecanismo de autenticación, como por ejemplo una contraseña de un solo uso remita al móvil registrado,

---

[1380] Cfr. ISO/IEC 9798-2:2008, con corrección técnica de 2013, actualmente en revisión.

[1381] Cfr. ISO/IEC 9798-3:1998, modificada en 2010, y con correcciones técnicas de 2009 y 2012, actualmente en revisión.

[1382] Cfr. ISO/IEC 9798-4:1999, con correcciones técnicas de 2009 y 2012.

[1383] Cfr. ISO/IEC 9798-5:2009. En estos mecanismos no se revela ninguna información secreta de la parte que se identifica (por ejemplo, se demuestra que se conoce una contraseña, para autenticarse, pero sin divulgar ninguna información acerca de la misma).

[1384] Cfr. ISO/IEC 9798-6:2010. En estos mecanismos no existen claves compartidas entre las partes que participan en el proceso de autenticación. De hecho, estos mecanismos se pueden precisamente emplear para establecer o intercambiar claves de forma fiable.

[1385] La primera edición de la norma se remonta a 1997.

adicionalmente al uso de una contraseña remitida desde un cliente web.

El dato importante a reseñar, en el ámbito de este trabajo, es que la aplicación de estos mecanismos técnicos genera testimonios de seguridad que evidencian la autenticación de la entidad, testimonios pueden ser almacenados por las partes para su uso en caso de disputa, por su indudable valor probatorio[1386], dentro del marco de autorregulación que las partes establezcan.

A.3.3 La autenticación en la práctica autorregulada de la seguridad de la información

Desde la perspectiva de las prácticas de seguridad, la norma internacional ISO/IEC 27002:2013 (2ª ed.)[1387] ofrece un conjunto de controles que resultan apropiados para establecer un nivel apropiado de seguridad de la información, con independencia de la naturaleza (pública o privada) y del tamaño de la organización.

Los controles descritos en esta norma constituyen una especie de nivel común de buenas prácticas, aunque lo cierto es que no contiene – no debe hacerlo – un nivel de detalle excesivo, precisamente para que las organizaciones que adoptan los citados controles puedan ajustarla a sus necesidades, en función de criterios de riesgo.

Respecto a la autenticación, la norma ISO/IEC 27002:2013 contiene normas particularmente enfocadas a los usuarios de la organización, en el sentido de empleados y contratistas externos, y no tanto a los usuarios externos, como ciudadanos o clientes, aunque también en este segundo caso establece alguna pauta concreta[1388].

En concreto, la sección 14.1.2 de la norma, referida al aseguramiento de los servicios de aplicación en redes públicas (como Internet) indica que, a los efectos de determinar los requisitos de seguridad de la información en este caso, se debe considerar el nivel de confianza que cada parte precisa respecto a la identidad alegada por la otra parte; por ejemplo, mediante el uso de mecanismos suficiente de autenticación[1389].

Asimismo, la sección 14.1.3 de la misma norma, referida a la protección de las transacciones de servicios de aplicación, determina la necesidad de garantizar que la información secreta de autenticación de todas las partes es válida y se ha verificado, precisamente porque en caso contrario no va a resultar posible confiar en la identidad de las partes.

De forma específica, hay que notar que la norma ISO/IEC 27002:2013 dedica un dominio

---

[1386] Desde una perspectiva jurídica, los testimonios de seguridad – en este caso, de autenticidad – son fuentes de prueba que accederán al procedimiento judicial como uno u otro medio de prueba, en función de lo que en cada caso determine la legislación procesal correspondiente.

[1387] El título de la norma internacional es Tecnología de la información – Técnica de seguridad – Código de práctica para controles de seguridad de la información. Se trata de la segunda edición, que revisa la de 2005. A su vez, ISO/IEC 27002:2005 es idéntica a ISO/IEC 17799:2005 y su corrección técnica de 2007, que revisa ISO/IEC 17799:2000, que a su vez procede de la norma inglesa BS 7799; es decir, que se trata de una norma con una ya larga trayectoria.

[1388] Curiosamente, estas recomendaciones se contienen dentro del dominio de controles dedicado a la adquisición, desarrollo y mantenimiento de los sistemas de información y, más en concreto, forman parte de la sección dedicada a la determinación de los requisitos de seguridad de los sistemas de información.

[1389] La norma menciona, en la misma sección, que los servicios de aplicación pueden hacer uso de métodos de autenticación seguros, como las firmas digitales y los terceros de confianza.

de controles completo a los que denomina controles criptográficos, que se deben emplear para la protección de la autenticidad e integridad de la información, al objeto de ofrecer soporte a diversos objetivos de seguridad, entre los cuales la integridad/autenticidad, la autenticación y la irrefutabilidad.

Como en el caso de las restantes normas internacionales de seguridad, tampoco la norma internacional ISO/IEC 27002:2013 concreta qué mecanismos específicos de autenticación se deberían emplear en cada caso, básicamente por su carácter de norma común a cualesquiera organizaciones, y porque para dicha determinación se debe acudir a criterios basados en el análisis de los riesgos.

No cabe decir que forma parte de este análisis de riesgos la propia regulación jurídica que en cada momento imponga requisitos de autenticación a las organizaciones, dado que el incumplimiento de la citada regulación se puede traducir en sanciones económicas y otros daños para la organización, como desde el punto de vista de la reputación.

La propia norma ISO/IEC 27003:2013 se refiere a esta cuestión en su sección 18, haciendo especial hincapié en la protección de los datos de carácter personal[1390], aunque desde luego existen otras normas sectoriales que establecen requisitos de autenticación, que la organización deberá cumplir, influyendo sobre su libertad de elección de los mecanismos y protocolos de autenticación a emplear, así como en relación a los procesos de autenticación.

A.3.4 La delegación de la autenticación a terceros, en especial en la Web Social

Desde otra perspectiva, anteriormente nos hemos referido a la existencia de diversos mecanismos y protocolos de autenticación en los que interviene un tercero de confianza.

En este caso, nos encontramos ante la autenticación como servicio prestado por terceros; esto es, ante la actividad de identificación y autenticación por proveedores de credenciales, también denominados proveedores de identidad digital[1391].

Se trata de una experiencia que cada vez resulta más familiar para las personas físicas usuarias de Internet, y que se ha desarrollado con particular intensidad con el advenimiento de la denominada Web Social, que permite acceder a una aplicación web de una organización empleando el sistema de autenticación asociada a la identidad digital hospedada en un prestador de servicios.

Por ejemplo, hoy resulta absolutamente común la posibilidad de crear un perfil de red social, como por ejemplo en LinkedIn, una red emitentemente empleada por profesionales

---

[1390] El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, contiene obligaciones concretas de autenticación, aplicables a las organizaciones que traten estos datos, bien como responsables o por encargo de terceros responsables (cfr. los artículos 93 y 98). Nótese que, a los efectos del citado Real Decreto, se define la identificación como el "procedimiento de reconocimiento de la identidad de un usuario", y la autenticación como el "procedimiento de comprobación de la identidad de un usuario".

[1391] En los últimos años se ha producido una verdadera explosión de protocolos técnicos para habilitar la delegación y federación de la identidad en Internet, incluyendo SAML, WS-Federation, WS-Security, WS-SecureConversation, WS-Trust, OpenID, OpenAuth... Para una introducción técnica más detallada, cfr. (Windley, 2005) o (Baier, Bertocci, Brown, Pace, & Woloski, 2010).

en su actividad, que cuenta con más de 300 millones de cuentas de usuarios, por lo que se anuncia diciendo que "LinkedIn es la fuente más grande y confiable de la identidad profesional".

Con el alta en LinkedIn, obtenemos nuestra identidad digital, y su correspondiente mecanismo de autenticación frente a LinkedIn, que esencialmente es una contraseña[1392], como se puede ver en la Ilustración 27.

La particularidad, en este caso, es que LinkedIn – igual que otros prestadores que implementan este protocolo particular – permite que también nos autentiquemos frente a terceros con nuestra contraseña, como por ejemplo para suscribirnos a un servicio de la sociedad de la información.

Para ello, el tercero al que queremos acceder habilita, además de su propio mecanismo de autenticación, la posibilidad de autenticación con la identidad de LinkedIn, algo que se representa gráficamente mediante un botón especial.

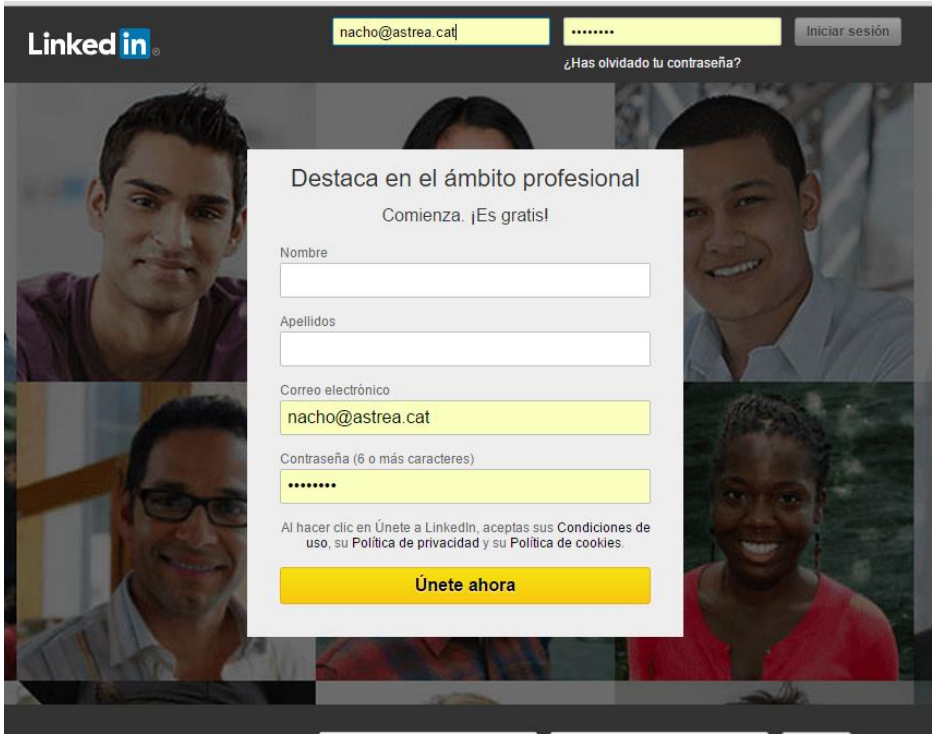


Ilustración 27. Autenticación frente a LinkedIn

Por ejemplo, en la siguiente ilustración se muestra la posibilidad de acceder a Bizzabo, una compañía que ofrece servicios de gestión de eventos empresariales o de otros tipos, empleando el servicio de autenticación ofrecido por LinkedIn:

[1392] LinkedIn se autentica frente a nosotros empleando el protocolo HTTPS; esto es, mediante un sistema criptográfico basado en la clave pública certificada de la empresa, y un sistema de intercambio de claves para establecer el cifrado de la conexión, ofreciendo por tanto la doble garantía de autenticación de entidad y de autenticación de origen de datos; mientras que los usuarios emplean una contraseña que se transmite en forma transformada y, por tanto, protegida, a LinkedIn, para corroborar nuestra identidad.

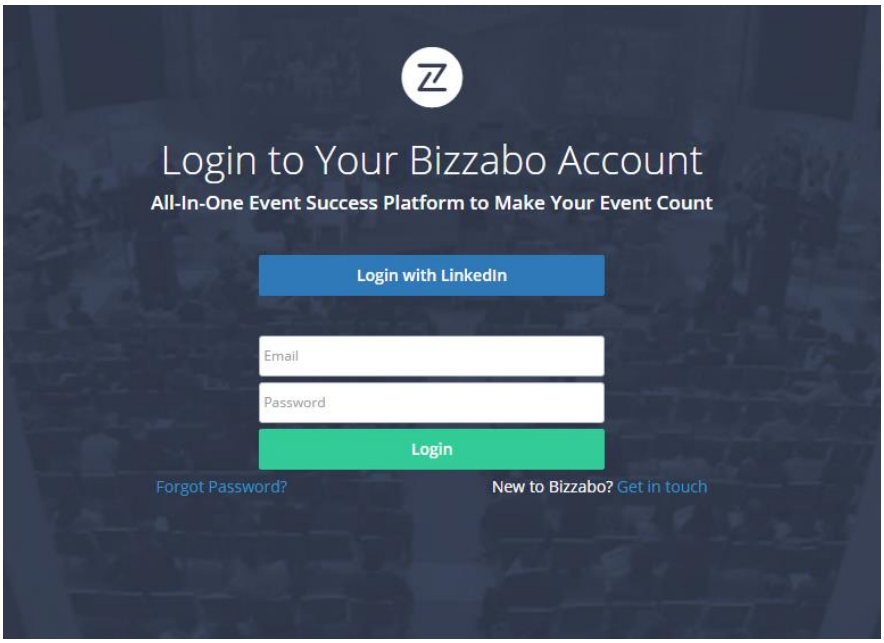


Ilustración 28. Acceso a una web con autenticación delegada a un tercero

Cuando nos pretendemos identificar con LinkedIn frente a esta organización, en lugar de crear una nueva cuenta de usuario, sólo debemos hacer clic en el botón "Login with LinkedIn" y se nos presenta la pantalla de autenticación, que se puede ver en la siguiente ilustración.

Entre bambalinas[1393], lo que ha sucedido – de forma invisible para el usuario – es que Bizzabo nos ha reenviado a LinkedIn, junto con un identificador temporal y una solicitud de autenticación y de acceso a diversos datos. A partir de los metadatos aportados por nuestro propio cliente web, LinkedIn nos ha reconocido y nos pregunta si queremos autenticarnos frente a Bizzabo, y darle acceso a los datos requeridos.

Como se puede ver, al estar identificado en LinkedIn – cosa que hemos pedido a nuestro cliente web que recuerde[1394] –, ya aparecen nuestro identificador y contraseña previamente cumplimentados, lo que nos facilita el acceso:

[1393] Para mayor detalle técnico del funcionamiento del sistema, cfr. la información que ofrece la compañía en su página web https://developer.linkedin.com/docs/signin-with-linkedin, así como en la página web https://developer.linkedin.com/docs/oauth2.

[1394] Se trata de una opción conveniente pero peligrosa, ya que cualquier persona con acceso a este cliente web podrá acceder en mi nombre al servicio, por lo que sólo hay que emplearla cuando confiamos plenamente en la seguridad en el acceso al ordenador donde la misma se ejecuta, por ejemplo.

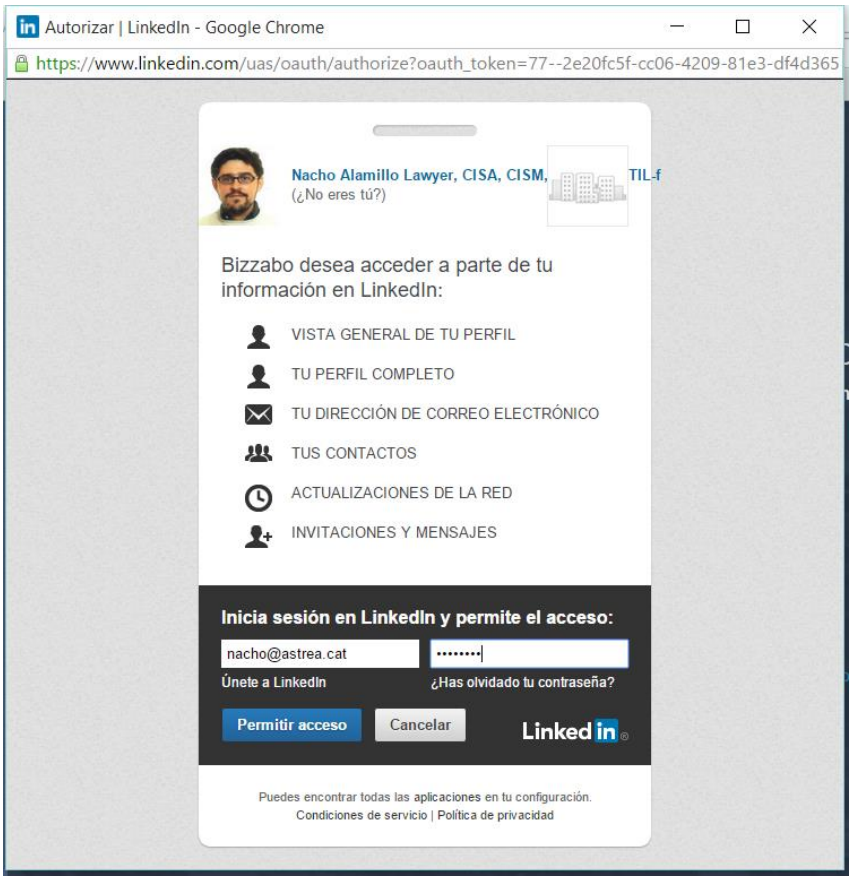


Ilustración 29. Autenticación delegada a LinkedIn

Una vez nos hemos autenticado frente a LinkedIn, empleando nuestra contraseña, se genera una credencial específica para informar a Bizzabo de mis datos, y para crear una asociación entre nuestro usuario de LinkedIn y nuestro usuario de Bizzabo, que permitirá a Bizzabo continuar accediendo a los datos de nuestro perfil de LinkedIn para los que nos ha solicitado y obtenido consentimiento expreso.

Una vez generada dicha credencial, LinkedIn nos remite de nuevo – de forma transparente, por supuesto – a la web de Bizzabo, donde se nos muestra la siguiente pantalla:

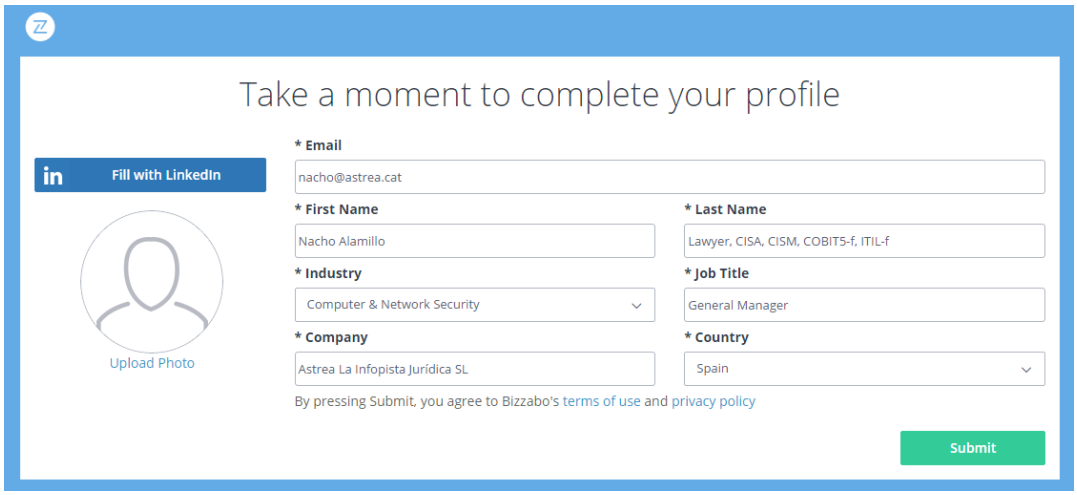


Ilustración 30. Provisión de usuario basada en LinkedIn

En esta pantalla, Bizzabo nos permite completar el registro, creando su propio perfil de usuario, tomando como punto de partida la información de identidad que hemos compartido desde nuestro perfil de LinkedIn, pantalla en la que, además, nos adherimos a los términos y condiciones, y a la política de privacidad de esta compañía.

Nótese que, desde la perspectiva de esta compañía, toda la autenticación se ha delegado a LinkedIn, sin que haya ulteriores procesos de comprobación. La compañía en cuestión va a confiar en la identificación que haya realizado LinkedIn, así como en las medidas de seguridad para la autenticación, seguramente porque, tras el correspondiente análisis de riesgos, habrá llegado a la conclusión que resulta más seguro delegar el proceso que implementarlo, en especial dado que el usuario ha creado un perfil social con más datos identificativos que los que podría obtener la propia compañía, caso de desarrollar su propio proceso de autenticación.

Dado que otros grandes prestadores de servicios de red social, o de servicios en Nube, como Facebook o Google, también ofrecen estos servicios de autenticación delegada, realmente nos encontramos ante la posibilidad de que nuestros perfiles de usuario en estos servicios sean empleados como identidades principales en nuestras relaciones en Internet.

Y es que, con un estimación de casi 1.800 millones de usuarios de redes sociales en 2015 (Statista, 2015), y con un crecimiento previsto sostenido en el tiempo, el valor de estas identidades digitales sociales es, en términos de externalidad de red, extraordinario[1395]; en especial cuando nos referimos a las redes con mayor volumen de usuarios activos (Statista, 2015).

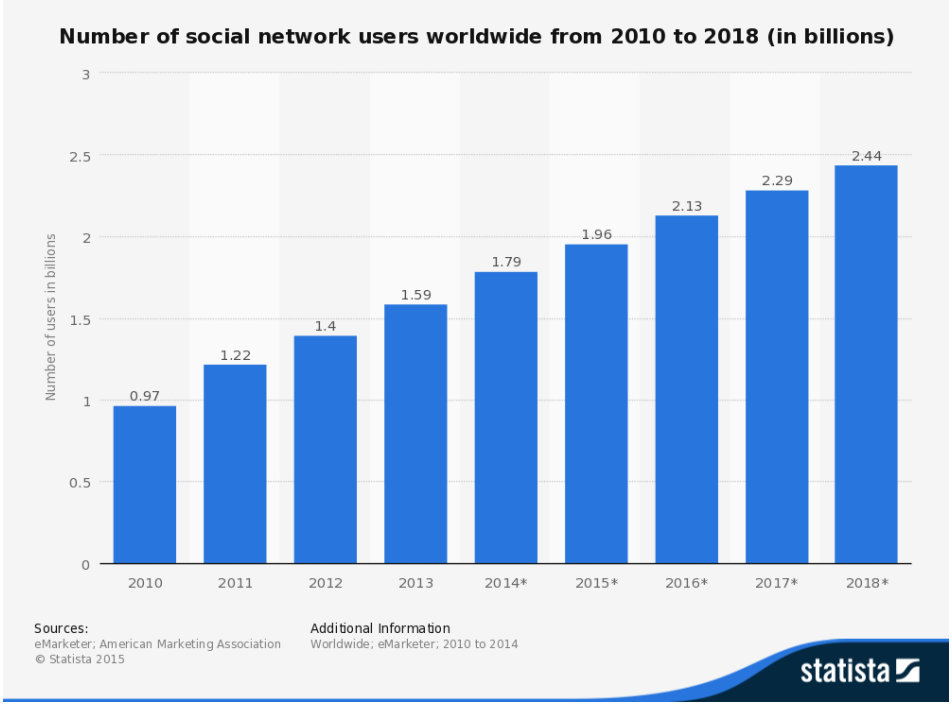


Ilustración 31. Crecimiento del número de identidades de red social

Desde una perspectiva técnica, estos procesos emplean mecanismos de autenticación

[1395] Cfr. (HageI III & Armstrong, 1999, pág. 27), para quienes existe, en los modelos de negocio de rendimientos crecientes –en particular, las comunidades virtuales– una relación directa entre el número de miembros de una red de negocios y el valor de la misma.

parecidos a los que hemos presentado anteriormente, pero en protocolos donde la participación de la tercera parte de confianza – en el ejemplo, el prestador del servicio de red social – adquiere una relevancia clave en la identificación y autenticación que se le delega.

En el modelo de negocio de estos prestadores de servicios de red social no se cobra cantidad alguna por la prestación de este servicio de identificación y autenticación electrónicos, sin perjuicio de que, en algunos casos, particularmente en Facebook, la red social también reciba informaciones adicionales desde las aplicaciones que han delegado la autenticación[1396], incrementando el activo principal de dichas redes, que no es otra cosa que los datos personales de sus miembros[1397].

Uno de los elementos más relevantes que hay que resaltar de estos servicios es que es el usuario quien se auto-identifica a sí mismo, mediante la agregación de datos en el perfil, algo que se ha venido en denominar identidad de primera parte o usuario-céntrica, frente a las identidades de segunda parte[1398] y de tercera parte[1399].

Algunos de los ejemplos realmente interesantes de identidad por agregación lo encontramos en el sector de la denominada economía colaborativa, como podemos ilustrar con el caso de AirBnB, que aplica una interesante colección de técnicas de identificación de sus miembros, para que se relacionen entre ellos en condiciones de confianza. En su proceso, la identidad se basa en diferentes datos, como una o varias cuentas de redes sociales, en la carga de fotografías de documentos nacionales de identidad y en la tarjeta de pago.

Claramente nos encontramos ante un cambio de paradigma en lo que se refiere a la autenticación, donde podemos anticipar la existencia de un rico ecosistema de identidades gestionado por prestadores de servicios, con diferentes niveles de calidad y seguridad, y que plantea una importante cantidad de retos (Rundle, y otros, 2007).

Dada la importancia y extensión de esta actividad, la misma se ha ido autorregulando en diversos instrumentos, entre los cuales cabe presentar, si quiera sucintamente, la norma internacional ISO/IEC 24760-1:2011 (1ª ed.)[1400] y la norma internacional ISO/IEC

[1396] Por ejemplo, si como usuario empleamos nuestra autenticación de Facebook para acceder al servicio de música bajo demanda Spotify, y siempre que no desactivemos esta posibilidad, Spotify remitirá a nuestro perfil social de Facebook información detallada acerca de la música que escucho. Esta información se incorporará al acervo de datos que conforman mi perfil social (un grafo de datos perfectamente estructurado y diseñado para la explotación de esta información, supuestamente siempre en mi beneficio).

[1397] Resulta muy expresiva la caracterización del asunto que realiza (Martínez Martínez, 2010, pág. 87), cuando indica que "en Internet la información personal constituye la fuente de riqueza por excelencia. Así, si se diseccionan los componentes últimos de la sociedad de la información hasta reducirlos a sus elementos esenciales se llega básicamente a dos: información personal y conocimiento. En la sociedad de la información, la moneda de cambio no puede ser otra que la información personal".

[1398] Un ejemplo de identidad de segunda parte lo hemos visto supra, cuando nos hemos referido a la identidad que usa un cliente para acceder a su banco.

[1399] Las identidades de tercera parte son aquéllas suministradas por terceros, públicos o privados. Por ejemplo, el número del documento nacional de identidad, con carácter oficial; o un certificado de identidad, expedido por un prestador de acuerdo con la legislación de firma electrónica.

[1400] El título de la norma internacional es Tecnología de la información – Técnicas de seguridad – Marco de trabajo para la gestión de la identidad – Parte 1: Terminología y conceptos.

29115:2013 (1ª ed.) [1401].

A.3.5 De la autenticación a la gestión de la identidad digital

La norma ISO/IEC 24760-1:2011 trata, de forma novedosa, acerca de la gestión de la identidad. Esta autorregulación parte del hecho de los sistemas de procesamiento de datos colectan y gestionan informaciones de sus usuarios, sean éstos personas, equipamientos o aplicaciones informáticas, y toman decisiones a partir de dichas informaciones, que en su caso implicarán el acceso a aplicaciones y otros recursos, y tiene el objetivo de hacer frente a la necesidad de implementar sistemas eficaces y eficientes que tomen decisiones basadas en la identidad[1402].

Para ello, y con el objetivo final de permitir el cumplimiento de las obligaciones legales, administrativas, contractuales y de negocio aplicables a los sistemas de información[1403], la norma ISO/IEC 24760-1:2011 especifica un marco de trabajo para la emisión, administración y uso de los datos informáticos empleados para caracterizar a los individuos, las organizaciones y los componentes de tecnología de la información que operan en nombre de los anteriores.

De particular interés resultarán – por su indudable valor interpretativo – las definiciones que la norma ofrece, incluyendo las siguientes:

- Identificación[1404] es el proceso de reconocimiento de una entidad, dentro de un dominio[1405] particular, como diferente de otras entidades en dicho dominio.
- Entidad[1406] es un elemento, dentro o fuera de un sistema de tecnología de la información y la comunicación, como por ejemplo una persona, una organización, un dispositivo, un subsistema, o un grupo de dichos elementos, que tiene existencia diferenciada reconocible.
- Identidad[1407] es un conjunto de atributos[1408] referidos a una entidad.

[1401] El título de la norma internacional es Tecnología de la información – Técnicas de seguridad – Marco de trabajo de aseguramiento de la autenticación de entidad.

[1402] Hay que aclarar que esta norma se aplica a cualquier sistema de información que procese información de identidad, y no sólo a aquellos que realizan autenticación. Lo que sucede es que, en el caso de los proveedores de servicios de autenticación a terceros (también denominados proveedores de identidad, o proveedores de credenciales), la gestión de la identidad forma parte del núcleo de su negocio.

[1403] La norma reconoce que la gestión de la identidad es crucial para mantener la seguridad de los procesos organizacionales, así como para la protección de la privacidad de las personas físicas.

[1404] Cfr. sección 3.2.1 de la norma.

[1405] Dominio se define como el entorno donde una entidad puede emplear un conjunto de atributos para la identificación y otros propósitos (cfr. sección 3.2.3 de la norma), como por ejemplo dentro de una empresa, o dentro de un departamento de la empresa.

[1406] Cfr. sección 3.1.1 de la norma.

[1407] Cfr. sección 3.1.2 de la norma.

[1408] Los atributos son características o propiedades de una entidad que se pueden emplear para describir su estado, apariencia u otros aspectos. Los valores de los atributos de una identidad describen a una entidad en un dominio concreto (cfr. 3.1.3 de la norma).

- Información de identidad[1409] es un conjunto de valores de atributos, opcionalmente con cualquier metadato asociado a una identidad.
- Identificador[1410], también denominado identidad única o identidad distinguida, es la información de identidad que distingue, de forma no ambigua, a una entidad de otra en un dominio dado.

  A título de ejemplo, el autor de este trabajo es una entidad (en concreto, una persona física), que tiene diversas identidades, para dominios diferentes. Cada identidad viene definida por uno o varios atributos, cuyos valores concretos determinan la información de identidad de dicha persona, y para cada identidad existe un identificador.

  En el dominio correspondiente a su hogar, su identidad viene determinada solamente por el atributo nombre (siendo la información de identidad el valor de dicho atributo; es decir, "Nacho"), dado que sirve perfectamente para distinguirle dentro de ese dominio (esencialmente porque no hay ninguna otra persona en su hogar con el mismo nombre, por lo que cuando alguien le interpela, no hay duda acerca de a quien se refiere la llamada). En este caso, su identificador es también "Nacho", ya que se trata de un dominio muy reducido y, por tanto, no hace falta más.

  En el dominio de WhatsApp Messenger[1411], su identidad viene dada por el atributo "número de teléfono", el "nombre" – real o inventado – que libremente elija y opcionalmente, una foto, dado dicho número de teléfono le distingue a nivel internacional de forma suficiente como para que pueda recibir los mensajes. La información de identidad será el citado número de teléfono de Nacho, más el nombre en cuestión (por ejemplo, la cadena de texto "Nacholezno"), más la foto correspondiente, que se puede ver a la derecha de este texto[1412]. El identificador será, posiblemente, el número de teléfono[1413].

  Ilustración 32. Nacholezno

  Finalmente, en el dominio correspondiente al Estado español, su identidad viene dada por los atributos "número de documento nacional de identidad", "nombre", "primer

[1409] Cfr. sección 3.2.4 de la norma.

[1410] Cfr. sección 3.1.4 de la norma.

[1411] Una popular aplicación de mensajería instantánea para teléfonos inteligentes.

[1412] Se trata del Minion Wolverine (o Lobezno Minion), creado por Darren Wallace, y que se puede obtener, junto a otros, en http://www.comicbookmovie.com/fansites/nailbiter111/news/?a=88948.

[1413] Aunque en la documentación de WhatsApp no informa de este extremo, parece deducirse el funcionamiento del sistema, sin perjuicio de que también interviene la identidad de la SIM del teléfono en cuestión.

apellido" y "segundo apellido", de forma que queda distinguido como nacional, dentro del territorio nacional y en aquellos Estados del espacio del Acuerdo de Schengen. La información de identidad será el número concreto del DNI de Nacho, la cadena de texto "Ignacio", la cadena de texto "Alamillo", y la cadena de texto "Domingo". El identificador será el número del documento nacional de identidad.

- Autenticación[1414] es el proceso formalizado de verificación[1415] que, si se ejecuta exitosamente, resulta en una identidad autenticada[1416]. Nótese que esta identidad autenticada es un artefacto con valor probatorio, por lo que debe ser adecuadamente registrada.
- Credencial[1417] es una representación de una identidad, típicamente creada para permitir la autenticación de los datos de la información de identidad; esto es, si empleamos una credencial en un proceso de autenticación para una identidad concreta, queda corrobora esa información de identidad.

Respecto a la privacidad, cuyo fomento es uno de los objetivos de esta norma, se definen los siguientes términos:

- Seudónimo[1418] es un identificador que contiene la información de identidad mínima para permitir a un verificador establecerla como un enlace a una identidad conocida.
- Anonimidad[1419] es una condición en la identificación que permite a una entidad ser reconocida como distinta (de otras), sin divulgar información de identidad suficiente para establecer un enlace a una identidad conocida.

La gestión de identidad se define[1420] como el conjunto de procesos y políticas involucrados en la gestión del ciclo de vida, y del valor, tipo y metadatos opcionales de los atributos de las identidades conocidas en un determinado dominio.

Además, la norma autorregula sucintamente las condiciones mínimas de los procesos asociados a la gestión de identidades, considerando la identificación – incluyendo la verificación de la información de identidad, la inscripción o alta y el registro –, la autenticación, y el mantenimiento.

Y no podemos dejar de hacer hincapié en el enfoque orientado a la privacidad que se desprende de la norma, que en su sección 12 ordena que los sistemas de gestión de

---

[1414] Cfr. sección 3.3.1 de la norma.

[1415] Esta verificación es el proceso para determinar si la información de identidad presentada, asociada a una entidad en particular, es aplicable para que la entidad sea reconocida en un dominio particular, en cierto momento del tiempo (cfr. sección 3.2.2 de la norma).

[1416] La identidad autenticada se define como la información de identidad correspondiente a una entidad, creada para registrar el resultado de la autenticación (cfr. sección 3.3.2 de la norma).

[1417] Cfr. sección 3.3.5 de la norma.

[1418] Cfr. sección 3.6.3 de la norma.

[1419] Cfr. sección 3.6.4 de la norma.

[1420] Cfr. sección 3.4.1 de la norma.

identidad que consideren el impacto de la privacidad en sus procesos, de forma que:

- Implementen mecanismos, incluyendo políticas, procesos y tecnologías, para la divulgación mínima[1421] de datos.
- Autentiquen a las entidades que usan información de identidad.
- Minimicen la posibilidad de enlazar identidades – basadas en seudónimos.
- Registren y auditen el uso de la información de identidad.
- Adopten protecciones para evitar la generación de riesgos a la privacidad.
- Implanten políticas para la divulgación selectiva[1422].
- Ofrezcan soporte al uso de seudónimos.
- Implanten políticas de consentimiento explícito al tratamiento de datos sensibles.

En desarrollo de lo establecido en esta norma, se ha aprobado la norma internacional ISO/IEC 24760-2:2015 (1ª ed.)[1423], que define una arquitectura de referencia para un sistema de gestión de identidad que incluye los elementos arquitectónicos más importantes y sus interrelaciones, descritos con respecto a implementaciones de modelos de gestión de identidad.

Además, especifica los requisitos para el diseño e implementación de un sistema de gestión de la identidad para que pueda cumplir con los objetivos de los actores involucrados en el despliegue y funcionamiento de dicho sistema, constituyendo un elemento importante en la autorregulación de esta actividad[1424].

A.3.6 La garantía de la autenticación de entidades

Por su parte, la norma ISO/IEC 29115:2013 parte del presupuesto de que las transacciones de negocio presentan requisitos de seguridad que dependen de un entendimiento del grado de confianza que se puede depositar en la identidad de las partes que intervienen en dicha transacción.

Para lograr este entendimiento, la norma autorregula el aseguramiento de la autenticación de entidad, refiriéndose por tal a la confianza depositada en la totalidad de procesos, actividades de gestión y tecnologías empleadas para establecer y gestionar la identidad

---

[1421] La norma define la divulgación mínima como un principio de la gestión de identidad orientado a restringir la petición o transferencia de información de identidad a terceros a la información mínima estrictamente requerida para un propósito particular (cfr. sección 3.6.2).

[1422] La norma define la divulgación selectiva como un principio de la gestión de identidad que permite a una persona un grado de control sobre la información de identidad a transferir a terceros, por ejemplo durante una autenticación (cfr. sección 3.6.1).

[1423] El título de la norma internacional es Tecnología de la información – Técnicas de seguridad – Marco de trabajo para la gestión de la identidad – Parte 2: Arquitectura de referencia y requisitos.

[1424] Actualmente se trabaja en la norma ISO/IEC 24760-3, que se refiere a los aspectos de práctica, con un mayor contenido de autorregulación, ya que estas prácticas abarcan aspectos de la garantía en el control del uso de la información de identidad, aspectos de control del acceso a la información de identidad y otros recursos, sobre la base de la información de identidad y objetivos de control que deben aplicarse cuando el establecimiento y mantenimiento de un marco de gestión de la identidad.

de una entidad para su uso en transacciones de autenticación.

La norma se estructura alrededor del concepto de credencial[1425], a la que define como el conjunto de datos presentados como evidencia de una identidad o permisos alegados[1426], que es emitido o gestionado por un tercero de confianza[1427], al que se denomina proveedor de servicio de credenciales[1428].

Como base para la confianza, la norma ISO/IEC 29115:2013 establece cuatro niveles de aseguramiento, donde cada nivel describe el grado de confianza que se puede depositar en los procesos de autenticación que la propia norma prescribe, por lo que se puede asumir que la entidad que hace uso de una identidad concreta es, de hecho, la entidad la que se asignó dicha identidad.

Los procesos autorregulados por la norma son los siguientes, organizados en bloques:

- Alta o inscripción[1429], incluyendo la solicitud e iniciación, la verificación de identidad personal y de otras informaciones de identidad, el almacenamiento de documentación acreditativa y el registro ante los servicios.
- Gestión de la credencial, incluyendo su creación, procesamiento previo, expedición, activación, almacenamiento, suspensión, revocación y destrucción, renovación y reemplazo, y almacenamiento de documentación acreditativa.
- Autenticación, incluyendo el almacenamiento de documentación acreditativa.

Por su parte, los niveles de aseguramiento que se definen en la norma son los siguientes:

- Nivel 1 o bajo, en el que existe una confianza mínima en la identidad alegada, pero alguna confianza respecto al hecho de que la entidad es la misma en diferentes operaciones de autenticación, no estableciéndose ningún requisito especial respecto al mecanismo de autenticación, ni obligación de uso de ningún método criptográfico[1430].
- Nivel 2 o medio, en el que existe alguna confianza en la identidad alegada, siendo aceptable cuando el riesgo asociado a una autenticación incorrecta es moderado. Resulta aceptable la autenticación de un solo factor, empleando un protocolo seguro de autenticación que permite el control de la credencial por parte del usuario.
- Nivel 3 o alto, en el que existe una alta confianza en la identidad alegada, siendo

---

[1425] Cfr. sección 3.8 de la norma.

[1426] En este contexto, credencial es un tipo de información de autenticación, término empleado en las normas ISO 7498-2:1989 e ISO/IEC 10181-2:1996. Algunos ejemplos de credenciales que se mencionan en la norma son las contraseñas, las características biométricas de la entidad, códigos de un solo uso o datos firmados digitalmente.

[1427] Cfr. sección 3.29 de la norma, que lo define como la autoridad, o su agente, en la que confían otros actores con respecto a actividades especificadas (por ejemplo, actividades relativas a la seguridad). En esta norma, se refiere específicamente a la expedición de certificados digitales, o de sellos de tiempo electrónico.

[1428] Cfr. sección 3.9 de la norma. En el ejemplo que hemos visto anteriormente, LinkedIn es el proveedor de servicio de credenciales, con respecto a Bizzabo.

[1429] Se correspondería con lo que anteriormente hemos denominado "identificación" de la entidad.

[1430] Por ejemplo, en el nivel 1 se puede emplear un nombre de usuario y contraseña en un proceso de auto-registro realizado por el usuario, a distancia.

requerido cuando el riesgo asociado a una autenticación incorrecta es sustancial. En este nivel se debe emplear autenticación basada en más de un factor; además, se debe emplear criptografía para proteger cualquier intercambio de información secreta de autenticación, así como cuando la misma se encuentra almacenada, aunque no se establecen requisitos concretos respecto a la generación o almacenamiento de credenciales.

- Nivel 4 o muy alto, en el que exista una muy alta confianza en la identidad alegada, siendo requerido cuando el riesgo asociado a una autenticación incorrecta es alto. En este nivel, además de los requisitos del nivel 3, se exigen requisitos de verificación presencial de la identidad personal de los usuarios, el uso de dispositivos físicos para la protección de las claves secretas o criptográficas, y el uso de criptografía para la protección de la información personal y sensible del usuario.

La norma, en definitiva, contiene un conjunto de reglas de adopción voluntaria por las organizaciones que deseen adherirse a la misma, que ofrece un marco de autorregulación suficiente para confiar en los servicios de autenticación, y que puede ser también empleado por los receptores de estos servicios para evaluar el nivel de garantía que ofrecen los proveedores, incluso aunque los mismos no lo adopten.

A.4 La integridad de datos

A.4.1 Concepto

La integridad de datos puede definirse como la propiedad (de la información) en virtud de la cual puede afirmarse que se preserva su precisión y consistencia, con independencia de los cambios realizados[1431], o, en una óptica más específica de seguridad, cuando los datos no han sido alterados o destruidos de forma no autorizada[1432], constituyendo otro servicio básico de seguridad de las tecnologías de la información y la comunicación.

Se trata también de un servicio altamente normalizado[1433] y utilizado, normalmente sin que los usuarios sean muy conscientes de ello, ya que se puede implementar sin que requiera actuación por parte del usuario, a diferencia de otros servicios, como la autenticación.

La norma ISO 7498-2:1989 se refiere al servicio de integridad de datos como aquel que contrarresta amenazas activas, diferenciando diversas modalidades, en función de si la integridad se refiere a unidades de datos individualizadas, o a corrientes de unidades de datos (esto es, transmisiones de datos).

Como mecanismos de integridad de datos, la norma se refiere al uso de valores de comprobación de bloques o valores de comprobación basados en criptografía, además de mecanismos de comprobación de secuencias de datos transmitidos, como la

[1431] Definición 2126247 de la norma internacional ISO/IEC 2382:2015. La definición 2126390 de la norma internacional ISO/IEC 2382:2015 se refiere a la autenticación de datos como el proceso empleado para verificar la integridad de los datos.

[1432] Sección 3.3.21 de ISO 7498-2:1989.

[1433] Sólo en ISO existen 310 normas técnicas que se refieren a la integridad de datos.

secuenciación, los sellos de tiempo o el encadenamiento criptográfico[1434], así como el uso de la firma digital[1435].

Adicionalmente, la norma ISO 7498-2:1989 identifica que los servicios de integridad de datos se deberían ofrecer en diversas capas del modelo conceptual de interconexión de sistemas abiertos[1436]:

- En la capa 3 o de red, que es donde se contienen los medios funcionales y técnicos para las conexiones entre dispositivos dentro de una misma red.
- En la capa 4 o de transporte, que es donde se contienen los medios funcionales y técnicos para las conexiones entre dispositivos de diferentes redes.
- En la capa 7 o de aplicación, que es donde los usuarios interactúan directamente con las aplicaciones.

En el caso de la red Internet, también se pueden considerar servicios de integridad de datos en las capas de transporte (como, por ejemplo, TCP[1437] y UDP[1438]) y de aplicación[1439].

Por su parte, la norma ISO/IEC 10181-6:1996 (1ª ed.)[1440], que regula de forma monográfica un marco de trabajo de seguridad referido a la integridad de datos, adopta la definición de integridad de la norma ISO 7498-2:1989.

La norma concreta que el servicio de integridad tiene como finalidad proteger la integridad de los datos y de sus atributos relevantes, dado que los mismos pueden verse comprometidos por su modificación, eliminación, creación, inserción o repetición no autorizadas.

El servicio de integridad protege la información de estas eventualidades mediante mecanismos de prevención o de detección posterior, sin posibilidad de recuperar los datos; mecanismos que pueden ser de diversa naturaleza, criptográficos o no, y que no

---

[1434] Cfr. sección 5.3.4 de la norma ISO 7498-2:1989.

[1435] En este caso, la norma sólo considera el uso de la firma digital para la integridad de datos individualizados o sin conexión.

[1436] Anteriormente nos hemos referido al modelo OSI.

[1437] De acuerdo con la sección 4.2.2.7 de la especificación técnica IETF RFC 1122:1989, en TCP resulta obligatorio generar un valor de suma de comprobación, definido en la sección 3.1 de la especificación IETF RFC 793:1981, que garantiza la integridad de los datos transmitidos.

[1438] De acuerdo con la sección 4.1.3.4 de la especificación técnica IETF RFC 1122:1898, en UDP no es obligatorio el empleo de valores de suma de comprobación, por lo que la integridad de los datos transmitidos es opcional.

[1439] El protocolo SSL/TLS, al que ya nos hemos referido con detalle con ocasión de la autenticación, ofrece también garantía de la integridad de los datos transmitidos, aunque sólo mientras están siendo transmitidos, y no posteriormente. Para ello emplea un mecanismo criptográfico denominado HMAC, empleando funciones de resumen seguro (como SHA-1). Un ejemplo de aplicación que implementa el servicio de integridad es S/MIME, empleando códigos de autenticación de mensaje (MAC), resúmenes criptográficos o firmas digitales.

[1440] El título de la norma es Tecnología de la información – Interconexión de sistemas abiertos – Marcos de trabajo de seguridad para sistemas abiertos: Marco de trabajo de integridad. Se trata de una norma idéntica a la Recomendación X.815 (1995) de la ITU-T.

tienen por qué transformar los datos cuya integridad protegen.

La norma categoriza los mecanismos de integridad de acuerdo con la siguiente clasificación[1441]:

- Mecanismos que impiden el acceso al medio donde se encuentran los datos cuya integridad se quiere proteger, como por ejemplo el aislamiento físico (del cableado), el control de direccionamiento del tráfico o el control de acceso[1442].
- Mecanismos que detectan modificaciones no autorizadas de los datos o de las secuencias de datos, incluyendo los casos de creación, eliminación y replicación no autorizados de los mismos. Estos mecanismos incluyen los sellos[1443], las firmas digitales, la replicación de datos[1444], las huellas digitales combinadas con transformaciones criptográficas y los números de secuencia de mensajes.

Como en el caso de la autenticación, la aplicación de estos mecanismos técnicos genera testimonios de seguridad que evidencian la integridad de la información, testimonios pueden ser almacenados por las partes para su uso en caso de disputa, por su valor probatorio[1445], dentro del marco de autorregulación que las partes establezcan.

A.4.2 La integridad en la práctica autorregulada de la seguridad de la información

Respecto a la integridad de datos, la norma ISO/IEC 27002:2013 contiene normas de aplicación común en las organizaciones que voluntariamente se adhieren a esta autorregulación.

En concreto, la sección 14.1.2 de la norma, referida al aseguramiento de los servicios de aplicación en redes públicas (como Internet) indica que, a los efectos de determinar los requisitos de seguridad de la información en este caso, se deben determinar y cumplir los requisitos de integridad de los contratos, así como establecer el nivel de confianza requerida para la integridad de los documentos esenciales, y considerar la necesaria integridad de cualesquiera pedidos, información de pagos, detalles de direcciones de entrega y acuses de recibo.

Asimismo, la sección 14.1.3 de la misma norma, referida a la protección de las transacciones de servicios de aplicación, determina la necesidad de garantizar que la información que se encuentra involucrada en dichas transacciones se encuentra protegida

---

[1441] Cfr. la sección 5.3 de la norma ISO/IEC 10181-6:1996.

[1442] En todos estos casos, se puede garantizar la integridad de la información sin necesidad de realizar ningún tratamiento específico de la misma, porque ninguna parte no autorizada puede acceder a la información y, por tanto, no puede hacer ninguna acción no autorizada.

[1443] La norma emplea este término para referirse a los valores de comprobación criptográfica, que se basan en el empleo que claves simétricas o compartidas entre las partes (cfr. sección 8.1.1 de la norma ISO/IEC 10181-6:1996).

[1444] En este caso, se almacenan datos en diversas ubicaciones, de forma que, en caso de ataque contra los datos, se podrá reconstruir la información (cfr. sección 8.2.1 de la norma ISO/IEC 10181-6:1996).

[1445] Desde una perspectiva jurídica, los testimonios de seguridad – en este caso, de integridad – son fuentes de prueba que accederán al procedimiento judicial como uno u otro medio de prueba, en función de lo que en cada caso determine la legislación procesal correspondiente.

para impedir su transmisión incompleta, así como su alteración o reproducción no autorizadas; esto es, garantizar su integridad, para lo cual ofrece diversas posibilidades.

Desde la perspectiva de la clasificación de la información, la sección 8.2.1 de la norma ordena que se consideren los requisitos de integridad de la información a clasificar, al objeto de determinar su sensibilidad para la organización, y en función de dicha sensibilidad, se deberán aplicar controles como, entre otros, los siguientes:

- En cuanto a la gestión de los medios removibles, la norma recomienda el empleo de mecanismos criptográficos para la protección de la información[1446].
- En el caso de la publicación del código fuente de las aplicaciones, se deben aplicar medidas específicas para garantizar su integridad, como la firma digital[1447].
- En el caso de la transmisión de datos a través de redes públicas o inalámbricas, se deben aplicar controles especiales para garantizar su integridad[1448].
- En el caso del intercambio de información con terceros, la norma recomienda considerar el uso de técnicas criptográficas para proteger la integridad de dicha información[1449].

Como ya hemos visto anteriormente, la norma ISO/IEC 27002:2013 no concreta los mecanismos de integridad que se deberán emplear, sino que los mismos deberán ser seleccionados a partir del correspondiente análisis de riesgos, y garantizando el cumplimiento de los requisitos legales correspondientes[1450].

A.5 El no rechazo

A.5.1 Concepto

El no rechazo – también conocido como "no repudio" – puede definirse como la situación en la cual se puede evitar la falsa denegación, por alguna de las entidades involucradas en una comunicación, de haber participado en la misma[1451].

La norma ISO 7498-2:1989 no ofrece una definición del servicio de no rechazo, sino que simplemente caracteriza dos formas del mismo:

- No rechazo con prueba del origen, en el que se proporciona al destinatario de los datos la prueba del origen de los datos, protegiéndole contra cualquier tentativa del expedidor de negar que ha enviado los datos o su contenido.
- No rechazo con prueba de la entrega, en el que se proporciona al expedidor de los datos la prueba de la entrega de los datos, protegiéndole contra cualquier tentativa

[1446] Cfr. sección 8.3.1 de la norma ISO/IEC 27002:2013.

[1447] Cfr. sección 9.4.5 de la norma ISO/IEC 27002:2013.

[1448] Cfr. sección 13.1.1 de la norma ISO/IEC 27002:2013.

[1449] Cfr. sección 13.2.1 de la norma ISO/IEC 27002:2013.

[1450] Como, por ejemplo, la normativa de protección de datos, que exige salvaguardar la información personal de los afectados por el tratamiento.

[1451] Definición 2126394 de la norma internacional ISO/IEC 2382:2015; sección 3.3.44 de la norma ISO 7498-2:1989.

ulterior del destinatario de negar que ha recibido los datos o su contenido.

Como mecanismos de no rechazo, la norma se refiere a la firma digital, la integridad de datos y la notarización[1452].

Adicionalmente, la norma ISO 7498-2:1989 identifica que los servicios de no rechazo se deberían ofrecer en diversas capas del modelo conceptual de interconexión de sistemas abiertos[1453]:

- En la capa 6 o de presentación, que es donde se produce la representación de la información que las entidades de aplicación comunican o mencionan en su comunicación, empleando una combinación apropiada de mecanismos de integridad de datos, de firma y de notarización.
- En la capa 7 o de aplicación, que es donde los usuarios interactúan directamente con las aplicaciones, empleando una combinación apropiada de mecanismos de firma y de integridad de datos de una capa inferior, posiblemente junto con el uso de notarios.

En el caso de la red Internet, también se pueden considerar servicios de no-rechazo en la capa de aplicación[1454].

Por su parte, la norma ISO/IEC 10181-4:1997 (1ª ed.)[1455], que regula de forma monográfica un marco de trabajo de seguridad referido al no rechazo, indica que el servicio de no rechazo consiste en la generación, verificación y registro de evidencia, y en la recuperación y nueva verificación subsiguientes de esta evidencia para resolver disputas; servicio que tiene como finalidad la de proporcionar pruebas sobre un evento o acción particular[1456].

También de acuerdo con esta norma, cuando participan mensajes, debe confirmarse la identidad del originador y la integridad de los datos para proporcionar prueba de origen; igualmente, para proporcionar prueba de entrega, debe confirmarse la identidad del

---

[1452] A esta última la caracteriza en los siguientes términos: "pueden garantizarse las propiedades sobre los datos comunicados entre dos o más entidades, tales como su integridad, origen, fecha y destino, mediante la provisión de un mecanismo de notarización. La seguridad es proporcionada por una tercera parte que actúa como notario, en el que las entidades comunicantes tienen confianza y que mantiene la información necesaria para proporcionar la garantía requerida de una manera verificable. Cada instancia de comunicación puede utilizar la firma digital, el cifrado y los mecanismos de integridad, según sea apropiado, para el servicio que es proporcionado por el notario. Cuando se invoca este mecanismo de notarización, los datos se comunican entre las entidades comunicantes por las instancias de comunicación protegidas y el notario". Nótese que el uso del término "notario" no tiene nada que ver con la institución jurídica del Notariado latino, sino que se debe entender en el sentido de un tercero de confianza, y precisamente en este sentido, la norma internacional ISO/IEC 10181-4:1997 define al notario como una "tercera parte confiable con la que se registran los datos de forma que pueda asegurarse ulteriormente la precisión de las características de los datos".

[1453] Anteriormente nos hemos referido al modelo OSI.

[1454] De hecho, es donde se van a encontrar la mayoría de ellos, dado que el no-rechazo suele involucrar al usuario.

[1455] El título de la norma es Tecnología de la información – Interconexión de sistemas abiertos – Marcos de trabajo de seguridad para sistemas abiertos: Marco de trabajo de no-repudio. Se trata de una norma idéntica a la Recomendación X.813 (1996) de la ITU-T.

[1456] Cfr. sección 5.1 de la norma.

receptor y la integridad de los datos. Finalmente, en algunos casos, también puede requerirse evidencia relativa al contexto (por ejemplo, fecha, hora y ubicación del originador/receptor).

El servicio de no rechazo ofrece diversas facilidades en orden a prevenir un intento de rechazo: generación de evidencia, registro de evidencia, verificación de la evidencia generada y recuperación y nueva verificación de la evidencia, facilidades que se ordenan en las cuatro siguientes fases del no rechazo[1457]: Generación de evidencia; transferencia, almacenamiento y recuperación de evidencia; verificación de evidencia y resolución de disputas.

Dichas fases, excepto la de resolución de disputas, se muestran en la siguiente ilustración[1458]:

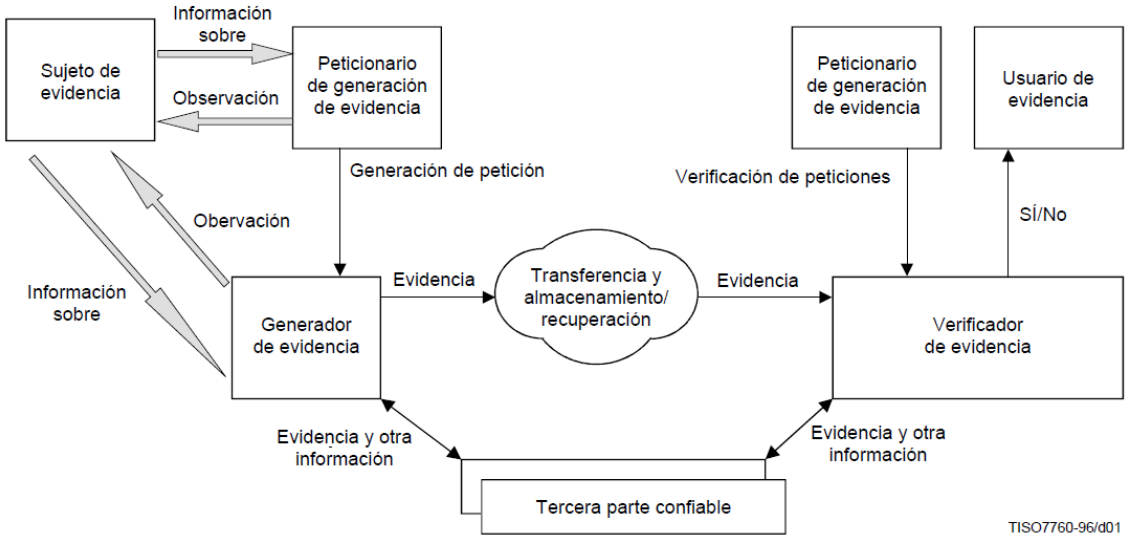


Ilustración 33. Fases del no rechazo (con y sin tercero de confianza)

La norma internacional ISO/IEC 10181-4:1997 identifica diversos mecanismos de no rechazo, incluyendo el uso de testimonios de seguridad producidos por terceras partes, con y sin utilización de módulos de seguridad; la firma digital, con o sin sellado de tiempo; el uso de terceros de confianza en línea; y la notarización.

Por su parte, la norma internacional ISO/IEC 13888-1:2009 (3ª ed.)[1459] desarrolla la norma que acabamos de presentar, definiendo mecanismos técnicos de no rechazo, basados en valores de comprobación criptográfica, como sobres digitales – basados en cifras simétricas – y firmas digitales – basadas en cifras asimétricas –, para las fases de generación, transferencia, almacenamiento y recuperación, y verificación de evidencia.

También prevé mecanismos de sellado de tiempo y de notarización, como complemento de los servicios de no rechazo que regula, que son los siguientes:

[1457] Cfr. sección 5.3 de la norma.

[1458] Sección 5.3 de la norma.

[1459] El título de la norma es Tecnología de la información – Técnicas de seguridad – No rechazo – Parte 1: General.

- No rechazo de origen, destinado a proteger contra la falsa negación del originador de haber creado el contenido de un mensaje y de haber enviado el mismo[1460].
- No rechazo de entrega, destinado a proteger contra la falsa negación de un destinatario de haber recibido un mensaje y conocido el contenido del mismo[1461].
- No rechazo de transmisión, destinado a proporcionar evidencia de que una autoridad de entrega[1462] ha aceptado un mensaje para su transmisión[1463].
- No rechazo de transporte, destinado a proporcionar evidencia al generador del mensaje de que una autoridad de entrega ha entregado un mensaje al destinatario[1464].
- No rechazo de creación, destinado a proteger contra la falsa negación de una entidad de haber creado el contenido de un mensaje (es decir, ser responsables por el contenido de un mensaje)[1465].
- No rechazo de recibo, destinado a proteger contra la falsa negación de un destinatario de haber recibido un mensaje[1466].
- No rechazo de conocimiento, destinado a proteger contra la falsa negación de un destinatario de haber tomado nota del contenido de un mensaje recibido[1467].
- No rechazo de envío, destinado a proteger contra la falsa negación del remitente de haber enviado un mensaje[1468].

La norma ISO/IEC 13888-1:2009 también es muy relevante porque concreta, para los diferentes mecanismos de no rechazo, los denominados testimonios de no rechazo[1469], que son testimonios de seguridad que contienen la evidencia y, opcionalmente, otros datos adicionales, que sustenta el no rechazo; mecanismos que son posteriormente regulados con detalle en las restantes partes de la norma internacional, indicando la colección de técnicas de seguridad que resultan apropiadas para cada caso concreto, incluyendo el uso de técnicas criptográficas simétricas[1470] y asimétricas[1471].

[1460] Sección 3.30 de la norma, denominado en inglés non-repudiation of origin.

[1461] Sección 3.25 de la norma, denominado en inglés non-repudiation of delivery.

[1462] Por ejemplo, un agente de transmisión de correo electrónico, o un tercero de confianza.

[1463] Sección 3.36 de la norma, denominado en inglés non-repudiation of submission.

[1464] Sección 3.39 de la norma, denominado en inglés non-repudiation of transport.

[1465] Sección 3.24 de la norma, denominado en inglés non-repudiation of creation.

[1466] Sección 3.33 de la norma, denominado en inglés non-repudiation of receipt.

[1467] Sección 3.29 de la norma, denominado en inglés non-repudiation of knowledge.

[1468] Sección 3.34 de la norma, denominado en inglés non-repudiation of sending.

[1469] Definidas en la sección 3.38 de la norma, denominados en inglés non-repudiation tokens.

[1470] Cfr. ISO/IEC 13888-2:2010. Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques. Las técnicas previstas en la norma sustentan los servicios genéricos de no rechazo, y servicios de no repudio de origen y de entrega.

[1471] Cfr. ISO/IEC 13888-3:2009. Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using asymmetric techniques. Las técnicas previstas en la norma sustentan los servicios de no

Dichos testimonios pueden ser almacenados por las partes para su uso en caso de disputa, por su indudable valor probatorio, dentro del marco de autorregulación que las partes establezcan.

A.5.2 El no rechazo en la práctica autorregulada de la seguridad de la información

Respecto al no rechazo, la norma ISO/IEC 27002:2013 también contiene normas de aplicación común en las organizaciones que voluntariamente se adhieren a esta autorregulación.

En concreto, la sección 13.2.2 de la norma, referida los acuerdos sobre la transferencia de información indica que dichos acuerdos deberían incorporar procedimientos para garantizar la trazabilidad y el no rechazo.

Por su parte, la sección 14.1.2 de la norma, referida al aseguramiento de los servicios de aplicación en redes públicas (como Internet) indica que, a los efectos de determinar los requisitos de seguridad de la información en este caso, se deben determinar y cumplir los requisitos de no rechazo de los contratos.

Otro elemento importante en la autorregulación del no rechazo son las denominadas políticas de no rechazo, previstas en la norma ISO/IEC 10181-4:1997[1472], y que pueden contener las siguientes reglas:

- Reglas para la generación de evidencia, como, por ejemplo, la especificación de las clases de actividad para las que debe generarse evidencia de no rechazo; las especificaciones de los terceros de confianza que se han de utilizar para generar evidencia; los cometidos en que pueden actuar dichos terceros; los procedimientos que deben seguir las entidades cuando generan evidencia.
- Reglas para la verificación de evidencia, como, por ejemplo, la especificación de los terceros de confianza cuya evidencia es aceptable; para cada tercero de confianza, las formas de evidencia que serán aceptadas de dicho tercero.
- Reglas para el almacenamiento de evidencia, como, por ejemplo, los medios que se han de utilizar para asegurar la integridad de la evidencia almacenada.
- Reglas para el uso de evidencia, como, por ejemplo, la especificación de las finalidades para las que puede utilizarse la evidencia.
- Reglas para el arbitraje, como, por ejemplo, la especificación del árbitro que puede mediar en una disputa.

Como se puede ver, una política de no rechazo regula detalladamente el ciclo de vida de la evidencia o prueba de la transacción, aportando confianza a las partes sobre la prueba del proceso al que se ha incorporado el servicio de no rechazo.

A.5.3 No rechazo de mensajes de correo electrónico: S/MIME y DKIM

Para ejemplificar las diversas posibilidades que existen en relación con el no rechazo,

---

rechazo de origen, de entrega, de transmisión y de transporte.

[1472] Cfr. la sección 6 de la norma.

podemos presentar dos casos relativos al correo electrónico.

En primer lugar, si queremos implementar un sistema de no rechazo a través del correo electrónico, podemos emplear el protocolo S/MIME[1473], que hace uso del mecanismo de firma digital para garantizar el no rechazo de los mensajes por sus remitentes, en este caso, sin intervención de notario. Básicamente, S/MIME es implementado por los clientes de correo electrónico, que nos permiten elegir la posibilidad de agregar una firma digital certificada al mensaje a remitir, especificando de forma bastante detallada, además, las opciones del mecanismo técnico a emplear[1474], como se puede ver en las siguientes ilustraciones[1475]:

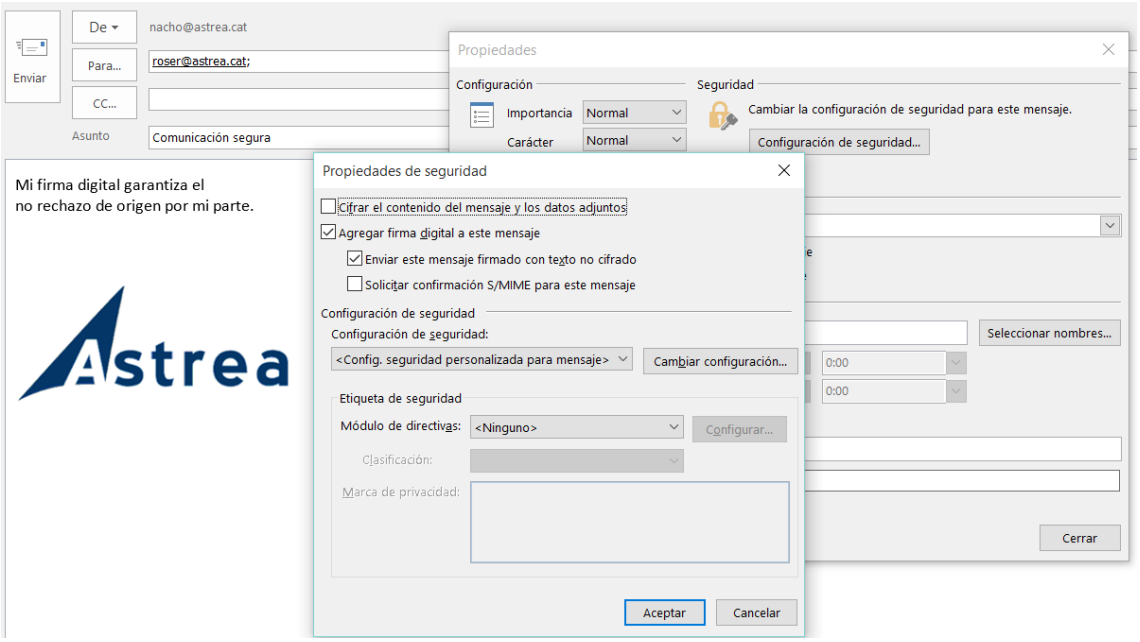


Ilustración 34. Firma digital S/MIME de correo electrónico

[1473] Este protocolo se encuentra actualmente definido en las especificaciones técnicas del IETF RFC 5750:2010 (Manipulación de certificados), RFC 5751:2010 (Especificación de los formatos de mensaje), y se basa en el uso de la sintaxis de mensajería criptográfica (CMS), definida actualmente en IETF RFC 5652:2009) y en diversas RFC adicionales que la amplían en aspectos concretos.

[1474] Hay que decir que en muchos casos estas opciones vienen determinadas por la política de seguridad de la organización, y que se pueden hacer obligatorias mediante la configuración corporativa de las herramientas.

[1475] En este caso, basadas en la aplicación de correo electrónico Microsoft Outlook 2013.

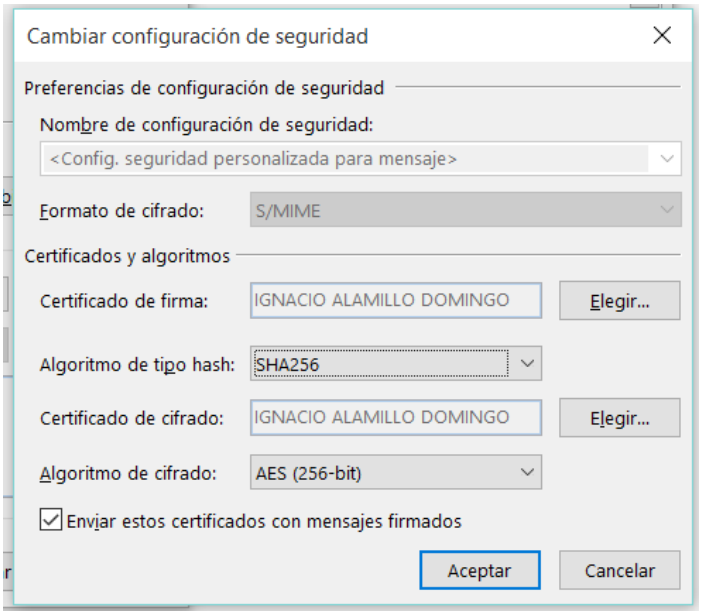


Ilustración 35. Opciones de seguridad de la firma digital S/MIME

Cuando se remite el correo electrónico, el sistema genera la firma digital[1476] y la adjunta al correo electrónico, remitiendo ambos al destinatario, que dispondrá del correo como prueba en caso de que rechacemos haberlo remitido.

En este sentido, el correo electrónico firmado S/MIME es un testimonio de no rechazo de origen[1477], al que pueden posteriormente agregarse otros testimonios de no rechazo, como por ejemplo la aportada por el agente de correo electrónico que ha entregado el correo electrónico a su destinatario.

En segundo lugar, y aunque de forma más limitada que S/MIME, ofrece sustento al no rechazo del correo electrónico el protocolo DKIM[1478], que emplea firmas digitales para la firma de los mensajes por parte de los agentes[1479] que intervienen en su gestión, pero no necesariamente por el usuario que los remite.

Un caso habitual es que este agente sea una organización que asigna cuentas de usuario la que firme estos mensajes de correo electrónico, incorporando la firma digital a la cabecera del mensaje, para su verificación por terceros; a título de ejemplo, cuando Google provee cuentas de correo electrónico a sus usuarios, emplea su clave privada para firmar con DKIM los mensajes salientes, de forma que los terceros receptores tienen una

---

[1476] Para ello emplea un formato definido en una sintaxis concreta, que incorpora la firma digital, el certificado del firmante y otras informaciones útiles, que veremos posteriormente con detalle.

[1477] Y también un documento firmado, que en su caso producirá efectos equivalentes a los que hubiere producido firmado de forma manuscrita con tinta sobre papel, en virtud de lo establecido por la legislación, que asimila la firma digital – a través de su institucionalización jurídica como firma electrónica avanzada – a la firma manuscrita.

[1478] Este protocolo se encuentra actualmente definido en las especificaciones técnicas del IETF RFC 6376:2011 (Firmas DKIM) y RFC 6377:2011/BCP 167 (DKIM y listas de correo).

[1479] Como por ejemplo, los agentes de usuario de correo, los agentes de remisión de correo u otros, como los gestores de listas de correo.

garantía de que dichos correos proceden de Google, algo que sustenta el no rechazo[1480] y permite luchar contra el envío ilegítimo de correos[1481].

Para ello, cada agente debe disponer de un par de claves de firma digital; como en DKIM no se emplean certificados digitales, la clave pública del agente de correo electrónico se debe registrar en un depósito públicamente accesible, que en este caso es el registro DNS correspondiente al nombre de dominio[1482].

A.5.4 No rechazo basado en servicio de tercero de confianza interpuesto: Logalty

También son servicios de no rechazo los que ofrecen compañías como Logalty, actuando como tercero de confianza interpuesto en línea, requerido por una parte de la comunicación para que registre y/u obtenga evidencia y para que responda de la validez de la misma, aportando mecanismos de autenticación, de integridad, de sellado de tiempo y de notarización[1483].

A continuación, se muestra la secuencia del proceso de tercero de confianza:

Ilustración 36. Proceso de contratación basado en servicio de no-rechazo

Para esta compañía, las garantías de la tercería son las siguientes:

- Acreditar con plena garantía que el contrato visualizado es el contrato que se ha firmado, dado que es el tercero quien gestiona los dispositivos de firma.
- Vincular con plena garantía el contenido del contrato a las firmas de los intervinientes, dado que es en el tercero, ajeno a las partes y con sus tercerías, donde se realiza el acto de la contratación.
- Disponer con plena garantía de prueba de puesta a disposición del contrato antes de la firma, dado que es el tercero quien recaba la prueba de puesta a disposición.
- Demostrar con plena garantía que el emisor no ha utilizado las firmas electrónicas para firmar otro documento, dado que es el tercero quien únicamente recaba y

---

[1480] Digamos que ya no se podrá rechazar que el mensaje ha sido modificado (o creado) fraudulentamente desde que ha salido de Google, reduciendo el riesgo.

[1481] Una de las técnicas de SPAM consiste en emplear una cuenta de otro dominio, algo que DKIM impide.

[1482] Por ello, la seguridad de DKIM depende de la seguridad del DNS del agente.

[1483] En el ámbito de la contratación electrónica con sujeción a Derecho español, esta figura ha sido parcialmente regulada en el artículo 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

custodia las firmas.

En el proceso de este prestador, el emisor se autentica frente al servicio de no rechazo empleando una firma digital basada en certificado, o alternativamente, contraseña; mientras que el receptor se autentica frente al servicio empleando diversos mecanismos de autenticación, incluyendo el uso de firma digital basada en certificado, contraseña de un solo uso remitida mediante SMS a su móvil registrado, o la firma capturada en tableta digitalizadora – nótese que el proceso de Logalty no se limita a las transacciones a distancia, sino que también implanta formalización presencial de contratos electrónicos.

De esta forma se muestra a continuación:

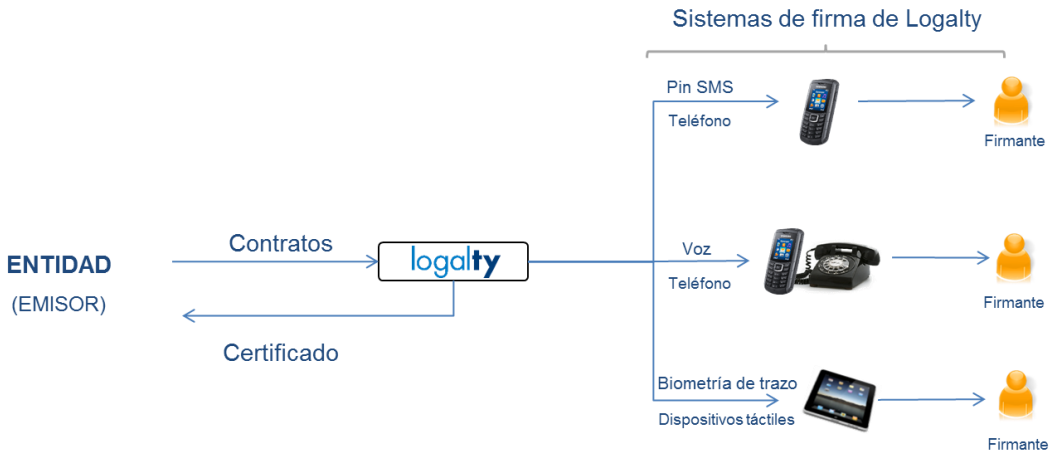


Ilustración 37.Sistemas de firma disponibles en el servicio de no-rechazo de Logalty

Por otra parte, Logalty emplea otros terceros de confianza, incluyendo la generación de sellos de tiempo electrónico por parte de la compañía española Firmaprofesional, o el depósito de los resúmenes criptográficos de las transacciones en diversos Notarios, con la finalidad de incrementar de forma significativa las garantías para las partes.

De forma gráfica, se muestra en la siguiente ilustración:

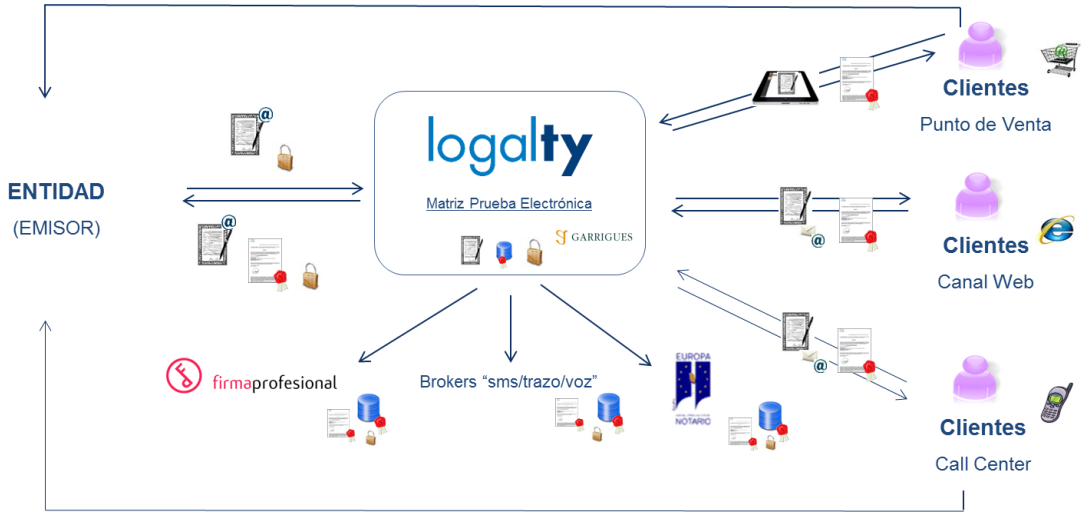


Ilustración 38. Esquema general del servicio de no-rechazo de Logalty

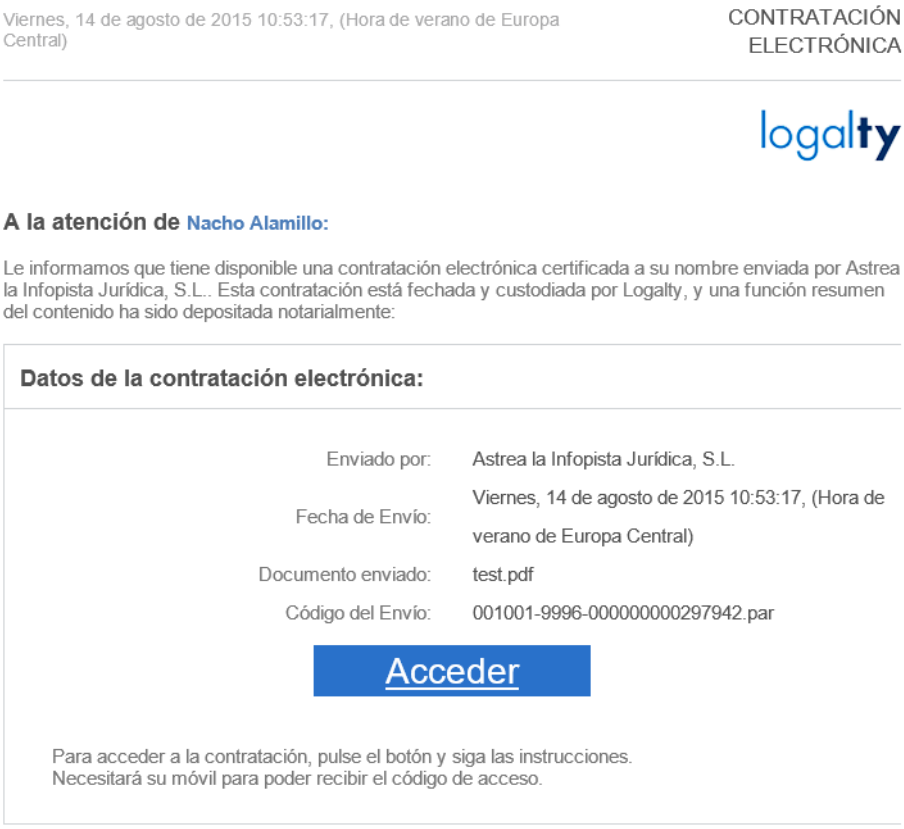
En este caso, el testimonio de no rechazo es la "matriz de prueba electrónica", un fichero generado y custodiado por Logalty que contiene evidencias de toda la historia de la

transacción[1484].

Desde la perspectiva de la experiencia de usuario receptor, el proceso de Logalty se inicia con la recepción un correo electrónico, remitido por Logalty, en el que se le informa de que tiene disponible una operación.

En dicha comunicación por correo electrónico se incluye información acerca de la fecha y hora de remisión de la comunicación, los datos personales del destinatario pretendido de la misma, y los datos del remitente de la misma (Logalty), que actúa por cuenta del emisor que le ha contratado (que en este caso es la empresa Astrea la Infopista Jurídica, SL).

Asimismo, en la misma se informa acerca del documento que se remite, identificado mediante un nombre y un código de envío, y se informa al destinatario de que la citada contratación electrónica certificada ha sido fechada y custodiada por Logalty, que el resumen de la misma ha sido depositado ante Notario, y que puede acceder a la contratación siguiendo en enlace. También se le informa de la necesidad de disponer de su teléfono móvil, para recibir el código de acceso, que le servirá de mecanismo de firma.


Viernes, 14 de agosto de 2015 10:53:17, (Hora de verano de Europa Central)

CONTRATACIÓN ELECTRÓNICA

logalty

A la atención de Nacho Alamillo:

Le informamos que tiene disponible una contratación electrónica certificada a su nombre enviada por Astrea la Infopista Jurídica, S.L.. Esta contratación está fechada y custodiada por Logalty, y una función resumen del contenido ha sido depositada notarialmente:

Datos de la contratación electrónica:

Enviado por:	Astrea la Infopista Jurídica, S.L.
Fecha de Envío:	Viernes, 14 de agosto de 2015 10:53:17, (Hora de verano de Europa Central)
Documento enviado:	test.pdf
Código del Envío:	001001-9996-000000000297942.par

Acceder

Para acceder a la contratación, pulse el botón y siga las instrucciones.
Necesitará su móvil para poder recibir el código de acceso.

Ilustración 39. Correo electrónico de aviso de operación de contratación

Cuando el receptor sigue el enlace[1485], accede a la pantalla de verificación de acceso a

[1484] Este fichero tendrá también, en su caso, la consideración de documento firmado, que en su caso producirá efectos equivalentes a la firma escrita (empleando firma digital, u otros mecanismos técnicos), en virtud de lo establecido por la legislación aplicable.

[1485] El enlace contiene un tique de acceso a esta página, sin el cual la misma no se muestra, por lo que resulta un mecanismo eficaz para que sólo el receptor, poseedor del mismo (en principio) pueda acceder a

Logalty, donde deberá autenticarse mediante su número del DNI[1486], impidiendo que terceros no autorizados por el emisor accedan al contenido. También se le pide a la persona que teclee un código generado aleatoriamente por Logalty, en este caso a efectos de evitar los ataques de automatización[1487]:

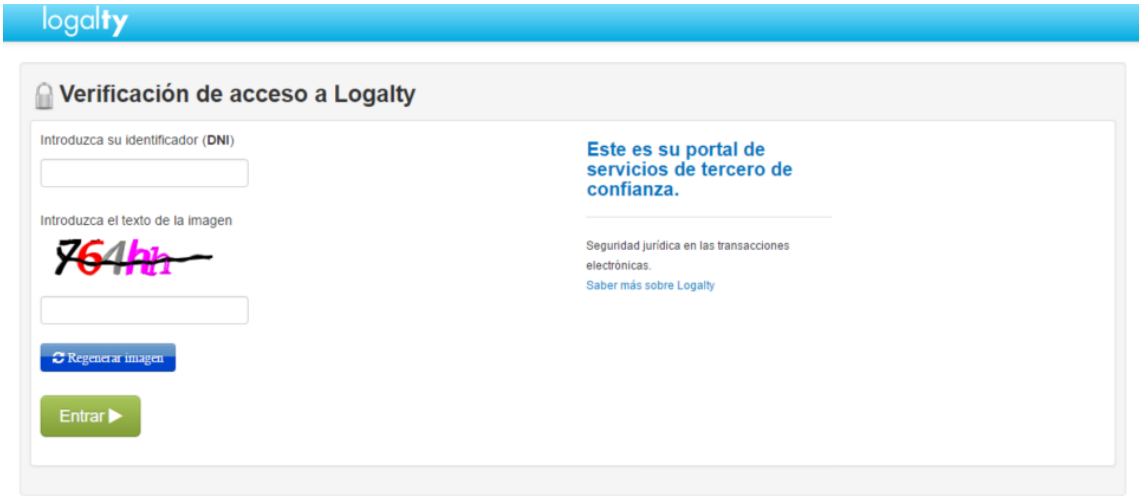


Ilustración 40. Pantalla de autenticación inicial del receptor

Cuando el usuario receptor introduce su identificador y el texto de la imagen, puede entrar en el portal, donde se va a encontrar con la necesidad de aceptar[1488] unas condiciones generales reguladoras del proceso de tercero de confianza:

---

la operativa. Este tique tiene 198 caracteres, con el siguiente aspecto:

q%2BK3VWsz5a%2FZVk0ymrMIYgqqIN4OD2G0GdokzSh2Iy7RJb0Mep%2F2wxJGreC8YdKe13MeZ4EQBSqVcqQZyFpl1LIeF7weG0eX6YWv8qYSoXjvzGEgp15hbvQYQCEa96%2B5vG%2BXniG1z1108H0xwKZcJF7Df1wehREIF4Z1Vvsf2n8UMY6jyt3YWA%3D%3D

[1486] Dado que, aunque es una posibilidad remota, podría suceder que alguien reciba este código por error, se exige a la persona receptora que introduzca su número de documento nacional de identidad, como segundo factor de autenticación antes de acceder al contenido de la operativa de contratación.

[1487] Este tipo de códigos se denomina CAPTCHA – Completely Automated Public Turing Test To Tell Computers and Humans Apart, un término acuñado en el año 2000 por Luis von Ahn, Manuel Blum, Nicholas Hopper y John Langford, de la Universidad Carnegie Mellon. Para más información sobre este mecanismo, cfr. (von Ahn, Maurer, McMillen, Abraham, & Blum, 2008).

[1488] El usuario puede descargarse las condiciones generales del servicio, para su constancia posterior.

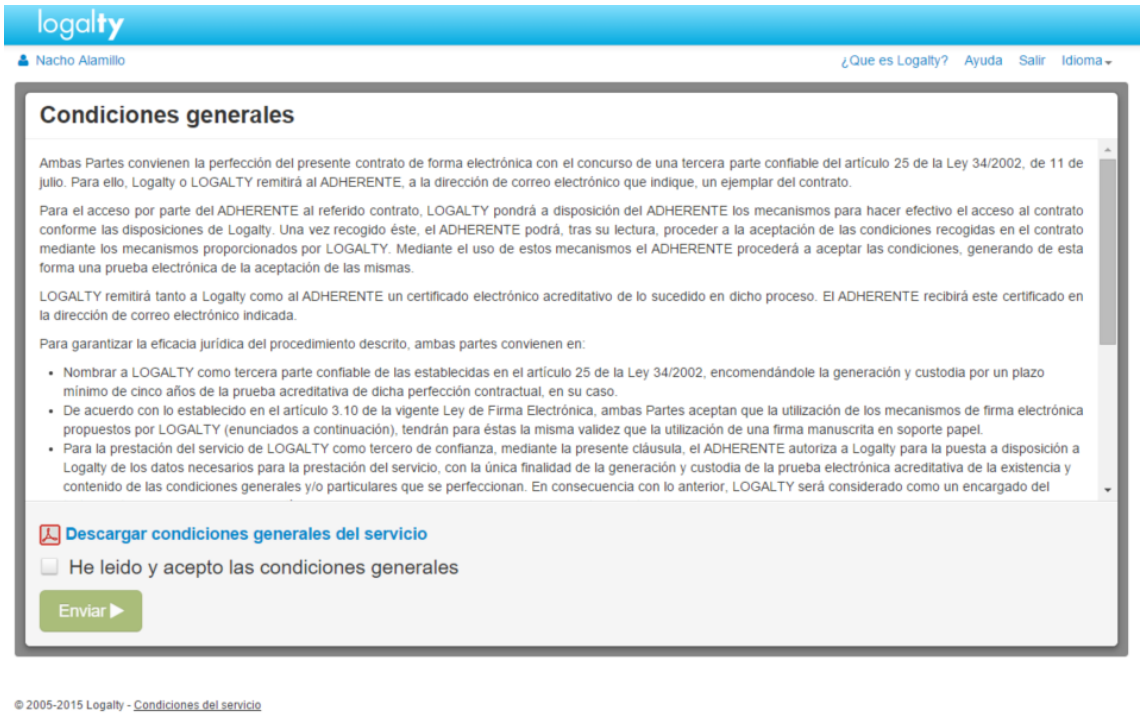


Ilustración 41. Pantalla de condiciones generales de usuario receptor

Si el usuario está conforme con las condiciones generales; esto es, con el servicio (y la política) de no rechazo que ha establecido el tercero de confianza, debe marcar la casilla correspondiente para poder continuar el proceso, designando a Logalty como tercero de confianza para esta transacción, y accediendo a la siguiente pantalla:

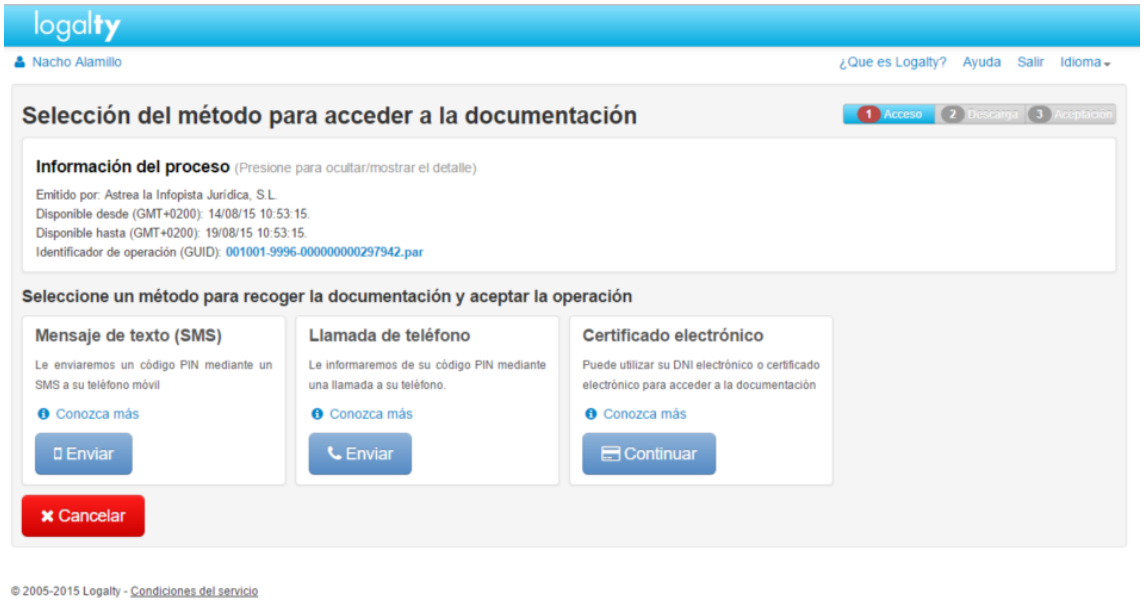


Ilustración 42. Métodos de firma disponibles para el receptor

Como se puede ver, y porque de esta forma lo ha decidido el emisor de la propuesta de contratación, el receptor podrá emplear uno de hasta tres mecanismos para recoger la documentación y, posteriormente, prestar su consentimiento; esto es, firmar:

Ilustración 43. Pantalla de acceso a la documentación por el receptor

En este caso, el receptor ha optado por la remisión por Logalty de un código de acceso específico y único para dicha operación mediante SMS, aunque también podría haber decidido la recepción del mismo mediante una llamada telefónica realizada por Logalty, o por la posibilidad de emplear un mecanismo de firma digital basada en certificado.

En todo caso, cuando el receptor introduce el código recibido, accede a la posibilidad de descargar la documentación a firmar, para su lectura y conservación.

La documentación a firmar es un PDF al que Logalty ha añadido determinados metadatos de la operación, así como su sello gráfico, para denotar que se trata de un documento intervenido y custodiado por Logalty en su condición de tercero de confianza, protegiendo al receptor frente a un eventual no rechazo por parte del emisor:

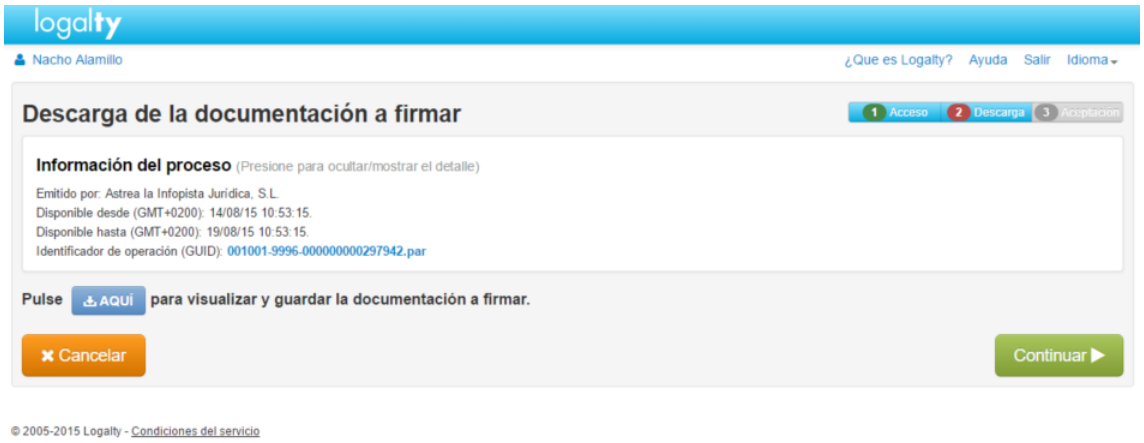


Ilustración 44. Pantalla de descarga de la documentación a firmar

Asimismo, una vez el receptor ha procedido a descargar la documentación a firmar, si decide continuar la operativa, accede a la pantalla de firma:

Ilustración 45. Pantalla de firma de documentación por el receptor

Se trata de una pantalla similar a la empleada para la descarga de la documentación, pero con el añadido de poder volver a visualizar la documentación, en caso de duda, o de cancelar la operativa por error en el número de teléfono móvil.

En caso de que el receptor introduzca el código y haga clic en el botón denominado "Firmar", prestará su consentimiento, firmando el contrato, y accederá a la última pantalla del proceso:

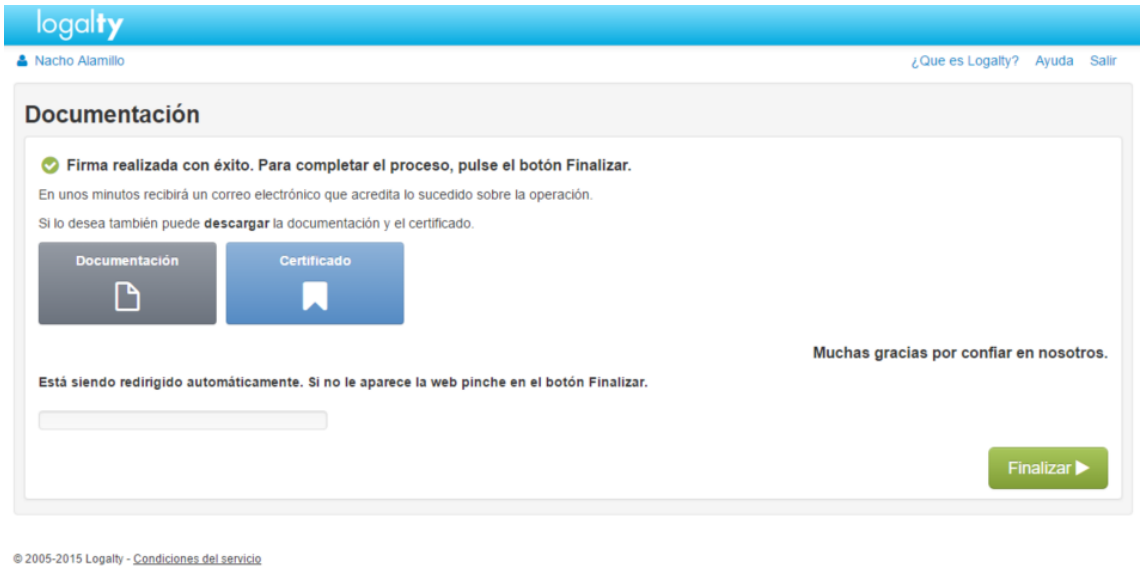
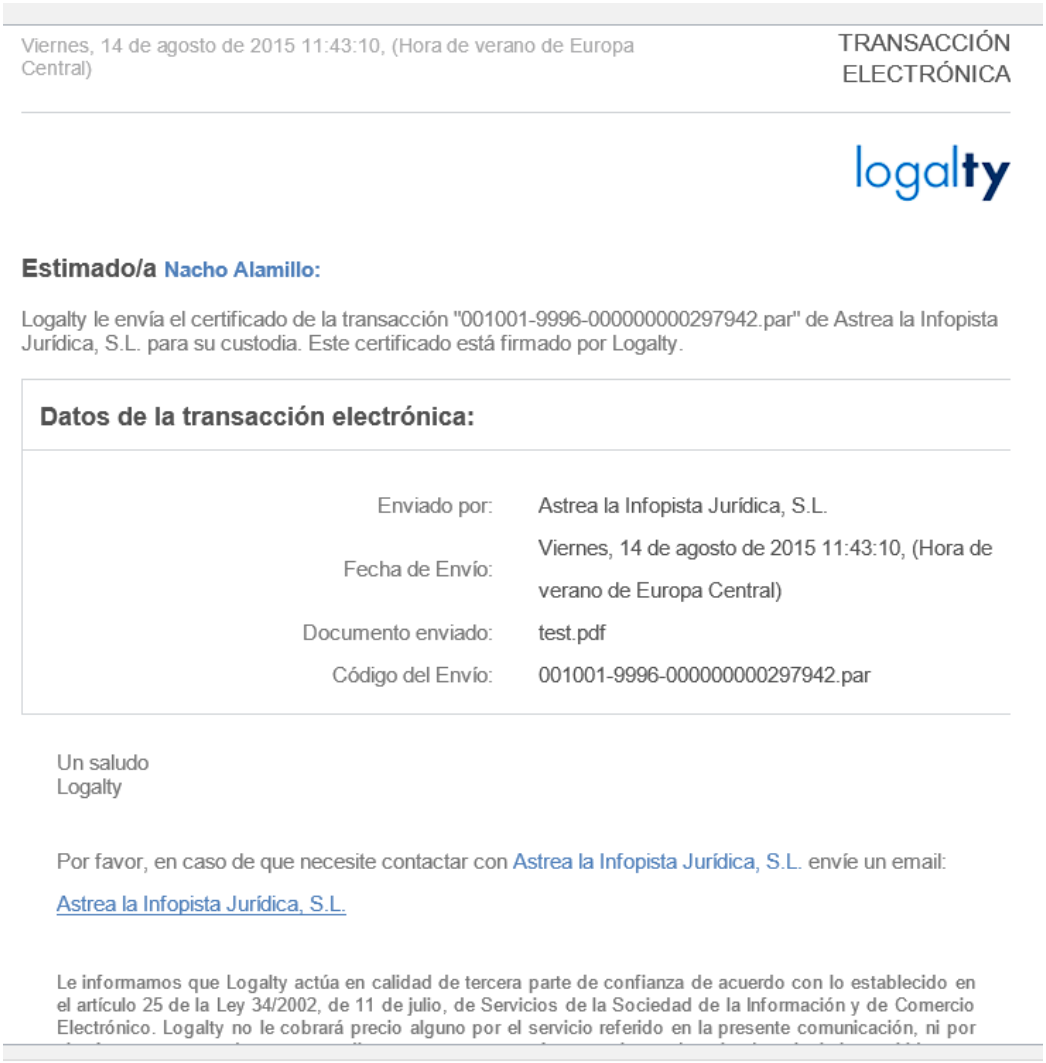


Ilustración 46. Pantalla de finalización del proceso de contratación con no rechazo

En este momento, el receptor podrá descargar el contrato firmado y un certificado, expedido por Logalty, acreditando la operación efectuada. Adicionalmente, y como se informa en dicha pantalla, Logalty envía al receptor un correo electrónico que contiene la información básica acerca de la transacción efectuada, y el contacto con el emisor.

Este correo incorpora, mediante adjunto, el documento firmado y el certificado de transacción que anteriormente hemos podido descargar de la web de Logalty, ofreciendo

al receptor que no lo haya realizado durante el proceso, de obtener acceso fácil, conveniente y, lo que es más importante, duradero, al contrato firmado, y al certificado acreditativo, expedido por Logalty, de la contratación realizada.



Viernes, 14 de agosto de 2015 11:43:10, (Hora de verano de Europa Central)

TRANSACCIÓN ELECTRÓNICA

logalty

Estimado/a Nacho Alamillo:

Logalty le envía el certificado de la transacción "001001-9996-000000000297942.par" de Astrea la Infopista Jurídica, S.L. para su custodia. Este certificado está firmado por Logalty.

Datos de la transacción electrónica:

Enviado por:	Astrea la Infopista Jurídica, S.L.
Fecha de Envío:	Viernes, 14 de agosto de 2015 11:43:10, (Hora de verano de Europa Central)
Documento enviado:	test.pdf
Código del Envío:	001001-9996-000000000297942.par

Un saludo
Logalty

Por favor, en caso de que necesite contactar con Astrea la Infopista Jurídica, S.L. envíe un email:

Astrea la Infopista Jurídica, S.L.

Le informamos que Logalty actúa en calidad de tercera parte de confianza de acuerdo con lo establecido en el artículo 25 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Logalty no le cobrará precio alguno por el servicio referido en la presente comunicación, ni por

Ilustración 47. Correo electrónico de confirmación de operación de contratación

Como hemos avanzado, se trata de un sistema que, por tanto, ofrece no rechazo de origen, protegiendo al receptor, pero también de destino, protegiendo al emisor, y se realiza de acuerdo con unas políticas que permiten a ambas partes confiar en el valor y la eficacia jurídica del contrato.

En definitiva, y como en el caso de los servicios de autenticación e integridad, la aplicación de estos mecanismos técnicos de no rechazo genera testimonios de seguridad que evidencian lo que ha sucedido, testimonios pueden ser almacenados por las partes para su uso en caso de disputa, por su indudable valor probatorio[1489], dentro del marco de autorregulación que las partes establezcan, y que es particularmente detallado en este

[1489] Desde una perspectiva jurídica, los testimonios de no rechazo son fuentes de prueba que accederán al procedimiento judicial como uno u otro medio de prueba, en función de lo que en cada caso determine la legislación procesal correspondiente.

caso.

ANEXO B. LA SINTAXIS DE LA FIRMA Y SELLO ELECTRÓNICOS AVANZADOS

Puede resultar interesante, al efecto de visualizar la noción de una firma o sello electrónico avanzado, decir algo acerca de la sintaxis que se emplea para representar y transportar informáticamente una evidencia criptográfica y, más en particular, la firma digital[1490].

La importancia de este punto debe quedar fuera de toda duda, ya que esta definición sintáctica nos va a indicar qué contenidos concretos encontramos "dentro" de una firma digital y, por tanto, con qué elementos contamos en caso de un eventual rechazo, para practicar prueba pericial, algo que a todo abogado ciertamente le interesa.

De nuevo, cabe acudir a la autorregulación de la industria en este punto, con especial atención a las grandes sintaxis de mecanismos criptográficos; a saber, la Sintaxis de Mensaje Criptográfico, conocida por su acrónimo inglés CMS, y la sintaxis de firma digital en XML. Dado que no existen grandes diferencias de contenido entre ambas, al menos desde la perspectiva relacionada con lo jurídico[1491], que es lo que ahora nos interesa, resultará suficiente con presentar sólo una de ellas.

CMS es una sintaxis[1492] definida actualmente en la especificación técnica del IETF RFC 5652:2009[1493], diseñada para firmar digitalmente con clave pública certificada[1494], resumir criptográficamente, autenticar o cifrar cualquier tipo de contenido. Esta sintaxis define un tipo de dato especial, que permite contener el resultado de una operación criptográfica, como una firma digital, y otros datos e informaciones relevantes, así como relacionarlo con el objeto protegido, por lo que su valor como fuente de prueba es muy relevante; esto es, es la información que debemos conservar y proteger para poder practicar prueba.

De hecho, CMS se puede ver como una especie de contenedor donde se incluye una gran cantidad de información interesante desde la perspectiva de los servicios de no rechazo que hemos presentado anteriormente, contenedor que ha sido ampliado posteriormente en

---

[1490] Anteriormente hemos visto los mecanismos criptográficos que se emplean para la garantía de la actuación electrónica, y más en concreto, la firma digital, "al desnudo", en forma de una explicación simple de las primitivas en que se basan los mismos (cfr. el Anexo A.1.1.3 de este trabajo).

[1491] Una diferencia relevante es que CMS sólo permite el empleo de firmas digitales con claves públicas certificadas, mientras que XMLDSig es algo más versátil, y permite también el uso de firmas digitales sin clave pública certificadas, así como el uso de códigos de autenticación de mensaje como HMAC.

[1492] Basada en ASN.1, una notación normalizada que se emplea para la definición de tipos de datos, valores y restricciones sobre tipos de datos, definida en la Recomendación de la ITU-T X.680:2011, también publicada como norma internacional ISO/IEC 8824-1:2008.

[1493] Esta especificación técnica fue originalmente desarrollada por una entidad privada, los laboratorios RSA, y se emplean en muchos protocolos y aplicaciones de Internet.

[1494] CMS se emplea, entre otros, en la firma de mensajes de correo electrónico seguro, conforme al protocolo S/MIME (Ramsdell & Turner, 2010); en la firma de documentos PDF (ISO, 2008); en la firma de controladores de hardware (Housley, 2005) o de paquetes de código para su distribución a usuarios finales; en la firma de puntos de confianza (Housley, Ashmore, & Wallace, 2010); o en la mensajería asociada a la gestión de puntos de confianza (Housley, Ashmore, & Wallace, 2010).

otras especificaciones técnicas[1495], hasta el punto de haberse convertido en el paradigma técnico de la firma electrónica avanzada normalizada por el ETSI europeo.

En concreto, el contenedor de firma definido en CMS, que se denomina `SignedData`, está formado por los siguientes elementos[1496]:

- Uno o varios firmantes del contenido firmado (campo `SignerInfo`). Las personas identificadas en este elemento serán aquellas a las que se podrá imputar la firma digital, por lo que esta información es esencial[1497].
- El contenido, a partir del cual se genera el resumen criptográfico para la firma digital (campo `encapContentInfo`), por lo que el mismo ya no podrá ser modificado sin que dicha modificación sea detectable por los terceros receptores del citado contenido.

  En este punto hay que decir que el contenido firmado puede no aparecer dentro de esta estructura de datos, sino almacenarse en otro lugar: si el contenido está incorporado dentro del contenedor de firma, se habla de "firma envolvente" –porque la firma es como una especie de "sobre" que contiene al propio contenido firmado –, mientras que en el caso contrario, se habla de "firma independiente" o "separada" del contenido, y en este caso, el contenido firmado está formado por uno o varios[1498] ficheros informáticos, y la firma digital, otro fichero informático diferente[1499].

  Normalmente son las especificaciones técnicas de los protocolos y las aplicaciones las que van a concretar esta cuestión, como por ejemplo en el caso del correo electrónico seguro S/MIME antes presentado, o en el caso de la firma digital de documentos en formato PDF[1500].
- Opcionalmente[1501], uno o varios certificados digitales útiles para la verificación de la clave pública del firmante (campo `certificates`), incluyendo el certificado de firmante, o los certificados de las autoridades de certificación que

---

[1495] Incluyendo IETF RFC 2634:1999, actualizada por RFC 5035:2007.

[1496] Otras informaciones que se incluyen son un número de versión de la sintaxis, que se emplea para la verificación técnica del objeto digital, y diferenciarlo de otras definiciones anteriores; y uno o varios identificadores de algoritmos de resumen, que se emplean para la generación de la firma digital por el firmante.

[1497] La especificación técnica permite también la generación de una firma sin que aparezca ningún firmante, pero se considera un caso degenerado, que sólo se emplea para empaquetar datos.

[1498] Cfr. (Housley, 2005) para un mecanismo que permite generar una única firma digital que se refiere a diversos ficheros diferentes.

[1499] Esto no implica que después no se pueda "incrustar" o "envolver" el fichero de firma dentro de otro fichero. Por ejemplo, en la firma de documentos PDF, la firma digital es un fichero independiente del contenido firmado, pero una vez generada, la misma se incrusta dentro del propio PDF porque resulta conveniente para su transmisión conjunta a terceros, para su validación, etc.

[1500] Cfr. la norma internacional ISO 32000-1:2008.

[1501] En este punto, la RFC es muy laxa, precisamente para facilitar diversas opciones de implementación, en función de las necesidades. En efecto, en algunos escenarios de aplicación se puede asumir que los certificados necesarios se podrán ir a obtener a un depósito público de Internet, por ejemplo, en lugar de incluirlos en la firma, para reducir su tamaño.

conforman la infraestructura de clave pública.

- Opcionalmente[1502], información de revocación de certificados, referida a los certificados empleados por el firmante, o por las autoridades que han intervenido (campo `crls`). Esta información puede ser una lista de revocación de certificados o bien una respuesta de estado de certificado[1503] expedida *ad hoc*.

Respecto al campo de información del firmante (`SignerInfo`), en el mismo podemos encontrar los siguientes contenidos[1504]:

- La identificación del firmante (campo `sid`), que esencialmente se realiza a través de su certificado digital[1505].
- El algoritmo de resumen empleado por el firmante para generar la firma digital (campo `digestAlgorithm`) como, por ejemplo, SHA-256.
- Opcionalmente, uno o varios atributos firmados (campo `signedAttrs`); esto es, sobre los que se calcula el resumen criptográfico para generar la firma digital. Al menos deben existir tres[1506] atributos firmados:
    - Un atributo (`content-type`) que describe el tipo de contenido que se firma[1507].
    - Un atributo (`message-digest`) que contiene el resumen criptográfico del contenido, que de esta forma queda indirectamente protegido por la firma digital[1508].
    - Un atributo que contiene un conjunto de metadatos del certificado digital correspondiente a la clave privada empleada para crear la firma (`signingCertificate` o `signingCertificateV2`)[1509], que tiene como objetivo principal el de prevenir ataques de sustitución y re-emisión del certificado; incluyendo la identificación del certificado y su resumen criptográfico[1510].

[1502] De nuevo en este caso la RFC es muy laxa, lo cual permite que ulteriores especificaciones técnica concreten las necesidades.

[1503] Siguiendo el protocolo OCSP que hemos visto anteriormente.

[1504] Otras informaciones que se incluyen son un número de versión de la sintaxis, que se emplea para la verificación técnica del objeto digital, y diferenciarlo de otras definiciones anteriores.

[1505] Éste se puede identificar mediante dos mecanismos alternativos: mediante el nombre de la autoridad de certificación que ha emitido el certificado y el número de serie del certificado en cuestión, o mediante la identificación de la clave del firmante (que puede ser el resumen criptográfico de la clave pública, por ejemplo).

[1506] Los dos primeros se encuentran definidos en CMS.

[1507] Excepto cuando se generan contrafirmas, en cuyo caso este atributo no debe aparecer.

[1508] Cuando un objeto de firma en CMS incorpora atributos, la firma digital se produce a partir del resumen criptográfico de los atributos, por lo que es preciso, antes de generar este resumen, incorporar el resumen criptográfico del contenido a firmas; es decir, que se firma el resumen del resumen del contenido.

[1509] Definido en (Hoffman, 1999) y complementado en (Schaad, 2007).

[1510] De esta forma, el certificado se "incorpora por referencia" en la firma y ya no puede ser sustituido por

La especificación CMS define también un atributo que incorpora el momento temporal en que supuestamente se ha creado la firma electrónica (`signing-time`), y que es una alegación realizada por el firmante, en la que se podrá – o no – confiar, en función del caso[1511].

- El algoritmo de firma digital empleado por el firmante para generar la misma (campo `digestAlgorithm`) como, por ejemplo, RSA.
- El valor numérico correspondiente a la operación de creación de la firma digital (campo `signature`).
- Opcionalmente, uno o varios atributos no firmados (campo `unsignedAttrs`); esto es, sobre los que se no calcula el resumen criptográfico para generar la firma digital, por lo que las informaciones que se incorporen serán, en su caso, falsificables, siempre que las mismas no hayan sido firmadas de forma previa[1512].

  CMS define únicamente un atributo para contrafirmar una firma anterior, permitiendo de esta forma la posibilidad de crear series de firmas, donde cada firmante protege con su firma las firmas anteriores[1513].

La idea a retener es que otras especificaciones técnicas pueden, si lo consideran oportuno, definir atributos adicionales, firmados o no firmados, en función de las necesidades correspondientes, por lo que podemos apreciar una importante diversidad de tipos técnicos de firma digital autorregulada.

Lo anteriormente expuesto es buena muestra del tipo de artefacto técnico en que consiste una fuente de prueba de las empleadas para la acreditación del consentimiento, y que ciertamente es diferente del trazo sobre el papel al que sustituye.

ANEXO C. EL CONTENIDO TÉCNICO DE LA LISTA DE CONFIANZA

En este anexo presentamos, con mayor detalle, los contenidos exactos de la Lista de Confianza (TL), que viene determinado, como se ha presentado anteriormente[1514], por el vocabulario XML descrito en ETSI TS 119 612, sección 5, con las modificaciones impuestas en la Decisión de listas de confianza eIDAS.

La TL tiene diversas secciones, al objeto de ordenar las diferentes informaciones. Una primera sección (campo `SchemeInformation`) se dedica a la información del sistema

---

un certificado falso, o ser reemitido de forma fraudulenta.

[1511] Desde una óptica pericial, esta fecha podrá ser más o menos fiable en función, por ejemplo, del contexto en el que se haya generado la firma digital. Si el ordenador en el que se ha generado la firma dispone de medidas de seguridad que impiden al firmante modificar la fecha del ordenador, se podrá confiar más en esta fecha que en caso contrario.

[1512] Por ejemplo, en el caso de un sello de tiempo hemos visto puede estar firmado por la autoridad que lo expide, y, por tanto, ser infalsificable.

[1513] La semántica legal de esta actuación podrá variar en función del caso, pero frecuentemente se considerará que cada firmante ha ratificado la firma de los anteriores intervinientes. Pericialmente, al menos queda acreditado que el firmante conocía la existencia de las firmas anteriores, algo que puede ser jurídicamente relevante.

[1514] Cfr. el epígrafe 7.1.4.1 de este trabajo.

al que pertenece y que regula la lista, mientras que una segunda sección (campo `TrustServiceProviderList`) se dedica a la información de los diferentes prestadores de servicios de confianza incluidos en la lista; finalmente, la última sección corresponde a la firma electrónica o sello electrónico avanzado (en formato XML Digital Signature) de las anteriores informaciones (campo `ds:Signature`).

C.1 La información sobre el sistema rector de la TL

Por lo que se refiere al sistema que regula la lista de confianza, se contiene la siguiente información:

- El identificador de versión de la TL (campo `TSLVersionIdentifier`, obligatorio), a los efectos de determinar el vocabulario para interpretar la lista, y que actualmente es la versión 5. Se trata de un valor que se incrementa para cada nueva versión del vocabulario que afecte al número o significado de los campos.
- El número de secuencia de la TL (campo `TSLSequenceNumber`, obligatorio), que empieza en 1 y se va incrementando para cada nueva TL emitida, de forma que se puedan serializar.
- El tipo de TL (campo `TSLType`, obligatorio), que se emplea para diferenciar las diferentes tipologías de listas de confianza que pueden existir, dado que la especificación técnica no se encuentra limitada a las listas de confianza que se puedan emitir al amparo del Reglamento eIDAS, sino que tiene vocación global y, de hecho, se ha adoptado en otros Estados, que no pertenecen a la Unión Europea como, por ejemplo, Perú[1515]. Para indicar que una TL se emite conforme al Reglamento eIDAS, en este campo se debe necesariamente incluir el valor "http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric".
- El nombre y dirección postal y electrónica del operador del sistema (campos `SchemeOperatorName` y `SchemeOperatorAddress`, obligatorios y multilingües), que será el del organismo nacional encargado de las operaciones relativas a la lista de confianza. El Reglamento eIDAS no impone restricción organizativa alguna en cuanto a qué entidad deba ser el operador del sistema, pudiendo ser el organismo de supervisión u otra entidad, pero sí que aclara que, en caso de ser diferentes, el organismo de supervisión deberá informar de la concesión o retirada de la cualificación al operador del sistema, a fin de que el mismo proceda a la actualización de la lista de confianza (artículo 22.2, tercer párrafo, del Reglamento eIDAS), dentro del plazo de tres meses desde la notificación realizada por el prestador, que ya sabemos resulta ampliable por otros tres meses.
- El nombre del sistema rector de la TL (campo `SchemeName`, obligatorio y multilingüe), que contiene el identificador del Estado miembro del operador del sistema, y el siguiente texto en inglés – por mandato del Capítulo II del Anexo I de la Decisión de listas de confianza eIDAS –: "`Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together`

[1515] Cfr. https://www.indecopi.gob.pe/web/firmas-digitales/lista-de-servicios-de-confianza-trusted-services-list-tsl-.

with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", al objeto de que cualquier usuario de la lista entienda su objeto[1516].

- Un listado de direcciones electrónicas con información sobre el sistema rector de la TL (campo SchemeInformationURI, obligatorio y multilingüe), en forma de URLs de Internet en la que se deben publicar determinados contenidos mínimos, que faciliten a los terceros usuarios de la TL una información suficiente acerca de la TL. Conforme al Capítulo II del Anexo I de la Decisión de listas de confianza eIDAS, debe incluirse un texto predeterminado por la propia Decisión, y determinadas informaciones adicionales.

  El texto predeterminado, que debe constar en inglés, es el siguiente: "The present list is the trusted list including information related to the qualified trust service providers which are supervised by (name of the relevant Member State), together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

  The cross-border use of electronic signatures has been facilitated through Commission Decision 2009/767/EC of 16 October 2009 which has set the obligation for Member States to establish, maintain and publish trusted lists with information related to certification service providers issuing qualified certificates to the public in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and which are supervised/accredited by the Member States. The present trusted list is the continuation of the trusted list established with Decision 2009/767/EC"[1517].

[1516] Se puede, opcionalmente, incluir la traducción en lengua nacional del texto, que en el caso español, es "Lista de confianza que incluye información relacionada con los proveedores de servicios de confianza cualificados que supervisa el Estado miembro de expedición, junto con información relacionada con los servicios de confianza cualificados que estos prestan, de conformidad con las disposiciones pertinentes establecidas en el Reglamento n.o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE".

[1517] Se puede, opcionalmente, incluir la traducción en lengua nacional del texto, que en el caso español, es el siguiente: "La presente lista es la lista de confianza que incluye información relacionada con los proveedores de servicios de confianza cualificados supervisados por [nombre del Estado miembro pertinente], junto con información relacionada con los servicios de confianza cualificados que estos prestan, de conformidad con las disposiciones pertinentes establecidas en el Reglamento (UE) n.o 910/2014 del

Por otra parte, se deberá incluir "información específica sobre el sistema de supervisión subyacente y, en su caso, los sistemas de aprobación (por ejemplo, acreditación) nacionales aplicables, en particular:

1) información sobre el sistema de supervisión nacional aplicable a proveedores de servicios de confianza cualificados y no cualificados y a los servicios de confianza cualificados y no cualificados que estos presten, según lo regula el Reglamento (UE) no 910/2014;

2) información, en su caso, sobre los sistemas de acreditación voluntaria nacionales aplicables a proveedores de servicios de certificación que han expedido certificados cualificados de conformidad con la Directiva 1999/93/CE".

Además, también conforme a la Decisión, "esta información específica incluirá, como mínimo, para cada sistema subyacente enumerado:

1) una descripción general;

2) información sobre el proceso seguido para el sistema de supervisión nacional y, en su caso, para la aprobación en el marco de un sistema de aprobación nacional;

3) información sobre los criterios que se siguen para supervisar o, en su caso, aprobar a los proveedores de servicios de confianza;

4) información sobre los criterios y normas que se utilizan para seleccionar los supervisores y auditores y definir cómo se evalúa a los proveedores de servicios de confianza y los servicios de confianza que estos prestan;

5) en su caso, otra información de contacto y general aplicable al funcionamiento del sistema".

- Un indicativo del enfoque de determinación del estado de los servicios de confianza (campo `StatusDeterminationApproach`, obligatorio), que se emplea para indicar que los servicios indicados en la lista tienen un estado concreto (de validez) determinado por el operador del sistema de lista de confianza mediante un sistema apropiado para un ámbito regulatorio concreto. Para indicar

---

Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

El uso transfronterizo de firmas electrónicas ha sido facilitado en virtud de la Decisión 2009/767/CE de la Comisión, de 16 de octubre de 2009, que estipula la obligación de los Estados miembros de establecer, mantener y publicar listas de confianza que incluyan información referida a los proveedores de servicios de certificación que expiden certificados cualificados al público de conformidad con la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, y que estén supervisados y acreditados por los Estados miembros. La presente lista de confianza es la continuación de la lista de confianza establecida por la Decisión 2009/767/CE".

que el enfoque emplear para determina que el estado de los servicios de confianza resulta apropiado en relación con el marco regulatorio del Reglamento eIDAS, en este campo se debe necesariamente incluir el valor "http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate".

- Un listado de direcciones electrónicas con información detallada sobre las reglas aplicables al sistema rector de la TL (campo `SchemeTypeCommunityRules`, obligatorio y multilingüe), en forma de URLs de Internet en la que se deben publicar determinados contenidos mínimos, que faciliten a los terceros usuarios de la TL una información más amplia acerca del régimen jurídico aplicable a la TL[1518]. En concreto, se debe informar acerca de las reglas y políticas específicas conforme a las que se aprueban y supervisan los servicios de confianza, a partir de las cuales se puede determinar el sistema o la comunidad (de usuarios); asimismo, se debe describir cómo emplear e interpretar el contenido de la lista de confianza.

  En este caso, la Decisión de listas de confianza eIDAS impone la incorporación obligatoria de dos direcciones, al menos en inglés, al objeto de informar acerca de las reglas comunes aplicables a cualquier TL, así como de las reglas específicas que pueda establecer cada Estado miembro[1519].

  La información general es idéntica para todos los Estados y se contiene en la URL "http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon". El texto se contiene en la Decisión de listas de confianza eIDAS e incluye información general sobre el Reglamento eIDAS y la cualificación, así como unas reglas interpretativas de la lista para facilitar su comprensión.

- El territorio al que resulta aplicable el sistema rector de la lista de confianza (campo `SchemeTerritory`, obligatorio).

- La política o el aviso legal de la TL (campo `PolicyOrLegalNotice`, obligatorio y multilingüe), que contiene, conforme al Capítulo II del Anexo I de la Decisión de listas de confianza eIDAS, información sobre "`la situación jurídica del sistema o los requisitos legales que cumple el sistema en virtud de la jurisdicción en el que se ha establecido y/o las restricciones y condiciones en virtud de las cuales se mantiene y publica la lista de confianza`", con el texto normalizado siguiente: "`El marco jurídico aplicable a la presente lista de confianza es el Reglamento no 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE`".

[1518] Sin embargo, de la observación de las TL actualmente publicadas por los diferentes Estados miembro, no se aprecia un uso muy consistente de ambos campos, que en la mayoría de los casos presentan la misma información, en formatos diferentes, o con pocas diferencias entre ellas.

[1519] Para ello se define una URL propia de cada Estado, que en el caso de España es "http://uri.etsi.org/TrstSvc/TrustedList/schemerules/ES/" y contiene detalle sobre el marco concreto español, con referencia a la aún vigente LFE. También informa de que no se incluyen en la lista de confianza servicios sin cualificación.

En este campo se podría también, opcionalmente, indicar otro marco jurídico nacional, algo que resultaría coherente en el caso de listas que incluyen servicios de confianza sin cualificación, o con cualificación sólo reconocida en sede nacional[1520].

- Indicación del periodo durante el que se mantendrá información histórica en la TL (campo `HistoricalInformationPeriod`, obligatorio), que por convención se establece en el entero "65535", que por la misma convención implica que dicha información se mantiene de forma permanente, al objeto, ya mencionado anteriormente, de facilitar la validación de firmas electrónicas, sellos electrónicos y otras pruebas electrónicas producidas en el pasado, con la información de la TL.
- Una o varias referencias a otras TLs relevantes (campo `PointersToOtherTSL`, obligatorio), que como mínimo debe contener una referencia (campo `OtherTSLPointer`, obligatorio) a la "lista de listas de confianza" publicada por la Comisión Europea, supuestamente para que, a partir de una lista de confianza nacional sea inmediato obtener la correspondiente "lista de listas".
- La fecha y hora de expedición de la lista (campo `ListIssueDateTime`, obligatorio), que debe resultar consistente con las fechas aplicables a las altas y bajas de los servicios objeto de publicidad, en especial en caso de cambio de estado – por ejemplo, en caso de retirada de la cualificación –, al objeto de evitar problemas de retroactividad.
- La fecha y hora prevista de expedición de la próxima TL (campo `NextUpdate`, obligatorio), que no podrá demorarse más de seis meses, y sin perjuicio de que deba expedirse una TL con anterioridad, si ello resulta preciso, normalmente por producirse cambios en la información a publicar.
- Uno o varios puntos de distribución de la TL (campo `DistributionPoints`, opcional), en forma de direcciones de Internet o URLs donde se pueda acceder al fichero con la TL, debiendo tratarse siempre de la última versión.

C.2 La información sobre el prestador de servicios, y sobre los servicios que presta

La TL contiene, dentro del campo `TrustServiceProviderList`, obligatorio siempre que existan prestadores[1521], la secuencia de todos los prestadores (campo `TrustServiceProvider`, obligatorio) de los que se ofrece información.

Por lo que se refiere a cada prestador de servicios de confianza (campo `TSPInformation`, obligatorio, contenido dentro del campo `TrustServiceProvider`), se contiene la siguiente información:

[1520] Aunque, como hemos visto, ése es el caso de la TSL danesa, no se hace uso de este campo, en una muestra del poco riguroso uso del vocabulario de la TSL que se hace actualmente.

[1521] Puede suceder que en Estado miembro no operase ningún prestador de servicios de confianza, como de hecho sucede en el caso de Chipre, si bien es el único caso.

- El nombre del prestador (campo `TSPName`, obligatorio y multilingüe), que se corresponde con la denominación formal de la persona física o jurídica, según consta en el registro correspondiente.
- El nombre comercial del prestador (campo `TSPTradeName`, obligatorio y multilingüe), que se emplea también para incluir otros nombres por los que se conoce al prestador, incluyendo obligatoriamente un número de identificación unívoco, como el número de identificación fiscal.
- La dirección postal y electrónica del prestador (campo `TSPAddress`, obligatorio y multilingüe), debiendo corresponder a las direcciones donde se ofrece atención al cliente.
- Un listado de direcciones electrónicas con información sobre el prestador (campo `TSPInformationURI`, obligatorio y multilingüe), en forma de URLs de Internet en la que se deben publicar las últimas versiones de las prácticas y/o políticas, los términos y condiciones, y otras informaciones genéricas acerca del prestador y los servicios que presta.

Por lo que se refiere a cada servicio de un prestador (campo `TSPServices`, obligatorio, contenido dentro del campo `TrustServiceProvider`, que a su vez contiene un campo `TSPService`, obligatorio, con la información para cada servicio), se ofrece la siguiente información[1522]:

- El identificador de tipo de servicio de confianza (campo `ServiceTypeIdentifier`, obligatorio), que se expresa mediante una URI predefinida en ETSI TS 119 612[1523], diferenciándose entre los siguientes tipos de servicio:
    - Servicios cualificados de confianza previstos en el Reglamento eIDAS. Las posibilidades previstas con las siguientes:
        - http://uri.etsi.org/TrstSvc/Svctype/CA/QC, que se refiere a un servicio de expedición de certificados cualificados (de firma electrónica, de sello electrónico o de autenticación de sitio web), incluyendo, en su caso, la generación y gestión de datos de creación de firma electrónica o sello electrónico.

          Conforme a las reglas de interpretación de la TL del Capítulo II del Anexo I de la Decisión de listas de confianza, cuando se indica este tipo de servicio, hay que entender que todos los certificados expedidos por la autoridad de certificación indicada, o por cualquier otra autoridad de certificación subordinada a la misma, es cualificado si el mismo contiene la declaración `id-etsi-qcs-`

[1522] La información de un servicio concreto está formada por una serie de campos que se pueden incluir en el campo ServiceInformation, cuando se trata de la última versión de la información, que se corresponde con el servicio actual, o en el campo ServiceHistoryInstance, cuando se trata de información de la versión anterior de un servicio. Todas las ServiceHistoryInstance se almacenan dentro del campo ServiceHistory. Los campos son los mismos, por lo que los presentamos de forma conjunta, por razones de espacio.

[1523] Se pueden – si es preciso – registrar otros identificadores en el ETSI, aunque no se podrán emplear para indicar servicios de confianza con cualificación, dado el modelo de lista cerrada al que ya nos hemos referido con anterioridad.

`QcCompliance`, o el OID de política 0.4.0.1456.1.1 o el OID de política 0.4.0.1456.1.2, aunque también es posible entender que un certificado que no contenga ninguna de estas informaciones es cualificado si la lista lo indica de forma expresa empleando el campo `Qualifications` contenido dentro del campo `ServiceInformationExtensions`, al que posteriormente nos referiremos.

- http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC, que se refiere a un servicio de información de validez de certificados basado en el protocolo OCSP, vinculado al servicio de expedición de certificados cualificados. Este servicio sólo se registra en la TL cuando la clave pública empleada para firmar las respuestas OCSP no ha sido certificada por la autoridad de certificación emisora de los certificados para los que se ofrece información.
- http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC, que se refiere a un servicio de información de validez de certificados basado en listas de revocación de certificados (CRLs), vinculado al servicio de expedición de certificados cualificados. Este servicio sólo se registra en la TL cuando la clave pública empleada para firmar las CRLs no ha sido certificada por la autoridad de certificación emisora de los certificados para los que se ofrece información.
- http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST, que se refiere al servicio cualificado de expedición de sellos de tiempo electrónico.
- http://uri.etsi.org/TrstSvc/Svctype/EDS/Q, que se refiere al servicio cualificado de entrega electrónica certificada.
- http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q, que se refiere al servicio cualificado de entrega electrónica certificada basado en correo electrónico (REM).
- http://uri.etsi.org/TrstSvc/Svctype/PSES/Q, que se refiere al servicio cualificado de conservación de firma electrónica o de sello electrónico.
- http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q, que se refiere al servicio cualificado de validación de firma electrónica o de sello electrónico.

Como ya se ha indicado anteriormente, sólo es posible dar publicidad a estos tipos de servicios, que se corresponden de forma exacta con los servicios cualificados previstos en el Reglamento eIDAS, sin perjuicio de la posibilidad de desglosar aspectos concretos del servicio de expedición de certificados cualificados, al poder resultar necesario producir entradas diferenciadas en función del modelo de confianza del prestador.

Por este motivo, la solicitud de cualificación es, como se recordará[1524], particularmente rígida en cuando al tipo de servicio para el que se solicita la citada cualificación.

- Servicios de confianza sin cualificación previstos en el Reglamento eIDAS. Las posibilidades previstas son las siguientes:
  - http://uri.etsi.org/TrstSvc/Svctype/CA/PKC, que se refiere a un servicio de expedición de certificados no cualificados (de firma electrónica, de sello electrónico o de autenticación de sitio web).
  - http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP, que se refiere a un servicio de información de validez de certificados basado en el protocolo OCSP, vinculado al servicio de expedición de certificados no cualificados. Este servicio sólo se registra en la TSL cuando la clave pública empleada para firmar las respuestas OCSP no ha sido certificada por la autoridad de certificación emisora de los certificados para los que se ofrece información.
  - http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL, que se refiere a un servicio de información de validez de certificados basado en listas de revocación de certificados (CRLs), vinculado al servicio de expedición de certificados no cualificados. Este servicio sólo se registra en la TL cuando la clave pública empleada para firmar las CRLs no ha sido certificada por la autoridad de certificación emisora de los certificados para los que se ofrece información.
  - http://uri.etsi.org/TrstSvc/Svctype/TSA, que se refiere al servicio no cualificado de expedición de sellos de tiempo electrónico.
  - http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-QC, que se refiere al servicio no cualificado de expedición de sellos de tiempo electrónico, ofrecido por un prestador que expide certificados cualificados para la validación y extensión del plazo de validez de una firma electrónica o de un sello electrónico.
  - http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-AdESQCandQES, que se refiere al servicio no cualificado de expedición de sellos de tiempo electrónico, ofrecido por un prestador de sellos de tiempo para la validación y extensión del plazo de validez de una firma electrónica o de un sello electrónico.
  - http://uri.etsi.org/TrstSvc/Svctype/EDS, que se refiere al servicio no cualificado de entrega electrónica certificada.
  - http://uri.etsi.org/TrstSvc/Svctype/EDS/REM, que se refiere al servicio no cualificado de entrega electrónica certificada basado en correo electrónico (REM).
  - http://uri.etsi.org/TrstSvc/Svctype/PSES, que se refiere al servicio no cualificado de conservación de firma electrónica o de sello electrónico.

[1524] Cfr. el epígrafe 7.1.2.1 de este trabajo.

- http://uri.etsi.org/TrstSvc/Svctype/AdESValidation, que se refiere al servicio no cualificado de validación de firma electrónica o de sello electrónico.
- http://uri.etsi.org/TrstSvc/Svctype/AdESGeneration, que se refiere al servicio no cualificado de creación de firma electrónica o de sello electrónico a distancia.

Como se puede ver, en este caso nos encontramos ante un listado mayor, del que destaca significativamente la existencia del servicio de creación de la firma electrónica avanzada o del sello electrónico avanzado a distancia, que es un servicio de confianza que no se puede considerar cualificado[1525].

- Servicios de confianza previstos en sede nacional, por Estados no miembro de la Unión o por organizaciones internacionales, entre los que actualmente se incluye el servicio de autoridad de registro[1526], el servicio de autoridad de certificación de atributos[1527], el servicio de autoridad de políticas de firma[1528], el servicio de archivo[1529], el servicio de verificación de identidad[1530], el servicio de depósito de claves[1531], el servicio de emisión de credenciales basadas en número de identidad personal o

[1525] Cfr. el epígrafe 1.3.1 de este trabajo.

[1526] Identificado por las URIs http://uri.etsi.org/TrstSvc/Svctype/RA y http://uri.etsi.org/TrstSvc/Svctype/RA/nothavingPKIid, en función de si se basa en claves certificadas o no. En el Reglamento eIDAS las funciones de la autoridad de registro no se configuran como un servicio de confianza independiente de servicio de expedición de certificado, sino que quedan absorbidas dentro del mismo.

[1527] Identificado por la URI http://uri.etsi.org/TrstSvc/Svctype/ACA. Se trata de un servicio que expide certificados que sólo contienen atributos, y que se refieren a la clave pública contenida en un certificado, cualificado o no.

[1528] Identificado por la URI http://uri.etsi.org/TrstSvc/Svctype/SignaturePolicyAuthority. Se trata de un servicio que expide publica y mantiene políticas de firma electrónica. Sobre el tratamiento de las políticas de firma en el sector público español, cfr. (Alamillo Domingo, 2012).

[1529] Identificado por las URIs http://uri.etsi.org/TrstSvc/Svctype/Archiv y http://uri.etsi.org/TrstSvc/Svctype/Archiv/nothavingPKIid, en función de si se basa en claves certificadas o no, que cabe suponer – porque ETSI TS 119 612 nada dice al respecto – que se refiera al archivo electrónico de documentos, al que nos referiremos posteriormente como servicio de confianza emergente.

[1530] Identificado por las URIs http://uri.etsi.org/TrstSvc/Svctype/IdV y http://uri.etsi.org/TrstSvc/Svctype/IdV/nothavingPKIid, en función de si se basa en claves certificadas o no.

[1531] Identificados por las URIs http://uri.etsi.org/TrstSvc/Svctype/KEscrow y http://uri.etsi.org/TrstSvc/Svctype/KEscrow/nothavingPKIid, en función de si se basa en claves certificadas o no.

contraseña[1532], el servicio de expedición de listas de confianza[1533], o de autoridad de certificación raíz nacional[1534].

Ciertamente sorprende la variedad de servicios de confianza con reconocimiento exclusivamente nacional, algo sobre lo que volveremos posteriormente.

- Otros que se puedan registrar, en su caso.

- El nombre del servicio de confianza (campo `ServiceName`, obligatorio y multilingüe) correspondiente.

- El identificador digital unívoco del servicio (campo `ServiceDigitalIdentity`, obligatorio), consistente con el tipo de servicio correspondiente, que en todos los servicios cualificados se trata de un certificado de clave pública del prestador del servicio que se emplea para la validación de las pruebas electrónicas generadas, en una nueva muestra de la ausencia de neutralidad tecnológica del marco europeo regulador de los servicios de confianza; en este caso, mediante la referencia en un acto de ejecución a una especificación técnica que restringe la calificación de toda tecnología que no se base en la infraestructura de clave pública.

- El estado actual del servicio de confianza (campo `ServiceStatus`, obligatorio), indicado mediante una URI normalizada.

  En el caso de los servicios cualificados de confianza, se prevé la cualificación concedida (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted) y la cualificación retirada (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/); mientras que en el caso de los servicios no cualificados previstos en el Reglamento eIDAS y en el caso de los servicios de confianza definidos en el nivel nacional, se prevé el estado de servicio "reconocido en el nivel nacional" (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel) y el estado de servicio "retirado en el nivel nacional" (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel).

  Existen, sin embargo, otros valores que se empleaban conforme a la DFE, cuyo uso se mantiene hasta el cambio de estado del servicio de confianza, en cuyo momento se deberán ajustar a las opciones anteriormente indicadas, algo que desde luego no ayuda a la comprensión del funcionamiento del sistema, ni tampoco a facilitar el procesamiento automático de la TL.

- La fecha y hora de inicio del estado actual (campo `StatusStartingTime`, obligatorio), que en caso de cambio de estado no podrá ser anterior a la fecha y hora de expedición de la lista, como ya se indicó, para evitar problemas de retroactividad.

[1532] Identificados por las URIs http://uri.etsi.org/TrstSvc/Svctype/PPwd y http://uri.etsi.org/TrstSvc/Svctype/PPwd/nothavingPKIid, en función de si se basa en claves certificadas o no.

[1533] Identificado por la URI http://uri.etsi.org/TrstSvd/Svctype/TLIssuer.

[1534] Identificado por la URI http://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC.

- Un listado de URI con información sobre el tipo de servicio, ofrecida por el operador de la lista de confianza (campo `SchemeServiceDefinitionURI`, opcional y multilingüe). Por ejemplo, en la TSL francesa se incluye una referencia al sistema de evaluación empleado en sede nacional basado en estrellas, aunque conforme a norma se debería incluir una URL con la dirección de Internet donde se encuentra la citada información.
- Un listado de direcciones electrónicas de acceso al servicio de confianza (elemento `ServiceSupplyPoints`, opcional).
- Un listado de URI con información sobre el tipo de servicio, ofrecida por el prestador del servicio de confianza (campo `TSPServiceDefinitionURI`, opcional, excepto si el tipo de servicio se corresponde con una autoridad de certificación raíz nacional, y multilingüe).
- Una lista de extensiones de información de servicio (campo `ServiceInformationExtensions`, opcional), que contienen informaciones adicionales relativas al servicio de confianza en cuestión.
    - La primera extensión (`expiredCertsRevocationInfo`) permite indicar la fecha desde la cual el prestador incluido en la lista mantiene anuncios de revocación de certificados revocados que han expirado, lo cual es importante para realizar una validación de firma en el pasado, dado que si el certificado revocado, al llegar la fecha en que debería haber expirado, se ha retirado de la lista de revocación (CRL), o del sistema de consulta OCSP, no será posible saber que el mismo fue jamás revocado.
    - La segunda extensión (`Qualifications`) permite explicitar informaciones acerca de los certificados cualificados que no se encuentran dentro de los certificados, por lo que resulta necesario incluirlas en la lista de confianza. Dichas informaciones permiten informar acerca de si los certificados son cualificados o no[1535], de si los datos de creación de firma o sello electrónico residen en un dispositivo cualificado o no[1536], de si los

[1535] La URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement indica que todos los certificados son cualificados conforme a la DFE, mientras que la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified indica que ningún certificado es cualificado.

[1536] La URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD indica que todos los certificados se refieren a datos de creación de firma o sello que residen en dispositivo seguro, conforme a la DFE, mientras que la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD indica que ningún certificado se refiere a datos de creación de firma o sello que residan en dispositivo seguro, conforme a la DFE; la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert indica que la información acerca de si los datos de creación de firma o sello residen en dispositivo seguro, conforme a la DFE, o no, se contiene en el correspondiente certificado; de manera análoga, la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD indica que todos los certificados se refieren a datos de creación de firma o sello que residen en dispositivo cualificado, mientras que la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD indica que ningún certificado se refiere a datos de creación de firma o sello que residan en dispositivo cualificado; la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert indica que la información acerca de si los datos de creación de firma o sello residen en dispositivo cualificado, o no, se contiene en el correspondiente certificado; finalmente, y sólo en relación con los dispositivos cualificados (no los seguros), la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf indica

certificados han sido expedidos a una persona jurídica[1537], y de si los certificados son de firma electrónica, de sello electrónico o de autenticación de sitio web[1538].

Dado que un prestador puede emplear una única autoridad de certificación para expedir diversos tipos de certificados, el vocabulario de la lista de confianza permite concretar a qué subconjunto de certificados se refiere esta información[1539].

- La tercera extensión (`TakenOverBy`) permite indicar qué prestador se ha hecho cargo de los servicios de un prestador ha cesado en su actividad.
- La cuarta extensión (`additionalServiceInformation`) permite indicar información adicional del servicio listado, mediante una URI y, opcionalmente, un texto que especifica más la clasificación del servicio, conforme al derecho nacional[1540], y, también opcionalmente, cualquier otra información adicional que considere oportuno incluir el operador de la lista de confianza.

  Todas las TL emplean esta extensión, a pesar de que la misma no resulta impuesta ni por la especificación técnica ni por la Decisión de listas de confianza eIDAS, para informar acerca del tipo de servicio del prestador[1541], o para cualificar adicionalmente la información acerca del tipo de servicio[1542].

Finalmente, se incluye la información histórica del servicio de confianza, empleando los mismos campos, información que resulta de extraordinario valor para las validaciones de pruebas electrónicas de versiones pasadas del mismo servicio, como por ejemplo en el caso de certificados emitidos conforme a versiones anteriores del servicio.

---

indica que todos los certificados se refieren a datos de creación de firma o sello que residen en dispositivo cualificado en el cual se ha generado y gestionado los datos de creación de firma o sello por cuenta de la persona identificada en el certificado.

[1537] Mediante el uso de la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForLegalPerson.

[1538] Mediante el uso de la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig, en el caso del certificado de firma electrónica; de la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal, en el caso del certificado de sello electrónico; o, por último, en el caso del certificado de autenticación de sitio web, de la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA.

[1539] Para ello se establecen filtros por política de certificado, por uso de claves o por otros criterios (uso extendido de claves, o atributos del nombre de la entidad identificada en el certificada).

[1540] Sin embargo, esta información sería redundante con la contenida en el campo SchemeServiceDefinitionURI, al que nos hemos referencia anteriormente, por lo que en la práctica no se emplea.

[1541] La URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures se emplea para indicar que el tipo de servicio (expedición de certificados, validación o conservación) es para la firma electrónica; mientas que la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals se emplea cuando el tipo de servicio se refiere a un sello electrónico. Para indicar la expedición de certificados de autenticación de sitio web, se emplea la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication, dado que en este caso no hay otros tipos de servicio que puedan resultar aplicables.

[1542] Para indicar que una autoridad de certificación es una autoridad de certificación raíz, se emplea la URI http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC.