



**UNIVERSIDAD DE MURCIA**  
**ESCUELA INTERNACIONAL DE DOCTORADO**

**TESIS DOCTORAL**

**The eIDAS2 Regulation: the European Union's Strategic  
Vision to Regulate a Digital Identity Metasystem under  
Citizens' Control as a Public Service**

**El Reglamento eIDAS2: la Visión Estratégica de la  
Unión Europea para Regular un Metasistema de  
Identidad Digital bajo el Control del Ciudadano como  
Servicio Público**

**Autora: Dña. María Cristina Timón López**

**2024**





**UNIVERSIDAD DE MURCIA**  
**ESCUELA INTERNACIONAL DE DOCTORADO**

**TESIS DOCTORAL**

**The eIDAS2 Regulation: the European Union's Strategic  
Vision to Regulate a Digital Identity Metasystem under  
Citizens' Control as a Public Service**

**El Reglamento eIDAS2: la Visión Estratégica de la  
Unión Europea para Regular un Metasistema de  
Identidad Digital bajo el Control del Ciudadano como  
Servicio Público**

**Autora: Dña. María Cristina Timón López**

Directores: Dr. Ignacio Alamillo Domingo y  
Prof. Dr. Julián Valero Torrijos





**DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD  
DE LA TESIS PRESENTADA PARA OBTENER EL TÍTULO DE DOCTOR**

*Aprobado por la Comisión General de Doctorado el 19-10-2022*

D./Dña. María Cristina Timón López

doctorando del Programa de Doctorado en

Derecho

de la Escuela Internacional de Doctorado de la Universidad Murcia, como autor/a de la tesis presentada para la obtención del título de Doctor y titulada:

The eIDAS2 Regulation: the European Union's Strategic Vision to Regulate a Digital Identity Metasystem under Citizens' Control as a Public Service

y dirigida por,

D./Dña. Ignacio Alamillo Domingo

D./Dña. Julián Valero Torrijos

D./Dña.

**DECLARO QUE:**

La tesis es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, de acuerdo con el ordenamiento jurídico vigente, en particular, la Ley de Propiedad Intelectual (R.D. legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, modificado por la Ley 2/2019, de 1 de marzo, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), en particular, las disposiciones referidas al derecho de cita, cuando se han utilizado sus resultados o publicaciones.

*Si la tesis hubiera sido autorizada como tesis por compendio de publicaciones o incluyese 1 o 2 publicaciones (como prevé el artículo 29.8 del reglamento), declarar que cuenta con:*

- La aceptación por escrito de los coautores de las publicaciones de que el doctorando las presente como parte de la tesis.*
- En su caso, la renuncia por escrito de los coautores no doctores de dichos trabajos a presentarlos como parte de otras tesis doctorales en la Universidad de Murcia o en cualquier otra universidad.*

Del mismo modo, asumo ante la Universidad cualquier responsabilidad que pudiera derivarse de la autoría o falta de originalidad del contenido de la tesis presentada, en caso de plagio, de conformidad con el ordenamiento jurídico vigente.

En Murcia, a 22 de abril de 2024

Fdo.: *Cristina Timón López*

*Esta DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD debe ser insertada en la primera página de la tesis presentada para la obtención del título de Doctor.*

Información básica sobre protección de sus datos personales aportados	
Responsable:	Universidad de Murcia. Avenida teniente Flomesta, 5. Edificio de la Convalecencia. 30003; Murcia. Delegado de Protección de Datos: dpd@um.es
Legitimación:	La Universidad de Murcia se encuentra legitimada para el tratamiento de sus datos por ser necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. art. 6.1.c) del Reglamento General de Protección de Datos
Finalidad:	Gestionar su declaración de autoría y originalidad
Destinatarios:	No se prevén comunicaciones de datos
Derechos:	Los interesados pueden ejercer sus derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento, olvido y portabilidad a través del procedimiento establecido a tal efecto en el Registro Electrónico o mediante la presentación de la correspondiente solicitud en las Oficinas de Asistencia en Materia de Registro de la Universidad de Murcia



*To those who dare to challenge the status quo*





## *Abstract*

Identity, in digital format now, emerges as the cornerstone for a society undergoing a profound technological transformation. However, to date, there is no harmonized form of digital identity, but its provision is assumed by very different providers relying on a limited or insufficient form of regulation. In an environment of regulatory insufficiency, digital identity ecosystems have evolved into models which raise critical challenges that existing regulations cannot effectively address. In particular, privacy and security are threatened in existing digital identity models, and essential processes have been monopolized by a reduced number of providers. The main drawback, however, is that citizens lack control and assurance over their digital existence.

Digital identity is governed in the European Union by the eIDAS Regulation, a multifaceted regulation with a dual legal regime covering electronic identification and trust services. Yet, the first version has been essentially limited to public services beyond other constraints in the digital identity model created that demanded its adaptation. However, identification is a national matter, and therefore, the eIDAS Regulation offers broad implementation possibilities leading to different results. While some countries have opted for a public approach, others have already authorized the participation of private providers, offering lessons that are particularly valuable today with the adoption of eIDAS2. The updated Regulation aims to transform the digital identity ecosystem, paving the way for a model where the role of the identity provider is assumed by different entities, and the user is placed at the center of the ecosystem. At the heart of this Regulation is the European Union Digital Identity Wallet, an innovative form of electronic identification means that also aims to unlock the potential of an ecosystem of identity credentials.

The arrival of eIDAS2 marks a key milestone in the digital identity sector, introducing a new form of harmonized digital identity at the European Union level, where Member States are bound to play a guarantor role in its provision. Consequently, independently of the entity that ultimately provides the service, it must do so subject to public service guarantees and obligations. It is suggested in this thesis that the configuration of the

Wallet as a public service and its associated legal effects may have repercussions in applicable national law. In the case of Spanish Administrative Law, it could entail the exercise of administrative power, which in turn demands compliance with the requirements for their attribution and exercise. Nevertheless, the provision of the Wallet is only the first step in the new ecosystem; for it to function properly, it is also necessary to define a statute of rights, obligations, and guarantees for its core participants.

Ultimately, this thesis aims to question the development that the digital identity layer of the Internet has experienced so far, as a domain predominantly in the hands of the private sector and with timid attempts by the public sector to regulate it. The ability to establish our existence in the digital realm is crucial for exercising our rights and participating effectively in society. Recent events, combined with the loss of sovereignty by the State, have significantly called for a change in the state of affairs in digital identity services, where the digital identity layer, at least for natural persons, must be a public service. However, while recognizing that the role of the State and Public Law will be crucial, it must be acknowledged that the digital sphere is something new and different and will play by different rules than in the past and that while upholding the rule of law is important, it is equally important not to rush to fit new ideas into old frameworks.

## *Abstract*<sup>1</sup>

En una sociedad cada día más digitalizada, en la que la práctica totalidad de actividades se desarrollan en formato electrónico, la identidad digital se erige como un elemento esencial. La identidad digital, no obstante, es un concepto complejo. De entrada, esta puede referirse a las personas físicas, las personas jurídicas o incluso a entidades no vivientes. Por otra parte, esta puede tener muy distintas acepciones dependiendo de la disciplina desde la que se observe. Esta tesis ofrece una breve introducción conceptual que busca facilitar al lector la comprensión de su objeto de estudio; no obstante, la investigación se centra específicamente en la identidad de las personas físicas, tomando como punto de partida la superación de un concepto de identidad digital limitado a los datos de identificación de la persona, para adoptar un concepto más amplio, en el que se incluyen todos los atributos vinculados de algún modo a la identidad de la persona. Además, esta introducción pretende mostrar al lector que, a pesar de las similitudes con la identidad en formato físico, la identidad digital tiene una serie de notas o características únicas, siendo especialmente destacable la complejidad que adquiere el proceso de autenticación en escenarios remotos. Asimismo, con el propósito de facilitar la comprensión de las secciones subsiguientes y la evolución de los modelos de identidad digital, se describen los diferentes roles o participantes en los ecosistemas de identidad digital. Estos incluyen una variedad de roles específicos, entre los cuales tres son particularmente significativos: el proveedor de identidad, el proveedor del servicio o parte usuaria, y el usuario final. En la práctica, estos roles pueden englobar una gama de funciones que pueden ser asumidas por una misma entidad o por entidades distintas.

Tras haber establecido los conceptos fundamentales para la comprensión de este ámbito, resulta esencial reconocer que, a diferencia de las ciencias exactas, en materia de identidad digital no existe una perspectiva o enfoque único. Para finalizar la introducción de esta tesis, se plantean los distintos enfoques en materia de políticas de identidad digital. Mientras que algunos Estados han optado por modelos fuertemente publicados, otros abren la puerta a la participación del sector privado o incluso delegan

---

<sup>1</sup> This summary in Spanish has been prepared pursuing the requirements established in Article 27.5 of the *Reglamento por el que se regulan las enseñanzas oficiales de doctorado en la Universidad de Murcia*.

los servicios de identificación y autenticación electrónica completamente a este. La existencia de distintos modelos muestra, de una parte, la complejidad y la novedad del tema que ha dado como resultado aproximaciones distintas a necesidades emergentes, en forma de respuestas fuertemente basadas en las costumbres y tradiciones de cada Estado. Por otra parte, las distintas aproximaciones evidencian la necesidad creciente de una mayor armonización y tendrán ahora un impacto en la forma en la que se aproxime el proceso de transformación. Concretamente, esta tesis se ha elaborado en un momento de transición, donde, aunque las reformas normativas admiten la diversidad de modelos vigentes, promueven decididamente un cambio “armonizado”. Este cambio se destaca particularmente por subrayar la necesidad de establecer una capa de identidad digital con garantía pública, al menos para las personas físicas.

Para entender la importancia y la motivación de este cambio, consideraba necesario realizar un estudio de la situación actual en que se encuentra la identidad digital, un sector, que al menos desde el punto de vista jurídico, ha recibido poca atención hasta ahora. En concreto, es importante tener en cuenta que partimos de un contexto en el que la identidad digital se encuentra fuertemente fragmentada y en el que utilizamos distintos “tipos de identidades digitales”, provistas por entidades del sector público o privado, dependiendo del tipo de servicio al que se accede. De forma paralela, las regulaciones aplicables varían, apreciándose una mayor incidencia regulatoria en el ámbito de las “identidades digitales del sector público”, mientras que en el sector privado las regulaciones aplicables carecen de referencias concretas, incluso en sectores tan cruciales para la identidad digital como la privacidad y la ciberseguridad. La ausencia de disposiciones normativas explícitas, como por ejemplo en el sector de la privacidad, han resultado en que, a pesar de existir soluciones técnicas capaces de mejorar la protección de la privacidad, tales como aquellas que previenen la recolección excesiva de datos personales, estas no se implementan adecuadamente en la práctica.

Pese a este contexto caracterizado por la insuficiencia normativa, las crecientes necesidades en el ámbito de identificación electrónica han fomentado la evolución de los modelos de identidad digital. Concretamente, el aumento en el número de procesos propició la adopción predominante de un modelo de identidad digital federada. En este

modelo, una entidad distinta del proveedor de identidad asume las funciones de identificación y autenticación. A su vez, esta entidad crea una federación porque el proveedor de identidad presta estos servicios a un número normalmente elevado de proveedores de identidad. A pesar de la conveniencia de este modelo y su facilidad de uso, también plantea importantes problemas desde la perspectiva de la privacidad y de la seguridad. En especial, el ejercicio del derecho a la privacidad, siendo este un derecho primordialmente articulado entorno a la protección de intereses individuales, plantea problemas en aquellos procesos en el que el daño se produce a un interés colectivo, como sucede en las prácticas de vigilancia a gran escala. Por otra parte, a pesar de la proliferación de los casos de suplantación de identidad en los últimos años, la criminalización de estas conductas todavía se plantea desafiante debido a las propias características inherentes al Derecho Penal que requieren de un lado, una definición concreta del tipo penal y, por otro lado, la delimitación de la jurisdicción competente, en delitos que se caracterizan esencialmente por su diversidad, así como las posibilidades de perpetración desde cualquier parte del mundo. Además, la era de la digitalización ha venido marcada por el creciente poder de las plataformas digitales y los proveedores de tecnología, desafiando las nociones establecidas en materia de derecho de defensa de la competencia. El carácter novedoso de la situación, unido a la falta de alternativas y la necesidad creciente de la tecnología ha dado como resultado una aplicación prudente de las regulaciones en este sector hasta el momento.

A pesar de las limitaciones de la regulación en el área de la identidad digital, en el ámbito de la Unión Europea ha existido una normativa clave, el Reglamento eIDAS. El Reglamento eIDAS es una regulación polifacética que se caracteriza por la convergencia de dos regímenes jurídicos distintos, concretamente, un régimen dedicado a la identificación electrónica y otro centrado en la regulación de los servicios de confianza. En lo que concierne a la identificación electrónica, el principal objetivo del Reglamento es el reconocimiento transfronterizo de los sistemas de identificación electrónica notificados por los distintos Estados Miembros. No obstante, el Reglamento ha demostrado tener limitaciones, ya que únicamente impone el reconocimiento obligatorio a los servicios públicos transfronterizos. Por otra parte, la identificación electrónica ha ocupado un lugar peculiar en el marco de los servicios de confianza al no

contemplarse explícitamente en ninguno de ellos. Sin embargo, la identificación del firmante que permite los certificados de firma o sello electrónicos, especialmente aquellos cualificados, ha dado como resultado su uso en procesos de identificación y autenticación. Dicho uso, no obstante, no deja de representar un resquicio en la regulación, que no cubre las demandas actuales en esta materia. Además, al margen de las limitaciones notorias en materia de identificación electrónica, el Reglamento eIDAS mostraba importantes deficiencias en materia de privacidad e incluso de seguridad. En el primer aspecto, el modelo de federación basado en la existencia de nodos facilita la creación de “pasarelas de control”. Además, la exigencia de un conjunto mínimo de datos de identificación contraviene el principio de minimización de datos, especialmente si se tienen en cuenta las posibilidades actuales de revelación selectiva de datos. En lo que concierne al segundo punto, parece que la exigencia en todo caso de autenticación multifactorial para alcanzar al menos un nivel de seguridad substancial podría contradecir el principio de neutralidad tecnológica que exige el Reglamento, demandando una mayor flexibilidad, un movimiento ya observado en otros sectores, como en la revisión de la Segunda Directiva sobre Servicios de Pagos.

Aunque de un análisis general del Reglamento eIDAS se puede concluir que el mismo ha presentado importantes limitaciones, desde un punto de vista práctico, las distintas implementaciones por los Estados Miembros han dado resultados muy distintos. En esta tesis, se han seleccionado una serie de países en función de los sistemas de identificación electrónica notificados, clasificándolos entre aquellos Estados Miembros que han elegido utilizar medios de identificación electrónica suministrados por el sector público y aquellos que permiten la participación del sector privado. En el primer grupo, países como España y Alemania han optado por la notificación del documento nacional de identidad electrónico, los cuales, a pesar del importante desarrollo en materia de seguridad y privacidad, notablemente en el caso de Alemania, han tenido un escaso uso, en especial en el sector de los servicios privados. Por el contrario, en otros países como Estonia, a pesar de seguir esta misma línea, el documento nacional de identidad electrónico ha tenido un mayor éxito gracias a las ambiciosas políticas de digitalización del país. Finalmente, en el grupo de países con modelos fuertemente publicados, encontramos el caso particular de Francia, que opta por un modelo que emula a las

grandes plataformas, pero siendo esta infraestructura proporcionada por el propio Estado. Por otra parte, en el grupo de países que han decidido abrir la puerta a la participación del sector privado, es particularmente destacable el caso de Italia, el cual crea un ecosistema de vigilancia y garantía pública en el que pueden participar entidades tanto públicas como privadas. En este mismo grupo, Bélgica también posibilita la participación de entidades privadas en servicios de identificación electrónica, previéndose explícitamente dicha posibilidad en la regulación belga la cual exige a estos proveedores privados “pasar” por una plataforma de autenticación de control público. Finalmente, el caso de Noruega es quizás el que presenta una diferencia más radical con los modelos europeos ya que el país nórdico opta por confiar a un consorcio de bancos la provisión del medio de identificación electrónica notificado conforme a eIDAS, un sistema que ha funcionado particularmente bien tanto en el acceso a servicios públicos, como privados.

Las distintas experiencias en la implementación de eIDAS, las cuales han ofrecido diferentes resultados, son particularmente valiosas en el momento actual con la adopción de eIDAS2. La versión actualizada del Reglamento está llamada a tener un impacto trascendental en materia de identidad digital, introduciendo un nuevo medio de identificación electrónica armonizado destinado a operar en un nuevo ecosistema de identidad digital, que se añade a los ecosistemas federados existentes. En el núcleo del ecosistema creado por eIDAS2 se encuentra la Cartera de Identidad Digital Europea. La Cartera se erige como un medio de identificación electrónica en sí misma, que además permite la obtención, almacenamiento y gestión de credenciales de identidad, bajo la figura jurídica de las declaraciones electrónicas de atributos. La modalidad de provisión de la Cartera de Identidad Digital Europea corresponde a cada Estado Miembro; sin embargo, como medio de identificación electrónica armonizado, esta deberá cumplir con una serie de requisitos muy concretos, especialmente en materia de seguridad, privacidad, así como interoperabilidad y exigencias de certificación. Además, una de las principales innovaciones de eIDAS2 es precisamente la obligación para una amplia variedad de prestadores de servicios de aceptar la Cartera de Identidad Digital Europea como medio de identificación y autenticación electrónica. Entre dichos operadores identificamos, aquellos servicios que requieren la autenticación reforzada del usuario,

así como las plataformas en línea de muy gran tamaño. En el caso de operadores de menor tamaño, la aceptación será voluntaria, aunque el objetivo es que la Cartera tenga un amplio uso, por lo que se pretende fomentar su aceptación a través de códigos de conducta. Si bien la Cartera de Identidad Digital Europea se erige como la pieza angular en el nuevo ecosistema de identidad digital, esta no aparece de forma aislada. En concreto, la versión actualizada del Reglamento aprovecha el régimen jurídico de los servicios de confianza para dar cobertura a la emisión de credenciales de identidad, por entidades públicas y privadas, bajo un nuevo servicio de confianza, los Emisores de Declaraciones Electrónicas de Atributos. Además, se introduce otro nuevo servicio de confianza fundamental, el Libro Mayor Electrónico, que se erige como la primera forma de regulación a nivel global para tecnologías de registro distribuido destinada a facilitar una amplia variedad de casos de uso, entre los cuales, en lo que concierne al tema de estudio de esta tesis, se encuentra la posibilidad de facilitar extensos ecosistema de confianza, así como la adopción de modelos de gestión de la identidad de naturaleza más propiamente auto-soberana, en las interpretaciones más ambiciosas de este concepto.

Desde un punto de vista más conceptual, las nuevas figuras jurídicas introducidas en la versión actualizada del Reglamento dan paso a un nuevo modelo de identidad digital, como se sugiere en esta tesis, de naturaleza descentraliza o incluso en cierta medida de identidad auto-soberana. No obstante, es esencial reconocer al mismo tiempo que el ecosistema creado por eIDAS2 tiene unas características propias muy singulares. En concreto, a pesar de ser un ecosistema en el que se prevé la convergencia de entidades públicas y privadas, la pieza angular del ecosistema, la Cartera de Identidad Digital Europea se erige como un bien de provisión pública garantizada, en relación con el cual, independientemente de la modalidad de provisión escogida, el Estado adquiere un rol de garante estando obligado a asegurar su provisión. Dicha obligación marca un hito en materia de política de identidad digital, y es que, sorprende la ausencia en el panorama regulatorio actual de un derecho a la identidad, contando con muy reducidas menciones en textos internacionales. Como consecuencia, tampoco se reconoce un derecho explícito a la identidad digital, una realidad que el mandato introducido por el eIDAS2 busca modificar. No obstante, es importante considerar las limitaciones inherentes al



Reglamento, así como las características y naturaleza del ordenamiento jurídico europeo que determinan en última instancia el alcance de este derecho.

Sea como fuere, dicho mandato de provisión de la Cartera de Identidad Digital Europea se encuadra en la evolución regulatoria, especialmente en materia de regulación digital, que ha experimentado la Unión Europea en los últimos años. A diferencia de las regulaciones de la primera mitad de los años dos mil, con un carácter más liberalista, las últimas regulaciones han optado por un intervencionismo público más fuerte. eIDAS2 forma parte de este segundo grupo en el que además de adoptarse un enfoque europeo común, el rol del Estado se alza como esencial en el nuevo ecosistema de identidad digital. Se trata de un enfoque que difiere esencialmente de aquellos adoptados en otros países más allá de las fronteras de la Unión, como es el caso de Estados Unidos, en el que la política de identificación y por ende de identificación electrónica es radicalmente distinta a la de la Unión, con una fuerte dependencia del sector privado, conllevando a que el proceso de transformación del modelo de identidad digital sea también radicalmente diferente. No obstante, estas perspectivas divergentes son esenciales ya que, por una parte, ofrecen lecciones valiosas para la incipiente implementación de eIDAS2 en el escenario europeo y, por otra parte, es crucial recordar que la identidad digital es una cuestión de alcance global.

El enfoque notoriamente garantista adoptado por eIDAS2 tiene una serie de implicaciones desde un punto de vista jurídico. Desde el punto de vista del derecho europeo, en esta tesis se sugiere que la Cartera de Identidad Digital Europea, en su propósito de configurarse como una capa de identidad digital para las personas físicas con garantía pública, reviste un interés general que resulta evidente en la sociedad actual y que implicaría su posible calificación como un Servicio de Interés General. La calificación de la provisión de la Cartera de Identidad Digital Europea como un Servicio de Interés General conllevaría el obligado cumplimiento de las garantías y obligaciones de servicio público, con independencia de la entidad, pública o privada, a la que finalmente corresponda su provisión. Igualmente, la naturaleza de servicio público puede conllevar consecuencias específicas en el marco de la implementación de eIDAS2 en un Estado Miembro concreto y su derecho nacional aplicable. En el caso de

España, esta tesis plantea que la provisión de la Cartera de Identidad Digital Europea, como medio de identificación electrónica en sí misma está concebida para la generación de efectos jurídicos frente a terceros y, por tanto, su provisión, desde mi punto de vista, conlleva el ejercicio de una potestad administrativa conforme al Derecho Administrativo español. Desde el punto de vista de nuestro derecho nacional, las potestades administrativas implican una serie de requisitos desde el punto de vista de su atribución y ejercicio, cuestión fundamental cuando se consideran las distintas modalidades de provisión de la Cartera de Identidad Digital Europea en el contexto nacional y que sugiere la necesidad de una ley específica en esta materia. Además, es fundamental tener en cuenta que la provisión de la Cartera de Identidad Digital Europea es solo el punto de partida en un nuevo ecosistema en el que aparecen nuevos roles o se modifican los roles existentes, en relación con los cuales deben articularse una serie de derechos y obligaciones, así como de garantías en el ejercicio de sus funciones. El resultado consistiría en la articulación de un estatuto jurídico de derechos y obligaciones, el cual considero al menos necesario en relación con el proveedor de la Cartera de Identidad Digital Europea, el usuario y los distintos proveedores de servicios o partes usuarias de la Cartera.

En definitiva, esta tesis busca demostrar que el cambio regulatorio en este sector, con regulaciones como eIDAS2, altera en última instancia los modelos de gobernanza de Internet, pasando uno de sus componentes fundamentales, la identidad digital de las personas físicas, a ser un componente con una garantía pública. Dicho enfoque es un cambio esencial si se tienen en cuenta las limitadas garantías que existían hasta la fecha, en un contexto marcado por la importancia y la necesidad de una capa de identidad digital como elemento habilitador para el ejercicio de derechos y la participación eficaz en sociedades profundamente digitalizadas. La formación de esta capa de identidad digital armonizada deberá desarrollarse respetando las políticas de identificación adoptadas a nivel nacional, si bien el momento actual de transformación también debe aprovecharse para incorporar las lecciones que ofrecen los distintos modelos existentes hasta la fecha. En línea con esta cuestión, es esencial tener en cuenta que, a pesar de la naturaleza jurídica de reglamento de eIDAS2, la delgada línea en la delimitación de competencias entre la los Estados Miembros y la Unión, y el carácter esencialmente

nacional de la identificación, hace que existan numerosos resquicios o puntos abiertos en el Reglamento que precisan de intervención nacional para su implementación y lo que es más, esta jugará un papel esencial en la determinación del alcance de los efectos jurídicos del Reglamento, pudiendo optar por su extensión. Finalmente, merece la pena llamar la atención del lector sobre el enfoque regulatorio radicalmente distinto que ofrece eIDAS2 en relación con otras regulaciones en el entorno digital. A diferencia de otras regulaciones, eIDAS2 no se limita a imponer una serie de requisitos o limitaciones en ecosistemas existentes, sino que, por el contrario, fomenta la creación de un nuevo ecosistema jurídico en el que se alteran tanto los distintos roles, como los flujos de comunicación. Este enfoque, sin duda más ambicioso, no está exento de dificultades o retos, desafiando algunas nociones establecidas, como sucede en el sector de la privacidad y de la protección de datos. Sin embargo, este enfoque es necesario a día de hoy, en un momento en el que ha quedado claro que, debido a la rápida evolución de los ecosistemas digitales, cada vez es más complejo lidiar con los desequilibrios de poderes que existen en el contexto actual. En esta situación, si bien la regulación deberá seguir imponiendo requisitos, considero que también debe mostrarse innovadora, ofreciendo nuevos conceptos jurídicos, fomentando la participación de forma regulada de las distintas partes interesadas para que, en última instancia, los avances se encaminen hacia una mejora de la sociedad actual.



# TABLE OF CONTENTS

<b>METHODOLOGY .....</b>	<b>1</b>
<b>INTRODUCTION. DIGITAL IDENTITY: CONVERGENCE OF NOTIONS, PARTICIPANTS AND MODELS. READY FOR TRANSFORMATION? .....</b>	<b>5</b>
DIGITAL IDENTITY: CONCEPT AND DIMENSIONS .....	6
DIGITAL IDENTITY LIFECYCLE .....	10
PARTICIPANTS IN DIGITAL IDENTITY ECOSYSTEMS .....	13
DIGITAL IDENTITY ECOSYSTEMS: EID MODELS .....	15
EMBRACING THE CHANGE: THE EVOLUTION OF EID MODELS .....	18
<b>CHAPTER I. FRAGMENTED DIGITAL IDENTITIES: ANALYZING DEFICIENCIES .....</b>	<b>21</b>
<b>1. MAPPING THE REGULATORY LANDSCAPE OF DIGITAL IDENTITY IN THE EU .....</b>	<b>22</b>
<i>1.1. Exploring the Spectrum of Digital Identity Types within Regulatory Boundaries ...</i>	<i>22</i>
1.1.1. Digital Identity in the Public Sector .....	22
1.1.2. Digital Identity in the Private Sector .....	25
1.1.3. Digital Identity in Financial Services .....	27
<i>1.2. Privacy and Cybersecurity as Fundamental Pillars of Digital Identity .....</i>	<i>31</i>
1.2.1. Privacy Considerations in Digital Identity Processes .....	31
1.2.1.1. User Awareness .....	32
1.2.1.2. Secure Data Storage .....	33
1.2.1.3. Cryptographic Functions for User Control .....	36
1.2.2. Cybersecurity Considerations in Digital Identity Processes .....	37
<b>2. THE ERA OF FEDERATED DIGITAL IDENTITY: CHALLENGES FROM A REGULATORY PERSPECTIVE .....</b>	<b>40</b>
<i>2.1. Federated Digital Identity .....</i>	<i>40</i>
2.1.1. Evolution of Digital Identity Models .....	40
2.1.2. Foundations of Federated Digital Identity .....	42
<i>2.2. The Limits of Regulation in Addressing the Challenges in the Digital Identity Landscape .....</i>	<i>44</i>
2.2.1. Enforcing Privacy Rights Amidst Surveillance Practices .....	44
2.2.2. Difficulties in Prosecuting Identity-Related Crimes .....	49
2.2.3. The Role of Competition Law in Addressing Power Disparities in the Tech Industry .....	53

3. DIGITAL IDENTITY, ESSENTIAL, YET NOT GUARANTEED .....	57
<b>CHAPTER II. THE EIDAS REGULATION: PIONEERING ELECTRONIC IDENTIFICATION LAW WITH NOTABLE LIMITATIONS .....</b>	<b>59</b>
1. THE EIDAS REGULATION: A FIRST STEP IN ELECTRONIC EVIDENCE, NOW FACING MODERN LIMITATIONS.....	61
1.1. <i>A Multifaceted Regulation: Electronic Identification and Trust Services</i> .....	61
1.1.1. Notified eID Means for Cross-border Processes in the European Union. ....	61
1.1.2. The Legal Framework of Trust Services .....	64
1.2. <i>Constraints and Limitations of the eIDAS Regulation for the Development of Digital Identity Ecosystems</i> .....	66
1.2.1. Electronic Identification: between National eID Schemes, Trust Services, and Private Providers.....	67
1.2.2. Privacy and Security Challenges within the eIDAS Regulation.....	70
2. FROM THEORY TO PRACTICE: EXAMPLES OF THE IMPLEMENTATION OF THE EIDAS REGULATION IN THE NOTIFICATION OF ELECTRONIC IDENTIFICATION SCHEMES .....	73
2.1. <i>State-owned Electronic Identification Solutions</i> .....	73
2.1.1. Good Design but Poor Usage of Electronic National Identity Cards: the Cases of Spain and Germany .....	73
2.1.2. Achieving Digital Identity Success: Lessons from Estonia's National Electronic Identity Card .....	78
2.1.3. State-Platform: France's Pursuit of Convenience .....	81
2.2. <i>Leveraging the Private Sector for Electronic Identification</i> .....	83
2.2.1. Italy's Surveilled Ecosystem of Public and Private Digital Identity Providers..	83
2.2.2. Private Sector Involvement in eID Provision: The Belgian Perspective .....	86
2.2.3. The Key Role of Banks for Electronic Identification in Norway .....	88
3. COMPLEXITY AND OUTDATEDNESS OF THE EIDAS REGULATION, BUT ESSENTIAL LESSONS FOR THE NEXT DIGITAL IDENTITY ECOSYSTEMS .....	91
<b>CHAPTER III. THE EIDAS2 REGULATION: BUILDING A NEW FOUNDATION FOR DIGITAL IDENTITY .....</b>	<b>95</b>
1. THE EIDAS2 REGULATION: A VISIONARY PROPOSAL FOR A HARMONIZED DIGITAL IDENTITY METASYSTEM.....	97
1.1. <i>The European Union Digital Identity Wallet as the Cornerstone of the eIDAS2 Digital Identity Ecosystem</i> .....	97
1.1.1. An Overview of Requirements and Functionalities.....	99

1.1.1.1. Mandate and Modalities of Provision .....	99
1.1.1.2. Functionalities .....	101
1.1.1.3. Security Requirements .....	102
1.1.1.4. Privacy Requirements.....	103
1.1.1.5. Standardization Requirements.....	104
1.1.1.6. Cross-Border Identity Matching.....	104
1.1.1.7. Certification Requirements.....	105
1.1.2. New Services Required to Accept the European Union Digital Identity Wallet .....	108
1.2. <i>New Trust Services in eIDAS2 and their Impact on Digital Identity Ecosystems...</i>	112
1.2.1. Issuers of Electronic Attestations of Attributes: Paving the Way for a Regulated Ecosystem of Identity Credentials .....	113
1.2.2. Electronic Ledgers: Unlocking the Potential of Distributed Ledger Technologies.....	116
2. FOUNDATIONS OF EMERGING DIGITAL IDENTITY ECOSYSTEMS .....	118
2.1. <i>Transformation in Roles and Communication Flows</i> .....	118
2.1.1. The Rise of Self-Sovereign Identity .....	119
2.1.2. New Ecosystems, New Benefits for the Different Stakeholders .....	124
2.2. <i>eIDAS2: within Emerging Digital Identity Ecosystems, but with its Own Unique   Features.....</i>	126
2.2.1. A Digital Identity Landscape integrated by Wallets and Identity Credentials.	126
2.2.2. The European Union Digital Identity Wallet as a form of State-backed Digital Identity.....	128
3. CHARTING THE COURSE TO A NEW DIGITAL IDENTITY ECOSYSTEM.....	130
<b>CHAPTER IV. THE ULTIMATE PUBLIC NATURE OF THE EIDAS2 DIGITAL IDENTITY METASYSTEM .....</b>	<b>133</b>
1. THE MANDATE FOR THE PROVISION OF THE EUROPEAN UNION DIGITAL IDENTITY WALLET.....	134
1.1. <i>Is there a Right to a Digital Identity?</i> .....	134
1.1.1. Detaching Identity from Privacy and Data Protection.....	134
1.1.2. The Inherent Regulatory Limitations of the European Union Digital Identity Wallet Provision Mandate .....	137
1.2. <i>The Provision of the European Union Digital Identity Wallet</i> .....	139
1.2.1. More than just a Wallet App, but an Electronic Identification Means in Itself. .....	139

1.2.2. A Form of Public Intervention to Facilitate Markets and Societal Transformation.....	143
2. A PARADIGM SHIFT IN THE EU: THE GROWING ROLE OF PUBLIC INTERVENTION IN THE DIGITAL AGE.....	146
2.1. <i>On the Path to Recovering Digital Sovereignty</i> .....	146
2.1.1. Evolution of the EU’s Digital Regulatory Landscape: Consequences for the Digital Identity Sector.....	147
2.1.2. Public Sector Leadership versus Market Dominance: A Comparison of EU and US Strategies in Digital Identity. ....	151
2.2. <i>Services of General Interest and Their Applicability in the Digital Sphere</i> .....	155
2.2.1. Digital Society’s Advancements Highlight the General Interest in a Digital Identity Layer.....	155
2.2.2. Conceptualizing the European Digital Identity Wallet as a Service of General Interest.....	160
3. THE PUBLIC SECTOR IS BOUND TO PLAY A CRUCIAL ROLE IN THE DEVELOPMENT AND GUARANTEE OF A DIGITAL IDENTITY LAYER, AT LEAST IN EUROPE.....	163
<b>CHAPTER V. UNKNOWNNS IN THE EIDAS2 REGULATION AND THE CALL FOR NATIONAL REGULATORY DEVELOPMENTS .....</b>	<b>167</b>
1. THE PROVISION OF THE EUROPEAN UNION DIGITAL IDENTITY WALLET FROM A PUBLIC LAW PERSPECTIVE .....	168
1.1. <i>The Provision of the European Union Digital Identity Wallet as a Manifestation of the Exercise of Public Powers</i> .....	168
1.1.1. The Attribution and Exercise of Administrative Authority. ....	169
1.1.2. Provision by the Public Sector.....	172
1.2. <i>Possibilities for the Provision of the European Union Digital Identity Wallet by the Private Sector: Public Procurement and The Act of “Recognition.”</i> .....	176
1.2.1. The Delegation of the Exercise of Administrative Authority to the Private Sector .....	176
1.2.2. Between Public Procurement and the Incorporation of the eIDAS2 "Recognition of Independent European Union Digital Identity Wallets" Option into National Law.....	180
2. A DEFINED STATUTE OF GUARANTEES, RIGHTS, AND OBLIGATIONS FOR PARTICIPANTS IN THE EIDAS2 DIGITAL IDENTITY ECOSYSTEM.....	186
2.1. <i>The Provision of the European Union Digital Identity Wallet</i> .....	186



2.1.1. Guarantees from the Perspective of the Provisioning Process and the Provider. .....	186
2.1.2. Guarantees, Rights, and Obligations from the User Perspective.....	191
2.2. <i>The Acceptance of the European Union Digital Identity Wallet and Possibilities for a Comprehensive Digital Identity</i> .....	197
2.2.1. Obligation and Possibilities for Reliance on the European Union Digital Identity Wallet and Registration Procedure.....	197
2.2.2. The Opportunity for a Dynamic, Rich Digital Identity through Electronic Attestations of Attributes .....	200
3. FURTHER REGULATORY DEVELOPMENTS WILL BE KEY IN DETERMINING THE SUCCESS OF THE EIDAS2 REGULATION .....	203
<b>CONCLUSIONS .....</b>	<b>207</b>
<b>REFERENCES.....</b>	<b>229</b>
<b>ANNEX A. THE DATA PROTECTION IMPACT ASSESSMENT IN “LAYERS”: A METHODOLOGY FOR EVALUATING TECHNOLOGICAL PROPOSALS.....</b>	<b>273</b>
ENSURING PRIVACY AT THE FOUNDATIONAL STAGES OF TECHNOLOGICAL INNOVATION	273
DPIA IN “LAYERS”: STEPS AND AN EXAMPLE OF THE ADAPTED METHODOLOGY .....	277
<b>ANNEX B. THE ROLE OF THE DATA CONTROLLER IN USER-CENTRIC TECHNOLOGIES: THE IDENTITY WALLETS .....</b>	<b>291</b>
SCENARIO OVERVIEW AND ANALYSIS.....	291
CONCLUSIONS AND RECOMMENDATIONS.....	294
<b>ANNEX C. CURRENT ADVANCEMENTS IN THE IDENTITY OF OBJECTS: A REFLECTION ON DEVICES’ IDENTIFIERS .....</b>	<b>299</b>
PROJECT DESCRIPTION.....	299
ARE DEVICE IDENTIFIERS PERSONAL DATA? .....	300
A CASE-BY-CASE ANALYSIS .....	302



## List of Figures

<b>Figure 1</b> Digital Identity Overview .....	10
<b>Figure 2</b> Digital Identity Lifecycle .....	13
<b>Figure 3</b> Participants in Digital Identity Ecosystems .....	15
<b>Figure 4</b> Levels of Assurance in Access to Digital Services .....	16
<b>Figure 5</b> Examples of Data Processing Activities in Identification and Authentication Processes .....	32
<b>Figure 6</b> Evolution in Digital Identity Models .....	42
<b>Figure 7</b> Communication Flows in Federated Digital Identity .....	44
<b>Figure 8</b> Cross-border Authentication Process through eIDAS Nodes .....	63
<b>Figure 9</b> Middleware-to Middleware Configuration .....	63
<b>Figure 10</b> Features and Functionalities of the EUDI Wallet .....	108
<b>Figure 11</b> Digital Identity Ecosystem Transition .....	123
<b>Figure 12</b> EUDI Wallet Provision .....	142
<b>Figure 13</b> Scenarios for the EUDI Wallet Implementation .....	145
<b>Figure 14</b> Outsourcing of Administrative Authority .....	180
<b>Figure 15</b> Layered Digital Identity in eIDAS2 & Legal Effects .....	203

## List of Tables

<b>Table 1</b> Regulatory Frameworks and Sector-Specific Digital Identities .....	30
<b>Table 2</b> Possibilities for the Provision of Identification Services and Applicable Regulations .....	70
<b>Table 3</b> Cross-border Reliance Comparison eIDAS1 versus eIDAS2 .....	110
<b>Table 4</b> Comparison of Core Features in Emerging Digital Identity Ecosystems .....	121

## List of Images

<b>Image 1</b> On the Internet, Nobody Knows You Are a Dog .....	49
<b>Image 2</b> Power Imbalance and Mutual Dependence .....	54



# ABBREVIATIONS

## A-E

---

<b>app:</b> Application	<b>EBA:</b> European Bank Authority
<b>ARF:</b> Architecture Reference Framework	<b>EBSI:</b> European Blockchain Service Infrastructure
<b>AML:</b> Anti-Money Laundering	<b>ECJ:</b> European Court of Justice
<b>A29 WP:</b> Article 29 Data Protection Working Party	<b>ECTHR:</b> European Court of Human Rights
<b>CDD:</b> Customer Due Diligence	<b>EDICG:</b> European Digital Identity Cooperation Group
<b>CIR:</b> Commission Implementing Regulation	<b>EUDI Wallet:</b> European Union Digital Identity Wallet
<b>DLT:</b> Distributed Ledger technology	<b>EAA:</b> Electronic Attestation of Attribute
<b>DID:</b> Decentralized Identifier	<b>ENISA:</b> European Union Agency for Cybersecurity
<b>DPIA:</b> Data Protection Impact Assessment	<b>EU:</b> European Union
<b>DSA:</b> Digital Services Act	
<b>DSP:</b> Digital Service Provider	

## F-K

---

<b>IdP:</b> Identity Provider	<b>ID:</b> Identity
<b>IA:</b> Implementing Act	<b>ITU:</b> International Telecommunication Union
<b>ICAO:</b> International Civil Aviation Organization	<b>ISO:</b> International Standards Organization
<b>ICT:</b> Information and Telecommunication Technologies	<b>ISS:</b> Information Society Service
	<b>KYC:</b> Know Your Customer

## L-P

---

<b>LoA:</b> Level of Assurance	<b>OES:</b> Operators of Essential Services
<b>mDL:</b> Mobile Driver License	<b>PID:</b> Person Identification Data
<b>NIST:</b> National Institute of Standards and Technology	<b>PKI:</b> Public Key Infrastructure
	<b>PSP:</b> Payment Service Provider

## Q-T

---

**RTS:** Regulatory Technical Standards

**RP:** Relying Party

**SCA:** Strong Customer Authentication

**SGEI:** Service of General Economic Interest

**SGI:** Service of General Interest

**SGSI:** Service of General Social Interest

**SSI:** Self-Sovereign Identity

**SSO:** Single Sign-On

**TEU:** Treaty of the European Union

**TFEU:** Treaty of Functioning of the European Union

**TJUE:** Tribunal of Justice of the European Union

## U-Z

---

**UDHR:** Universal Declaration of Human Rights

**US:** United States

**VC:** Verifiable Credential

**W3C:** World Wide Web Consortium

**ZKP:** Zero-Knowledge Proof

## Regulatory Abbreviations

---

**ECHR** European Convention on Human Rights

**AML Directives** The term can refer to the various directives, identified by the number (fifth AML Directive, sixth AML Directive...). In this thesis, we mainly refer to the fifth AML, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

**CDR (EU) 2018/389** Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

<b>CIR 2015/1501</b>	Commission Implementing Regulation (EU) 2015/1501 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
<b>CIR 2015/1502</b>	Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
<b>DMA</b>	Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
<b>DSA</b>	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
<b>eIDAS Regulation</b>	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
<b>Proposal for Revision of the eIDAS Regulation/ eIDAS2 Proposal/ eIDAS2</b>	Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity
<b>GDPR</b>	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
<b>NIS Directives</b>	The term can refer to two versions, NIS1 and NIS2. In this thesis, we refer to both NIS1, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union and NIS2, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high

common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

**PSD2**

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC



# METHODOLOGY

What is the role of Public Law in upcoming digital identity ecosystems? This thesis aims to explore this question to understand how Public Law is bound to be a nuclear component for an identity layer of the digital medium. The study of this topic raises important challenges due to its strong technical nature. In order to understand the main drawbacks of existing models and their legal implications, it is necessary to comprehend, at least from a conceptual perspective, the different models that have existed for digital identity until now.

The nature of the topic required a qualitative research methodology. This approach enables an in-depth exploration of the nuances, intricacies, and complexities tied to the research subject. The topic has required the examination of both emerging and applicable regulations (at least still at the moment of writing this thesis) that have been contextualized within the technological capabilities and societal challenges digital societies face. The objective of this approach was that both technological and societal realities were observed through the lens of regulatory challenges.

It can be said that, given the scarcity of scientific doctrine assessing the topic of digital identity from a regulatory perspective, the main source of this thesis has been legislative texts, notably the eIDAS Regulation and its successor, eIDAS2. Nevertheless, this “raw” analysis of the legislative texts has been complemented by reports produced by public and private institutions, legal commentaries, scientific papers, and other types of publications and resources that are listed in the bibliography of this thesis. Occasionally, it has been necessary to analyze very specific case law, but this is not abundant in this thesis, which is logical given the cutting-edge nature of the subject of study. Furthermore, to understand the complex interplay between new technologies and the law, it was necessary to review a large amount of technical documentation, like scientific papers published in information technology journals or technology standards.

Nevertheless, this thesis also has a strong practical nature because, during these years of research, I have actively participated in different activities. More specifically, this thesis has incorporated the insights gathered from discussions with professionals in the field and semi-structured interviews. I would like to express my gratitude to the professionals who generously gave me their time to discuss the challenges of the digital identity domain. In particular, John Erik Setsaas accompanied me during almost all of my research period, and our monthly discussions always raised new interesting questions that have been incorporated into this thesis. Combining technical and legal knowledge was extremely valuable in acquiring an overall perspective on the topic, particularly because he was always able to look beyond the technology itself. In addition, my regular discussions with Arthur van der Wees helped me broaden my views and understand digital identity as a core part of a broad digital ecosystem in which numerous regulations converge. Likewise, joining the excellent research group coordinated by Prof.Dr.Antonio Skarmeta Gómez gave me the opportunity to be directly involved in the technological field and to learn so much by working hand in hand with technical experts. The knowledge that I was able to acquire during the time I spent working with my colleagues in the faculty of computer science has been decisive in shaping my professional profile, which, although still a legal profile, has acquired the ability to communicate effectively with technical experts and to understand complex technological concepts.

Furthermore, during the time writing this thesis, I was selected to be part of the cohort that conducted a research sprint with the Berkman Klein Center for Internet & Society on the topic of digital identity. This research sprint helped me realize that digital identity is a global issue and that even though this thesis is contextualized in the EU, it needs to be developed further to understand how these considerations could potentially apply in a global context. It is also worth mentioning that I have been part of two EU-funded research projects: the EU project OLYMPUS<sup>2</sup> and the EU project ERATOSTHENES<sup>3</sup>. These projects focus both on cutting-edge technological innovations in the field of digital identity, the first exploring the possibility of developing more secure digital

---

<sup>2</sup> Grant agreement ID: 786725

<sup>3</sup> Grant agreement ID: 101020416

identity solutions for citizens and, in particular, more respectful with their rights and freedoms, while the second has a strong focus on the security of connected devices, which, although in principle seems to refer to the identity of non-living entities, ultimately affect the person behind them. These two projects were very valuable for me because I was able to learn about the latest technological developments in the sector, and they taught me the importance of understanding the technology to perform a good legal analysis. Some of the results of these projects are included in the annexes of this thesis because I think that even if they are not part of the nuclear discourse, they are essential ramifications of the topic that shall be considered when analyzing the implications of the transformation of the digital identity ecosystem.

In addition, my two and a half years of practical experience in the consulting sector have been essential in the writing of this thesis. During this time, I was involved in consulting projects on digital identity with the company Explicit Selection, which gave me a more practical view of the industry impact of regulatory changes. Notably, this experience has allowed me to become familiar with some of the stakeholders who will be required to implement the changes discussed in this thesis, giving me some understanding of their impressions, worries, and concerns, a more realistic perception that is not exclusively academic. The reader may notice that in the thesis there are several references to financial services, especially emerging regulatory proposals in this sector, which are due to the knowledge gathered thanks to the projects I have participated in with Explicit Selection as well as my participation in the research group LegalCripto led by Prof. Dr. Carmen Pastor Sempere at the University of Alicante, which has allowed me to integrate my knowledge on digital identity in the sector of crypto assets and financial services.

Furthermore, I have also been working as an external consultant for the European Commission on topics such as the EUDI wallet and the development of a blockchain services infrastructure across Europe, specifically the EBSI project. Working on these two topics with the European Commission has been fundamental to understand, on the one hand, the strong public-led initiative to develop and regulate digital identity

ecosystems, but also the challenges that are raised when this is done in a political infrastructure that is integrated by many diverse and different States.

It might draw the reader's attention that this thesis covers various topics, including legal and technical aspects, and although the research has been produced in the frame of Public Law, on various occasions, it has been necessary to refer to legal institutions specific to Private Law. The reason for this approach is simply that there was no direct predecessor for this thesis, and despite the few legal studies that have provided extraordinarily valuable conclusions for digital identity from a regulatory perspective, these were not exclusively focused on the topic of digital identity itself. Consequently, the aim of this thesis is to conduct one of the first studies on digital identity from a legal point of view, which has required the adoption of a holistic approach, starting with a first broad exploration of the subject to delineate it from a legal perspective. The final objective of this research is to provide new perspectives from a regulatory standpoint on a subject that has primarily been technical in nature until now, notably leveraging the current moment of change and where I encourage regulations to take an active role instead of lagging behind.

Yet, it is important to note that this study is fundamentally interpretive, and as is characteristic of all legal analyses, interpretations can diverge. Furthermore, the study is based on EU regulations within a specific time period. This focus might not encompass a thorough global or local overview. This intentional limitation aims to provide more precise legal insights based on specific regulations. Even so, I believe that several lines of reasoning can be extracted from the EU context and evaluated within a more global framework. In fact, reaching the widest possible audience interested in the topic was the driving force behind the decision to write this thesis in English, a choice that comes with inherent challenges and might result in occasional mistakes or inaccuracies for which I apologize in advance.

# INTRODUCTION

## **DIGITAL IDENTITY: CONVERGENCE OF NOTIONS, PARTICIPANTS AND MODELS. READY FOR TRANSFORMATION?**

The past twenty years have witnessed an unexpected evolution of the Internet. Originally invented as a medium of communication and information exchange, it has become an indispensable element in our lives today. The Internet has changed, for example, the way we shop, bank, or socialize, affecting every aspect of our daily lives.

The number of users interconnected through the Internet has experienced a significant increase, evolving from a reduced group of academics to an indefinite number of participants, which might include natural persons, legal entities, or even “things” or objects, raising the need to identify them (Preukschat & Reed, 2021, p.2). The identification of individuals over the Internet is essential in the guarantee of safe and trustworthy online activities where digital identities emerge as critical pieces of current societies and global markets, but also represent one of the main challenges of the Internet era.

Indeed, digital identities are complex. On the one hand, digital identity is essentially interdisciplinary, involving technology, law, ethics, philosophy, and sociology, among other areas. On the other hand, depending on the entity type, digital identities will have different functions, limits, and constraints. Therefore, the regulatory environment has been unable to address some of the key risks and challenges involved in identification services<sup>4</sup>.

---

<sup>4</sup> One of the most widely known examples in recent years is the Cambridge Analytica scandal. Facebook provided unauthorized access to more than 87 million users' personally identifiable information to the data firm Cambridge Analytica. Cambridge Analytica integrated this information with a range of data from social media platforms, browsers, online purchases, voting results, and more. By adding OCEAN analysis to the other private and public data acquired, Cambridge Analytica developed the ability to “micro-target” individual consumers or voters with messages most likely to influence their behaviour.

A rapidly changing environment, combined with the intrinsic connection between identification services and States' sovereignty in a global Internet context, are all contributing factors to this limited legal landscape.

As a consequence, the Internet is an infrastructure that has developed mainly in the hands of the private sector, and that has, in some cases, led to undesirable results and now requires additional forms of control or supervision, particularly in order to prevent the damage that could be caused by the lack of respect for the most basic and fundamental human and societal rights and values. In this context, identity emerges as a core element, not only in the attribution but also in the exercise of these rights, but in its digital form, in a wide range of scenarios, its provision is not guaranteed or has been left to the willingness of public or private operators.

Before entering the discussion of this thesis, this section aims to introduce a set of basic concepts to enable readers to understand the subject, its particularities, and the conclusions achieved.

### **Digital Identity: Concept and Dimensions**

The concept of entity is the point of departure in the study of identity. An identity describes an entity within a specific scope, defined as “a set of all characteristics attributed to an entity within a scope” (Joosten et al., 2008, as cited in Alpár et al., 2011, p.5). The ITU (2018, p.4) defines identity as a “representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context.”

The definition of identity requires putting it in connection with the definition of an entity. “An entity is a real-world thing” (Clarke, 2010), which, in my view<sup>5</sup>, includes

---

The OCEAN analysis was paired with a large number of targeted messages in “Project Alamo,” which was employed for the election campaign of President Donald Trump. Jim & Mina (2018, pp.56–57).

<sup>5</sup> Also, according to other digital identity experts, such as Guy De Felcourt, who provided me with the material for this section on the different types of digital identities according to the entity to which they relate.

and, at the same time, distinguishes at least between natural or legal persons and objects. All of these can be considered entities and, therefore, have an identity. However, the content will differ depending on the specific entity it pertains to, as well as the unique characteristics of the digital medium.

- a) Natural persons. There exist several definitions for natural persons' digital identity, such as "the unique representation of an individual in an online transaction" (NIST, 2017, p.4) or "combined biometric and biographic attributes that apply uniquely to that person" (ICAO, 2018, p.8). When referring to natural persons, the concept of digital identity must be designed and constrained by the particularities of application to human beings.

By way of example, the use of certain data can be a source of discrimination or enable user tracking in undesirable circumstances (e.g., biometrics, unique identifiers<sup>6</sup>...). User privacy should be preserved as much as possible during identification and authentication processes<sup>7</sup>, and the digital identity design should ensure it is understandable for the user in specific contexts, according to its social role.

The digital identity of natural persons is usually managed by electronic versions of governmental ID documents, such as electronic identification cards<sup>8</sup>, user credentials (e.g., usernames and passwords)<sup>9</sup>, or biometrics<sup>10</sup>.

---

<sup>6</sup> ISO/IEC 24760-1:2019 defines an identifier as an "attribute or set of attributes that uniquely characterizes an identity in a domain."

<sup>7</sup> In this thesis, I have opted to maintain the term "authentication," as technical scholars commonly understand it, the "confirmation of the identity of a previously identified person." However, it is important to note that, as already observed by Martín Delgado over a decade ago (2012, p.515), from a legal point of view, there has been confusion between the accreditation of identity and the manifestation of a particular will, and still, nowadays, in my opinion, there is a lack of clarity between these two terms, at least in the legal domain.

<sup>8</sup> By way of example, we could note the Spanish national electronic identification card (*DNIe*).

<sup>9</sup> Examples of user credentials could be Cl@ve in the Spanish public sector, or "login with Facebook, Google or Amazon" in the private sector.

<sup>10</sup> Biometrics can be defined as biological measurements, or physical characteristics, that can be used to identify an individual. Kaspersky. (n.d.) *What is Biometrics? How is it used in security?* Kaspersky. Retrieved August 23, 2023 from <https://www.kaspersky.com/resource-center/definitions/biometrics>

- b) Legal entities. The digital identity of legal entities is subject to fewer constraints and usually refers to other attributes, such as the legal name, the logo, or the electronic seal. It does not fulfill a social role, but it is thought of in the context of administrative procedures or economic transactions.

The identity of legal entities is usually managed through identifiers or register numbers<sup>11</sup>.

Furthermore, legal entities rely on legal representatives (thus, natural persons) acting on the entity's behalf. Under these circumstances, the capacity to prove the link with the entity the natural person pretends to act on behalf of becomes crucial.

- c) Objects, resources, and documents. Factors to consider in the “digital identity of things” could be whether these objects allow interconnection, have Internet access, or are subject to specific regimes that justify their traceability. Secondly, the particular purposes could be logistics, commerce, fraud prevention, or traceability during the lifecycle.

The digital identity of objects is managed through different techniques such as identifiers (e.g., Globally Unique Identifier or Universally Unique Identifier), codes, radio-identification, or even IPV6 or network technologies in the case of connected devices.

The concept of identity has different definitions depending on the discipline, evidencing its complexities when it aims to be extrapolated to the digital medium. For example, in subjective psychology, identity is understood as the individual's “true self.” The integrity of such self-identity is essential for the proper functioning of an individual.

---

<sup>11</sup> In this regard, the Legal Entity Identifier (LEI) is a global initiative to create a record to identify legal entities across countries by assigning unique alphanumeric codes and creating a unified record that contains legal entities' transaction-relevant information (e.g., shareholders, subsidiaries, location...). Global Legal Entity Identifier Foundation. (n.d.) *Introducing the Legal Entity Identifier (LEI)*. GLEIF. Retrieved August 23, 2023 from <https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei>



Conversely, from the social sciences perspective, identity construction is an interactive process of determining someone's identity within and against society (Tajfel & Turner, 1979, as cited in McLeod, 2023). Individuals define themselves as members of certain groups assuming specific roles; therefore, identification and identifiers demonstrate adherence to these groups and the roles assigned therein.

The definition given by Wood & Smith (2005, p.52) includes both perspectives, "an identity is a complex personal and social construct, consisting in part of who we think ourselves to be, how we wish others to perceive us, and how they actually perceive us." In other words, "the construction of identity is a public process that involves both the identity announcement made by the individual claiming an identity and the identity placement made by the others who endorsed the claimed identity, and an identity is established when there is a coincidence of placements and announcements" (Stone, 1981, as cited in Zhao et al., 2008, p.1817).

Pfitzmann & Hansen (2010, p.30) introduce the concept of partial identities, which is now particularly relevant in an ecosystem of presentations of identity attributes. Identity is "any subset of attributes of an individual person which sufficiently identifies this individual person within any set of persons." None of these identities could ever comprise the totality of the entity they describe and refer to. Therefore, "an identity of an individual person may comprise many partial identities of which each represents the person in a specific context or role." "A person (whether a human or a legal entity) may present many identities to different people and organizations in different contexts, and these identities might change over time (i.e., are dynamic) since assertions about an entity might change" (Bauer et al., 2005, pp.52–53).

The digital medium has brought new considerations to the concept of identity, which includes both its format and content. For example, digital ID cards<sup>12</sup>, biometrics, or Internet accounts all have their own characteristics. Moreover, the definition of identity

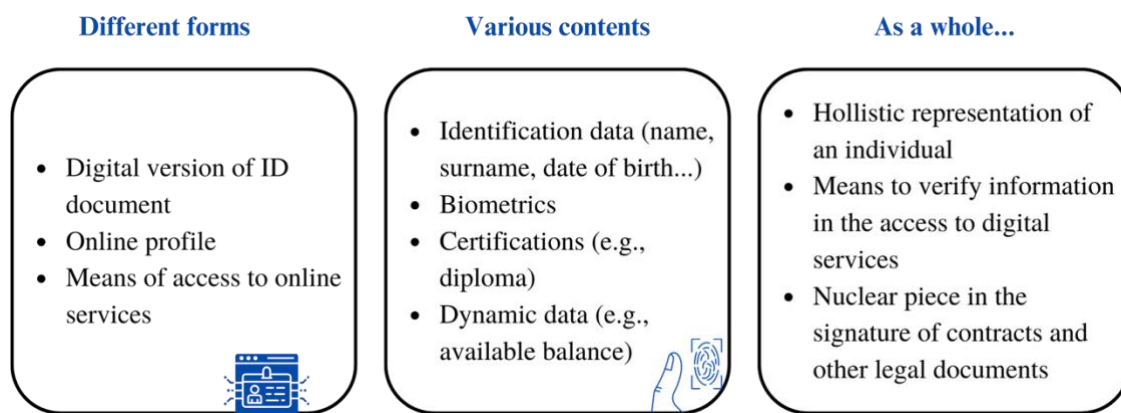
---

<sup>12</sup> The terms "ID," "identity," and "identification means" or "eID," "digital identity," or "electronic identification means" are used interchangeably in this thesis according to the desired aesthetic of a specific sentence.

has widened from simple identification information to include a variety of attributes that constitute our identities. Yet, in spite of the different requirements and conditions demanded by the digital medium, the ultimate functions can be compared to those of the physical forms of identity, that is, representing the individual, providing access to services, and establishing legal relationships.

**Figure 1**

### Digital Identity Overview



### Digital Identity Lifecycle

Digital identities go through several stages, from their creation and modification in response to different events to their inactivation or deletion. Although similarities exist in the physical identity lifecycle, there are also significant differences, particularly in remote scenarios. For instance, when presenting identity evidence, authentication factors must be applied to confirm the presenter's claimed identity.

The NIST SP 800-63<sup>13</sup> states that the digital ID process involves two basic components. The first component includes identity proofing and enrolment; the second refers to

---

<sup>13</sup> The NIST SP 800-63 series is a set of technical guidelines created by the NIST that focus on digital identity. The guidelines provide recommendations on identity proofing and authentication of users when they interact with government IT systems over open networks. Federal agencies can use the series to implement digital identity services, as it covers processes, technologies, and metrics related to digital identity.

authentication and identity lifecycle management. A third optional component would be integrated by portability and interoperability mechanisms. The World Bank notes (2019, p.18):

Identity lifecycle is not a one-time event. Rather, it is a process that starts when a person first registers and their identity is created, continues with authentication of that identity and updates to their attributes and credentials over time, and ends when an identity record is retired or invalidated.

Depending on the type of identity, the lifecycle phases differ. While a customer identity type will usually function outside the enterprise context, enabling digital business between the owner of the customer identity and the enterprise, workforce identity is created to function in an enterprise context. On the other hand, device or system identity is used to provide identification and representation on a digital network (Cameron & Grewe, 2022, pp.2–3).

At least three phases can be generally identified:

- a) Registration. Registration requires identification or answering the question “Who are you?” and involves the following actions or flows:
  1. Identity claim or collection. The first step in the process is that the person must establish their identity by providing personal information, relevant supporting documents, or other sources of evidence. It might involve showing proof of their attributes in hard copy (paper version) or digital format, such as a mobile driver's license, for instance. Some attributes, like biometrics, are inherent to an individual's identity.
  2. Identity proofing. It implies:
    - Validation. To be sure that identity information is both accurate and truthful, validating its authenticity and reliability. It may be necessary to consult a reliable source for comparison, and the information has to match up.
    - De-duplication. The identification of an individual's own identity in a particular population or milieu.

- Verification. This process includes verifying that the confirmed identity belongs to the person whose identity has been proven (e.g., through physical presence or comparing photos).

Once the digital identity has been created and validated, this phase finishes with the enrolment of the user and credentialing or the issuance of authenticators (account, document, token...). This process binds the subscriber's unique, verified identity to one or more authenticators.

- b) Use. Using a digital identity involves two successive steps: authentication and verification.

Authentication is the test of asserted credentials/factors in establishing confidence that the person is who they claim to be. It answers the question, "Are you the identified/verified individual?" and can rely on different authentication factors and processes.

The authentication factors can be separated into three basic categories:

Knowledge factors or "something you know."

Ownership factors or "something you have."

Inherence factors or "something you are."

On the other hand, authentication processes can be classified as:

Single-factor authentication [1FA]: uses only one authenticator.

Multi-factor authentication [MFA] uses two or more independent authenticators from at least two different authentication factor categories.

Finally, verification implies verifying the validity and authenticity of the specific attributes for the purpose of the transaction. The verification of attributes leads to authorization, that is, the verification of corresponding rights and fulfillment of requests.

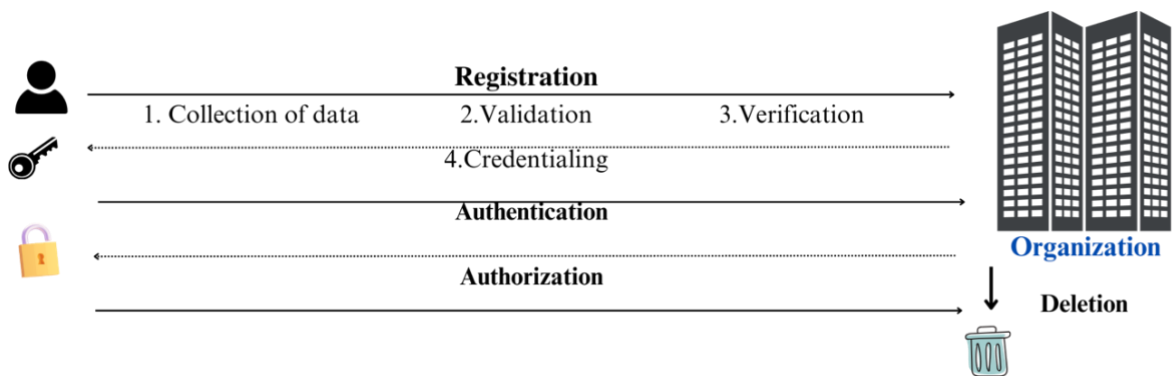
- c) Management. Maintenance of identity and credentials, which might include updating, revoking, retiring... as well as correcting errors or communication and consultation with people and users.

The stages of the identity lifecycle might take place at different times and in various ways. For example, an identity may be authenticated through physical ID proofing (e.g., visiting the office) prior to issuing credentials, yet that resulting credential is used for remote interactions. On the other hand, documents can be presented and verified online (e.g., through video calls) but used for offline scenarios (e.g., boarding a plane).

Independently of the particular lifecycle, each phase is a fundamental part of digital identity. As a result, all of these phases must be considered in the design and implementation of digital identity systems.

**Figure 2**

Digital Identity Lifecycle



### Participants in Digital Identity Ecosystems

Digital identity ecosystems consist of multiple participants who can play different roles in various phases of the digital identity lifecycle. The same or different entities can take up these roles and are essential to understanding digital identity ecosystems. We identify three fundamental function-based roles in digital identity ecosystems.

Regarding entities receiving digital identity services, the term “user” is widely utilized. This refers to a real-life individual (or legal entity, depending on the digital identity’s subject) who has gone through the process of proving their identity, enrolling, getting credentials, and being authenticated by a digital identity system. The user can have different sub-roles, such as the “applicant,” who applies for a digital identity and provides supporting evidence until it is verified and an identity account is created. Once this happens, the applicant becomes a “subscriber,” who can then use authenticators to prove their identity. Lastly, a “claimant” is a subscriber who asserts ownership of their identity to an RP and seeks to have it verified using authentication protocols to obtain associated rights.

On the side of the entities providing digital identity services, the main role is the IdP, which manages a subscriber’s primary authentication credentials and issues assertions derived from credentials. Nevertheless, there can also exist different sub-roles that can be assumed or not within the same legal entity, such as the “identity verification service provider” that conducts the identity proofing (collection of data, validation, verification) or the “credential service provider” in charge of issuing authenticators and corresponding electronic credentials (binding the authenticators to the verified identity<sup>14</sup>) to users. The “registration authority” (or identity manager) is the entity that registers (enrolls) the applicant and its authenticators (credentials) after identity proofing. Finally, the “verifier” confirms the claimant’s identity to an RP by confirming the claimant’s possession and control of one or more authenticators using an authentication protocol<sup>15</sup>.

Digital identities can be presented to the issuing party or different parties from the ones that have issued them. The entity for whom the identification/authentication is performed (that receives the result of this process) is called RP or SP, a natural or legal

---

<sup>14</sup> The “credential service provider” is responsible for maintaining the subscriber’s identity credential and all associated enrolment data through the credential’s lifecycle and providing information about credential status to verifiers.

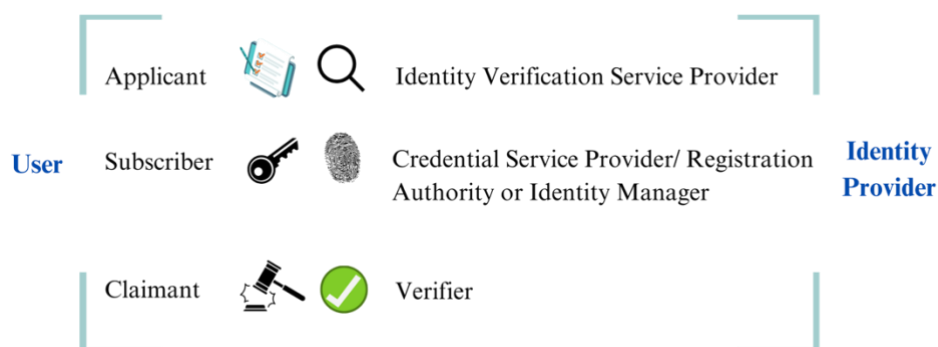
<sup>15</sup> The “verifier” confirms that the authenticators are valid by interacting with the credentials service provider. It might also need to confirm the link between the user and the authenticators in its possession.

person that relies on a subscriber’s credentials or authenticators or a verifier’s assertion of a claimant’s identity to identify the subscriber, using an authentication protocol. An RP relies on the results of an authentication protocol to establish confidence in the identity or attributes of a subscriber to establish a relationship or authorize access and associated rights and privileges with that identity.

In digital identity ecosystems, one or multiple legal entities can take on different roles. Currently, the IdP is responsible for providing most of the digital identity services; however, emerging digital identity ecosystems challenge this perspective, in some cases forcing and in others enabling these roles to be played by different legal entities, with the user holding a key role in interacting with all of them.

**Figure 3**

Participants in Digital Identity Ecosystems



### Digital Identity Ecosystems: eID Models

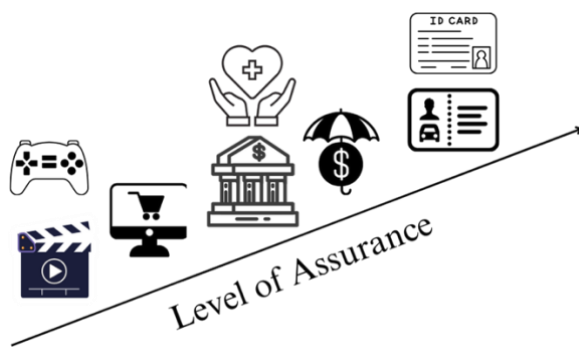
Digital identity ecosystems have evolved differently, driven by the specific requirements of their scope of application, the regulatory framework, or legal traditions in each State. In these ecosystems, it is essential to distinguish between the digital form of legal identity and other types of identities independent from it (e.g., a Facebook account). “Legal identity is understood to be the combination of factors that enable a person to access rights, benefits, and responsibilities; that is, the legal registration and documentation of name, personal data, date of birth, and unique identification, whether

in the form of biometric data or a unique identifying number” (Harbitz & Tamargo, 2009, p.1).

Nevertheless, the separation between the different types of identities in practice is not clear and becomes even cloudier in digital ecosystems. The “levels of assurance” are key in the interrelation of the different types of digital identities. Although this is a specific concept under EU Law (we will refer to it later in this thesis, abbreviated as LoAs), it is also generally used by the digital identity sector for referring to the required level of authenticity, accuracy, and veracity of the information provided during the ID proofing and the security in the authentication and management of an eID means<sup>16 17</sup>.

#### Figure 4

Levels of Assurance in the Access to Digital Services



Depending on the approach that States have taken for the provision of eID services, I suggest the identification of at least three types of eID models. These models vary depending on how the digital form of legal identities are provided and how these can be used across different services. While private providers of identification services have evolved consistently with the market needs, States have approached digitizing ID means in different ways. Some States have provided digital tools for identification. Some have

---

<sup>16</sup> The “levels of assurance” aim to address questions such as “Is the person who claims to be? Is this person a criminal? Is this person going to pay? Is this account stolen? Is this person eligible for this benefit?” among others and depending on the type of service.

<sup>17</sup> I would like to credit Mario Natella-Verschuren for the idea of representing the levels of assurance to digital services as an increasing line.



outsourced them, and some have taken an intermediary approach of allowing outside providers onto their territory under very strict governmental supervision.

Following this idea, at least three different models can be identified. In the “public model,” the government is the main source of identity verification and might collaborate with private providers to provide eID options. This is the model found in almost every European country, where ID cards typically include eID as an optional feature<sup>18</sup>.

In the “private model,” the government decides to rely on the private sector for the provision of electronic identification means that meet specific requirements. An example is the US, where the private sector offers credentials that meet the NIST SP 800-63 Digital Identity Guidelines standards to access federal websites.

Finally, the term “hybrid model” refers to a model whereby independent private solutions are recognized (accepted) by or developed jointly with the government in order to access certain public (and private) services. This model exists in Nordic countries, as is the case of Norway, Sweden, Finland, and Denmark. Thanks to the collaboration of major banks in these countries, strong Bank IDs have been developed, under which business opportunities are possible. These also benefit many other services besides banking itself<sup>19</sup>.

The reason why different identification systems exist is that States have differing views on the person who should provide digital identity services to allow citizens access to public services. Some States believe that these services should be exclusively provided by the public sector, while the private sector should rely on their own identification means. Some other countries have extended State-issued digital identity means to the private sector, and some have even relied upon or collaborated with the industry for the development of digital identification means to be used in public and private services.

---

<sup>18</sup> For example, it is the case of Belgium, Estonia, Latvia, Luxembourg Portugal or Spain, among many others.

<sup>19</sup> For example, in Norway, Bank ID can be used in many different scenarios, from virtual doctor’s visits, apartment rentals, car leasing, consumer platforms, or even naming a baby. In the case of Denmark, it can also be used in consumer platforms, consumer finance, car leasing, or accessing health records.

These choices reflect diverse cultures and traditions; however, as will be argued throughout this thesis, the forthcoming evolution of digital identity ecosystems may require them to merge under very specific regulatory conditions.

### **Embracing the Change: The Evolution of eID Models**

This thesis has been written at a time of drastic change from both technical and regulatory perspectives. This change is motivated by the strong limitations found in the current ecosystem and a desire to break away from outdated ways of thinking, institutions, and procedures that can be turned upside down with technological development.

We cannot foresee the progress of technology, and this is also true with respect to digital identity. Although digital identity is a prerequisite to the Internet's proper functioning<sup>20</sup>, it has been poorly regulated, and there has been no harmonized public-private approach toward digital identity. As a consequence, most of the existing eID models have been found to be limited in practice, and their deficiencies are becoming apparent.

In the face of this situation, the EU has put forward regulatory proposals to shift digital identity ecosystems. Therefore, regulations are not there only to correct problems, but these aim to effect a change in a whole ecosystem, implying not only new processes but even new players; a transition that is taking place in various parts of the world, primarily driven by technological advancements.

Nevertheless, with any change comes uncertainty. Making major changes can be particularly challenging during the development and implementation stages. We can already advance that, in the next digital identity ecosystems, one of the core features is a softer boundary between public and private sectors, aiming at a more comprehensive digital identity layer, which in turn could raise important political and regulatory

---

<sup>20</sup> I would even go so far as to say that it is essential for the functioning of all processes today because the digital sphere is not only formed by online (Internet-based) scenarios but could also take place through the simple connection of devices in local mode.

challenges, especially in those countries with deeply rooted governmental or public views on digital identity.

The current literature on regulations governing digital identity is scant, so we suggest starting this research by reviewing the situation and determining its shortcomings. It is also necessary to grasp the main regulation on digital identity in the EU, the eIDAS Regulation, and how various countries implement it. We will then present the update of the eIDAS Regulation, eIDAS2, in order to later take a critical view where we try to analyze the potential changes that can be motivated by it from the perspective of the role of the State or Public Law. More specifically, the fundamental question I am trying to answer in this thesis is whether the digital identity sector, which up to now has been fragmented and in many cases in the hands of private operators, requires some rethinking, in particular, to assess the need for a public form of guarantee behind it. I believe that this approach is in line with the latest regulation in this sector, eIDAS2, and this is why this thesis proposes to examine the consequences of including an obligation for Member States to provide EU citizens with at least one electronic identification means guaranteed by Member States that can be widely used and how this obligation can reconcile with the characteristics of the digital services market while simultaneously ensuring the rights and freedoms of citizens.

The next two chapters explain where we stand in a field that legal scholars have not explored thoroughly. However, this part is essential to provide an overview of the reasons for the change and key factors for it to be implemented effectively.



# CHAPTER I

---

## **FRAGMENTED DIGITAL IDENTITIES: ANALYZING DEFICIENCIES**

---

The regulation of identification and authentication processes has been an area insufficiently studied by legal scholars. The limited number of studies is probably due to the lack of a nuclear regulation for digital identity; instead, there exist “collateral regulations” that pertain to specific aspects of digital identity, such as data protection or cybersecurity, or regulations that only apply to processes occurring within a defined scope.

In the EU, the primary regulation governing digital identity is the eIDAS Regulation; however, in practice, it has been mainly limited to cross-border public services. On the other hand, there exist regulations concerning identification and authentication processes, but these only apply to certain areas, as could be the case of financial services. Meanwhile, privacy, data protection, and cybersecurity regulations apply broadly but do not provide enough guidance on these specific processes (i.e., in the digital identity scope).

Following the regulatory landscape, I suggest distinguishing three basic scopes for digital identity. First, digital identity processes in the public sector have been regulated by the eIDAS Regulation in the cross-border context, while at national level, the rules have usually been introduced by the applicable Administrative Law. Secondly, digital identity processes in the private sector have been largely unregulated and have been dependent on market demands and service needs. Thirdly, digital identity in financial services has been implemented by the financial industry independently from other sectors because of the special obligations and the convergence of public and private interests.

The lack of a comprehensive regulatory framework for digital identity services has shown significant drawbacks, chiefly in the private sector, where only a few entities have come to dominate the market for identification services and have provided users with weak safeguards for their rights and freedoms. Furthermore, adding the underlying technologies to the equation only worsens this situation, as current digital identity models have favored surveillance practices and created new possibilities for cybercrime.

This first chapter is dedicated to presenting the shortcomings of the current regulatory framework for identification and authentication processes in the scope of the EU. These limitations have resulted in fragmented identities and varying levels of protection for rights and freedoms depending on the use context. Additionally, the technologies employed have aggravated the problems, favoring surveillance and cybercrime, as well as the monopolization of these services by a reduced number of providers, which, added to the inadequate or insufficient regulatory response, reveal a pressing need for a paradigm change.

## **1. Mapping the Regulatory Landscape of Digital Identity in the EU**

### ***1.1. Exploring the Spectrum of Digital Identity Types within Regulatory Boundaries***

Digital identities can take on different forms and come from all kinds of sources, public or private. However, there is no clear regulatory framework for digital identity defining the types of digital identities that exist and how they are to be used. This has led to numerous regulations coming into effect, creating a complex and fragmented regulatory landscape for digital identities.

***1.1.1. Digital Identity in the Public Sector.*** The eIDAS Regulation has addressed identification and authentication processes at the EU level. At the moment of writing this thesis, the Proposal for Revision of the eIDAS Regulation has not yet come into force, and the references in this section pertain to the first version of the eIDAS Regulation.

Although the eIDAS Regulation is the main rule in the EU applying to these processes, it does not create a new electronic identification means, but instead, it facilitates cross-border recognition of existing national eIDs in the access, at least, to public services in other Member States.

To enable cross-border recognition, it establishes a set of common high-level rules or principles and technical standards, completed by technical specifications, allowing different national eID schemes in the EU to interoperate. More specifically, Article 6.1 of the eIDAS Regulation contains the requirements for mutual recognition of eID means, which refer, on the one hand, to notification requirements (i.e., Member States must notify the electronic identification means that must be included in the list published by the European Commission) and, on the other hand, to security requirements, (i.e., the electronic identification means must have an LoA equal to or higher than the one required for accessing a public service in the Member State, and at least be substantial according to the eIDAS Regulation).

Pursuing Recital 16 of the eIDAS Regulation, assurance levels “characterize the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is, in fact, the person to which the identity was assigned.” Nevertheless, although EU Law uses the term LoAs to refer to specific technical criteria, it is also a term generally used to determine the required level of confidence and security according to the risk of use of electronic identification in a specific service, and as such it can be found in other contexts or jurisdictions<sup>21</sup>.

---

<sup>21</sup> For example, the NIST uses the term Identity Assurance Level, defined as “a category that conveys the degree of confidence that a person’s claimed identity is their real identity, as defined in NIST SP 800-63-3 in terms of three levels: IAL 1 (Some confidence), IAL 2 (High confidence), IAL 3 (Very high confidence)”. NIST. (n.d.). *Identity Assurance Level (IAL)*. Computer Security Resource Center. Retrieved August 8, 2023 from [https://csrc.nist.gov/glossary/term/identity\\_assurance\\_level](https://csrc.nist.gov/glossary/term/identity_assurance_level). Another example is the case of Mastercard, which also uses the term Identity Assurance Profile in the frame of their proposal for a digital identity network to “represent the degree of assurance in the individual’s identity, based on the evidence types and the number and/or origin of sources used to verify the individual.” Mastercard. (2020). *Digital Identity: Our Service*. <https://idservice.com/content/dam/public/mastercardcom/idservice/pdf/digital-identity-our-service.pdf>

From the perspective of the eIDAS Regulation, the specific requirements for each LoA are contained in the Annex of the CIR (EU) 2015/1502. This legal text sets the elements or technical specifications and procedures to determine how the requirements and criteria of Article 8 of the eIDAS Regulation shall be applied. It distinguishes between enrolment and authentication phases and management tasks and envisages three LoAs: low, substantial, and high. In addition, the eIDAS Regulation also determines the minimum mandatory attributes<sup>22</sup> that shall be provided in cross-border identification and authentication processes under the eIDAS Regulation in Section 1 of the Annex of the CIR (EU) 2015/1501.

Consequently, the eIDAS Regulation does not constitute the legal basis for regulating electronic identification means but only for their mutual recognition between Member States, ensuring the mutual recognition of those electronic identification means complying with the requirements set out in Article 6.1, at least in access to public services. Electronic identification means not fulfilling the abovementioned requirements can still be used, but these will be subject to voluntary recognition by Member States.

Although notified electronic identification means can also be used in the scope of private services, mutual recognition is only guaranteed in relations between individuals and public sector bodies<sup>23</sup> (Article 6). In other words, only cross-border public sector bodies are mandated to accept notified electronic identification means under eIDAS; consequently, although the eIDAS Regulation aimed to encourage the use of notified eID means by private operators<sup>24</sup>, it has been limited in practice.

---

<sup>22</sup> Section 1 of the Annex to the CIR (EU) 2015/1501 imposes the obligation to use the following attributes for the identification of a natural person: a) Current family names; b) Current name; c) Date of birth and d) A unique identifier drawn up by the issuing Member State in accordance with the technical specifications for cross-border identification purposes and as persistent as possible over time. Likewise, the following additional attributes are authorized: a) Name or family name at birth; b) Place of birth; c) Current address; and d) Gender.

<sup>23</sup> In accordance with Article 3 (7) of the eIDAS Regulation, public sector bodies are defined as “a state, regional or local authority, a body governed by public law or in association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such mandate.”

<sup>24</sup> For example, in this sense, Recital 17 of the eIDAS Regulation.



However, it is important to recall that, as mentioned above, the eIDAS Regulation only applies to cross-border identification processes; therefore, at the national level, the electronic identification of citizens in their relations with public sector bodies must be regulated by national law, usually by Administrative Law. In this regard, we have a clear example in Spanish Administrative Law, which establishes the accepted electronic identification means in their relations with Public Administrations in Article 9 of the *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*.

**1.1.2. Digital Identity in the Private Sector.** The private sector's digital identity services (e.g., login with Facebook, Google, or Amazon, but also any other digital identity service provided by a private entity) have been characterized in the EU for the absence of specific references to them in regulations governing “digital services.” Although the specific delimitations with the eIDAS Regulation will be discussed in more detail in the second chapter of this thesis, there exist complexities in placing digital identity services provided by private entities under a concrete regulatory framework.

In my opinion, the main discussion on this point could be whether digital identity services fall within the scope of ISS and, consequently, the applicable regulations thereof. The term ISS was first introduced by the Directive 2000/31/EC or e-Commerce Directive, whose main motivation was “the development of information society, ensure legal certainty and consumer confidence through the coordination of national laws, and clarify legal concepts for the proper functioning of the internal market, to create a legal framework to ensure free movement of Information Society Services between Member States” (Baistrocchi, 2003, p.112). The e-Commerce Directive has recently been replaced by the DSA, which, apart from important innovations that we will not discuss in this thesis, maintains the focus on ISS.

The ISSs are defined by the DSA (by reference to the Directive (EU) 2015/1353) as “any service normally provided for remuneration, at a distance, by electronic means at the individual request of a recipient of a service.” Although, at first sight, digital identity

services could fit into this definition, the requirement for remuneration<sup>25</sup> raises some challenges, particularly for those providers whose only source of revenue is user data. Although we will not go deeper into this point because it could lead to an entirely new topic, it is worth noting that the qualification of data as a form of remuneration depends on whether it exceeds the needs for the provision of the services or are used for different purposes (Arroyo Amayuelas, 2022, p.25). In the scope discussed, the boundary is particularly thin, notably because even if the provided data are not used in a “strict sense” for other purposes, these will enable surveillance and the advantage gained by the digital identity service provider from the mere possibility to “observe” exceeds the data provision's initial purpose and could thus, in my opinion, be seen as a form of remuneration<sup>26</sup>. Yet, as noted, this is an entirely new topic that would require dedicated consideration, particularly because the qualification of data as remuneration would trigger the application of the contractual regime<sup>27</sup>.

On the other hand, the e-Commerce Directive provided three liability exemptions in Articles 12 to 15, now abrogated and covered by the DSA as “intermediary services.” However, we argue that identification and authentication services are not covered by this concept, considering that the digital identity service provider takes an active role in transmitting data for a specific purpose, delineated by their terms and conditions for digital identity services.

Apart from the challenges in defining its scope, services under the e-Commerce Directive presented important limitations. Notably, the Directive lacked explicit references to digital identity services, and this lack of references has been maintained in the DSA. Consequently, although the eCommerce Directive, or now, the DSA, might

---

<sup>25</sup> The requirement of remuneration has been interpreted in a broad sense, as in the emblematic *Pasavva* case, where it was accepted that advertising revenue could be considered remuneration.

<sup>26</sup> For example, consider the potential revenues that can be subsequently obtained from personalised advertisement.

<sup>27</sup> As Prof.Dr.María del Carmen Plana Arnaldos pointed out in a personal discussion, the application of the contractual regime would imply the possibility of requesting certain "service levels" in the provision of identification services, as well as the termination of the contract and the return of the data provided. I recommend reading in this regard: Plana Arnaldos, M.C. (2021). Economía de los datos y propiedad sobre los datos. *Revista de educación y derecho*, (24). <https://dialnet.unirioja.es/servlet/articulo?codigo=8103852>

apply to private digital identity services falling under the definition of ISS, the effectiveness of these regarding digital identity services is limited<sup>28</sup>. As a result, the provision of these services ultimately relies upon bilateral or multilateral agreements<sup>29</sup> between the digital identity services provider and the website or service, determining which resources can be accessed using a concrete digital identity.

In exceptional cases, some national regulations, such as in France, the *Code des postes et des communications électroniques* have introduced rules for electronic identification means provided by private sector providers. This is the case of Article L102 of this Code, which recognizes the possibility of the provision of electronic identification services by private entities, provided they fulfill the required level of assurance or guarantees according to the *Agence Nationale de la sécurité des systèmes information*, and these are accepted in the private sector sphere, as it is the case of financial services.

**1.1.3. Digital Identity in Financial Services.** Digital identity in financial services has been subject to its own particularities, given, on the one hand, the specific requirements imposed by the law when performing identification and authentication processes in their scope and, on the other hand, the liability burden for these entities. Consequently, it is a sector that has tended to develop its own digital identification and authentication procedures.

Digital identity in the financial sector has been mainly observed from two perspectives: digital onboarding (e.g., to open a bank account) and payment authentication. The first has been mainly covered by the AML Directives, while the second aspect is regulated by the Payment Services Directives.

---

<sup>28</sup> Some countries, like France, have their “digital laws,” such as the *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*, but they are not comprehensive in the scope discussed either.

<sup>29</sup> In most cases, it is not a traditional contractual agreement; instead, digital services integrate this identification means as a “tool,” accepting the terms and conditions established by the provider. In this sense, for example, Facebook provides an extensive guideline named Meta for Developers. Meta for Developers. (n.d.). *Facebook Login*. Facebook. Retrieved August 8, 2023 from <https://developers.facebook.com/docs/facebook-login/>

AML Directives refer to a set of regulatory requirements aiming to combat money laundering and terrorist financing by Member States. For that purpose, these turn efforts into a specific set of institutions called obliged entities<sup>30</sup>, among whose responsibilities is CDD, part of the KYC principle. According to Cox, “KYC is essentially the work conducted by a firm to undertake background checks on clients and customers to enable the firm to obtain and confirm additional information regarding its customers” (Cox, 2014, as cited in Lucas da Silva, 2022, p.10).

The fourth AML Directive included specific references to identification obligations in the scope of CDD<sup>31</sup>. Nevertheless, it is important to note that the KYC requirement goes beyond user identification and includes the verification of other data, such as the beneficial owner of an account or assessment of the purpose of the business relationship, among others. Yet, it is particularly noteworthy that the fifth AML Directive opened the door to the use of eIDAS-notified schemes and trust services as the base of KYC processes<sup>32</sup>. It is also possible that a given KYC scheme may allow placing an eIDAS-compliant scheme on top of it, as is the case of Bank ID in the Nordics. However, again, this convergence would not be absolute as the eIDAS minimum data set will just cover part of the identification needs in a KYC process, which demands examining additional attributes<sup>33</sup> from a dynamic perspective (i.e., during the time the legal relationship exists).

From the perspective of payments, the focus has been on the authorization process of electronic transactions, and therefore, in determining whether a transaction was

---

<sup>30</sup> The list of obliged entities includes institutions engaged in certain business activities that represent a higher risk of being misused for money laundering.

<sup>31</sup> Article 13 establishes that CDD shall comprise “identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source.”

<sup>32</sup> Article 13 letter a “identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust serviced as set out in Regulation (EU) No 910/2014 or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by relevant national authorities.” Other specific references can be found in Article 27.2, Article 40.1, or Recital 22.

<sup>33</sup> For natural persons, other attributes shall be studied, such as the consideration of politically exposed persons, tax address, or the source of funds. For legal entities, it is essential to identify the ultimate beneficial owner, source of funds, or legal name.

authorized, customer authentication becomes essential for discharging the liability of PSPs. The regulation of electronic payments has been one of the EU's key priorities, and the first version of the Payment Services Directive was adopted in 2007 but presented several deficiencies<sup>34</sup> and was replaced by the PSD2 in 2015.

PSD2 applies to PSPs, "an entity that provides payment services." The primary purpose of PSD2 was to create a uniform legal framework for payment services across the EU, but it also achieved other objectives, such as enhancing the security and consumer position in payments where a "high risk" of fraud exists. One of the measures in enhancing security and consumer position was precisely the introduction of the SCA requirement (Article 97). SCA is defined as the use of an authentication process based on two or more factors from different categories of knowledge, possession, and inherence. These elements must be independent so that the breach of one of them does not compromise the reliability of the other, and the authentication must be designed in such a way as to protect the confidentiality of the data (Article 4 (30)). SCA is required when the payer accesses its payment account online, initiates an electronic payment transaction, or carries out any action through a remote channel that may imply a risk of payment fraud or other abuses<sup>35</sup>.

The definition of SCA has been the subject of several works, particularly by the EBA with the development of RTS. The CDR (EU) 2018/389 introduced important requirements, such as the obligation to generate authentication codes to establish a dynamic link<sup>36</sup>. However, there is no closed list of SCA-compliant methods, but the EBA has opted for a model of high-level rules that leave a certain margin of freedom to the affected subjects by the Directive for its further clarification<sup>37</sup>.

---

<sup>34</sup> The first Payment Service Directive already presented several deficiencies. By way of example, it required that both the payer's and the payee's services were located within the EU.

<sup>35</sup> The specific actions requiring SCA are delineated in the Directive as well as in the RTS, although these are expected to be subject to review according to the published text of the Commission's Proposal for a Payment Services Regulation.

<sup>36</sup> So as to make the user aware at all times of the amount being authorized and the payee of the transaction the user is authorizing.

<sup>37</sup> Nevertheless, it should be taken into account that the EBA's Opinion of the 21st of June 2019 clarifies the specific requirements that authentication factors shall fulfill in their respective categories.

In conclusion, it can be said that digital identity expressions in the scope of financial services are usually deployed in-house or rely on external specialized companies via contractual agreements<sup>38</sup>. The interaction with public sector eID means, such as those notified under eIDAS, is limited<sup>39</sup> and mainly found in Nordic countries. On the other hand, interaction with privately issued eID means varies depending on the country, but at least it can be said that those provided by Big Techs are generally not accepted since these cannot provide enough assurance to fulfill legal requirements (e.g., using a Facebook login to open a bank account). However, concerning this last point, the tendency to leverage digital wallets in payment authentication (e.g., type Apple Pay) has also been observed, an aspect that will be reconsidered later in this thesis in the scope of the EUDI Wallet.

**Table 1**

Regulatory Frameworks and Sector-Specific Digital Identities

Public Sector	Digital identities typically issued by governments (e.g., national electronic identity documents, Cl@ve, FranceConnect, etc.) to be used within public services and residually in private services. These are regulated by European and/ or national regulations.
Private Sector	Digital identities issued by digital platforms (e.g., login with Facebook, Google, or Amazon, etc.) or other private providers of identity services, normally to be used within private online services. These usually lack dedicated regulations and rely on contractual agreements to determine their functioning and reliance.
Financial Sector	Digital identities typically issued by financial services (e.g., bank credentials, payment credentials or customer digital account) to be used within their financial services. The design of these identities is framed by specific regulations in the financial sector. In some cases, there is an interaction with digital identities provided by the public and private sectors.

---

<sup>38</sup> For example, Onfido, among many other companies, provides these services.

<sup>39</sup> These are mainly used for the purpose of ID proofing during onboarding processes, but once these have concluded, the financial services issue their own credentials.

## ***1.2. Privacy and Cybersecurity as Fundamental Pillars of Digital Identity***

Besides the specifics associated with the different “digital identity types” presented in the previous section, I have identified two common pillars or dimensions that are applicable to the majority of identification and authentication processes: privacy and cybersecurity. Protecting privacy is key for a natural person's digital identity, notably within the EU, where the GDPR applies. However, existing literature has not explicitly addressed the manifestations or dimensions of privacy and data protection regulations within this field. On the other hand, cybersecurity stands as a critical element for successful digital processes and also plays a crucial role in protecting privacy.

***1.2.1. Privacy Considerations in Digital Identity Processes.*** In the course of digital identification and authentication, personal data is usually<sup>40</sup> processed through a series of data flows. Data processing activities<sup>41</sup> taking place during identification and authentication processes concern the different subjects and entities participating in the ecosystem and materialize in concrete measures, technologies, and obligations.

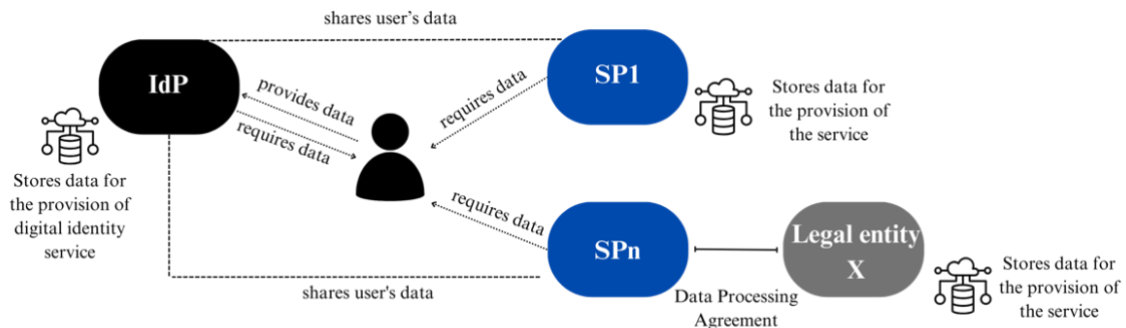
---

<sup>40</sup> Identification and authentication processes that only refer to “things” might not trigger direct privacy concerns. Yet, an analysis of the potential implications of privacy and data protection is always recommended, as suggested in Annex C.

<sup>41</sup> The application of the GDPR is subject to the processing of personal data. Personal data, as defined in Article 4 (1) of the GDPR, means “any information relating to an identified or identifiable individual. An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” On the other hand, data processing is defined in Article 4 (2) of the GDPR as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.” Therefore, almost any form of management of data that could potentially identify a natural person falls in the scope of processing personal data.

**Figure 5**

Examples of Data Processing Activities in Identification and Authentication Processes



*Note.* The user will be asked to provide personal information by the IdP and usually by the SPs to verify their eligibility for the services provided by the SPs. The IdP shares the user's information with the SPs in the provision of identification and authentication services.

We have divided this section into the following subsections to offer a systematic view of the main privacy components that affect digital identity services.

**1.2.1.1. User Awareness.** Identification and authentication processes usually involve the disclosure of personal data to different parties. Typically, the disclosure will take place to RPs who need to “confirm” certain personal data about an individual for the provision of their services, but it can also refer to the IdPs who ultimately act as a SP of identity services. Before performing any of these processes, the user must understand the implications of the processing.

From the perspective of user awareness, general obligations apply<sup>42</sup>. Personal data must be processed according to any of the legal basis established in Article 6 of the GDPR, and the user shall be able to recognize that legal basis. When the legal basis for the processing of personal data is consent, this shall meet the conditions set out in Article 7; that is, the information must be clear and distinguishable, and users shall be aware of their right to withdraw their consent at any time.

---

<sup>42</sup> Pursuing Article 5.1. letter a GDPR, “personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.”



On the other hand, general information obligations apply (Articles 12, 13<sup>43</sup>, 15–22, and 34 GDPR) requiring transmitting the data subject information relating to the processing in a concise, transparent, and easily accessible form, using clear and plain language. Such obligations relate to the so-called privacy notice<sup>44</sup> as a crucial instrument to explain the purposes, categories of data processed, period of retention, and data subject rights, among other key data processing elements.

Likewise, GDPR rights apply<sup>45</sup>, and pursuing Article 30 GDPR, each controller shall maintain a record of processing activities under their responsibility, containing the information included in the cited Article<sup>46</sup>.

While essential, current obligations do not fully guarantee user awareness in the scope of digital identity services. As a result, potential alternatives like the "authorization" or "permission" model or user-traceability mechanisms are being considered in upcoming regulations, specifically in the context of eIDAS2, as will be presented later in this thesis.

**1.2.1.2. Secure Data Storage.** During identification and authentication processes, personal data is shared and normally stored by the different parties participating in the ecosystem (i.e., users, RPs, or IdPs) in external or device-based resources. Either way, it requires the adoption of security measures.

---

<sup>43</sup> Pursuing Article 13 GDPR the controller shall provide the data subject with a) The identity and contact details of the controller or its representative; b) The contact details of the data protection office, where applicable; c) Purposes and legal basis for the processing; d) Legitimate interest when it is the legal basis for the processing; e) Recipients or categories of recipients of personal data, if any; f) Data transfers and related measures, when applicable; g) Data subject GDPR rights; h) Right to lodge a complaint; i) Consequences of failure to provide the personal data when the processing is based on a statutory or contractual requirement; j) Existence and logic involved in automated decision-making and envisaged consequences for such processing.

<sup>44</sup> A privacy notice is a public document from an organization that explains how that organization processes personal data and how it applies data protection principles pursuing Articles 12,13 and 14 of the GDPR.

<sup>45</sup> The right of access (Article 15), the right of rectification (Article 16), the right to erasure (Article 17), or when applicable, the right to restrict the processing (Article 18), or the right to data portability (Article 20).

<sup>46</sup> Name and contact details of the controller, the purposes of the processing, description of categories of data subjects and personal data, among other data.

Article 32 of the GDPR mandates the adoption of technical and organizational measures to ensure a level of security appropriate to the risk<sup>47</sup>. Risk management is necessary to determine the potential damages or risks to which an activity is exposed. Each risk source materializes on threats of likelihood and impact variables.

Understanding the relationship between security and privacy can be complex. While a security risk may also involve a privacy risk, they are not always interconnected. When considering an attack that affects security, to determine whether it also affects privacy, three dimensions are of interest: the integrity of the data, the confidentiality of the data, or the authenticity of users and information. Attacks that compromise the security of the processing may not necessarily result in a privacy breach, but they can affect other aspects, like the availability of the service.

A simple and effective measure to ensure the security of personal data is to refrain from requesting unnecessary data or data that, given their high risk, does not seem proportionate according to existing guidelines<sup>48</sup>. This point is clearly linked to the special categories of personal data mentioned in Article 9 of the GDPR, whose processing is prohibited unless specific conditions are met.

Such concern can be adopted from the perspective of external storage, so controllers/processors could only ask for these data when any of the specific causes included in Article 9 are met and higher security measures are adopted. Nevertheless, Article 9 of the GDPR does not impose any concrete enhanced security measures, which

---

<sup>47</sup> Article 32 GDPR “taking into account state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk”. Other obligations concerning security can be found, such as the notification of a personal data breach to the supervisory authority (Article 33) or the communication of a personal data breach to the data subject (Article 34).

<sup>48</sup> The Spanish Data Protection Agency provides criteria to determine the proportionality of the data processing, such as the limitations for rights and freedoms, the respect of the right's essence, judgment of purpose, suitability, and necessity, and judgment of proportionality in the strict sense.

are left to national legislation pursuing Article 9.4<sup>49</sup>. In addition, it must be noted that the processing of these specific categories of personal data not only takes place “externally” but, notably, in recent years, has been characterized by the use of device-based biometrics.

Biometric identification and authentication might be the most common use cases involving special categories of personal data in the scope of digital identity processes. Pursuing Article 9 of the GDPR, the processing of biometric data of natural persons is included among the special categories of personal data<sup>50</sup>; however, not all processes involving biometric data imply the processing of special categories of personal data. According to the Report 0036/2020 of the Spanish Data Protection Agency, which analyzed the processing of biometric data in the context of facial recognition for identity verification and control in online exams, concluded that when biometric data are used for authentication purposes only and not for comparison and identification by third parties, it shall not be considered as the processing of special categories of personal data. For this conclusion, the Report considered the European Commission's White Paper on Artificial Intelligence, as well as A29 WP Opinion 3/2012 on developments in biometrics technologies, adopting a distinction between biometric identification as the process of comparison of biometric data with templates or data stored in a database (search of correspondence), and biometric authentication, as the process of comparison of biometric data with a single biometric template stored in a device, which is not considered as the processing of special categories of personal data.

This conclusion is, in my opinion, at least debatable as the nature of biometric data and the high risk in the event that these data get compromised still exist<sup>51</sup>. Therefore, I would still suggest carefully studying their implementation possibilities, limiting them to

---

<sup>49</sup> For example, in the case of Spain, the Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de derechos digitales in Article 9.2 mandates that a regulation with the status of law is needed for the processing of personal data pursuing letters g), h) and i) Article 9.2 GDPR.

<sup>50</sup> Which leads to concrete obligations, such as conducting a DPIA pursuing Recital 84 and Article 35 GDPR.

<sup>51</sup> Group-IB researchers recently released a report about a new Trojan capable of collecting facial recognition data. Group-IB. (2024, February 15). *Face Off*. <https://www.group-ib.com/blog/goldfactory-ios-trojan/>

scenarios where these are strictly necessary, leveraging and maximizing the device security, and recurring, when possible, to techniques such as homomorphic encryption<sup>52</sup> or other advancements that might emerge in the coming years.

**1.2.1.3. Cryptographic Functions for User Control.** The performance of identification and authentication processes involves the disclosure of personal data by the user. When collecting personal data, the principle of data minimization (Article 5.1 letter c of the GDPR) requires personal data to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed and kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which personal data are processed (Article 5.1 letter e of the GDPR).

To comply with their obligations, SPs must request only the necessary data and for a limited time period to deliver their services. However, from the perspective of user control, it also means that the user can choose to share only the necessary data for the service to be provided. Compliance with this requirement can be met through several techniques, such as selective disclosure or, when possible, zero-knowledge proofs<sup>53</sup>. Furthermore, it connects with other possibilities, such as pseudonymous authentication<sup>54</sup> (Articles 6.4 letter e or Article 25.1 GDPR, among others) or even anonymous authentication<sup>55</sup>, which would not fall in the category of personal data pursuing Recital 26 of the GDPR.

Furthermore, compliance with the abovementioned principles requires data to be stored for the necessary term. This involves, on the one hand, RPs retention policies, but, on

---

<sup>52</sup> Homomorphic encryption is a cryptographic method that enables mathematical operations to be conducted on encrypted data without needing first to decrypt it. This technique preserves privacy while still allowing data analysis and processing.

<sup>53</sup> A zero-knowledge proof is a mathematical protocol that generates an assertion that certain information is true or false without revealing the exact data. For example, Mark is 25 years old. A zero-knowledge proof of that data will be that Mark is over 18 years old.

<sup>54</sup> I would identify it as the process through which some type of consistent identifier is used, but the real identity is not disclosed (e.g., instead of Peter, it is user123).

<sup>55</sup> I would identify it as the process through which certain information related to an individual's identity is confirmed, but no identifier is presented. We could think of the case of the Covid Passport. However, in practice, these use cases are limited since they could cause detriment of users' rights.

the other hand, from the perspective of user control, the possibility to generate one-time attestations that make that storage technically impossible, or, if this cannot be avoided, the possibility to request the deletion of such data and mechanisms to control that it effectively takes place.

In addition, given the risks raised by surveillance practices, it is also key from this dimension the possibility for users to hide their activity and prevent traceability, a topic that will be explained in more detail when referring to underlying technical models in current digital identity ecosystems, as well as in the next chapters of this thesis.

Consequently, the main purpose of this subsection was to highlight that although all of these techniques align with GDPR principles, the lack of explicit provisions and the uncertain regulatory implications, at least for some of them (e.g., anonymous authentication), has led to poor practical implementation to date, which demanded concrete regulatory changes.

***1.2.2. Cybersecurity Considerations in Digital Identity Processes.*** Cybersecurity is another critical component in digital identity processes and services and one of the key priorities of the EU. In the words of Commissioner Mariya Gabriel (reproduced in Vandystadt & Waldstein, 2018, p.1), “enhancing Europe's cybersecurity and increasing the trust of citizens and businesses in the digital society is a top priority for the European Union.” Furthermore, despite it being closely linked with protecting privacy, cybersecurity involves more than just data breaches and comprises other types of attacks that might affect the overall quality and functioning of the service.

Although I will not delve too deeply into this topic, I think it is important to at least mention that at the EU level, there are two essential regulations concerning cybersecurity. On the one hand, the NIS Directive has focused on imposing a set of cybersecurity obligations on the basis of the essential or critical nature of the service provided by obliged entities or, more broadly, specific sectors. On the other hand, the Cybersecurity Act focuses on the provision of a European framework for the certification of cybersecurity products, processes, and services.

Regarding the first one, the NIS Directive was the first horizontal legislation at the EU level for the protection of network and information systems. The first version entered into force in August 2016, with a deadline for national transposition in May 2018, and distinguished two categories of undertakings: OESs and DSPs. The OES category included public and private entities in specific sectors that fulfilled the criteria listed in Article 5.2<sup>56</sup>. Member States needed to identify and draw up a list of OESs that will be reviewed periodically by the individual Member States and the European Council. To ensure that all Member States follow a common approach for identifying OES, a list of each sector, subsector, and type of entity was provided in Annex II to serve as a roadmap in the identification process. On the other hand, the NIS Directive imposed security and incident notification obligations to a second category of undertakings, the DSPs. These include any legal person providing a digital service in the scope of at least one of the three defined categories in Annex III: online marketplace, online search engine, or a cloud computing service.

At the present time, the second version (NIS2) has already entered into force with a deadline for transposition in October of this year. This distinction is not maintained by the NIS2 Directive, which considers it to be obsolete (Recital 6) and instead identifies essential and important entities pursuing sectors listed in Annexes I and II<sup>57</sup>.

However, in both versions, conclusions are similar with regard to identification services, with some exceptions. In principle, digital identity services are not observed per se as a sector of high criticality obliged by the NIS Directive; therefore, an entity providing digital identity services would only fall in the scope of the Directive insofar

---

<sup>56</sup> a) An entity that provides a service which is essential for the maintenance of critical societal and/or economic activities; b) The provision of that service depends on network and information systems; c) An incident would have significant disruptive effects on the provision of the service. The directive defines an incident as critical when the continuity of the provided operations and services are negatively affected and general criteria are provided in Article 6.1 to distinguish critical incidents (the number of users, dependency of other sectors, impact, in terms of degree and duration, market share, geographic spread...). Further to these general criteria, Member States should define sector-specific factors.

<sup>57</sup> Annex I includes sectors of high criticality: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), Public Administration, and space. Annex II lists other critical sectors: postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing, digital providers, and research.

as it also provides any of the services covered by it (e.g., banking or health sectors, Public Administration, digital providers...). However, it is important to note that, concerning the topic discussed in this thesis, although the NIS2 Directive does not explicitly refer to identification services, it does include trust services<sup>58</sup>, a provision that will have significant implications when connected to eIDAS2. Furthermore, the second version of the Directive also recognizes social networking platform providers as important entities, leading to the inclusion of the digital identity services they offer (i.e., login with Facebook).

On the other hand, the EU Cybersecurity Act entered into force in June 2019 and applies from June 2021. The Act has two main purposes: allocating a permanent mandate to ENISA and establishing a European cybersecurity certification framework for ICT products, services, and processes with the aim of maintaining trust as well as security. Although the Cybersecurity Act does not include a specific certification regime for digital identities, it includes some mentions to ENISA's role in promoting and supporting the Union policy on electronic identity as well as trust services (Article 5.5 letter a). Furthermore, the Act provides for certification schemes in individual sectors within the European Cybersecurity Certification Framework, and there is an interaction between it and the eIDAS2 Regulation, as will be explained later.

Nevertheless, the conclusion at this moment is that, from a regulatory perspective, the relationship between cybersecurity and digital identity in both cases (NIS Directives and the Cybersecurity Act) has been rather roundabout. Yet, as the importance of digital identity is catching on in the cybersecurity field, it is expected that stricter cybersecurity requirements will be increasingly demanded in the provision of these services, particularly in the advancements toward cross-sectorial and “more integrated” digital identity solutions, something already noticeable in the updates made in NIS2.

---

<sup>58</sup> In this thesis, we use the terms "trust services" and "trust services providers" interchangeably.

## **2. The Era of Federated Digital Identity: Challenges from a Regulatory Perspective**

### ***2.1. Federated Digital Identity***

For digital identities to function, they must exist within a technical framework; that is to say, they must be managed. Identity management is concerned with the lifecycle of digital identities. Following the definition given by L. Rosner (2014, p.92):

Identity management is an operational and technical framework that defines and administers the lifecycle, use, and security of digital identities. Authentication and the management of credentials are key focuses of identity management systems. They are transactional and operated by organizations.

Identity management remains a challenge in the field of information security and privacy, as well as usability and user experience, authentication methods, trust, and reputation management, among others. To date, the prevalent model for digital identity in the private and public sectors has been federated digital identity. Nevertheless, other models have also existed, notably depending on the specifics of the sector and the number of services targeted.

***2.1.1. Evolution of Digital Identity Models.*** Managing digital identities is complex and requires balancing different values. Traditionally, digital identity systems were designed to be used internally within organizations and companies (silo model). In this model, digital identities enable to interact with the entity that provides them, and identification services operate as an “in-house service.” This model has not disappeared and is still common in the case of financial services, which usually rely on their own identification systems.

The increasing number of processes in a context of identity fragmentation (the users were obliged to have several accounts for each SP) evidenced the limitations attached to this model and led to the configuration of digital identity as a service. The evolution of digital identity as a service resulted in delegated or outsourced digital identities, which enable users to interact with organizations or entities different from the ones that



provide them. In this scenario, there exist separate legal entities whose relations might have a statutory<sup>59</sup> or contractual basis.

The configuration of digital identity as a service ended by favoring the creation of federations and the emergence of federated digital identity. In federated digital identity, the user can access different services using a single accreditation. Although this model stands out for its user convenience and interoperability, it also raises problems in terms of security and privacy. More specifically, there is a clear tension between user convenience and privacy because, although this type of model relieves the user from repeating enrolment processes in different entities, the ecosystem it creates enables large-scale sharing of personal data and grants IdPs control over user access to digital services by using their electronic identification means.

These tensions remain unresolved and vary or change in each specific context where this digital identity model is deployed. Examples can be found in Mastercard's proposal for a "Global Digital Identity Network"<sup>60</sup> or in the case of eHealth systems<sup>61</sup>. In both cases, digital identity faces conflicting forces of interoperability, privacy, and security.

Over the last several years, a shift toward the emergence of new ecosystems has been observed. The first attempts move from network-based digital identity systems to claim-based digital identity systems. In the first scenario, the IdP gives the user an identification/authentication token, which they then pass on to the RP. The RP then verifies the authenticity and validity of the token with the IdP. In the second model, the

---

<sup>59</sup> It could be for example the case of the identity federation regulated by eIDAS, in which each Member State acts as an IdP but also admits and recognizes other Member States as IdPs.

<sup>60</sup> Mastercard ID Services is an initiative that aims to create a new digital identity ecosystem with Mastercard at the center. It develops a new governance model that connects the different stakeholders in the industry (Users, Trust Providers, Identity Verification Providers, and Relying Parties) and enforces a set of rules and standards for them to follow, enabling potentially "global" interoperable digital identity ecosystems. Mastercard. (n.d.). *Digital Identity Services*. Mastercard. Retrieved August 9, 2023 from <https://idservice.com/en/home.html>

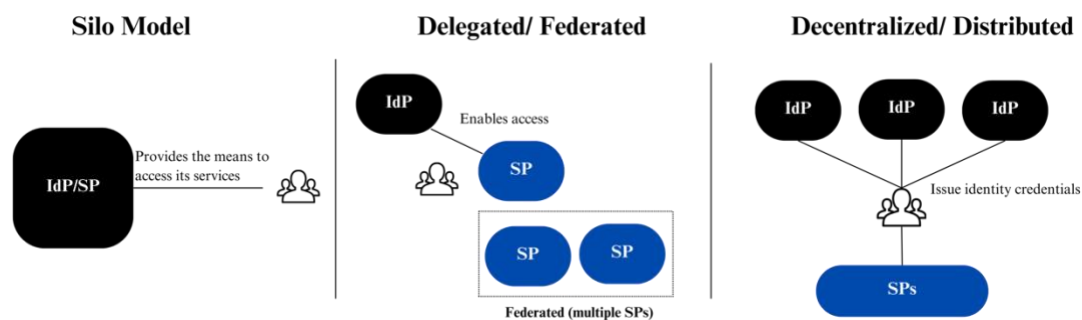
<sup>61</sup> As Halperin & Backhouse (2008, p.74) note, sharing data between healthcare systems (within the same country or across different countries) will enable doctors in different locations to access the data and know, for example, patients' needed treatment from different locations, security breaches in this area would have significant privacy consequences.

user manages claims issued by the IdPs and shares them with the RP, who can verify them without connecting to the IdP.

However, insofar as there is a single IdP we will be in a delegated form of digital identity. This traditional approach of having a single entity that assumes the role of IdP is being challenged by decentralized ecosystems, where different entities take on the task of the IdP, resulting in a distribution of power. There are various ways of implementing this ecosystem and possible degrees of decentralization that will be analyzed in more detail in the third chapter of this thesis.

**Figure 6**

### Evolution in Digital Identity Models



**2.1.2. Foundations of Federated Digital Identity.** Federated digital identity refers to a model that enables cooperation among the collaborating entities, i.e., IdPs and SPs or RPs, on identity processes and technologies. In this model, user identities are federated at a central location, and the IdP is responsible for managing the user’s identity-relevant information and normally passing authentication tokens to the RPs.

In federated digital identity, a relationship of trust is established between the IdP and the respective SPs that will accept the IdP’s confirmation of user identity. From a legal perspective, when the relationship of trust is not established on a statutory basis (e.g., the eIDAS Regulation), it will require the signature of multiple bilateral agreements or a multilateral agreement between the IdPs and SPs.

From a technical perspective, the first federated protocol was Microsoft Passport, which was not published but guessable from existing publications. Nevertheless, the prime standards in support of federated digital identity have been SAML<sup>62</sup> and Open ID<sup>63</sup> (Open ID Connect protocol nowadays). Both serve as protocols for exchanging authentication and authorization data between IdPs and SPs. They also enable SSO and are frequently used in scenarios involving federated identity, where a user's digital identity and rights are stored across multiple separate digital identity systems.

Federated digital identity ecosystems can take various forms, but they all share a common principle: IdPs must verify a user's identity to RPs. Therefore, it is a limited form of digital identity that relies on third parties. Besides, we can conclude that at least three common features are identified in federated digital identity ecosystems. Firstly, there is a trusted relationship between at least one IdP and multiple SPs. Secondly, users can access multiple services using the same credentials. Lastly, the IdP manages the user's identity information and attributes when they authenticate to an SP.

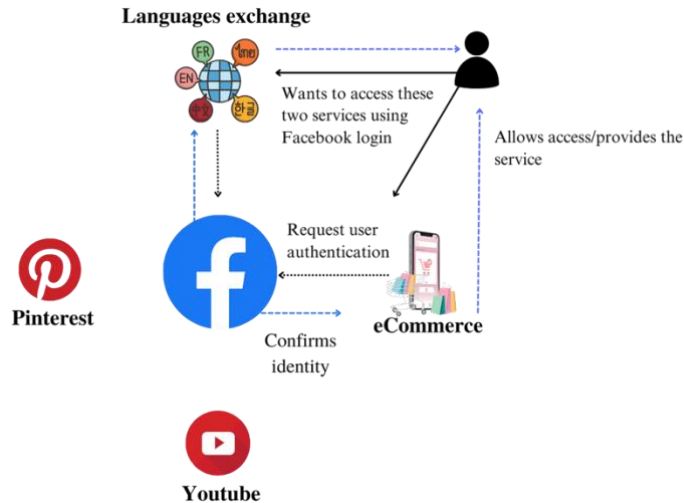
---

<sup>62</sup> SAML is an open XML-based standard for exchanging authentication and authorization data between security domains. SAML 2.0. gives the user the possibility to have authentication and sign-on on Internet-based services and e-commerce applications, using a network or a domain once from any device and then applying to different web services from multiple websites (SSO). In this approach, user authentication is requested just once at the login. SAML assumes that the user has been enrolled with at least one IdP in charge of providing local authentication to the user itself. See, among others, Pfitzmann, B. & Waidner, M. (2005). Federated Identity-Management Protocols. In Christianson, B., B. Crispo, B., Malcolm, J.A., & Roe, M. (Eds.), *Security Protocols 2003* (pp. 153-174). Springer. [https://doi.org/10.1007/11542322\\_20](https://doi.org/10.1007/11542322_20)

<sup>63</sup> OpenID is an authentication protocol (built on top of OAuth 2.0) that allows the user to have a unique username even for different websites, allowing an easier way to have online transactions on an Internet scale. In 2014 OpenID Connect emerges as the latest protocol supported by large companies like Amazon, Google, Microsoft and PayPal. In 2015 Google announced that developers should abandon the preceding protocol, OpenID 2.0 (OpenID) and recommended switching to its OAuth 2.0 (OAuth) based successor OpenID Connect. Central to Open ID Connect is a cryptographically signed document, the ID token. It is created by the user's IdP and serves as a one-time proof of the user's identity to the RP. See, among others Mainka, C., Mladenov, V., Schwenk, J., & Wich, T. (2017). SoK: Single Sign-On Security - An Evaluation of OpenID Connect, *Proceedings - 2nd IEEE European Symposium on Security and Privacy*, 251-266. <https://doi.org/10.1109/EuroSP.2017.32>; Fett, D., Kusters, R., & Schmitz, G. (2017). The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines. *Proceedings - IEEE Computer Security Foundations Symposium*, 189-202. <https://doi.org/10.1109/CSF.2017.20>

Figure 7

Communication Flows in Federated Digital Identity



## 2.2. The Limits of Regulation in Addressing the Challenges in the Digital Identity Landscape

The increasing prevalence of federated digital identity has raised several challenges concerning the protection of individual rights, societal values, and democratic systems. However, current laws were designed for a physical world and do not provide suitable responses to the unique difficulties raised by digital ecosystems, and this is particularly the case of digital identity. As Canals Ametller noted (2021a, p.6), “while Fundamental Rights and Freedoms are present in the digital ecosystem, the traditional mechanisms for guaranteeing and protecting them are not”; consequently, there is a need for new or adaptive regulatory measures to address the challenges posed by digital ecosystems.

**2.2.1. Enforcing Privacy Rights Amidst Surveillance Practices.** Digital identity plays a crucial role in either facilitating or challenging surveillance practices. In delegated and federated systems, the IdP acquires a privileged position to oversee users' online activities (i.e., the online services accessed via their electronic identification means). Nevertheless, contrary to the case of delegated digital identity where the surveillance possibilities are limited (i.e., access to the services for which credentials have been

provided) in federated digital identity, users utilize the same electronic identification means to access multiple services, creating a situation where the IdP has the ability to track user activity and link accounts across various services, potentially becoming a "Big Brother" figure<sup>64</sup>.

The surveillance culture is becoming a product of contemporary late-modern society or digital modernity<sup>65</sup>. It became more visible at the turn of the 21<sup>st</sup> century, especially after the 9/11 attacks in the US and the advent of social media<sup>66</sup>. The term surveillance refers to “the monitoring developed by an entity in a position of authority, with respect to the indented subject of the veillance, that is transmitted, recorded or creates an artifact” (Ali & Mann, 2013, p.243). There exist different types of surveillance, but in this thesis, we refer to the phenomena of data surveillance, understood as the collection of information about an identifiable individual, often from multiple sources, that can be assembled into a portrait of that person’s activities.

Public and private sector entities participate in surveillance ecosystems<sup>67</sup>; however, public and private surveillance respond to different interests. Private surveillance aims to maximize profits by using individuals’ data (e.g., web surfing habits, interests..., etc.) with economic value for the extraction of patterns derived from making connections between information concerning individuals or a group of individuals. On

---

<sup>64</sup> Although the recent criticism has focused on electronic identification means provided by private operators, concerns also exist in the public sector with systems such as Cl@ve or in any system based on the online verification of certificate status, as noted by Valero Torrijos & Sánchez Martínez (2007, p.10) with regard to the *DNIe*, which allowed the traceability of users' interactions with Public Administrations as well as those electronic communications with private operators established through the use of the *DNIe*.

<sup>65</sup> As noted by Lyon (2017, p.825), from the later 20<sup>th</sup> century especially, corporate and State modes of surveillance, mediated by increasingly fast and powerful technologies, tilted toward the incorporation of everyday life through information infrastructures and our increasing dependence on the digital in mundane relationships.

<sup>66</sup> As noted by Harcourt (2015, p.50), the growth of social media culture has enabled corporate surveillance based on the pleasure or fun of the user. Conversely to Orwell’s perspective, where surveillance power was yoked to destroy desire and passion (desire was thoughtcrime), today, these have become the means of surveillance, enabling digital exposure.

<sup>67</sup> For example, social media providers, telecommunication companies, or manufacturers of devices, but also financial services and insurance or even the public sector and critical societal domains like education or healthcare. As Barrio Andrés notes (2020, p.54), there is an interest by States to leverage private communications to guarantee public order, but also by multinational corporations that reuse the data in the scope of their business.

the other hand, public surveillance is justified in the existence of public interest as a means to provide security to citizens<sup>68</sup>. However, it is necessary to say that precisely one of the main characteristics of this surveillance age is the difficulty of separating surveillance by governments or commercial entities, as they tend to use the same technologies or even agree on some forms of partnership. Furthermore, the government has the power to take away liberty and centralize all private sector data.

Irrespective of their origin, surveillance practices can affect individuals' rights and freedoms and threaten the basis of free and democratic societies. Intellectual privacy is essential for a meaningful guarantee of privacy and free societies. Furthermore, as noted by Neil M. (2020, p.1935), the gathering or accessing of information affects the power dynamic between the subjects involved. This situation gives the "observer" power to influence or direct the behavior of the subject being observed, potentially materializing in different practices such as blackmail or persuasion or even in some forms of discrimination<sup>69</sup>.

Although mass surveillance is not a legal term, it can be identified with the term untargeted<sup>70</sup> surveillance, that is, when "data are not gathered about a specific person or group (for example, those suspected of having committed a particular crime), rather they are gathered about an undefined number of people during an undefined period of time without a pre-established reason. The potential value of the gathered data becomes clear only after they are subject to analysis by computer algorithms, not beforehand" (Van der Sloot, 2016, p.414).

Mass surveillance has an impact on Human Rights in various ways. The primary rights affected by mass surveillance are the right to privacy and the right to data protection (Article 8 ECHR or Article 12 UDHR). The right to privacy ensures self-expression and

---

<sup>68</sup> This "pre-emptive surveillance" is based on the collection of personal data generated by ordinary in the context of everyday activities, pretending to be on behalf of the public interest. An example of these surveillance programs is the Pentagon's "Total Information Awareness."

<sup>69</sup> In particular the possibilities for discrimination from the vast collection of data are increased with the introduction of machine learning and artificial intelligence techniques which can develop bias.

<sup>70</sup> While targeted surveillance has traditionally been codified into laws in most countries, untargeted surveillance remains a blurry territory regarding regulatory aspects.

personal autonomy, which are vital for self-determination. As noted by Lamer (2017, p.405), “people who are watched or who think that they are being watched behave differently from their unwatched selves; they exercise self-control and self-censorship” (the so-called chilling effect). Therefore, any chilling effect immediately brings into play rights such as freedom of expression (Article 10 ECHR or 19 UDHR), freedom of association, and freedom of assembly (Article 11 ECHR or 20 UDHR), as “it will impact upon the ability of individuals to access information freely, to develop their understanding of specific issues, to engage in communication or meet with particular individuals or organization, and so on” (Murray, 2019, p.44). Furthermore, in specific circumstances, other rights could also be affected due to the information gathered, such as the right to equality and non-discrimination.

However, it can be difficult for a person to take legal action for restitution of their rights when required. The main challenge is that with mass surveillance, personal data is processed on an aggregated level, and profiles are created on a group level (where the individual is often simply unaware), becoming more and more difficult for an individual to point out their specific personal interest and personal harm. Consequently, although the ECtHR admits exceptions under certain circumstances<sup>71</sup>, the existing legal framework may not always be sufficient for covering all potential damages and harms of technological advancements.

It is important to consider that legal proceedings in the ECtHR or the ECJ have their specific characteristics. These courts generally aim to hold Member States accountable for not upholding the ECHR or the application of EU Law. However, in the case of private organizations violating data protection laws, the most common consequences

---

<sup>71</sup> Van der Sloot (2016, pp.415-429) notes this aspect. In particular, the author remarks that in the invocation of the right to privacy under article 8 ECHR, the Court, in principle, does not admit *in abstracto* claims, nor *actio popularis*. Still, the Court has taken a step further in some occasions, and held that an individual may, under certain conditions, claim to be the victim where there is a “reasonable likelihood” that the applicants were affected by the measures complained of (Klass and others v. Germany) or the doctrine of “future harm”, in particular in relation to laws that discriminate or stigmatize certain groups in society (inter alia, Marckx v. Belgium, Dudgeon v. The United Kingdom and Norris v. Ireland), or even allowed standing without the need to demonstrate of any risks that surveillance measures were applied, if national systems do not provide an effective remedy for individual to challenge such surveillance (Mr Roman Andreyevich Zakharov vs. Russian Federation).

will be sanctions from data protection authorities rather than court action. Yet, numerous examples do show that these sanctions are not very effective, especially when the reward gained from illegal data processing surpasses any penalty paid<sup>72</sup>, suggesting potential developments in Criminal law in what concerns offenses in the digital sphere, along with advances in holding every individual (i.e., natural or legal persons) accountable for their actions.

The study of legal remedies to surveillance practices can be extensive and is not the objective of this thesis. Nevertheless, it is clear from a legal point of view that the current surveillance practices violate some basic principles of the GDPR, like the principles of purpose limitation or data minimization, and even before the GDPR came into force, European case law had already rejected these practices<sup>73</sup>. A conclusion that can be reached from this brief analysis and the practice generally observed is that there exists a clear tension between the traditional legal and philosophical discourse and the new technological reality, as is the case of the surveillance possibilities brought by federated digital identity. Most of the conversation around Fundamental Rights or Human Rights tends to lean toward individuals, but data processing has an impact on larger societal structures. This means that we may need to “renovate” our legal system to consider the various sectors and industries involved in data processing because,

---

<sup>72</sup> By way of example, Facebook's parent company, Meta Platforms Inc., agreed to pay \$725 million to settle a class-action lawsuit accusing it of allowing third parties, including Cambridge Analytica, to access users' personal data. However, this amount is minuscule compared to the profits this company makes from data. See, among others, Raymond, N. (2022, December 23) *Facebook parent Meta to settle Cambridge Analytica scandal case for 725 millions*. Reuters. <https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/or>; Brook, C. (2022, December 28) *Google Fined 57M by Data Protection Watchdog Over GDPR Violations*. *Digital Guardian's Blog*. Frotra. <https://www.digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations> or; Bodoni, S. (2021, July 30) *Amazon Gets Record 888 Million EU Fine Over Data Violations*. Bloomberg. <https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach>

<sup>73</sup> For example, in *Digital Rights v. Ireland* the ECJ annulled the Data Retention Directive on the grounds that “the EU legislature had failed to comply with the principle of proportionality in the EU Charter of Fundamental Rights, considering the system of mass, blanket surveillance set out by the Directive disproportionate and in breach of the rights of private life” (Paragraph 69).



essentially, how we manage personal data will play a significant role in shaping the future of technology-driven societies<sup>74</sup>.

**2.2.2. Difficulties in Prosecuting Identity-Related Crimes.** Digital identities require both user identification and authentication, which involves verifying that a legitimate user's identity is registered and that it is the same person who is accessing it at a later stage. Nevertheless, nowadays, one of the main challenges of the Internet is ensuring we are "talking" to the intended receiver on the other end.

### Image 1

On the Internet, Nobody Knows You Are a Dog



Note. Image authored by Peter Steiner, *The New Yorker*, 1993.

In a context where many operations, processes, and interactions have been digitalized, identity theft represents a large majority of digital crimes<sup>75</sup>, and the methods for its commission are being refined. Impersonation can take place by different means. It can

---

<sup>74</sup> As Albrecht and Citro state (2020, p.110), "surveillance culture can lead to further exacerbate and entrench postcolonial structures through the appropriation of an increasingly valuable resource-persona data."

<sup>75</sup> In a survey conducted in Australia in 2020, almost 1 in 4 Australians surveyed (24,5%) reported having been victim at some point in their lives. Jorna, P., Smith, R., & Norman, K. (2020). *Identity crime and misuse in Australia: Results of the 2018 online survey*. Australian Institute of Criminology. <https://www.aic.gov.au/publications/sr/sr19>

occur by compromising the IdP itself or its products (i.e., identity tokens) but also by compromising users' identification means. This is the most common way of impersonation and can take place through different types of cyberattacks<sup>76</sup>, including social engineering techniques, which represent one of the most common modalities of commission.

Federated digital identity provides the same authentication methods as other models. Hence, it also presents the same security risks to the confidentiality, integrity, and availability of data. However, it has the particularity that if the user credentials get compromised, it can grant access to a larger number of services, increasing the potential harm caused by impersonation.

The EU has established rules to protect personal information and punish unauthorized access under data protection laws. However, in cases where this access results in other consequences, such as identity theft, it triggers the intervention of Criminal Law. Despite this, criminalizing digital identity-related crimes presents challenges.

Attacks on digital identity are not limited to specific conduct but can materialize in different forms and conducts. Furthermore, not all cases of digital identity manipulation represent an attack<sup>77</sup>. Consequently, in line with the particularities and requirements of Criminal Law, the criminalization of attacks on digital identity raises two fundamental challenges: the determination of the fundamental elements or conduct of the crime and the delimitation of the applicable jurisdiction.

On the first point, experts agree that the regulation of digital impersonation is poor or even non-existent in some Member States and call for the criminalization of certain conducts in the form of punishable offenses. This requires a precise correspondence between the definition of the crime and the actions committed, in particular considering

---

<sup>76</sup> For example, web scraping, spoofing, or spyware looking for abusive access into a system, or social engineering techniques, such as phishing, smishing, vishing, or pharming.

<sup>77</sup> For example, in the case of identity when two people have the same name or when a wrong email address is used.

that Criminal Law is an area where the application of the analogy is not possible. In English, three terms are commonly used: identity theft, identity fraud, and identity abuse<sup>78</sup>. However, no clear agreement on the definition of these three terms exists.

Koops & Leenes (2006, p.556) proposed a terminology according to which all of these would be considered identity-related crimes. Identity-related crimes are “punishable activities that have identity as target or principal tool.” Among the types of identity-related crime, identity fraud is usually used as the broader term. Fraud refers to a lucrative purpose, the obtention of goods or contract of services. Therefore, identity fraud refers to all forms of using others’ identity or identity data to unlawfully obtain goods or contract services.

On the other hand, identity theft is usually associated with impersonation or identity takeover. Identity takeover can take place in different ways but normally requires unauthorized appropriation by means of unauthorized access. Once the data have been accessed, an appropriation shall take place. Nevertheless, does the act of taking identity data alone constitute identity theft, and is it necessary for the perpetrator to have gained unlawful profits from it? In other words, is identity theft a form of identity fraud? The boundaries between Criminal Law and data protection come into play when determining whether possession without the use of such data is a punishable offense.

Other questions that arise are whether identity theft requires replacing the full person’s identity or just making use of any of their identity-related attributes<sup>79</sup>, as well as the scenarios of extra limitation of powers when authorization exists to use the identity, that cannot be qualified as an identity takeover but more as an identity abuse.

---

<sup>78</sup> To add even more difficulty to the topic, other languages, such as Spanish or French, use the term *usurpación de identidad* or *usurpation d’identité*. However, Solís Arreondo notes (2018, p.142) that, “the *Real Academia de la Lengua Española*, defines *usurpación*, as the offense committed by seizing with violence or intimidation another’s real property or right in rem, and that the identity as a complex whole is more a Human Right than a right in rem.”

<sup>79</sup> According to Sullivan (2009, p. 83), intercepting and using another person’s identity proofs issued for authentication purposes (e.g., tokens/ credentials) would also fall in the scope of impersonation, as when the person presents them at the time of the transaction, it is assuming the right to exclusive use thereof.

This discussion is identified in the different regulations. For example, in the UK, identity theft is included under the guise of identity fraud<sup>80</sup>. In France, it is envisaged as usurpation without requiring fraudulent use<sup>81</sup>. In the case of Spain, identity theft is not directly considered a crime but is indirectly punished through other provisions, such as the usurpation of the civil status<sup>82</sup> or access and disclosure of personal data<sup>83</sup>.

Furthermore, cybercrimes raise challenges in determining the applicable jurisdiction<sup>84</sup> because of the extraterritorial nature of the Internet. Cybercrime has its particularities, demanding its own rules to avoid a situation of impunity. To prevent this, some experts note alternatives, such as the possibility of regulating them as transnational crimes<sup>85</sup> (different from international crimes in the sense of Public International Law).

Given legal complexities, extensive technical work has been conducted to prevent the possibility of impersonation. Although passwords have been the most common authentication means, these are hard to remember, and people often write them down or use the same password for multiple accounts. Other propositions have emerged for the purpose of facilitating the task of remembering passwords, such as cognitive

---

<sup>80</sup> Section 2 Fraud Act.

<sup>81</sup> Article 226-4-1 *Code Pénal*.

<sup>82</sup> Article 401 *Código Penal*.

<sup>83</sup> Article 197.2 & 3 *Código Penal*.

<sup>84</sup> By way of example, the *Ley de Enjuiciamiento Criminal* establishes in Article 23 a set of criteria according to which Spanish tribunals have jurisdiction to prosecute a crime. According to Article 23, Spanish tribunals will have jurisdiction over those crimes committed in Spanish territory (*forum loci delicti commissi*), but also when any extraterritorial jurisdictional rule applies: nationality of the offender, protected legal right, or the principle of universal jurisdiction. We will not discuss these rules in detail, but to highlight the difficulties that emerge in the scope of cybercrime, and more in particular of digital identity-related crimes, note that for the application of the first case (i.e., the offender is a national from Spain), it will be necessary first, to know that the person is from Spanish nationality, and second, from where has committed the crime (to determine whether it is a punishable act in the respective State). On the other hand, the principle of universal jurisdiction is thought in the scope of Public International Law, for the prosecution of crimes against humanity. However, these crimes must be defined as such in the International Treaties and their purpose is to be enforced by the International Community. Most of the crimes involving identity theft will not qualify for that, except those that might lead to some form of cyberterrorism.

<sup>85</sup> Transnational crimes refer to crimes that have actual or potential effects across national borders and crimes that offend fundamental values of the international communities. However, these require some common features, such as being committed by criminal organizations or individuals that are part of this type of organization, which will not usually be the case in identity-related crimes of persons with non-public relevance.

questions, images, or innovative options, like the Expanded Password System method<sup>86</sup>. However, their implementation has yet to be widely accepted.

During the last few years, biometrics has become a popular method of authentication, and extensive work has been conducted in this line. The latest and most widespread protocol for authentication involving biometrics is FIDO, which aims to increase security while protecting biometric data that will be stored on the user's device. However, there are no perfect solutions available yet, and identification and authentication processes remain a challenge in security, particularly for online means. Nevertheless, this is a sector where extensive research is being conducted, focusing on alternatives that offer a higher level of reliance, such as comparing local biometrics and biometrics stored in a credential. However, these solutions are still being consolidated for widespread implementation.

**2.2.3. The Role of Competition Law in Addressing Power Disparities in the Tech Industry.** When dealing with the problems of digital identity ecosystems, studies have focused on surveillance practices and identity theft. Consequently, these have usually disregarded another key issue, as is the situation of power imbalance that exists in current digital identity ecosystems. This power imbalance, on the one hand, results from surveillance, where the observer can control (and benefit from knowing) the behavior of the observed, as well as from the dependency on resources.

As it has already been introduced, federated digital identity ecosystems have been characterized by a reduced number of IdPs that concentrate digital identity functions and processes, creating a situation of power imbalance where users depend on these

---

<sup>86</sup> The Expanded Password System consists in an authentication method that introduces the possibility of converting text passwords into images. The user is given the possibility to select a set of images from their device (their last trip, furniture...). During the authentication, the user will be shown these images, among other random images. As the creator notes, the combination of these "personal" images is not only easy to remember but hard to forget as they are associated with the user's autobiographical memory. See, among others, Kokumai, H. (2018, August 1). *Assurance by our own volition and memory Part 1*. Payments Journal. <https://www.paymentsjournal.com/identity-assurance-by-our-own-volition-and-memory-part-1>; Kokumai, H. (2019, September 30). *Passwords made of unforgettable images*. Payments Journal. <https://www.paymentsjournal.com/passwords-made-of-unforgettable-images>; Kokumai, H. (2020, April 28). *'Easy-to-Remember' is one thing, 'Hard-to-Forget' is another*. Payments Journal. <https://www.paymentsjournal.com/easy-to-remember-is-one-thing-hard-to-forget-is-another/>

providers to access various services online. This statement is particularly true if we consider that several websites are now eliminating their in-house identification services and requiring users to register with a federated IdP.

According to Casciaro & Piskorski (2005, pp.169–171), in Emerson’s exchange framework, the power capability of actor X in relation to actor Y is the inverse of Y’s dependence on X. In turn, dependence is a function of resource criticality and the availability of alternative providers. An actor Y, therefore, is dependent upon actor X in proportion to Y’s need for resources that X can provide and in inverse proportion to the availability of alternative actors capable of providing the same resources. This dyadic approach to resource dependence yields two distinct dimensions of power in dyad: power imbalance and mutual dependence. Power imbalance captures the difference in the power of each actor over the other, while mutual dependence captures the existence of bilateral dependencies in the dyad, regardless of whether the two actor’s dependencies are balanced or imbalanced. According to the level of dependency of each actor, the degree of power imbalance and mutual dependency might vary.

## Image 2

### Powe Imbalance and Mutual Dependence

		j's Dependence on i		
		Low (1)	Medium (2)	High (3)
i's Dependence on j	High (3)	Configuration 7: Power imbalance: 2 Mutual dependence: 4	Configuration 8: Power imbalance: 1 Mutual dependence: 5	Configuration 9: Power imbalance: 0 Mutual dependence: 6
	Medium (2)	Configuration 4: Power imbalance: 1 Mutual dependence: 3	Configuration 5: Power imbalance: 0 Mutual dependence: 4	Configuration 6: Power imbalance: 1 Mutual dependence: 5
	Low (1)	Configuration 1: Power imbalance: 0 Mutual dependence: 2	Configuration 2: Power imbalance: 1 Mutual dependence: 3	Configuration 3: Power imbalance: 2 Mutual dependence: 4

*Note.* Retrieved from “Power Imbalance, Mutual Dependence, and Constraint Absorption: A Closer Look at Resource Dependence Theory” by T. Casciaro.t & J. Piskorski. (2005). *Administrative Science Quarterly*, 50(2), p.171.

In a scenario of a reduced number of IdPs, the degree of dependency of the user is high as there are no multiple alternatives for the provision of the same resource (digital

identity services). Conversely, the dependence of the IdPs on the user can be considered low when referring to a single user/individual. It could be argued that, from a collective perspective, the IdPs' dependency on users would also be high, but for this, a collective withdrawal from the service would be necessary. Therefore, in the relationship between the reduced number of IdPs and a single user, the degree of power imbalance would be high.

The main concerns have been focused on the scope of private providers, notably the so-called Big Techs<sup>87</sup>. It is challenging to determine the correct regulatory response to the concentration of power held by these entities. This is due to an information asymmetry that prevents the implementation of competitive market mechanisms and also makes it difficult for regulators to identify monopolistic behaviors and determine the most effective timing and scope for anti-monopoly enforcement (e.g., secret algorithms).

As Tian & Xin Yi (2021, pp.777–778) note, research into platform monopoly issues is still in the initial stage, and the limited experience calls for a prudent antitrust enforcement approach to online platforms to avoid excessive law enforcement that could lead to chilling effects on innovations, which could in turn undermine consumer welfare. Applying antitrust or monopoly rules implies the concurrence of specific requirements, particularly a certain market share. Determining the market share in the case of digital platforms/providers is complex. These are providing innovative services, making it difficult to determine their effective control of the company, and these are expanding to various sectors<sup>88</sup>.

---

<sup>87</sup> Coveri et al. (2021, pp.3–4) note four drivers through which control is exerted and dominated by digital platforms. To highlight three in this thesis: a) Growth and diversification, dominating “strategic” sectors and services that are fundamental for many other goods to be produced and distributed, as it is the sector of identification services; b) R&D technological developments, by investing in domains such as Artificial Intelligence or Machine Learning, key to controlling information networks and their physical counterparts (e.g., users trading privacy for free accessing these services); c) Government and retaliatory power, leveraging a retaliatory power to counter hostile institutions and regulations (e.g., regulations aimed at limiting the appropriation of personal data, increasing taxation....).

<sup>88</sup> The expansion to various sectors is justified for the centrality of the data as a basic resource that drives these companies. Expansions to other sectors can also raise problems of indirect monopolies, that is to say, reducing consumer choices in other areas by using a prevalent position in an interdependent sector.

While Big Tech companies are currently under scrutiny, the concerns raised extend beyond a single corporation and apply to the entire tech industry. This creates a challenge for applying Competition Law, which is a law that applies generally and not to any specific industry. One solution could be to establish industry-specific regulations that address the unique concerns that arise within the regulated industry. These regulations would typically impose a set of obligations on businesses operating for the public interest or public convenience and necessity, a topic that we explore further in this thesis in the scope of digital identity services.

Supporting this idea, some authors note the doctrine of public utility or essential facilities. As Feld (2019, p.55) notes:

It is enough to observe that digital platforms have clearly reached a level of prominence in our economy and in our lives to constitute a business affected with the public interest. No other sector of the economy, with the possible exception of the physical infrastructure through which digital platforms reach their users, has so much power to affect us in so many ways, yet remains subject to such little public oversight.

The intervention of the State in the regulation of a particular company or industry sector must be justified by the existence of a public interest in the services and/ or a market failure. Such an approach would not be new. In this regard, Clemons & Madhani (2010, p.57) conveniently note the example of computerized reservation systems, that way before modern technologies dominated the market for travel agency reservations systems, ultimately leading to a change in the rules from the Civil Aeronautics Board<sup>89</sup>. Nevertheless, it is important to recall that the issue of power imbalance is not exclusive to the private sector. Federated digital identity can also result in an unequal distribution of power in the public sector, which may be seen as disproportionate depending on the State's culture and traditions<sup>90</sup>. This underlines the need to introduce more effective

---

<sup>89</sup> As the authors explain, the computerized reservations systems (CRS) are positioned between the airlines and their passengers. If one CRS drops an airline, then all agencies that use the CRS and all of that agency's customers are denied access to one (and only one) airline. The agency may not care, and the customer may not even know and bypassing CRS at that time, before the presence of search engines and online booking, was almost impossible. The consequence was that despite the high fees, no airline voluntarily removed itself from any CRS.

<sup>90</sup> Think for example in the case of Thailand where it is common that the State performs a strong identification process based on biometrics from a very young age. Smertnik, H. (2020, June 4). *Confusing*



regulations for the digital identity industry and, notably, to develop identification technologies that operate independently from third parties.

### **3. Digital Identity, Essential, yet not Guaranteed**

The main objective of this chapter was to provide an overview of the complex and fragmented regulatory landscape for digital identity services within the EU. As we have presented, different “types” of digital identities can be identified depending on their purpose or context of functioning. However, all of these digital identities tend to share a common problem: that is, there are no regulations that guarantee their issuance. By way of example, we have noted the eIDAS Regulation, which failed to mandate the notification of an eID means by Member States, resulting in scenarios where the eID means were provided but not notified or simply not provided. Consequently, to date, some Member States have not notified any, preventing their citizens from engaging in operations requiring cross-border electronic identification and authentication processes. In the private sector, we have not identified either an obligation to issue electronic identification means. Therefore, private providers will only offer them if they prove to be profitable (in economic or data terms, as discussed above). Finally, the digital identity of the financial sector used in the public and private sectors in some countries, as in the case of BankID, may exclude certain population groups, specifically those already excluded from the financial ecosystem.

We have highlighted that privacy and cybersecurity are two essential components common to all digital identities<sup>91</sup>. However, the lack of specific regulatory provisions has led to poor implementation, and IdPs have prioritized their own interests, and the potential harms for the user have been disregarded. This situation is also aggravated by the complexities linked to obtaining legal remedies and damage restoration, considering the gap between law and technological reality.

---

*biometric ID experiences at a young age: voices from Thailand*. Medium. <https://medium.com/caribou-digital/confusing-biometric-id-experiences-at-a-young-age-voices-from-thailand-abe6579ff45b>

<sup>91</sup> Although in a potentially different degree depending on the concrete scope of provision and use of that digital identity.

An important part of the problems in this sector nowadays lies with the technical models behind it, creating an “enabling ecosystem” for certain practices. Although the criticism has focused until now on the private sector, it is important to acknowledge that these issues are inherent to the technical model and, therefore, also exist when it is deployed by entities within the public sector. Ultimately, relying on third-party digital identities can lead to the same problems and limitations irrespective of the nature of the entity (i.e., public or private) providing it.

The main ideas that must be gleaned from the chapter are the absence of a general law in the EU<sup>92</sup> that mandates the provision of digital identity services in a context where these are essential to enable public and private interactions in the digital medium. In addition, we face a reality in which, except in some concrete cases<sup>93</sup>, privacy and cybersecurity enforcement rely on the interests of the entity providing the electronic identification services. On top of this, as it has been repeatedly noted, current debatable technological models for digital identity raise concerns that current regulations cannot address effectively and, after all, evidence the need for a complete shift from existing digital identity ecosystems.

In short, we can say that the digital identity layer is “broken” and does not work properly, and what is more worrying is that the rights and freedoms are not sufficiently guaranteed, not just about how these digital identities work, but even about whether or not I have a right to digital identity in a specific scope. While this is understandable, considering how the Internet, as a privatized infrastructure, has evolved up to this point, it is time to rethink this aspect and offer better solutions, especially solutions that guarantee the adequate development of a society governed by the introduction of digital means.

---

<sup>92</sup> In the national landscape, however, it is very possible to have a right, stipulated in the laws, to obtain an electronic identification means, such as the national electronic identity cards. However, the limitations of use that come with these electronic in many countries suggest that the degree of guarantee of a “functional digital identity” is low.

<sup>93</sup> Basically, those digital identities that must comply with the eIDAS LoAs or similar requirements at the national level, at least in what concerns cybersecurity requirements.

## CHAPTER II

---

### THE EIDAS REGULATION: PIONEERING ELECTRONIC IDENTIFICATION LAW WITH NOTABLE LIMITATIONS

---

The accelerated technological development and the digitalization of processes have led to the fast evolution of digital identification services, particularly in the private sector, that are subject to fewer regulatory constraints. However, regulations have been unable to keep pace with these developments. This delay can be attributed to the normal evolution of regulation, usually a few steps behind technology, but also because of the complexities of the subject and the inherent link between identification powers and Member States' sovereignty. The consequence, as has already been presented in the first chapter, is a very fragmented regulatory framework, where applicable regulations vary depending on the entity that provides the identification service and the service that aims to be accessed, and these regulations usually have in common the lack of a general guarantee for the provision of electronic identification means<sup>94</sup>.

Despite its limitations, the most important regulation on electronic identification in the EU has been the eIDAS Regulation. Yet, the effectiveness of this Regulation can be considered to be partial, as it only imposes mandatory acceptance of notified eID means in the access to public services; therefore, being limited to “digital identities in the public sector,” except for a few cases in the European landscape.

This limitation must be understood, considering that the eIDAS Regulation conceives electronic identification means as a service provided by or under the supervision of Member States. Consequently, private entities are not allowed to offer electronic

---

<sup>94</sup> An exemption to this could be the laws that establish the right to obtain the national identity card (which includes the possibility to activate the electronic national identity card), such as in Spain the *DNI* as set out in Article 8 of the *Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana* and Article 2 of the *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*.

identification means without the State's prior intervention. Nevertheless, there has existed a “chink” or a “loophole” through the figure of the digital certificate, which, although it has been used successfully to cover this need, does not meet current market demands for identification services. In addition, although the eIDAS Regulation only dates from 2014, it is now confronting a different technical reality and is perceived in some cases as a privacy and security obstacle, notably due to its requirements and underlying technical model (i.e., the eIDAS nodes).

Furthermore, it is essential to note again that the eIDAS Regulation does not create a new European identity but establishes the criteria for mutual recognition across Member States. Consequently, each Member State decides on the provision of its own eID means, which has resulted in different implementations. While in some Member States, we find eID means owned and deployed by the public sector, in other countries, there have been some formulas to open participation to private providers or even complete provision by private providers.

The purpose of this chapter is to explain the regulation of electronic identification within the eIDAS Regulation as a sector “curiously” allocated between different legal regimes within the Regulation itself. We also find it important to explain the main limitations of the Regulation in this sector for the purpose of understanding the driving forces behind the Proposal for Revision of the eIDAS Regulation. In addition, to provide a more practical view, we have selected seven European countries that have notified at least one eID means under the eIDAS Regulation and exhibit different modalities for implementation of this Regulation. However, the reader should be aware that the objective of this second section is not to offer a comprehensive comparison of all eID options available in this country but just to provide them with a quick overview of different possible eID models. To elaborate this section, I have consulted available public resources, and in some cases, conducted semi-structured interviews with professionals in the Member States under study.

## **1. The eIDAS Regulation: a First Step in Electronic Evidence, Now Facing Modern Limitations**

### ***1.1. A Multifaceted Regulation: Electronic Identification and Trust Services***

The eIDAS Regulation is usually described by legal scholars as a complex regulation with varied and differentiated content. Its subject matter can be defined as heterogeneous, as it lays down, on the one hand, the conditions for the recognition by one Member State of electronic identification means notified by another Member State and, on the other hand, the basic rules for trust services and a legal framework for trust services that may be subject to qualification. The legal effects are essentially different in both cases. While in the first case, the Regulation is limited to establishing the conditions under which a notified electronic identification means must be recognized in another Member State, in the second case, the eIDAS Regulation creates a legal framework for these “electronic proofs” (Alamillo Domingo, 2018, p.25).

I would like to point out that at the time of writing this thesis, eIDAS2 had not yet been adopted or entered into force, so the first version of the eIDAS Regulation remained in force, and this section is written in the present tense. In the event of reading this section after the eIDAS2 Proposal enters into force, this section will only require the use of the past tense in certain contexts.

***1.1.1. Notified eID Means for Cross-border Processes in the European Union.*** The eIDAS Regulation does not create a new form of digital identity, but instead, it establishes the legal basis that allows the different national electronic identification schemes to interoperate. In the previous chapter, we discussed how the eIDAS Regulation imposes a set of conditions in Article 6.1 for the mutual recognition of electronic identification means. In addition, it provides a set of technical specifications in the CIR (EU) 2015/1502 to determine whether the electronic identification means fulfill a certain LoA and, therefore, can be notified for cross-border use.

As part of eIDAS, Member States are encouraged to notify their national electronic identification schemes for mutual recognition (i.e., a certain eID scheme notified by Member State A can be utilized to access services in this Member State B by a national of Member State A). The notification procedure begins with the pre-notification, where the Member State receives preliminary feedback. After this phase, a formal notification takes place, where detailed information on the eID scheme is provided. A peer review process is then initiated, where other Member States evaluate the scheme and provide their comments. Based on this review, the European Commission finally decides whether to recognize the electronic identification scheme or not.

By 2020, only 13 countries had notified their electronic identification schemes, a number that showed the relative “failure” of the eIDAS Regulation. This number has, however, significantly increased during the past years, reaching 24 countries<sup>95</sup> and motivated by the publication of the Proposal for Revision of the eIDAS Regulation that now mandates the notification of at least one electronic identification scheme containing at least one eID means.

Once an eID means has been notified and published in the Official Journal of the EU, there is a delay of 12 months for their acceptance in cross-border public services. For the purpose of ensuring this acceptance, the eIDAS Regulation mandates Member States to ensure that RPs are connected to an eIDAS node. Nevertheless, from a technical perspective, two configurations exist to ensure interoperability.

On the one hand, in the “proxy configuration,” there is software (a node) acting as an intermediary or gatekeeper for requests. The purpose of this proxy is to receive identification requests from other eIDAS nodes, verify them, and “translate” them to the local identification system. It is common that both Member States interact through their eIDAS Nodes, resulting in the proxy-to-proxy approach, where these create a “bridge” between the IdPs and SPs located in different Member States. Although this approach is particularly beneficial from the interoperability perspective, it raises

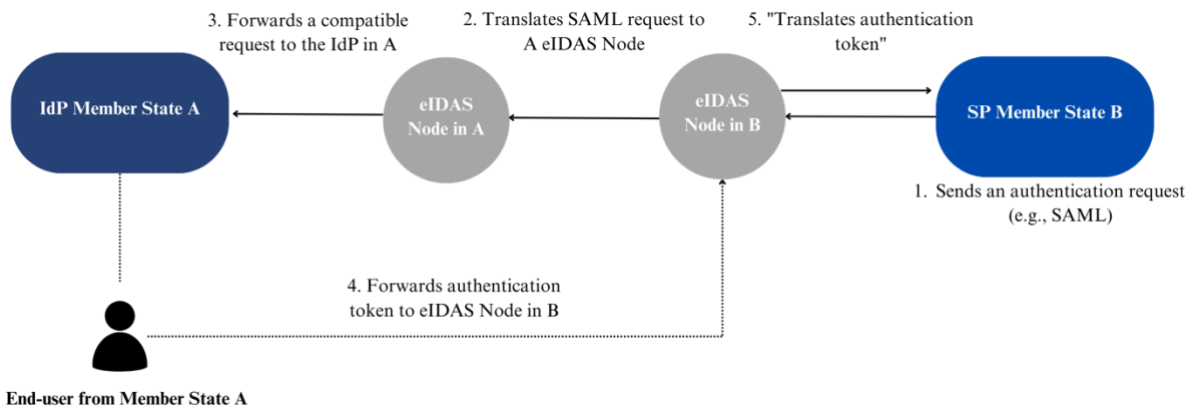
---

<sup>95</sup> At the time of writing this section: Liechtenstein, Czech Republic, Estonia, France, Italy, The Netherlands, Sweden, Spain, Malta, Poland, Latvia, Germany, Slovakia, Croatia, Norway, Belgium, Austria, Luxembourg, Lithuania, Slovenia, Denmark, Portugal, Bulgaria, and Cyprus.

privacy concerns as the centralized eIDAS nodes (e.g., the Spanish and the Italian nodes) create a "bridge" enabling control of the cross-border authentication operations that occur within it.

**Figure 8**

Cross-border Authentication Process through eIDAS Nodes

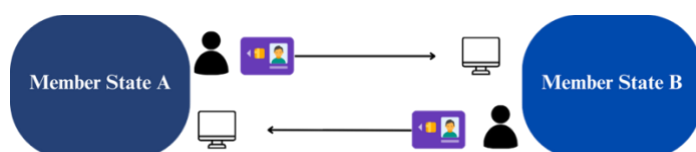


*Note.* Processes in proxy-to-proxy configuration when a user from Member State A aims to access a service in Member State B.

Although this is the most common configuration (i.e., proxy configuration), we already identify alternatives in some Member States, as is the case in Germany. The German case opts for the so-called middleware approach. In this modality, the idea is that devices can communicate directly without the need for any intermediaries (insofar as it is a middleware-to-middleware approach). This middleware serves a similar purpose as a proxy, handling protocol conversion, data transformation, and other necessary interactions to enable the local system to participate in the eIDAS network.

**Figure 9**

Middleware-to-Middleware Configuration



This approach provides for better privacy, but it is also more complex. Firstly, it demands the installation of specific software beforehand (e.g., a public organism in Spain would need to download the software in advance to receive authentications coming from a German electronic identification card). Additionally, it may be challenging to guarantee a free service, as required in Article 7 eIDAS.

Although the first approach has been widely used due to its simplicity and alignment with technical models like federated digital identity, the alternative approach proposed by other notified eID means, such as the German electronic national identity card, is becoming increasingly relevant, particularly in a context where offering better privacy and data protection is essential, as it will also be discussed in the next chapter in light of the eIDAS2 Regulation.

**1.1.2. The Legal Framework of Trust Services.** The eIDAS regulation is a key legislative piece to ensure legal certainty on the Internet within the EU. Beyond the part dedicated to the regulation of electronic identification means, this Regulation aims to support the development of the Digital Single Market, with a particular emphasis on electronic signature, but also establishing “further” trust services to digitalize processes that were previously analog, ensuring trustworthy electronic transactions that offer users significant legal certainty. Its ultimate goal is to make cross-border electronic transactions<sup>96</sup> simple and secure for citizens, businesses, and public authorities.

While one fundamental part of electronic transactions is the identification of the participants, it is not the only one. Equally crucial is to attest the will of the parties toward a certain agreement (i.e., electronic signature) or the moment in which this agreement has been reached (i.e., electronic time stamp). We could place trust services in this second “group.” However, as discussed in the next section, the separation is not absolute.

---

<sup>96</sup> And it could be even claimed that national digital transactions.



The eIDAS Regulation does not contain a definition of trust services. Article 3.16 of the eIDAS Regulation is limited to an enumeration of these services: a) The creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or b) The creation, verification, and validation of certificates for website authentication; or c) The preservation of electronic signatures, seals or certificates related to those services.

As Alamillo Domingo notes (2018, p.58), “these services provide trust to those business processes in which they are used, mainly thanks to the legal effect associated.” The eIDAS Regulation distinguishes two levels: qualified and non-qualified trust services. The eIDAS Regulation only defines qualified trust services (Article 3.17) as the trust services that meet the applicable requirements laid down in the eIDAS Regulation. Therefore, those trust services for which the eIDAS Regulation does not envisage specific requirements for qualification will be forcibly operating under the form of non-qualified trust services<sup>97</sup>.

Qualified trust services are crucial for users to establish trust. While non-qualified trust services lack detailed regulation, and the user must construct their own state of confidence regarding that service, qualified trust services are extensively regulated and are granted a particular recognition with associated legal effects. Even though there are some common security and audit requirements (Article 19), qualified trust services are subject to high-level security requirements and specific supervision requirements (Article 20), as well as ex-ante and ex-post fulfillment of legal requirements (Articles 21 & 24). Furthermore, Article 13.1 of the eIDAS Regulation establishes a key probatory provision providing that, while the burden to prove the intention or

---

<sup>97</sup> Alamillo Domingo (2018, p.55) lists the different services that can be subject to qualification: a) Services that can be qualified: Issuance of qualified electronic certificates for electronic signature of natural persons, electronic seal of legal entities and website authentication (Article 28 & Annex I, Article 39 & Annex III and Article 45 & Annex IV eIDAS); Qualified electronic timestamps (Article 44 eIDAS); Qualified validation for electronic signatures and electronic seals (Article 33 & 40 eIDAS). b) Services that cannot be qualified: Creation of electronic signature (simple and advanced) and electronic seals (simple and advanced) remotely; Validation of certificates for electronic signature, electronic seal and website authentication; Preservation of certificates of electronic signature and electronic seal.

negligence of a non-qualified trust service shall lie with the natural or legal person claiming the damage, in the case of a qualified trust service provider, intention or negligence shall be presumed unless the qualified trust service proves it otherwise.

Although the eIDAS Regulation provides a common framework, Member States may have national laws that complement or further detail its provisions within limits set by the Regulation. For example, a Member State may have national laws specifying procedures for the supervision of trust service providers or for the application of the eIDAS Regulation in specific sectors. Examples of this can be found in Germany, the *Vertrauensdienstegesetz* or in Spain, the *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza*. Furthermore, Member States can define other trust services, but these would not be covered by the legal effects provided in the eIDAS Regulation.

In what concerns electronic identification services, among trust services, digital certificates have acquired special relevance for their “identifying” use. Electronic certificates are essential for verifying the authenticity and integrity of electronic signatures, seals, and for website authentication (Article 3 (16) letters a & b), which fall under the category of trust services as per the eIDAS Regulation. Additionally, these certificates also help in accurately identifying the owner, creating a certain intersection between trust services and electronic identification, as discussed in the next section.

## ***1.2. Constraints and Limitations of the eIDAS Regulation for the Development of Digital Identity Ecosystems***

Even though it is the main rule for electronic identification services in the EU, the eIDAS Regulation, dating only from 2014, has quickly become outdated. This rule has some limitations; particularly, it could be said that it is limited to covering electronic identification services in the access to public services, leaving electronic identification processes in the scope of private services out of this Regulation. In addition, privacy and security concerns have increased since this Regulation came into force, leading to strong criticism that demanded its adaptation.

**1.2.1. Electronic Identification: between National eID Schemes, Trust Services, and Private Providers.** Although from the eIDAS perspective electronic identification refers to a collection of public services, it does not entirely close the door to their provision by private entities. Article 7 letter a of the eIDAS Regulation provides that the electronic identification means must be issued: i) by the notifying Member State; ii) under the mandate from the notifying Member State, or; iii) independently of the notifying Member State but notified and recognized by that Member State.

Consequently, three possible legal regimes for electronic identification depending on the issuing subject can be distinguished, all of them having in common the necessary prior intervention of the State for cross-border recognition and the exclusion of “purely private provision.” Behind the reasoning for such exclusion is the eIDAS liability regime for electronic identification means, which directly refers to the notifying Member State<sup>98</sup>. However, they remain free to choose the means of electronic identification they wish to introduce and whether the private sector should be involved in the provision of these services, although always under its responsibility.

On the other hand, the reason why electronic identification is not included as a trust service in the eIDAS Regulation is that it is considered a national prerogative, which allows the State to maintain it as a public service without being obliged to authorize its provision by private operators (Alamillo Domingo, 2018, p.57). Considering that electronic identification is not envisaged as a trust service in the eIDAS Regulation, electronic identification means issued independently by the private sector (i.e., different from those recognized by a Member State under an electronic identification scheme) will require agreement or voluntary cross-border recognition by the parties.

However, there exists a “chink” or “loophole” in the eIDAS Regulation for the provision of electronic identification services independently by private entities, which has led to the emergence of a pseudo market in this area. This is due to the fact that other trust services already enable the electronic identification of the natural person or

---

<sup>98</sup> As it can be inferred from Recital 18, “this Regulation should provide for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation.”

the legal entity. According to Article 26 letter b, an advanced electronic signature is “capable of identifying the signatory,” in particular when it is issued on the basis of a qualified electronic certificate<sup>99</sup> including the mandatory attributes set out in Annex I of the CIR (EU) 2015/1501.

Nevertheless, it must be recalled that since electronic identification is not envisaged per se as a trust service, it will also need to be covered by another trust service included in the eIDAS Regulation (e.g., electronic signature). More specifically, the certificate whose sole purpose is identification, but not the creation of an electronic signature or seal, will remain outside the harmonized regulation, possibly subject to national regulation or relying on the free will of the parties (Alamillo Domingo, 2018, p. 90). Such requirements seem unjustified when the only objective pursued is to provide an electronic identification service, and as noted by Martín Delgado (2010, p.469) more than ten years ago, depending on the concrete type of operation carried out by electronic means, it will be necessary to show the identity or, in addition, authenticate the will. In this regard, as the author remarked, if the only will of the citizen is to access and know certain personal data, such as personal data related to our working life, it will be enough with their identification without requiring proof of will.

Besides this “chink” or “loophole” in the eIDAS Regulation, Member States also have the possibility to recognize new trust services or even regulate some other types of private services through national provisions. However, in the first case, these new trust services will not be covered by the effects of the eIDAS Regulation (that provides a closed list of trust services) and could ultimately lead to divergences between Member States. The second possibility will only provide for effects in the national scope.

In addition, the electronic certificate will be covered by the eIDAS legal regime for trust services (and not for electronic identification). While the regulation on electronic identification does impose mandatory acceptance of notified eID means, the regulation

---

<sup>99</sup> A certificate means an electronic attestation that links electronic validation data to a natural person and confirms at least the name or the pseudonym of that person, and this confirmation is presumed to be legally true when the certificate is qualified.

on trust services is limited to establishing a rule of functional equivalence in some cases (e.g., the digital signature shall have the equivalent legal effect of a handwritten signature), as well as the probatory rules and non-discrimination effects for such services<sup>100</sup>. Therefore, the logic behind both legal regimes is essentially different.

Finally, shifting the focus from the provider of identification services to the entity whose services are being accessed, the extension of the scope of cross-border electronic identification to cover private transactions is one of the main objectives in the Proposal for Revision of the eIDAS Regulation, a modification that was necessary from the perspective of increasing and enhancing the conditions of electronic transactions, but also for consistency between EU Law. This possibility was already included in some EU legislation, such as the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing<sup>101</sup>, the Regulation (EU) 2017/2018 on cross-border portability of online content services in the internal market<sup>102</sup>, or the Commission Recommendation (EU) 2014/478 of 14<sup>th</sup> July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from online gambling<sup>103</sup>. Furthermore, the consequence of the exclusion of the private sector has already been developed in the previous chapter, that is, the monopolization of the private sector identification and authentication processes by the Big Techs, with the consequences that, as already noted, this has for the Fundamental Rights and Freedoms of citizens and the values of a democratic society.

---

<sup>100</sup> Beyond the cross-border recognition effect.

<sup>101</sup> Article 13.1 letter a allows to identify the customer on the basis of information obtained from a reliable and independent source, including where available, electronic identification means or relevant trust services as set out in the eIDAS Regulation.

<sup>102</sup> Article 5.1 letter a expressly authorizes the possibility of using electronic identification means to verify the state of residence of a subscriber to an online content service at the time of the conclusion or renewal of the contract

<sup>103</sup> Points 18 and 20 introduce mandatory third-party identification controls, encouraging Member States to adopt electronic identification systems in the registration process.

**Table 2**

Possibilities for the Provision of Identification Services and Applicable Regulations

<b>Public entity (or private entity under public control)</b>	Member State’s		eID means notified under eIDAS
	An entity other than the notifying Member State but under its mandate in accordance with national laws		
<b>Public/Private entity</b>	Trust Service	Qualified	Digital certificate for electronic signature/seal, and residually for identification purposes under regulation for trust services in eIDAS
		Non-qualified	
<b>Private entity</b>	Entity that issues an eID means recognized and notified by the Member State		eID means notified under eIDAS
	Another legal entity		Private eID means relying on contractual agreements for recognition

**1.2.2. Privacy and Security Challenges within the eIDAS Regulation.** Even though the eIDAS Regulation dates from 2014, it has quickly become outdated in terms of technology. New emerging types of technology offer better security and privacy features, which do not always align with the requirements of the eIDAS Regulation, particularly for electronic identification.

The eIDAS Regulation shall comply with data protection and facilitate privacy by design<sup>104</sup>. However, in practice, it is very debatable whether the eIDAS Regulation complies with these requirements nowadays. This is particularly noticeable in the proxy scheme presented above, where eIDAS nodes exert a centralized form of control, limiting actual privacy in the authentication process. These considerations were already raised by Alamillo Domingo (2018, p.179), who noted that “this network of single-points intermediates all cross-border authentication by the Public Administration, which

---

<sup>104</sup> Section 3 letter c of Article 12.

makes evident the risk for the surveillance of citizen's activities and the creation of profiles, interests, etc." Furthermore, the eIDAS Regulation is designed for identification purposes, which differs from sharing attributes in a privacy-preserving manner. As a result, cryptographic techniques such as selective disclosure or zero-knowledge proof were not allowed under the eIDAS Regulation since they do not comply with the minimum data set required by Section 1 of Annex I of CIR (EU) 2015/1501.

Although this requirement could be initially justified for security reasons, at present, such a rigid approach goes against the GDPR's principle of data minimization, which requires personal data to be collected for the intended purpose, that should allow, in turn, disclosure of the data strictly needed for that purpose. In addition, this requirement poses challenges for unlinkability and highlights inconsistencies between the eIDAS Regulation and the GDPR's definition of pseudonymized data<sup>105</sup>. Similarly, the most recent opinions of data protection authorities are in the direction of reducing, for example, the provision of the entire identity document, which is considered excessive<sup>106</sup>.

As Alamillo Domingo notes (2020, p.120–126), the need to cover the presentation of separated attributes has probably been ignored because there already exists sector-specific legislation that covers the value or legal effects of the proof of some attributes, such as the case of the Directive 2005/36/EC on the recognition of professional qualifications<sup>107</sup>. In this regard, the author already pointed out potential solutions, such as the creation of a general framework for the lifecycle of the attestation or a new parallel trust framework for issuing and sharing other identity attributes by extending

---

<sup>105</sup> Pursuing eIDAS alongside the pseudonym, each dataset has to contain at minimum the rest of the mandatory identifiers.

<sup>106</sup> In this regard, the Spanish Data Protection Agency 48/2023 recalled that the Agency's criterion is that it should only be subjected to processing when the regulation establishes it, be excessive when it is only intended to identify and consider that the *DNI* number is particularly sensitive. Agencia Española de Protección de Datos. (2023). *Informe 0048/2023*. <https://www.aepd.es/documento/2023-0048.pdf>

<sup>107</sup> Article 4 "the recognition of professional qualifications by the host Member State allows the beneficiary to gain access in that Member State to the same profession as that for which he is qualified in the home Member State and to pursue it in the host Member State under the same conditions as its nationals."

Chapter II of the eIDAS Regulation or including it in the framework of trust services, by modifying Chapter III of the eIDAS Regulation. The last possibility has been finally adopted by eIDAS2.

Furthermore, the eIDAS Regulation required other modifications to ensure technology neutrality and improve security. In this regard, Article 7 requires that the LoA for mutual recognition must be equal to or higher than what the public sector body requires for online service access, emphasizing that secure electronic identification schemes are essential for trustworthy cross-border mutual recognition of electronic identification means<sup>108</sup>. To determine whether the means for electronic identification fulfill these LoAs, the Annex of the CIR (EU) 2015/1502 sets the elements of technical specifications and procedures to determine how the requirements and criteria of Article 8 of the eIDAS Regulation shall be applied. However, these requirements were devised in 2015, given the state of the art technology and the fast development of the technique nowadays demand their adaptation.

While the legal text does not explicitly mention multifactor authentication, dynamic authentication is often interpreted in this context. Consequently, electronic identification methods that do not envisage multifactor authentication are not accepted, regardless of their security level. These restrictions would contravene, in my opinion, the principle of technology neutrality nowadays as organizations and individuals would be prevented from using different electronic identification means that do not involve multifactor authentication methods for cross-border operations, contravening Recital 16<sup>109</sup> or Article 12.3 letter a<sup>110</sup> of the eIDAS Regulation.

A solution to this matter could be the modification of the CIR 2015/1502 to include a methodology based on general principles that allow for the use of various technologies. These adaptations would not be something new, but these are already occurring in

---

<sup>108</sup> Recital 19.

<sup>109</sup> "It should be possible to achieve the necessary security requirements through different technologies."

<sup>110</sup> "It aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State where possible."



sectors like digital payments. A very recent example is the Proposal for a Regulation on Payment Services, which will, in principle, allow both factors in an SCA process to belong to the same category (Article 85 paragraph 12 of this Regulation). In addition, the industry had already demanded an adaptation of the “methodology” to evaluate SCA-compliant solutions, shifting toward a principle-based approach<sup>111</sup>. This modification evidences an advance in the direction toward more “open” guidelines for authentication procedures tailored to the specific actions being undertaken, something that also concerns the sector of electronic identification given the broad range of actions and procedures that might include.

## **2. From Theory to Practice: Examples of the Implementation of the eIDAS Regulation in the Notification of Electronic Identification Schemes**

### ***2.1. State-owned Electronic Identification Solutions***

When access to a certain service requires a high level of guarantee or assurance, it is common to recur to the electronic functionality of the ID card, a feature that has been implemented in several countries in the EU. However, in practice, not all countries have achieved the same level of success in their use, limiting their usability to very residual cases. Also, there are countries that have explored State-owned alternatives beyond the introduction of eID functions to their national identity cards.

***2.1.1. Good Design but Poor Usage of Electronic National Identity Cards: the Cases of Spain and Germany.*** Spain has only notified the *Documento Nacional de Identidad electrónico* or *DNIe* under the eIDAS Regulation. The *DNIe* was initially defined in Article 15.1 of the *Ley 59/2003, de 19 de diciembre, de Firma Electrónica*<sup>112</sup> as “the national identity document that electronically accredits the personal identity of its

---

<sup>111</sup> In this sense, we identify some of the contributions to the public consultation on the revision of PSD2 that took place between May and August 2022. European Commission. (2022). *Payment services – review of EU rules*. [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_en)

<sup>112</sup> This law has been now abrogated by the *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los Servicios Electrónicos de Confianza*.

holder and allows the electronic signature of documents.”<sup>113</sup>On the other hand, Article 8.1 of the *Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana* determines that "the *Documento Nacional de Identidad* is a public and official document and will have the protection granted by the law, as well as sufficient value alone for the accreditation of the identity and personal data of its owner,” establishing as Alamillo Domingo notes (2018, p.135) “a clear public regime and monopolistic, reserved to the State and, more specifically, to the *Ministerio de Interior*, which exercises it through the *Dirección General de Policía*.”

In Spain, the national ID card is issued by the *Ministerio de Interior*, specifically through the National Police, although its manufacturing is assumed by the *Fábrica Nacional de Moneda y Timbre (FNMT-RCM)*. The *FNMT-RCM* is a public corporation, a type of State-owned entity operating under the *Ministerio de Transformación Digital*.

Despite the high-security standards<sup>114</sup> of the *DNIe*, usability levels have been very low<sup>115</sup>. Although the *Ley de Firma Electrónica* required public and private sector entities to recognize its validity for confirming the identity and personal data of its holder, it did not mandate its acceptance as a means of electronic identification. The *Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información*, although initially included the obligation for certain categories of companies providing services to the public to provide an electronic communication channel through the use of recognized certificates of electronic signature, removed this mention in the modification of the norm in 2020. The nowadays applicable *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los Servicios Electrónicos*

---

<sup>113</sup> Consequently, two functionalities appear clearly differentiated: electronic identification and electronic signature.

<sup>114</sup> The *DNIe* has been notified with a LoA high.

<sup>115</sup> As Alamillo Domingo notes (2018, p.137), for example, according to the Report presented to the Council of Ministers on 10 January 2014 on the degree of progress of the implementation of e-administration in the General State Administration, with data referring to the 2012 financial year, only 2.41% of the validations of electronic signature certificates corresponded to electronic signature certificates corresponded to the electronic *DNI*; on the other hand, the Survey on Equipment and Use of Information and Communication Technologies in households conducted by the by the National Statistics Institute (*INE TIC-Hogares*) for 2013 reports that only 14.9% of users in possession of an electronic ID card use it to interact with the electronic administration, while up to 4.9% use it to interact with the private sector use it for relations with the private sector.

*de Confianza* has not included either any provision in this regard, perpetuating the reluctance among private providers to make the necessary investments for its acceptance.

Although the *DNIe* has been the only electronic identification means notified by Spain, in the national scope, there exist other eID means, such as the case of *Cl@ve*<sup>116</sup> or digital certificates, whose use in relationships between citizens and public services is accepted by Article 9.2 of the *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*<sup>117</sup>.

Besides the Spanish *DNIe*, there exist other examples of national electronic identity cards within the EU. Among these, it is particularly relevant the German eID based on Extended Access Control electronic identification scheme, notified under the eIDAS Regulation and which includes the National Identity Card, the Electronic Residence Permit, and the eID Card for Union Citizens and EEA Nationals.

The current version of the German eID card dates from the first decade of the 2000s. In 2009, the Federal Council passed the law on electronic personal ID cards, and the first new identity card, the *neuer Personalausweis* or *nPA*, was issued in November 2010. The new ID Card Act (*PAuswG*) explicitly addresses the card's authentication function, such as in Paragraph 18, which states that "the holder of the ID card, who must be at least 16 years of age, can use their identity in public and non-public units." In addition,

---

<sup>116</sup> As Alamillo Domingo notes (2018, p.139), *Cl@ve* is an electronic identification and authentication system implemented by the Government of Spain for access to public services at a national, regional, or local level. *Cl@ve* was adopted under Article 16 of the *Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos* by Agreement of the Council of Ministers, of 19 September 2014, published by Order PRE/1838/2014, of 8 October, and was initially defined as the common platform of the State Administrative Public Sector for identification. Although *Cl@ve* has improved convenience, it is designed for access to public services and relies on a federated digital identity model, placing *Cl@ve* in a privileged position to control user identification and authentication processes.

<sup>117</sup> Article 9.2 of the *Ley de Procedimiento Administrativo Común* establishes that "interested parties may identify themselves electronically to the Public Administrations through the following systems: a) Systems based on qualified electronic certificates for electronic signature issued by providers included in the "trust list of certification service providers"; b) Systems based on qualified electronic certificates for electronic seal issued by providers included in the "trust list of certification service providers"; c) Any other system considered valid by the Public Administration under the terms and conditions established, that enable the prior register of the user and prior communication to the *Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital*.

this law deals with electronic signatures. However, on this last point, contrary to the Spanish model, the signature certificates are not issued by ID card authorities but by special signature providers.

The *nPA* is issued by the local registration office or *Bürgeramt* on behalf of the Federal Republic of Germany. Nevertheless, its production, including its embedded digital features, is managed by the *Bundesdruckerei*, a company specializing in secure identity solutions that is primarily owned by the German government.

The *nPA* complies with a LoA high and is particularly interesting to study because it presents innovative features from the privacy and security perspectives:

- a) It includes a data-protection-friendly pseudonym function allowing for the recognition of the eID card without any transfer of personal data (e.g., for age verification). This pseudonymity function is produced between the cardholder and the SP<sup>118</sup>.
- b) Direct communication via a secure end-to-end protected channel between the RP and the chip of the eID is established. This functionality enables the middleware-to-middleware approach.
- c) Mutual authentication. Not only does the holder of the eID authenticate via the eID to the RP, but the RP also authenticates directly to the chip of the *nPA*.
- d) SPs are required to transmit an authorization certificate to the card to get access to the data on the *nPA*, and these are limited to the specific data fields and functions they wish to access<sup>119</sup>.
- e) Card-specific revocation token. To check whether the *nPA* is valid, a card-specific revocation token for comparison with the RP's revocation list and the indication of whether the eID card is expired are transmitted as part of the

---

<sup>118</sup> The pseudonym can be generated at the moment of login, in order to access the account in a later moment to identify the user when no additional personal data is required or even for the transmission of cardholder's attributes without a name.

<sup>119</sup> Public sector bodies of other Member States of the EU are authorized to request personal identification data from the German eID. Authorizations for further RP are issued by the Issuing Office for Authorization Certificates upon application in accordance with the *PAuswG*. The certificate contains the name of the organization, plus other details such as its registered office, the name of the data protection officer, the duration of the certificate's validity and the purpose.

authentication (upon request by the RP). The individual RP's revocation lists are generated by the Authorization Certification Authorities using a generic revocation list obtained from the revocation service.

- f) Offline use. The German federated digital model (with the government as IdP) functions only in an "offline mode." Consequently, it is impossible for the government to track or know the online activities of cardholders, which is prevented "by design" by the system's architecture.

The German electronic identity card, or more broadly, identity ecosystem, presents other interesting features that are not explicitly detailed in this thesis, such as the absence of a central database for eIDs or the user "authorization model."<sup>120</sup>

From the beginning, the authentication feature of the *nPA* was intended for use with both e-government applications and commercial ones. However, in practice, its use has been mainly limited to the public sector. Despite its excellent security and privacy features, the German *nPA* presents the same or even worse problems in terms of convenience as the *DNIe*. As some experts in the area note, "the German case has mitigated all possible risks by eliminating the user." Still, we identify some attempts to foster its use<sup>121</sup>, such as the *PAuswG-AMD*, the *Onlinezugangsgesetz*, or the nine-point plan for a digital Germany. Nevertheless, the current scenario is that private suppliers still show little or no interest in integrating the German solution, which is particularly tedious not only due to the technical complexities of its implementation but also because of the excessively bureaucratic organization<sup>122</sup> and the small targeted market<sup>123</sup>.

---

<sup>120</sup> When the cardholder uses the *AusweisApp*, it displays all of this information on their screen prior to entering her PIN, providing a first example of the "authorization model" that will be discussed later.

<sup>121</sup>Pursuing Pedrolí et al. (2021, p.53), in 2017 the Electronic Identification Promotion Act (*PAuswG-AMD*) entered into force, promoting the use of online identification through a national eID card. The new legislation promoted the activation and use of the eID functionality by making opt-out rather than opt-in. Later that year, the *Onlinezugangsgesetz* envisaged that the federal state and local governments must offer their administrative services digitally by 2022. Finally, the nine-point plan for a digital Germany included a set of objectives, among which we identify the implementation of functionalities on mobile phones, at the time user convenience is improved and there is an involvement of industry in the commercial use of the eID function.

<sup>122</sup> For example, to get permission to access certain data in the German electronic identity card.

<sup>123</sup> It is estimated that by 2019 only around the 50% have activated the electronic functionality of the German identity card. Thales. (2017). *June 2017: New German ID cards are "switched on"*. Thales.

**2.1.2. Achieving Digital Identity Success: Lessons from Estonia's National Electronic Identity Card.** Estonia is considered one of the most digitized European countries and most advanced in terms of implementation of eID solutions, credited by the ITU as “having by far the most highly developed national ID card system in the world” (2018, p.45). The first eGovernment strategy in Estonia dates from 1998–2003, and it already defined the principles of the Estonian Information Policy, focusing on the promotion and entrenchment of democracy, the development of ICT infrastructure, as well as of eCommerce and eBanking.

In Estonia, multiple eID means are grouped under their notified eID scheme, holding the national ID card a key role. More specifically, Estonia has different types of cards and mobile identities for cross-border recognition under the eIDAS Regulation: the identity card (ID card), residence permit card (RP card), Digi-ID, e-residency Digi ID, Mobile-ID, and Diplomatic identity card.

The national ID card-based eID has been offered since 2002. The *Isikut tõendavate dokumentide seadus* of 2004 established the framework for the issuance of electronic identity documents in Estonia and has, therefore, been the legal basis for the provision of the Estonian national electronic ID card. The eID function embedded in the national ID card is based on PKI technology<sup>124</sup> and works through two qualified certificates: one certificate for authentication and another certificate for electronic signatures.

The issuance of the electronic identity card in Estonia is assumed by the Police and Border Guard Board, which is an agency under the jurisdiction of the Ministry of Interior. However, for the manufacture of the card, the Estonian government has opted to outsource it to a private entity, Oberthur Technologies<sup>125</sup>. It is important to highlight that the eID function of the electronic identity card is voluntary, but contrary to the cases presented in the previous subsection, a high percentage of Estonians have activated it

---

<https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/eid-in-germany>

<sup>124</sup> It is national State-backed PKI.

<sup>125</sup> In 2017, Oberthur Technologies merged with Safran Identity & Security (Morpho) to form IDEMIA.

and frequently use their eID and the digital signature functionality. In fact, it is estimated that approximately 98% of Estonians possess an ID<sup>126</sup> card and use it to identify themselves and access a plethora of e-services securely, ranging from e-government and banking/financial services to public transportation, e-commerce, or telecommunications services, among others.

In general, it can be said that Estonia is a small and highly centralized country. The Estonian government has a leading role in Estonia's National Digital Identity Framework, acting as regulator<sup>127</sup> and primary digital identity provider simultaneously. However, Estonian policy has also been influenced by the Nordic approach. As Nielsen notes (2017, p.4), the result has been a relatively small Public Administration, a focus on public-private partnerships, outsourcing (e.g., the manufacturing of the national identity card), and a high level of fluidity between the public and private spheres.

Estonia's national electronic ID card is not particularly remarkable for its privacy features. Contrary to the German case, the civil identity (i.e., name and date of birth) and unique identifier are stored directly in the electronic certificate and disclosed at each authentication session. Consequently, the system relies on legal barriers to prevent surveillance and correlation of users. However, the Estonian case stands out for the huge efforts made to enable the country's digitalization. In this regard, the case of the X-Road platform, a government “connection platform” where data are not centrally held, is noteworthy. It links individual servers through end-to-end encrypted pathways, letting information live locally. Although X-Road is a government platform, it has become, owing to its ubiquity, the network that many major private firms build on too (Heller, 2017, p.3).

Another key concept in Estonia has been e-residency. An e-resident is an alien to whom Estonia has created a digital identity that allows them to participate in public and private

---

<sup>126</sup> invest in estonia. (n.d.). *e-identity*. Invest in Estonia. Retrieved 2023, August 14 from <https://investinestonia.com/business-opportunities/cyber-security/e-identity/>

<sup>127</sup> As regulator, it provides guidance and control on the National Digital Identity Framework, producing specific laws, regulations, criteria, conditions, procedures and directly controlling the management of digital identities.

law operations in Estonia, regardless of physical location, by justifying a current or former relation with Estonia. This makes it easier for migrant Estonians to maintain a connection to their country, but more specifically, it attracts investment to Estonia by registering a company in Estonia with the e-residency card.

Therefore, compared to other central European countries with strong boundaries between the public and private sectors, in the case of Estonia, there exist open interactions between public agencies and the private sector. Under the eIDAS scope, eID can be deployed on other “carriers,” such as Digi ID<sup>128</sup> or Mobile-ID<sup>129</sup>. However, to set up these other modalities or carriers, particularly in remote scenarios, there exists a strong reliance on the national ID card<sup>130</sup>.

At present, Estonia's Digital Agenda focuses on the development of a smart solution and enabling infrastructures such as speed and capacity of the Internet, user control over their personal data, and improving policy and decision-making. The new Internal Security Development Plan 2020-2030 envisages that by the year 2030, Estonia should be a world leader in issuing secure digital documents, and a stable and sustainable system of digital identity policy should be established, taking into account the need to ensure public safety and national security. In addition, a user-friendly and modern eID application environment should be offered (Pedroli et al., 2021, p.43).

---

<sup>128</sup>Also, based on a smartcard, Digi ID allows the same actions as the main eID without being a National ID document. It is also provided by the Estonian Police and Border Guard Control.

<sup>129</sup> Mobile-ID was introduced to the Estonian market by the largest mobile operator EMT in cooperation with SK, the Estonian Certification Authority. It requires replacing the SIM card with a PKI-capable one. While the Mobile-ID service is offered by private mobile network operators, it is regulated and recognized by the Estonian government, and the SIM cards are issued in cooperation with the Police and Border Guard Board.

<sup>130</sup> Although other private providers are also able to act as “identity carriers” (for example, Smart ID) and provide alternative identification means, the underlying identity remains the same. To set up the new identity means, these private solutions draw on and store the identity provided by the State.



**2.1.3. State-Platform: France's Pursuit of Convenience.** France has notified one electronic identification means with a LoA substantial: *L'identité numérique La Poste* (application *La Poste Mobile*). *L'identité numérique La Poste* is one of the six identities that are offered via *FranceConnect*.

Before *FranceConnect*, the French government launched *Idénium*. *Idénium* was based on the use of a certificate linked to a mobile device (i.e., USB or mobile phone) that contained certain information about the user that this could use to access a number of services. However, this certificate was paid for and did not succeed in practice as it was used by a very reduced number of SPs (Goudet, 2010). In this context, *FranceConnect* was introduced in 2015 by the *Arrêté du 8 novembre 2018 Relatif au Teleservice dénommé "FranceConnect"*<sup>131</sup> which defines it as a teleservice whose purpose is to offer users the possibility to identify and authenticate, in online services, by means of devices implemented by partner IdPs.

*FranceConnect* is a digital identity solution created by the *Direction Interministérielle du Numérique (DINUM)*, which is the government department responsible for modernizing and improving French citizens' accessibility to digital, information, and communication technologies. From a more technical perspective, *FranceConnect* is a connection button that enables authentication of natural persons and access to several public and private services, that is, similar to social network solutions (e.g., type Facebook login). More specifically, *FranceConnect* is an identity federation (based on the OpenID Protocol) where the user can connect utilizing a previous account in one of the six available IdPs: *impots.gouv.fr*, *ameli.fr*, *l'identité numérique de La Poste*, *l'identité numérique MobileConnect* et *Moi d'AriadNEXT*, *le compte de la Mutualité sociale Agricole* and *l'identité numérique YRIS d'AriadNEXT*.

Once the user is recognized by any of the IdPs that are part of the federation, this one transmits a federation key containing the *identité pivot* that will enable the service to identify the user. This *identité pivot* includes a minimum dataset integrated by the

---

<sup>131</sup> Pursuing this *Arrêté*, administrative authorities should be able to simplify their procedures and ensure the security of information exchanges pursuing the *Code des relations entre le public et l'administration*.

gender, birth date, name, surname at birth, and INSEE code from the birthplace. *FranceConnect* transfers this *identité pivot*, which is verified by the SP through the *Répertoire National d’identification des personnes physiques*, as well as a technical identifier, and enables the exchange of data one-off and cryptographies. It is also worth noting that once the user is successfully connected with an IdP, they no longer need to reidentify to access another service, acting as an SSO solution.

Furthermore, this “meta-platform” also enables the secure exchange of data and services from different Public Administrations. The user can opt between requesting the Public Administration to transmit the data or using traditional means. In addition, *FranceConnect* enables some selective disclosure techniques (e.g., transmitting only the relevant tax information instead of the full tax documentation).

Despite its practicality, the solution is not exempt from risks, in particular, due to the federated nature of the digital identity ecosystem<sup>132</sup>. In the spring of 2015, the *Commission Nationale Informatique & Libertés* created a traceability register that enables tracing connections and data shared. In addition, the user must be able to exercise active surveillance over personal data, even after the service is provided. The operational model of *FranceConnect* limits traceability as it only knows the IdP used, not other usage details (i.e., the IdP knows the user but not the services they access, only that requests come through *FranceConnect*). Therefore, tracing user activity requires correlating information from both *France Connect* and the IdP.

In terms of usability, *FranceConnect* can be considered a success, with a number of users over 40 million<sup>133</sup>. In principle, the system was designed to access public and private services, and specific attempts to encourage its use in the private sector have

---

<sup>132</sup> For example, the Access by France Connect using Améli needed to be suspended due to the phishing suffered by Améli accounts in summer 2022. Libération. (2022, September 1). *Cyberattaque. Piratage de FranceConnect: ce que l’on sait*. Libération. Retrieved August 14, 2023 from <https://rb.gy/b4kfgj>

<sup>133</sup> République Française.(n.d.).*FranceConnect simplifie les démarches de plus de 40 millions de personnes* Retrieved August 14, 2023 from <https://franceconnect.gouv.fr/>

existed<sup>134</sup>. Yet, the number of private services compared to the public sector services is around 10%.

The most recent version of *FranceConnect* is *FranceConnect+*, introduced in 2021, which added some extra security measures that enable it to reach the LoA substantial or high according to the eIDAS Regulation but without introducing significant differences. In the form of conclusion, it can be said that what characterized France's approach is the key role of the State in facilitating the country's digital transformation and the prioritization of convenience, opting for models that have already proved to be successful, as is the case of Facebook and other federated IdPs' logins. Nevertheless, this approach is not exempt from challenges and risks; notably, the model is essentially centralized, enabling the State's control over citizens' online activities, and private providers aiming to participate (e.g., *AriadNEXT*) depend on a government platform ultimately.

## ***2.2. Leveraging the Private Sector for Electronic Identification***

While the usual approach in Europe is to depend strongly on the government for electronic identification, especially in accessing public services, some other countries have taken different paths where private providers play a key role. Nevertheless, control and participation from the government in these scenarios differ, potentially resulting in different models or approaches.

### ***2.2.1. Italy's Surveilled Ecosystem of Public and Private Digital Identity Providers.***

Italy has notified two electronic identification schemes to the European Commission under the eIDAS Regulation. On the one hand, the national electronic ID card, or *Carta d'identità Elettronica Italiana (CIE)*, traditionally with a LoA high (although it recently introduced the possibility of operating with a LoA low and substantial). On the other

---

<sup>134</sup> For example, to encourage its use, the State is offering an additional year to companies in the health, social, education, transport, property, and vehicle rental sectors to join the *FranceConnect* experiment. jewelbai.(2022, September 10). *DINUM extends FranceConnect experimentation. Technology News.* <https://trends.akashtdr.com/dinum-extends-franceconnect-experimentation/>

hand, the *Sistema Pubblico di identità Digitale (SPID)* can operate in any of the LoAs (low, substantial, or high).

The *CIE* presents interesting features but is not essentially different from the national electronic identity cards presented above. Therefore, this subsection will focus on the innovative and public-private collaborative approach offered by *SPID*. *SPID* could be described as a circuit based on a public-private partnership where IdPs and SPs participate on the basis of a common legal framework and under the surveillance of a supervisory authority.

Three participants integrate *SPID*: IdPs, SPs, and Attribute Authorities<sup>135</sup>. The number of IdPs has been stable since 2018. Of the nine IdPs, only one is a public entity, and seven are qualified trust service providers<sup>136</sup>. These nine IdPs offer the same product supervised by the State<sup>137</sup>. The basic service (basic identification and authentication) must be provided free of charge, while additional services can be charged from a controlled price list<sup>138</sup>.

According to Article 64.2 ter of the *Codice dell'Amministrazione Digitale*, *SPID* is controlled by the *Agenzia per l'Italia Digitale* or *AgID*, which shall define the characteristics of the *SPID* system (architectural and organizational model of the system, procedures, and requirements for accreditation of digital identity managers, technological standards and protocols, procedures for joining citizens and business...).

---

<sup>135</sup> These are not operational yet. However, it is interesting that this role was already introduced in 2014. In principle, the first Attribute Authority will focus on the attribute of legal mandate. Furthermore, it will rely on a central registry managed by a Public Administration.

<sup>136</sup> The user has the possibility to choose between nine identity providers that offer different level of assurance: *TIM id, SpidItalia, SIELTE id, Poste ID, Namirial ID, lepidia, intesa ID, InfoCert ID, aruba.it ID*. Spid. (n.d.). *How to choose between digital identity providers* AGID. Retrieved 2023, August 15 from <https://www.spid.gov.it/en/what-is-spid/how-to-choose-between-digital-identity-providers/>

<sup>137</sup> This implies that differentiation strategies cannot rely on one identity being more powerful than another, given that SPs accept identities from any IdP. Therefore, the differentiation results from the different identification methods, the presence on the territory, and the existence of contracts with Registration Authorities.

<sup>138</sup> For example, *Aruba SPID* for Professional ID costs 30 euros VAT per year, for *SPID Business ID* 35 euros plus VAT, and other services, such as recognition using webcam 19.90 euros plus VAT.) aruba.it. (n.d.). *Price list*. aruba.it. Retrieved August 15, 2023 from <https://www.aruba.it/en/spid-price-list.aspx>

Additionally, Article 64.3 ter states that accredited digital identity managers within the SPID ecosystem are recognized as public service managers. Such qualification has an impact, for example, on their ability to access free-of-charge administrative sources, like that relating to information on IDs lost or stolen.

*AgID* works as a hub for contracts, surpassing a previous model where each involved party had to sign a contract with each participant. Besides, *AgID* also functions as a Certification Authority, enabling the different participants in the circuit, as well as a registry (publishing metadata of each participant) and, in general, providing information about *SPID* or other collateral services (like software or digital assets).

Furthermore, *AgID* writes the technical rules and guidelines<sup>139</sup>. The *Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014* established the basic rules of the *SPID* circuit and assigned *AgID* the power to define rules and vigilance over the entire system. *AgID* published the first version of its Technical Rules in July 2015, choosing SAML as the underlying protocol. Currently, *SPID* is progressing within the industry to incorporate the OpenID Connect protocol.

The Italian government imposed the adoption of *SPID* (and *CIE* or *Carta Nazionale dei Servizi*<sup>140</sup>) by the entire Public Administration<sup>141</sup> in October 2021 by the *Decreto-Legge 16 luglio 2020 n. 76*. The use of *SPID* in the private sector, although optional<sup>142</sup>, is becoming more common as companies are increasingly utilizing it for their operations, notably in financial services, gambling, and insurance, with an estimated number of 174 private services.

---

<sup>139</sup> See, among others, *AgID*. (2014). Guidelines containing the Technical regulations of managers of qualified attributes pursuant to Article 1(1)(m) of the Prime Ministerial Decree of 24 October 2014 (*Official Gazette No. 285 of 9-12-2014*) or *AgID*. (n.d.) Agreement for adhesion to the public digital identity management system [Template], *AgID*. <https://www.agid.gov.it/>

<sup>140</sup> The *Carta Nazionale dei Servizi (CNS)* was launched in March 2004 by a Joint Decree by the Minister of Economy and Finance and the Minister for Innovation and Technology. It was exclusively for online authentication as it only has microchips with similar characteristics to those of *CIE*. The *CNS* can be issued by any Public Administration that acquires the relevant certificates.

<sup>141</sup> Article 64.2 quarter *Codice dell'Amministrazione Digitale*.

<sup>142</sup> Article 64.2 quinquies *Codice dell'Amministrazione Digitale*.

*SPID* enables not only users access to the companies that have implemented their system but also companies to use *SPID* credentials to confirm their identity with other companies or Public Administrations. Concerning the business model behind it, *SPID* can charge private providers but must make its services free for public providers<sup>143</sup>. Nevertheless, the business model of *SPID* presents a challenge in a country with Italy's dimensions and population, having required public funding by the government.

Finally, the *CIE* (as well as the *CNS*) is a possibility for authentication in the *SPID* system, removing the need to perform physical or remote (via webcam) ID proofing. These have also been notified under the eIDAS Regulation and can be used in cross-border public (and eventually private) services. The *CIE* even offers possibilities for attribute proofing, but these are limited to the attributes specifically contained in the card, while *SPID* offers a more flexible approach, allowing the inclusion of additional attributes.

In conclusion, the Italian solution of *SPID* offers a very interesting and innovative approach to open the door to the participation of private entities in digital identification services while ensuring their operation according to certain quality and affordability standards thanks to the overseeing role of the State. Such an approach ensures the well-functioning and quality of services within the ecosystem; at the time, it also creates market opportunities and increases efficiency, effectively balancing public and private interests.

**2.2.2. Private Sector Involvement in eID Provision: The Belgian Perspective.** Belgium has notified two electronic identification schemes under the eIDAS Regulation. The Belgium eID Scheme FAS/ eCards, which groups the Belgian Citizen eCard and Foreigner eCard and the Belgian eID Scheme FAS/ itsme, which includes the itsme mobile app.

---

<sup>143</sup> Article 64.2 decies *Codice dell'Amministrazione Digitale*.

Belgium was one of the first countries in the world to implement eID at national level, and for that, it developed a framework containing a series of legislative acts<sup>144</sup>. The latest law is the *Loi relative à l'identification électronique du 18 juillet 2017*, which complemented the eIDAS Regulation and introduced the possibility that, besides public providers, external private providers can also develop and operate electronic identification means to access public services. Both types of providers pass through the Federal Authentication Service<sup>145</sup>. Furthermore, the *Service Public Fédéral Stratégie et Appui* shall authorize these services that must comply with the conditions for providing electronic identification services envisaged by the Council of Ministers and established through a Decree.

The Belgian government also provides a national electronic ID card<sup>146</sup>, but conversely to these countries where the eID function is voluntary, in Belgium, the eID card is compulsory for all citizens above 12 years old. The issuance of the national eID card in Belgium corresponds to the public sector but is manufactured by the Thales Group, which is a private company. The involvement of a private company in the manufacturing process does not change the nature of the eID means, which is essentially identical to the ones previously described.

However, besides the national eID card, Belgium has other eID means which are of interest, notably the so-called itsme mobile app. The itsme mobile app is a digital identity service that enables users to prove their identity and sign documents online. This app uses a mobile phone, SIM card, and a personal itsme code to provide a high level of security and is provided by private sector entities. More precisely, itsme has been developed by Belgian Mobile ID SA, which is a private company that includes four major banks in Belgium (Belfius, BNP Paribas Fortis, ING, KBC) and three telecom operators in Belgium (Orange, Proximus, Telenet). Concerning the business

---

<sup>144</sup> *Arrêté royal relatif aux cartes d'identité* or *Arrêté royal portant la décision de procéder à l'introduction généralisée de la carte d'identité électronique*.

<sup>145</sup> The Federal Authentication Service is a gateway that supervises the identification and authentication of users, without interacting with the app's internal processes.

<sup>146</sup> Since 2003, Belgium has been issuing chip-based ID cards. By 2008, every Belgian citizen over the age of 12 had an ID card which made accessing digitised government services more efficient.

model, services to natural persons are provided for free, while potential revenues are generated from business customers<sup>147</sup>.

Public data show that itsme is nowadays a success and widely used in Belgium, with a number of users of approximately 6.7 million, accounting for 80% of adult Belgians. This success is in part thanks to the recognition by the Belgian government as an official mobile identity app, which enables access to public services, but also due to its increasing popularity among private services, which in turn represents an increase in revenues for the company<sup>148</sup>.

In summary, in Belgium, both public and private sectors offer electronic identification services, which are subject to the public sector's control. The Federal Authentication Service oversees the provision of services to ensure certain guarantees are met, although it does not intervene in the actual processes. Private providers are allowed to participate under specific conditions. The result is that the private sector enjoys more opportunities at the time it increases the effectiveness and competitiveness of electronic identification means. However, on the other hand, their participation in the provision of these services can also be seen as a potential threat, particularly due to the overreliance on private solutions.

**2.2.3. The Key Role of Banks for Electronic Identification in Norway.** Norway, and in general, the Nordic countries, present a decisive intervention of banks in providing electronic identification means for accessing public and private services. From the perspective of eIDAS, Norway has notified two electronic identification means with a LoA high of mandatory recognition from October 2023: BankID and Buypass.

---

<sup>147</sup> In their website the prices and contact duration are specified for business users. The set-up cost is 1.500 euros, while the maintenance and support fee is 200 euros. The minimum contract duration is 3 years. itsme. (2023). *Get started with itsme*. Itsme. Retrieved August 15, 2023 from <https://www.itsme-id.com/en-BE/get-started>

<sup>148</sup> According to available data the number of private sector partners is also increasing every year, with over 900 companies now using itsme. belga news agency. (2023, March 28). *Itsme reaches 6.7 million Belgian users, app is now profitable*. belganewsagency. <https://www.belganewsagency.eu/itsme-ziet-aantal-gebruikers-stijgen-tot-67-miljoen-en-is-voor-eerst-winstgevend>



Norway has undergone a peculiar digital transformation driven by the private sector with the introduction of BankID. BankID is a PKI solution today de facto standard for electronic identification, authentication, and electronic signature in Norway. The origin of BankID dates from the late 90s when the major banks in Norway agreed to work toward a common eID infrastructure. The banking industry created a group named BankID Cooperation, which prepared a draft of standards for architecture and interfaces and associated rules and regulations for governing the proposed structure. By June 2003, the common BankID infrastructure was largely in place, and it began distributing one-time password tokens to its customers toward the end of 2004. The government followed this up in 2004 by publishing specifications for national eID solutions.

It took several years of negotiations to align the interests of the banking sector and the government. While the banking sector prioritized generating benefits and leveraging economies of scale, the government aimed to develop a national eID infrastructure. In April 2012, the Norwegian government opened up a tendering process for secure electronic identity to access online public services, and in November 2012, the government announced that it had signed contracts with a number of commercial suppliers, including BankID. The result of this process was that Norwegian citizens have the choice of three commercial eID solutions (BankID, Buypass, and *Commfides*), as well as the existing government legacy solution (MinID).

All Norwegian banks are part of the cooperation for BankID. While BankID has several issuers, it appears as one eID to both users and SPs. Eaton et al. (2018, p.72) conceptualize the emergence of Bank ID Norway as a process of “financialization” that results from the interaction between public and financial actors in order to achieve successful development and adoption of shared solutions. In doing so, governments and financial actors are able to overcome their differences and work together in order to generate a common eID for use by citizens. The authors consider the theory of collective action<sup>149</sup> to explain the broad conditions under which actors are able to cooperate to establish a common good.

---

<sup>149</sup> The theory of collective action reflects the conflict between individual and group-level rationality. While from the individual perspective, there exists a temptation to not contribute (free-riders), the lack of contribution by every individual will result in a detriment of collective interests. See, among others,

The Norwegian government has established a commercial relationship with each of the private suppliers, paying them the number of eID transactions that they enable in a given period. Concerning private service providers, these can integrate BankID by selecting a BankID partner to buy from.

Since its launch, BankID has been widely adopted by the local and regional government, health authorities, and the Norwegian Postal Service. Furthermore, all adult Norwegians have a BankID, and nearly 3 million have a BankID Mobile<sup>150</sup>, enabling access to public and private services. However, no law has been identified mandating its acceptance in access to public services; instead, it seems to rely on its prevalence and convenience. The same can be stated with regard to private services. Conversely to models like Spain or Germany, BankID is also commonly used to access private services such as insurance companies, telecommunications, or even some e-commerce sites.

Besides BankID, other eID means also exist, such as Buypass,*Commfides*, or MindID<sup>151</sup>. However, Bank ID is the most widespread digital identity solution in Norway. To implement this approach to eID, the Norwegian government needed to overcome its ideological concerns about being dependent on a single commercial

---

Willer, R. (2009). A status theory of collective action. *Altruism and Prosocial Behavior in Groups (Advances in Group Processes)*, 26, pp. 133–163. [https://doi.org/10.1108/S0882-6145\(2009\)0000026009](https://doi.org/10.1108/S0882-6145(2009)0000026009)

<sup>150</sup> There exist a regular version and a mobile version. The regular version of BankID uses “one-time codes” to confirm identity that are typically generated via a physical “code brick” that allows you to generate a one-time code as and when needed. The mobile version (BankID Mobile) was launched in 2009 (initially with Telenor), using SIM cards and now is available for all telcos operating in Norway. It requires users to get a BankID from their bank to later obtain a BankID Mobile. A recent version that is app-based has been recently introduced which functions on the basis that the user accepts a requesting ID approval and authenticates before the device (user-device authentication). Nikel, D. (2022, January 27). *BankID: Norway's Digital ID System Explained*. Life in Norway. <https://www.lifeinnorway.net/bankid-norway/>

<sup>151</sup> Buypass is a well-recognized trust service provider for qualified and other certificates for natural persons. All primary healthcare medical practitioners and a large part of hospital practitioners use Buypass cards for signing prescriptions and more. It started with smartcard-based solutions, but now it also offers app-based solutions. *Commfides* provides similar functionalities to Buypass and is mainly used by hospital practitioners. From the perspective of the public sector, ID-porten is the authentication portal for the Norwegian public sector and MindID is the government's own eID solution that can only be used by public services through ID-porten. MindID was launched as a quick solution during the negotiations with eID providers and now is kept mainly because of the young population who are not the required age to obtain a Bank ID and need it to apply for high school education. Norge. No. (n.d). *Electronic ID*. Norge. No. Retrieved August 15, 2023 from <https://www.norge.no/en/digital-citizen/electronic-id>

supplier (Eaton et al., 2018, p.12). To reduce this effect, it still lets the door open to different solutions and lets the individual choose the one they prefer. Although the interdependency of resources could be criticized and might not be the ideal system to deploy in every country, in the case of Norway, it seems to be a success. The Norwegian banks benefit from the revenues that they are making from the government's use of BankID under a commercial relationship, and at the same time, the Norwegian government has benefited from the installed base of BankID users to drive up the usage of e-government services.

### **3. Complexity and Outdatedness of the eIDAS Regulation, but Essential Lessons for the Next Digital Identity Ecosystems**

The eIDAS Regulation has a complex nature, integrating a dual regulatory regime. The first regime concerns electronic identification, focusing on cross-border recognition of digital identities. The second regime affects trust services, harmonizing the legal effects in some cases and probatory and non-discrimination rules among Member States. On the first regime (cross-border electronic identification), the eIDAS Regulation does not prescribe a concrete implementation but instead lets different implementation possibilities open to Member States. The Member States presented throughout this thesis were selected for their diverging approaches in the implementation of the eIDAS Regulation.

In the case of those countries that have resorted to national electronic identity cards, such as Spain or Germany, their lack of convenience has overshadowed their privacy and security features. The case of Estonia can be considered an exemption to this point, but this is logical if we consider that the country's digitalization efforts are notably more advanced than those in Spain and Germany. Yet, as the transition toward digital wallets is advancing at a fast pace, other carriers, such as Mobile ID, are also gaining popularity.

The approach taken by France, while still allocated in the scope of State-owned solutions, has focused on solving the convenience challenge by offering a digital identity that functions similarly to that of social media platforms. However, the increase

in convenience comes at a cost, particularly the power concentration with the State in charge of operating the platform.

Beyond these models, having in common the dominant role of the State in the provision of electronic identification means, other countries like Italy or Belgium have opted for a hybrid approach, enabling the participation of private providers but under a certain control or supervision of the State. Conversely, other countries, such as Norway, present a complete reliance on private providers. However, the participation of private providers normally requires the existence of a viable business model. In the case of Italy and Belgium, a basic identification and authentication service for individuals is provided for free, but additional functionalities or identification of businesses may come at a cost. On the other hand, the Norwegian model is characterized by a commercial partnership between the State and BankID, so the State will be charged for each authentication. Yet the topic of business models for private providers participating in digital identification services is a subject that deserves extensive research and which might affect all sectors where the balance between “free services” and data as a source of revenue has now been questioned.

Nevertheless, I believe that all these experiences are particularly valuable for the European legislator since, as Alonso García notes (1989, p.261) “the development of a more perfect and advanced European Public Law is due to the abstraction and redefinition at the European level of the institutions that already exist in national law, and will ultimately benefit those national laws that regain those institutions that have been improved by the different national experiences.” This is particularly noticeable in the Proposal for Revision of the eIDAS Regulation, which will be explained in the next chapter. eIDAS2 will require Member States to reassess their own digital identity services and to offer a new ecosystem, the EUDI Wallet ecosystem, which will have to function in addition to the existing federation. While the two will have to co-exist rather than replace each other, the lessons learned from past experiences are particularly valuable for the design of the EUDI Wallet ecosystem, which does not necessarily have to follow the approach taken so far. Instead, eIDAS2 represents a unique opportunity to reformulate the digital identity ecosystem, now learning from the limitations in the legal

text, but also in practice, ensuring it has an elevated level of guarantees at the same time it abrogates for the practical success of the solution.



## CHAPTER III

---

### **THE eIDAS2 REGULATION: BUILDING A NEW FOUNDATION FOR DIGITAL IDENTITY**

---

Although the eIDAS Regulation only dates from 2014, it has quickly become outdated, not being able to keep up with the pace of technological and societal evolutions and resulting in the Proposal for Revision of the eIDAS Regulation, commonly known as eIDAS2. The Proposal for Revision of the eIDAS Regulation was published in June 2021, and at the moment of finalizing this thesis, the Proposal was in the final stages of the ordinary legislative procedure, having received the Parliament's final approval on the 29<sup>th</sup> of February 2024 and the Council's formal adoption on the 26<sup>th</sup> of March, and finally signed by the co-legislator on the 11<sup>th</sup> of April 2024.

The insufficiency of the eIDAS Regulation has been recognized in public documents, such as the "Evaluation study of Regulation no.910/2014 (eIDAS Regulation)" published by the European Commission. This report noted that the eIDAS Regulation had only partially achieved its objective for mutual recognition of eID means because, on the one hand, it did not include an obligation for Member States to notify eID schemes, and, on the other hand, because the acceptance of a notified eID scheme requires that the eIDAS node is in production and accepts the notified eID as a receiving country and that the RP is connected to the national node, which is not always the case<sup>152</sup>.

---

<sup>152</sup> Not all Member States' eIDAS nodes are up and running. In particular, there is a reduced number of eIDAS nodes that are operating sending capabilities, and other nodes are not at all running. In addition, there is currently no monitoring and no accessible repository of the number of service providers connected to the national eIDAS node and the fact that a service is connected does not necessarily mean the possibility to perform cross-border authentications.

The lack of acceptance of notified eIDs has concerned both the public<sup>153</sup> and the private sector. Nevertheless, in the second case, the “poor rates of acceptance” are essentially due to the exclusion of the private sector from the obligation of mutual recognition. Therefore, even if some countries have opted for accepting notified national eID schemes in the access to private services, these would not be covered under the eIDAS Regulation for cross-border use.

In addition to this, as already noted, one of the key motivations behind the eIDAS2 Proposal is the high number of identity solutions falling out of the scope of eIDAS. As we have already noted in the first chapter, these identity solutions typically raise privacy and security concerns. In addition, these cannot effectively respond to all sectors, notably when a high degree of certainty is required. Thirdly, the ecosystem that naturally emerges favors the concentration of market power by large technology providers.

Under these circumstances, the eIDAS2 Regulation fosters a transformation in the digital identity ecosystem, aiming to respond, at least partially, to the issues identified. This Regulation lays on the collective and harmonized action of Member States for the purpose of recovering the EU's digital sovereignty; at the time, this attempt is consistent and recognizes the technological advancements made by companies in the field of identification and authentication solutions.

This chapter aims to offer a summarized and clear overview of the modifications introduced by the eIDAS2 Regulation and the impact of the legislative changes on the transformation of digital identity ecosystems. A political agreement on the final text of the eIDAS2 Proposal was reached by November 2023 after an intense phase of dialogues. Therefore, in this section, we refer to the articles included in the final text version currently available, which is expected to be the final one, so that the updates required by this section, will normally consist in removing the reference “Proposal,” (in

---

<sup>153</sup> According to European Commission, Data Collection performed by the CEF eID Building Block, as cited in Ceccanti, et al. (2021, p.36), among EU Member States, only 14% of the key public services (declaring tax, criminal record check, applying for or converting the driving license, applying for a pension, obtaining a residence certificate, accessing social security services, applying for university) are allowed for authentication via eIDAS eID, while 44% of public service providers are allowed to sign in only via a national eID.



this chapter and in the rest of chapters in this thesis) as well as some potential updates in the number of the articles, once both legislative texts merge into an official consolidated version. Nevertheless, given that I have been following the evolution of the legislative text while writing this thesis, this section also includes some references to the Commission's Proposal, as well as the Council's and Parliament's compromise texts.

## **1. The eIDAS2 Regulation: A Visionary Proposal for a Harmonized Digital Identity Metasystem**

### ***1.1. The European Union Digital Identity Wallet as the Cornerstone of the eIDAS2 Digital Identity Ecosystem***

The core objective of the eIDAS2 Proposal is to provide all citizens of the EU with an eID means<sup>154</sup>. Furthermore, these electronic identity solutions shall be highly secure, provide access to public and private services, enable the user to control their personal data, and disclose the data strictly needed for the specific service requested. In that regard, eIDAS2 overcomes the vision of rigid digital identities toward identity attributes relying upon legal identity or a “foundational identity” provided by Member States.

Four different options were considered<sup>155</sup>. Option 3 has been the preferred option by the eIDAS2 Proposal, which requires defining a legal and technical framework for deploying the European digital identity as a user-controlled digital wallet app. As the

---

<sup>154</sup> In this sense, as established in the legislative text, “at least 80% of the citizens should be able to use a digital ID solution to access key public services by 2030.”

<sup>155</sup> Option 0 consisted in not proposing any changes to the current legislation. Therefore, the eIDAS regulation and its framework will remain in force integrating measures envisaged under secondary legislation. Despite this option would have the benefit of not involving significant costs, the weakness in the current legal framework would be expected to persist. Option 1 would have involved creating a European Digital Identity in the form of a strengthened legislative framework for national eIDs notified under eIDAS. It would have required Member States to make eIDs available to all citizens and companies for cross-border use, with harmonized cost and liability rules, extended data sets, and access obligations. Option 2 was already partially introduced in the second chapter and consists of an extension of the eIDAS framework to support the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes across borders. The scope of eIDAS would be expanded to cover this new trust service and will create new opportunities in the market, but the situations of divergence, in particular in the access to these services in the different States, might persist.

Proposal stated, “digital identity wallets are perceived more and more by the public and private sectors as the most appropriate instrument allowing users to choose when and with which private service provider to share various attributes, depending on the use case and the security needed for the respective transaction.” Also, “digital identities based on digital wallets stored securely on mobile devices were identified as a main asset for a future-proof solution, and the government and the private market is already moving in this direction” (Commission’s Proposal, Results of Ex-Post Evaluations, Stakeholder Consultations and Impact Assessments, p.6).

The selected option shows a high level of ambition by the EU in terms of harmonization and recovering digital sovereignty that had been lately lost in favor of tech platforms. Nevertheless, this solution is equally ambitious and complicated. Further to legal requirements, common standards and/or technical references for the wallet app need to be developed<sup>156</sup>. This is because the requirements envisaged in eIDAS2 have a strong technical nature, requiring further instruments for their detail and implementation.

If we compare the eIDAS2 proposal with its predecessor, it is obvious that there is a higher level of harmonization. This is because eIDAS2 introduces a new harmonized eID means, the EUDI Wallet, which is also bound to unlock the potential of a whole new digital identity ecosystem. To achieve the desired level of harmonization the Regulation defines a set of legal requirements for the eID wallet, in particular with regard to its functionalities, as well as privacy, security, and design requirements. However, as will be seen in this section, these requirements are still defined at a high level, leaving their development to the relevant IAs adopted through the exam procedure and in application of Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission’s exercise of implementing powers<sup>157</sup>.

---

<sup>156</sup> For that purpose, the Commission adopted the Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity to work towards the development of a Toolbox to avoid divergent approaches and endangering the future implementation of the European Digital Identity framework.

<sup>157</sup> As Alamillo Domingo (2018, p.76) notes, this means, on the one hand, the willingness of the Member States to guarantee uniform conditions of execution by the Commission and, on the other hand, to

**1.1.1. An Overview of Requirements and Functionalities.** The eIDAS2 Regulation is structured around a nuclear piece, the EUDI Wallet. The EUDI Wallet goes beyond a simple wallet app and emerges as an electronic identification means, requiring a binding process between the app and user identification data (specifically, the PID).

The EUDI Wallet is defined in Article 1 (3,i,42) as “an electronic identification means, which allows the user to securely store, manage and validate identity data and electronic attestations of attributes, to provide them to relying parties and to other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals.”

The definition of the EUDI Wallet has evolved in the successive versions of the legislative text. Initially conceptualized in the Commission’s Proposal as a “product and service,” it is now defined as an electronic identification means. The Parliament’s and the Council’s compromise texts have incised in the nature of the EUDI Wallet as an electronic identification means, and some of the Parliament’s amendments have been maintained in the final definition, such as the storage, management, and validation functionalities and the inclusion of other users of the EUDI Wallet. Furthermore, the final definition only establishes a distinction between identity data (legal identity) and EAAs, somehow delimiting, as we will see later in this thesis, the type of “identity attestations” that might interact with it from a legal perspective.

Explaining the EUDI Wallet can be long and complex. Therefore, for the purpose of making this section more understandable, we have divided it into a set of subsections in line with the key points, features, or requirements for the EUDI Wallet set out in the eIDAS2 Regulation.

**1.1.1.1. Mandate and Modalities of Provision.** The provision of the EUDI Wallet is regulated in Article 6a under the title of “European Digital Identity Wallets.” This

---

maintain control over the Commission's actions, essentially because this type of procedures are articulated around the formation of a committee composed by the representatives of Member States with the mission of reaching an agreement with enough quality and consensus on the concerning Act.

Article establishes that “Member States shall provide a EUDI Wallet within 24 months after the entry into force of the implementing acts referred to in paragraph 11 and Article 6c paragraph 4” (i.e., those specifying the features and functionalities of the EUDI Wallet and its certification). The second paragraph includes three different possibilities for the provision of the EUDI Wallet, in line with, as we already noted in the previous chapter, the modalities for issuance of electronic identification means in eIDAS1.

First, it can be directly developed and provided by Member States (letter a). However, it is also possible that a private entity provides the EUDI Wallet under certain circumstances. Among these two possibilities, letter b does not differ significantly from letter a, insofar as the private entity operates under the mandate of a Member State. Therefore, the EUDI Wallet is indirectly provided by it. Nevertheless, in letter c, an entity provides the EUDI Wallet independently. Yet, this private entity will require recognition from the Member State where it is provided, but it opens the door to the provision of the EUDI Wallet by private entities not directly controlled by the State.

This Article has suffered some modifications influenced by the Council's and the Parliament's texts. The Council's text proposed changes encouraging member States to disclose the source code of software components used for processing personal data and data of legal persons<sup>158</sup>. Meanwhile, the Parliament's text called for open-source code for the EUDI Wallet<sup>159</sup> and suggested modifications aiming to prevent practices, such as seeking out the most advantageous Member State for independently issued wallets, requiring them to be recognized by the Member State where these are provided<sup>160</sup>.

The final text maintains the modifications suggested by the Parliament and mandates in Article 6a paragraph 2a that the source code of the application software components of the EUDI Wallets shall be an open-source license. However, it must be noted that this obligation only refers to software components, and as such, there is a possibility that Member States, for duly justified reasons, decide that specific components other than

---

<sup>158</sup> Recital 11a Council's text.

<sup>159</sup> Article 6a 2a Parliament's text.

<sup>160</sup> Article 6a paragraph 2 letter c Parliament's text.

those installed on users' devices shall not be disclosed. In addition, Article 6a paragraph 2 letter c of the final text mandates that those EUDI Wallets provided independently of a Member State shall be recognized by “that” Member State, preventing some sort of “forum shopping practices” across Member States.

**1.1.1.2. Functionalities.** The functionalities of the EUDI Wallet are described in Article 6a paragraph 3. More specifically, letter a of this Article establishes that the EUDI Wallet shall enable the user to “securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, offline in order to use public and private services, while ensuring that selective disclosure of data is possible.”

Pursuing this definition, the EUDI Wallet shall enable at least the legal identification of its owner<sup>161</sup> and shall also have the capacity to receive, store, combine, and selectively present, associated or not to the legal identity, proof of attributes. In addition, letter b states that the EUDI Wallet shall allow the user to sign with qualified electronic signatures or seals (depending on whether the user of the EUDI Wallet is a natural or a legal person), thus demonstrating an interrelation between electronic identification and trust services already existing in notified electronic identification means, such as the *DNIe*.

The latest eIDAS2 text has introduced additional functionalities in Article 6a paragraph 3. These additional functionalities refer to the ability to generate pseudonyms, store and encrypt them locally (letter ac). The EUDI Wallet shall also enable the user to authenticate other users' EUDI Wallets (letter ad) and access the record of all transactions (letter ae), including a list of SPs or users with whom you have connected and, where applicable, exchanged data. In addition, the EUDI Wallet shall enable the user to request the deletion of data or, when necessary, report unfair or unlawful behavior to the competent authorities. Furthermore, they shall be capable of

---

<sup>161</sup> Except in those cases of use of the EUDI Wallet on behalf of other person (e.g., child, person with disabilities...).

downloading user data, EAAs, and configurations (letter ba) and exercise the right to data portability whenever technically possible (letter bb).

In the provision of these functionalities, the EUDI Wallet is subject to a set of requirements from the perspective of privacy, security, and the use of common standards.

**1.1.1.3. Security Requirements.** Article 6a paragraph 4 letter c introduces a crucial security requirement as it demands the EUDI Wallet to meet the LoA high, in particular, applied to the requirements for ID proofing and verification and eID means management and authentication. Although the aim of this requirement was to create secure and reliable eID means, it has led to a lot of controversies due to the difficulties and efforts that it involves for those countries that had already notified and widely used electronic identification means with a LoA substantial.

Nevertheless, the Council's text introduced the possibility of achieving a LoA high by eID means with a LoA substantial<sup>162</sup>, and this modification has been maintained in the final text. More specifically, Article 6a paragraph 11a provides that the Commission shall refer to standards that facilitate the onboarding to the EUDI Wallet of users of electronic identification means conforming to LoA substantial in conjunction with additional remote onboarding procedures.

In addition, from a security standpoint, it is also remarkable the requirement for mutual authentication contained in Article 6a paragraph 4 letter d that mandates the EUDI Wallet to include a mechanism that allows RPs to authenticate themselves to the user pursuing Article 6b<sup>163</sup>, as well as the Parliament's text requirement for security-by-design<sup>164</sup> that is maintained in Article 6a 6.

---

<sup>162</sup> Article 6a 11a Council's text.

<sup>163</sup> Note that, as explained in the previous chapter, the mutual authentication functionality already existed in eID means such as the German national eID card.

<sup>164</sup> Recital 3a, Article 6a 6a Parliament's text.

**1.1.1.4. Privacy Requirements.** In addition to the user traceability functionalities, which become a key element in the latest text of the Proposal, the EUDI Wallet is subject to other privacy requirements that aim to limit surveillance practices by providers of digital identity services. In this regard, Article 6a paragraph 4 letter b establishes that “Digital Identity Wallets shall ensure that trust service providers issuing electronic attestations of attributes cannot receive any information about the use of these attributes.” Therefore, technologies like SAML or OpenID Connect would not be possible under this requirement because they cannot prevent traceability.

Furthermore, Article 6a paragraph 7 establishes that the user shall be in full control of the EUDI Wallet<sup>165</sup> and, therefore, EUDI Wallet Providers shall only request the necessary data for the provision of the wallet. In addition, to avoid potential abuses resulting from data combination, the EUDI Wallet Provider shall keep data necessary for the provision of the wallet physically and logically separated from any other data, and in the event that the wallet is provided by a private entity, this must create a separate legal entity.

Another key privacy requirement introduced by the eIDAS2 Proposal is the non-traceability requirement. Originally, the Commission’s Proposal limited this requirement to qualified trust services providers. However, the Council’s text and the Parliament’s text extended the non-traceability requirement to all trust services providers<sup>166</sup>, and this amendment has been maintained in Article 6a paragraph 4 letter b.

Furthermore, the final text has included some mentions to the technical framework of the EUDI Wallet. More specifically, Article 6a paragraph 7b letter a provides that the EUDI Wallet must prevent Issuers of EAAs from obtaining data that allows for tracking, linking, correlating, or obtaining knowledge of the user's transactions or behavior unless explicitly authorized by the user. In addition, Article 6a paragraph 7b letter b states that

---

<sup>165</sup> In addition, Article 6a 3 already establishes that the use of the EUDI Wallet shall be transparent and traceable for the user.

<sup>166</sup> Article 6a paragraph 4 letter b Council’s text and Parliament’s text.

the EUDI Wallet must enable privacy-preserving techniques that guarantee unlinkability where, in the proof of certain attributes, the identification of the user is not required.

Finally, Article 6a paragraph 7c includes a general obligation of compliance with the GDPR and for the introduction of national legislative provisions by Member States.

**1.1.1.5. Standardization Requirements.** The final text of the eIDAS2 Proposal has significantly extended the obligation for the EUDI Wallet to support common protocols and interfaces in Article 6a paragraph 4 letter a. The final text includes the issuance and validation of PID and EAAs (1 & 2), both qualified and non-qualified. In addition, it should facilitate the secure sharing and presentation of these data (including selective disclosure), both online and offline (3). Likewise, the interfaces should allow user interaction with the wallet, including the display of a “EUDI Wallet trust mark ” (4), and support protocols for the secure on-board of the user, the interaction between EUDI Wallets (4a), the authentication of users and the verification of the authenticity and validity of the wallets (4c, 4d and 4e). Furthermore, the Article includes mechanisms that enable the user to request the deletion of personal data or the report of suspicious or unlawful data requests (4h & 4i). Finally, the EUDI Wallet shall also provide a common interface for the creation of qualified electronic signatures or seals (4j).

The Regulation does not specify any technical standards. However, these requirements are being defined at a technical level in line with the functionalities presented above, particularly privacy and security requirements, and included in the ARF<sup>167</sup>, which prepares the IA provided in Article 6a paragraph 11.

**1.1.1.6. Cross-Border Identity Matching.** One of the most discussed obligations included in the eIDAS2 Regulation is the requirement for a unique and persistent identifier. More specifically, Article 6a paragraph 4 letter e and Article 11a paragraph

---

<sup>167</sup> The explanation of this document is included during the following sections. The ARF document cites specific standards and protocols vital to this process. In particular, it mentions the ISO/IEC 18013-5:2021 standard and the W3C Verifiable Credentials Data Model 1.1.



2 require ensuring that PID (i.e., those minimum identification data that will enable the provision of the EUDI Wallet) uniquely and persistently represent the natural person associated with it. While the requirement for a “unique” identifier is not something new, the requirement for it to be persistent has created an important debate about the feasibility of the eIDAS2 Proposal, where the obligation to have a unique and persistent identifier may violate Constitutional rules in some Member States<sup>168</sup>.

This Article has been renamed in the several versions of the legislative text. The Council’s text renamed Article 11a as “Record Matching” and mandated conformity with Union and national law. On the other hand, the Parliament’s text renamed this Article as “Cross-border user identification.” Besides the change in the denomination, both texts opened the door to national interpretations of the unique identifier, which might be RP or sector-specific, as long as they uniquely identify the user across the Union<sup>169</sup>.

The final eIDAS2 text has adopted a combination of the Council's and Parliament’s compromise texts and opted for the term "Cross-border identity matching." This requirement applies to electronic identification means and EUDI Wallets. The legislative text does not detail its implementation, but following some existing national approaches, it could lead to sector-specific or SP identifiers, as long as it uniquely identifies the user across the EU.

In fact, this cross-border identity matching is not something new, but we already identify examples of this in the public sector, such as the case of Cl@ve, where access from other Member States triggers the generation of an *NIE* “on demand,” ensuring the unique identification of that person.

**1.1.1.7. Certification Requirements.** The approach to the certification of the EUDI Wallet has suffered significant modifications in the last version of the legislative text. While the Commission’s Proposal requirement on certification focused on privacy and

---

<sup>168</sup> For example, it is the case of Germany, France or Austria.

<sup>169</sup> Article 3 letter i 55a Council’s text and 11a 3 Parliament’s text.

cybersecurity certification, the new Article introduces a generic certification requirement in accordance with the minimum standards or requirements stipulated in Article 6a as set out in the IA provided in paragraph 11 of Article 6a and feasible possibilities for certification of cybersecurity requirements in a reasonable time.

Regarding cybersecurity certification, the Council's text provides the EU Common Criteria Certification Scheme (EUCC scheme) published under the Cybersecurity Act as a transitory regime for cybersecurity certification until ENISA certification is available<sup>170</sup>. This modification has been maintained in the final text, which establishes that pursuing Article 6c paragraph 3, certification must be carried out in accordance with the cybersecurity schemes established pursuant Regulation (EU) 2019/881 (Cybersecurity Act) and the IAs that provide for the processes and specifications for the certification of the EUDI Wallet.

In accordance with Article 6c paragraph 2a, for those aspects other than cybersecurity, Member States shall develop their own certification schemes following the processes and requirements established by the IAs provided in Article 6c paragraph 3. In addition, they will have to submit a draft of their national certification schemes to the EDICG, which is included in Article 46d of the final text of eIDAS2.

Concerning privacy certification, despite the modifications in the Council's compromise text<sup>171</sup> to cover the "EUDI Wallet Issuer data processing activities," in the final text, we can say that privacy certification "disappears." The drafting of Article 6c paragraph 3 substitutes the term "shall" with "may," leaving the certification of privacy requirements up to Member States. This modification is understandable if we consider the complexities associated with GDPR certification in this concrete scenario<sup>172</sup>.

---

<sup>170</sup> Article 6c 1 Council's text. The preparation of a cybersecurity scheme by ENISA can take up to two years.

<sup>171</sup> Article 6c 2 Council's text.

<sup>172</sup> The adoption of an EU-level GDPR certification (The European Data Protection Seal) is a complex procedure that requires the submission of the certification scheme by scheme owners or certification bodies and that involves the European Data Protection Board. In addition, there exist complexities in determining the data processing operations and controllership in the EUDI Wallet. First, because the final version of the eIDAS2 final text makes a general reference to Article 6a, which includes not only data processing operations in the provision of the EUDI Wallet, but also in its functioning itself. Secondly,

Pursuing Article 6d paragraph 1, Member States are required to inform the Commission and the EDICG of any certified EUDI Wallet provided. The Commission will, in turn, compile and update a list of these certified wallets, similar to the list for electronic identification schemes notified under eIDAS1. However, there is an essential difference between the certification regime for the EUDI Wallet and for electronic identification schemes. While the peer-review method continues to be the procedure for the certification of electronic identification schemes pursuing Article 12a of the final text of the Regulation, in the case of the EUDI Wallet, the certification procedure is that of the certification of an activity (which also includes a product), being, therefore, more similar to the one of trust services.

Finally, Article 6da mandates that in the event of a security breach in the EUDI Wallet, the providing Member State shall, without delay, suspend the issuance, revoke the validity, and inform other Member States and the Commission. In the event this breach is not remedied within three months, proceed to the withdrawal accordingly.

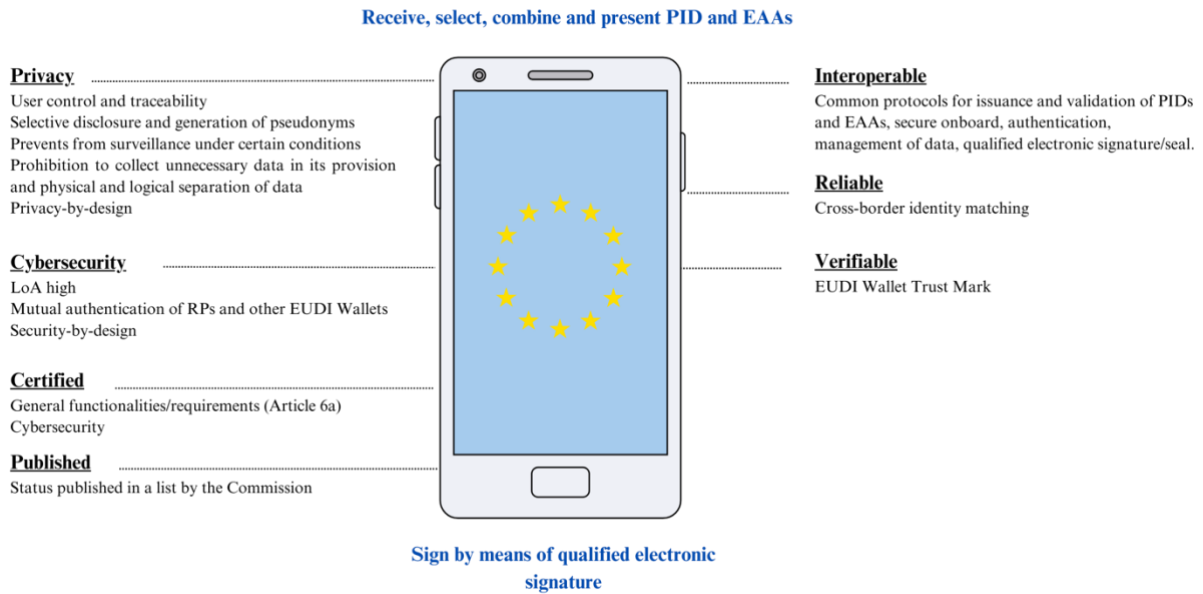
To close this overview, it is important to retain that the EUDI Wallet aims to become a secure and privacy-respectful digital identity means that enable the user to identify themselves and to manage and control their personal data during identification and authentication processes, in public and private services. On this last point, eIDAS2 introduces, in my opinion, the second key amendment, the extension of the mandatory scope of acceptance of the EUDI Wallet to private providers.

---

because the provision of the EUDI Wallet is a complex scenario that might involve different roles, challenging the traditional allocation of GDPR roles of data controller/processor. This topic is more detailed in Annex B.

**Figure 10**

Features and Functionalities of the EUDI Wallet



**1.1.2. New Services Required to Accept the European Union Digital Identity Wallet.**

The eIDAS2 Regulation creates an innovative, harmonized, “EU-level” eID means. However, the EUDI Wallet would have very limited effectiveness if it were not made of mandatory acceptance for a wide range of RPs in the public and private sectors. The Article 6db in eIDAS2 final text introduces an essential change in this regard as it requires a set of categories of RPs to accept the EUDI Wallet for identification and authentication processes under the title “Cross-border reliance on European Digital Identity Wallets.”

In this sense, paragraph 1 maintains online services provided by public sector bodies (already included in eIDAS1). However, the main change has been the inclusion of private services. Paragraph 2 establishes that “where relying parties providing services are required by national or Union law to use strong user authentication for online identification, or where strong user authentication is required by contractual obligation (...) private relying parties shall accept the use of European Digital Identity Wallets.”

This section lists a set of sectors included in this category: transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education, or telecommunication. While this list covers a broad range of categories, it lacks specific details about the services offered within them. Additionally, there is a coincidence between the concepts of "strong customer authentication" in PSD2 and "strong user authentication" in eIDAS2, causing concern in the payment sector<sup>173</sup>.

Paragraph 3 is the most innovative inclusion in the scope of mandatory reliance on the EUDI Wallet. More specifically, it establishes that very large online platforms shall also accept EUDI Wallets. To define very large online platforms, eIDAS2 refers to Article 25.1 of the DSA<sup>174</sup>, which defines them as those with a number of users equal to or higher than 45 million in the scope of the Union. It is worth noting that although eIDAS2 mandates the acceptance of the EUDI Wallet by these platforms, the EUDI Wallet is voluntary. Therefore, the obligatory acceptance of the EUDI Wallet shall not mean the impossibility of continuing to use alternative identification means.

In addition, the eIDAS2 text introduces specific privacy requirements for very large online platforms that shall only request the minimum attributes necessary for the specific online service for which identification/authentication is requested. The Parliament introduced a different drafting providing the user's right to pseudonyms and the prohibition to combine personal data with any other data collected through any of

---

<sup>173</sup> The European Credit Sector Associations are questioning the approach of including payments in eIDAS2. They believe it could result in excessive costs for merchants and service industries that accept card payments under PSD2, as well as due to the lack of clearly defined liability rules in eIDAS for payments. They propose limiting the mandatory use of the EUDI Wallet to only verifying the user's identity. European Credit Sector Associations. (2023). *European Credit Sector Associations call for removing payments from the scope of the Digital Identity Regulation*. [https://www.wsbi-esbg.org/wp-content/uploads/2023/04/ECSAs-Public-Statement\\_final-1.pdf](https://www.wsbi-esbg.org/wp-content/uploads/2023/04/ECSAs-Public-Statement_final-1.pdf)







<sup>174</sup> Article 25.1 DSA states that "this Section shall apply to online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3." Pursuing paragraph 3, "the Commission shall adopt delegated acts in accordance with Article 69, after consulting the Board, to lay down a specific methodology for calculating the number of average monthly active recipients of the service in the Union, for the purposes of paragraph 1. The methodology shall specify, in particular, how to determine the Union's population and criteria to determine the average monthly active recipients of the service in the Union, taking into account different accessibility features."

the services they provide unless necessary or explicitly requested by the user<sup>175</sup>. However, these specifications have not been maintained, at least in the text of the Regulation.

In the case of RPs of medium and small size, the Proposal does not impose mandatory acceptance of the EUDI Wallet. Yet, it states the Commission’s obligation to encourage and facilitate the development of self-regulatory codes at the Union level (codes of conduct<sup>176</sup>) to contribute to the wide availability and usability of the EUDI Wallet. These should ensure the acceptance of the EUDI Wallet, particularly for SPs relying on third-party electronic identification services.

**Table 3**

Cross-Border Reliance Comparison eIDAS1 versus eIDAS2

	eIDAS1 Cross-border acceptance of notified eID means	eIDAS 2 Cross-border acceptance of the EUDI Wallet
<b>Mandatory</b>	 Services offered by public sector bodies	 Services offered by public sector bodies  Services requiring strong user authentication  Very large platforms
<b>Voluntary</b>	 Services offered by the private sector	 Other providers and platforms with less than 45 million of users in the Union

Article 12b is not envisaged as a rigid clause. Paragraph 5 establishes that the Commission shall make an assessment within 24 months after deployment of the EUDI Wallet, showing availability and usability, considering the cross-border presence of SPs, technological developments, and evolution in usage patterns and consumer demand. In the Commission’s Proposal, this clause provided the possibility of including additional

<sup>175</sup> Article 12b paragraph 3 Parliament’s text.

<sup>176</sup> A code of conduct is a set of rules that businesses or industry groups voluntarily adopt to regulate their behaviour in a certain area. Although codes of conduct are not legally binding, they are subject to oversight by regulatory authorities to ensure that they are being followed.

private online service in the mandate to accept the use of the EUDI Wallet strictly upon voluntary request of the user (i.e., coexisting with other identification and authentication means). This is not explicitly stated in the last version of eIDAS2, which I believe is reasonable in terms of offering enough legal certainty for SPs. Nevertheless, this Article has been drafted using broad concepts. On the one hand, the delimitation of very large online platforms will depend on the designations made according to the DSA. On the other hand, in the case of those parties requiring strong user authentication, eIDAS2 leaves a broad margin of discretion in their determination. It is worth noting that the legal text only establishes a specific deadline for those RPs requiring strong user authentication, 36 months after the adoption of the IAs concerning the technical specifications and procedures for the EUDI Wallet. In the case of public sector bodies and very large platforms, there is no specific deadline included in the Regulation, which, in my opinion, could cause some concerns, in particular considering the reluctance of some very large platforms to integrate the EUDI Wallet.

Concerning procedural requirements, Article 6b mandates RPs to communicate to Member States their intention to rely on the EUDI Wallet and its intended use. Although this requirement can facilitate better traceability, particularly concerning privacy policies, it raises some challenges, such as for individual terminals used in scopes like traffic control or police officers. The Council's and the Parliament's texts introduced some amendments that have been combined in the final text of the Regulation. Article 6b mandates a registration procedure by RPs, as suggested in the Parliament's text. Nevertheless, it requires this procedure to be cost-effective and proportionate to risk, pursuing the Council's text. Regarding the information to be provided, RPs will have to communicate the Member State where they are established, the name of the RP and registration number, contact details, and the intended use of the EUDI Wallet.

The final Article emphasizes that RPs shall not request any data beyond what they have registered for, imposing stricter compliance with the data minimization principle<sup>177</sup>. However, other requirements included in the Parliament's text, such as the need for

---

<sup>177</sup> As suggested in Article 6b 1d Parliament's text.

special approval when the RPs intend to process special categories of personal data, disappear. In addition, the final text emphasizes the obligation of RPs to authenticate to the user, such as in paragraph 2a. Likewise, although the EUDI Wallet is mandated to include mechanisms that enable the validation of PID and EEAs, the responsibility for carrying out data authentication procedures lies on RPs (Article 6b paragraph 3).

Finally, some additional inclusions in the final text have been the obligation for RPs not to deny the use of pseudonyms where user identification is not required by Union or national law and the specific provision concerning intermediaries or identity brokers in paragraph 3a that forbids intermediaries to register any data related to the transaction.

In conclusion, the eIDAS2 Regulation extends its scope of application and ensures that the solution of the EUDI Wallet achieves a high level of usability by imposing mandatory acceptance. Nevertheless, the use of the EUDI Wallet is voluntary. Therefore, it shall concur with alternative options, and its success will strongly rely on the citizen's desire to use it. Yet, imposing mandatory acceptance to these private RPs is a big step, in particular for very large platforms, as an attempt, in collaboration with the willingness of the user, to limit their predominant role in digital identity ecosystems.

### ***1.2. New Trust Services in eIDAS2 and their Impact on Digital Identity Ecosystems***

Besides the EUDI Wallet, the eIDAS2 Proposal introduces other essential modifications for the creation of an entirely new digital identity ecosystem. In particular, the updated regulation offers new possibilities for a combination of the legal regime for electronic identity with trust services. More specifically, the eIDAS2 Proposal creates a new trust service that enables the provision by public and private entities of identity credentials, extending the form of “legal identity” embodied in the EUDI Wallet with a wide range of identity attributes. In addition, the Proposal introduces other modifications in the scope of trust services of great importance; however, for the purpose of making this section consistent with the subject of study in this thesis, the analysis will be limited to those with a relevant impact on digital identity ecosystems.



***1.2.1. Issuers of Electronic Attestations of Attributes: Paving the Way for a Regulated Ecosystem of Identity Credentials.*** The new trust service of Issuers of EAAs is another key piece of the eIDAS2 Proposal, creating a regulated market (at least partially<sup>178</sup>) for the provision of identity credentials participated by private entities. This is a possibility that until now was not included in the eIDAS Regulation, and the “chink” or “loophole” of the digital certificate for electronic signature was disproportionate and did not meet current demands.

Through the creation of this new trust service, the eIDAS2 Proposal overcomes the limited vision of identification to a legal or “foundational identity,” including all sorts of attributes that can be related to a natural person, legal person, or even things (e.g., that a certain vehicle is an ambulance). This section has been strongly modified. Both the Council’s and the Parliament’s text identified an important shortcoming, which was the lack of a specific regulatory provision that enables public entities to issue EAAs. The final text has included the Council’s approach, which proposed specific legal effects for these EAAs, subject to concrete requirements.

The Proposal only includes a brief definition of EAAs in Article 1 (44) as those electronic attestations in electronic form that allow the authentication of attributes. However, it dedicates Section 9 to EAAs. The legal effects of EAAs are defined in Article 45a. Paragraph 1 provides that these “shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form, or it does not meet the requirements for qualified electronic attestations of attributes.” This effect, common to all trust services, applies to both qualified and non-qualified EAAs. Nevertheless, paragraph 2 adds that when the EAA is qualified or issued by or on behalf of the public sector body responsible for an authentic source, this shall have the same legal effect as a lawfully issued attestation in paper form. Furthermore, pursuant paragraph 3, in the case of EAAs issued by or on behalf of a public sector body responsible for an authentic source, this shall be recognized as such

---

<sup>178</sup> We claim that the regulation is partial because it does not aim to cover all type of identity credentials that might exist, and which might not fall under the category of EAAs. Still, the definition of EAAs is notably broad, hence, it could be expectable that most of identity credentials that do not fulfil the requirements of qualified EAAs, fall under the category of non-qualified EAAs.

(i.e., EAA issued by or on behalf of the public sector body responsible for an authentic source) in all Member States<sup>179</sup>.

This new possibility, the EAAs, has resulted in an innovative double legal configuration. On the one hand, the regulation for trust service providers maintains the traditional distinction between qualified and non-qualified trust services with their associated legal effects, as previously described in the second chapter of this thesis. On the other hand, a specific legal regime for the issuance of public entities responsible for authentic sources (or other entities that might act on behalf of authentic sources) of EAAs with specific associated legal effects.

Concerning the distinction between qualified and non-qualified EAAs, this new trust service has maintained the traditional separation between both modalities. Article 45c only establishes the requirements for qualified EAAs, leaving non-qualified EAAs with very little regulation. This Article refers to Annex V, which establishes the requirements for qualified EAAs<sup>180</sup>. Concerning the EAAs issued by or on behalf of a public sector body responsible for an authentic source, the specific requirements are contained in Article 45nd. Notably, these EAAs will have to include the data mandated in Annex VIa, but also comply with concrete obligations that enable the identification and validity of the issuing authority or authentic source, as included in this Article<sup>181</sup>.

---

<sup>179</sup> It should be noted, however, that in the case of public sector bodies, EAAs shall not obligatory substitute the electronic identification means used in this scope unless specifically allowed by the Member States (Article 45b).

<sup>180</sup> Annex V provides that a qualified EAA shall contain: a) An indication, at least in a form suitable for automated processing that is a qualified EAA; b) A set of data that unambiguously represents the qualified trust service provider, including at least the Member State where is established. In the case the EAA is issued by a legal person, the name and registration number. If issued by a natural person, the person's name; c) A set of data unambiguously representing the entity to which the attested attributes are referring, and indicate if a pseudonym is used; d) Attested attribute or attributes, including necessary information to identify the scope of those attributes; e) Attestation's period of validity; f) Attestation identity code, which must be unique for the qualified trust service provider and if applicable the indication of the scheme of attestations is part of; g) The location where the certificate supporting the advanced electronic signature or advanced electronic seal is available free of charge; and i) The information or location of the services that can be used to enquire about the validity status of the attestation.

<sup>181</sup> At this point, I strongly recommend the research work of Jose María Delgado Báidez, who studies the differences between the identity wallets and the already existing data spaces within the public sector, such as the *Carpeta Ciudadana* in Spain. Delgado Báidez, J.M. (2023). La Cartera de Identidad Digital Europea y el principio de "solo una vez" en Derecho español. *Revista de Privacidad y Derecho Digital*, (32), pp.19-73.

Furthermore, to ensure the functioning of this new “market of identity credentials,” eIDAS2 includes in Article 45d an interesting clause enabling the consultation by qualified trust service providers of data held by public sources. More specifically, it mandates authentic sources within the public sector to take measures to allow qualified trust services providers of EAAs to verify, at the request of the user, the authenticity of an attribute directly against the relevant authentic source defined at national level or via intermediaries. Although this obligation is limited to the attributes referred to in Annex VI<sup>182</sup>, it is expected that it might enable faster and more efficient services by these providers, enabling the offer of other legal procedures that typically require the previous attestation of these data.

On the other hand, Article 45f includes a set of privacy rules in the provision of EAAs. A general rule for both qualified and non-qualified EAAs is the impossibility of combining personal data relating to the provision of those services with personal data from any other services offered by them, requiring to be kept logically separate from other data held. In addition, in the case of qualified EAAs, a functional separation from any other service they provide is required. Although this legal provision will have to be interpreted<sup>183</sup>, the final aim is to limit practices that are common among big tech companies. When an entity combines its digital identity services with other services it offers, such as a social network, it creates opportunities for surveillance and profiling.

Finally, Article 45e has included an “interoperability rule” mandating that providers of EAAs shall provide EUDI Wallet users with the possibility to request, obtain, store, and manage the EAAs irrespective of the Member State where the wallet is provided and in the case of qualified providers, these shall provide an interface with the EUDI Wallet pursuing Article 6a.

---

<sup>182</sup> The minimum list of attributes: address, age, gender, civil status, family composition, nationality, educational qualifications, titles and licenses, professional qualifications, public permits and licenses, and financial and company data.

<sup>183</sup> The Commission’s Proposal originally required a physical separation from any other data held and the creation of a separate legal entity.

This new trust service is a crucial part of the ecosystem that will involve both public and private entities, creating business opportunities for private providers and for the public sector for the improvement in the provision of their services. It is important to note, however, that despite the interoperability rule mentioned above, the EUDI Wallet and the EAAs are two separate pieces. Consequently, although these are thought, in principle, to work together, it is not necessary in all cases, and it is essential to keep in mind that these are subject to different legal regimes. As such, the mandatory acceptance of the EUDI Wallet provided in Article 6db of the eIDAS2 Proposal only concerns the EUDI Wallet as an electronic identification means. The admission and validity of EAAs depend on the specific provisions introduced in this section and, in general, the common regulation on trust services or national or sectorial regulation.

To conclude, it is important to note that although in this section we have referred to the issuance process for the purpose of easing its understanding, this trust service involves other key processes/services as it is the validation of EAAs, specifically included in Article 1 (16, letter fa). As such, it is possible that a single entity can perform all processes, but it also leaves room for the potential emergence of separate legal entities/trust services.

***1.2.2. Electronic Ledgers: Unlocking the Potential of Distributed Ledger Technologies.*** The eIDAS 2 Proposal introduces other new trust services with a potential impact on digital identity ecosystems, among which one is particularly noteworthy: the “Electronic Ledgers.” The new trust service of “Electronic Ledgers” introduced in Section 11 represents a step forward in regulating innovative technologies and opens the door to “more purely decentralized” digital identity ecosystems.

Following the principle of technology neutrality, the eIDAS2 Proposal does not make any reference to a concrete technology. However, the definition and, more notably, the requirements for qualified electronic ledgers seem to hint at a specific technology. An “electronic ledger” is defined in Article 1 (53) of the Proposal as a sequence of electronic data records, ensuring their integrity and the accuracy of their chronological

ordering. Article 45i establishes that qualified Electronic Ledgers shall<sup>184</sup> ensure the uniqueness, authenticity, and correct sequencing of data entries recorded in the ledger; the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry; and record data in such a way that any subsequent change to the data is immediately detectable. Based on these traits, we can deduce there is a correlation with the typical features found in DLT or, more specifically, blockchain.

Non-qualified Electronic Ledgers are exempt from meeting the criteria set forth in Article 45i, but these do not benefit from a presumption of accuracy. Qualified Electronic Ledgers enjoy the presumption of data uniqueness and authenticity. In addition, they guarantee the accuracy of their timestamps and their sequential chronological ordering within the ledger. As a result, the definition of qualified Electronic Ledgers is more specific, demanding stricter requirements in the underlying technology, while non-qualified Electronic Ledger admits broader types of technologies insofar as these guarantee the integrity and accuracy of the chronological order. The distinction, however, might be subtle in practice, particularly in scenarios where the same technology is utilized (e.g., blockchain technology), and the only differentiation lies in the official recognition as a qualified trust service provider.

Despite the political debate surrounding this trust service, it will be retained in the final text of eIDAS2. The inclusion of this new trust service facilitates ensuring the quality and guarantee of such technologies and their implementation in a very broad spectrum of scenarios. One such scenario is digital identity ecosystems, opening the door to technologies such as DIDs or blockchain. Furthermore, it can have an essential impact on the establishment and maintenance of trust lists, increasing transparency and resilience, but notably, for technical feasibility, “considering that only taking into account Spanish municipalities, there would be roughly 10.000 issuers and they would all need to be added to a trust list, something unmanageable with PKI technology” (Alamillo Domingo, whose words were reproduced in Tinianow, 2023). In addition, this new trust service grants greater legal certainty to existing projects affecting the

---

<sup>184</sup> In addition, these shall also be created by one or more qualified trust service providers.

digital identity landscape, as is the case of EBSI<sup>185</sup>, which offers very interesting exploitable features for digital identity by unlocking the potential of blockchain technology.

Nevertheless, this new trust service is limited to the regulation of “a form of technology” and might only act as an anchor piece, leaving room for sector-specific legislation that could regulate other aspects (such as the composition of the ledger, liability, etc.) in the particular sector where this technology is implemented.

## **2. Foundations of Emerging Digital Identity Ecosystems**

### ***2.1. Transformation in Roles and Communication Flows***

The eIDAS2 Regulation is the start of a new paradigm in digital identity ecosystems. The Regulation is not limited to setting new legal roles, but it also demands a profound change in the ecosystem participants' dynamics. More specifically, it forces the transition from a centralized model with a single or limited number of IdPs toward an open ecosystem where various public and private entities can assume the IdP role. At the same time, the EUDI Wallet empowers the users to control their identity information, enabling direct communication channels and reducing the reliance on external IdPs.

The model behind this transition has been described under various terms, such as user-centric digital identity, decentralized digital identity, or SSI. However, there is no consensus on the precise definitions of these terms, resulting in conflicting notions and interpretations. At the same time, the eIDAS2 approach is unique and combines various features from these models.

---

<sup>185</sup> Before eIDAS2, the European Union had already taken steps to develop a cross-border services infrastructure based on Blockchain called the European Blockchain Services Infrastructure (EBSI). European Commission. (n.d.). *What is EBSI?* European Commission. Retrieved October 21, 2023 from <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi>

**2.1.1. The Rise of Self-Sovereign Identity.** The paradigm shift in the digital identity ecosystem has been the result of progressive advancements during the last ten years in the industry and Academia<sup>186</sup>. Among the contributions, the developments in standardization by W3C and ISO have been key, and other technologies, such as blockchain, have played a key role in this transition.

The change implies that traditional centralized models where a single authority governs identity information are gradually making way for a system where individuals or entities maintain direct control over their identity data. The change focuses on users' capability (instead of the IdP's capability) to manage their identity information and control data access across different services.

Nevertheless, as noted above, there is no consensus on the definition of these ecosystems. Some authors, such as Stockburger et al. (2021, p.3), suggest that user-centric identities aim to give users greater control over their digital identities. However, these models are usually associated with technologies like OpenID or OAuth, where the users ultimately rely on some form of centralized IdP. Conversely, in SSI, there is an aim to provide users with total control over their identity, "setting them free" from any central provider or services that could potentially alter, block, or delete identity credentials.

Avellaneda et al. (2019, p.11) align with this idea. However, the authors take a step further and already reference the potential of DLTS to enhance users' control. The authors stress that SSI aims to give users control over their identities and related information, ideally achieved through a decentralized identity infrastructure like DLT. In this model, individuals or other entities can use DLT-based identifiers to present claims related to those identifiers. Therefore, although these will still need to request credentials/attestations from third-party issuers (trusted by the RPs), SSI enables the

---

<sup>186</sup> In this regard we can note the EU-funded Research Projects ARIES, OLYMPUS or ERATOSTHENES, with the participation of the University of Murcia, but also others, such as the Project STORK and STORK 2.0.

identity holder to maintain "sovereign" control over their digital wallet and digital credentials.

Preukschat & Reed (2021, pp.1–13) have made significant contributions to the concept of SSI and note that the potential of this new concept goes beyond a mere technological transformation, aiming for the redefinition of the fundamental infrastructure and power dynamics on the Internet. The authors highlight that SSI is essentially decentralized and surpasses the account-based system. The ecosystem aims to resemble the identity model in the physical world, founded on direct, peer-to-peer interactions and where neither party has ownership or control over the mutual connection.

Nevertheless, the authors emphasize that SSI does not imply completely disregarding government-issued identities. Instead, they believe that SSI and traditional forms of identification can coexist without conflict. SSI aims to provide individuals with control over their identities and credentials from trusted authorities, including governments, rather than replacing them<sup>187</sup>. This is the line of thought also expressed by the creator of the SSI concept (Allen, 2023), who insists that SSI is a concept that has evolved from foundational ideas related to sovereignty, melded with the unique characteristics of the digital world. The author highlights essential ideas and theories that converge to form the SSI concept. More specifically, the author observes that “individuals are seen as living systems, intertwined with each other and with other layers of systems, each with permeable boundaries serving as their membranes. As in living systems theory, my principles needed to highlight the need for a balance between maintaining individual autonomy and engaging in an interconnected digital world; as in Ostrom’s principles, that balance would be based on strong boundaries and clear rules, and as in the Universal Declaration of Human Rights, those rules needed to protect agency and human dignity.”

---

<sup>187</sup> With the SSI system, a government can provide a digital credential for important documents like driver's licenses or passports. People can store and manage these credentials in their personal digital wallets and present them as needed. This maintains the credibility of government-issued credentials while giving individuals control over their identity data. It can improve privacy, reduce dependence on centralized identity providers, and make digital transactions more secure and flexible.



In my opinion, decentralization is essential to the SSI concept, particularly if there is an aim to reshape power dynamics in the digital identity ecosystem. In addition, it is essential to grant users control over their own identity information. These two key features can have various degrees of implementation. In this regard, an ecosystem can achieve a greater degree of decentralization by implementing technologies such as DIDs or blockchain. Likewise, depending on the design and functionalities of the wallet and its interaction with other parties in the ecosystem, it can result in varying levels of user control.

**Table 4**

Comparison of Core Features in Emerging Digital Identity Ecosystems

	User-centric	Decentralized	SSI
Multiple IdPs	No	Yes	Yes
Wallet under User Control	Yes	No	Yes

On the other hand, the SSI ecosystem is structured around three principal roles: Issuer, Holder, and Verifier. The Issuer is responsible for creating and providing credentials to a Holder. The Holder, in turn, receives these credentials from the Issuer, sharing them with a Verifier when requested/necessary. Finally, the Verifier's task is to receive and authenticate the credentials provided by the Holder, which might require or not connect with the Issuer.

In addition, SSI ecosystems are based on a set of nuclear or core technologies. In particular, four technologies can be said to form the backbone of these systems: VCs<sup>188</sup>,

---

<sup>188</sup> Pursuing W3C Recommendation 03 March 2022 on Verifiable Credentials Data Model v1.1, in the physical world a *Credential* might consist of information related to identifying the subject of the credential (e.g., photo, name, identification number...), or information related to specific attributes or properties of the subject of the credential, the issuing authority, related to the type of credential or information related to how the credential was derived and or its constraints (e.g. terms of use, expiration date, etc.). This information can be presented digitally, while the world *Verifiable* refers to their characteristic “as being able to be verified by a verifier.” It allows an evaluation of whether this information is an authentic and timely statement is possible by checking: whether the credential conforms to the specification, the proof method is satisfied and, if present, the status check succeeds. It does not involve mean an evaluation of the truth of the claims encoded in the credential. In the scope of Verifiable

DIDs<sup>189</sup>, digital wallets<sup>190</sup>, and DLTs. Among these, VCs and digital wallets could be considered the heart of the system. These technologies play a key role in the materialization of the ecosystems presented above, with the purpose of empowering users to receive and manage their identity credentials independently, ultimately removing the need to rely on third parties for these functions.

Although these three roles (i.e., Issuer, Holder, and Verifier) are key in the characterization of the ecosystems, they can materialize in other sub-roles, depending on the final design or configuration of a specific ecosystem. For example, a DLT could be implemented to support a distributed (or even potentially decentralized) governance infrastructure. Likewise, there might be entities holding a certain oversight or control role, authorizing other entities to issue certain credentials, or even entirely new roles could potentially emerge.

Furthermore, there is no limited list of standards that these ecosystems must incorporate. For example, although it does not traditionally fall under the SSI umbrella, the mDL<sup>191</sup>

---

Credentials, it shall be distinguished: a) Verifiable ID: is a special form of a Verifiable Credential that a Natural Person or Legal Entity can put forward as evidence of whom they are (comparable with a passport, physical ID card, driver's license, social security card, member card...). b) Verifiable Attestation: a special form of a Verifiable Credential that a Natural Person or Legal Entity can put forward as evidence of certain attributes/properties or as evidence of a permit/attestation/authorisation they received. World Wide Web Consortium. (2019). *Verifiable Credentials Data Model 1.0* (Recommendation). <https://www.w3.org/TR/vc-data-model/>

<sup>189</sup> Pursuing W3C Recommendation 19 July 2022 v1.0, DIDs are a new type of identifier that enables verifiable, decentralized digital identity. A DID can refer to any subject, such as a person, organization, thing, data model, abstract entity, etc., as determined by the controller of the DID. DIDs are designed to be decoupled from centralized registries, identity providers, and certificate authorities, so the controller of a DID can prove to control over it without requiring permission from any other party. World Wide Web Consortium. (2022). *Decentralized Identifiers (DIDs) v1.0* (Recommendation). <https://www.w3.org/TR/did-core/>

<sup>190</sup> Pursuing the W3C Editor's Draft 22 February 2023, a wallet is defined as a small, flat case that can be used to carry small personal items like paper currency, credit cards, and identification documents. This definition is extended to the digital realm as a universal wallet, which is a digital wallet that supports cryptocurrencies, verifiable credentials, and cards. World Wide Web Consortium. (2023) *Universal Wallet*. (Editor's Draft 22 February 2023). <https://w3c-ccg.github.io/universal-wallet-interop-spec/>

<sup>191</sup> The mDL is a secure digital version of the data that is stored in a driver's license. All relevant information is embedded into individual fields, allowing for easy compartmentalization. The data is also digitally signed by the Issuer (Issuing Authority, depending on the country). The mDL ISO standard, ISO/IEC 18013-5:2021, specifies the interface requirements for implementing a mDL on a mobile device, detailing the interaction between the mDL, mDL reader, and the issuing authority infrastructure. It also enables various parties to access and verify the mDL data digitally, promoting the transition from physical

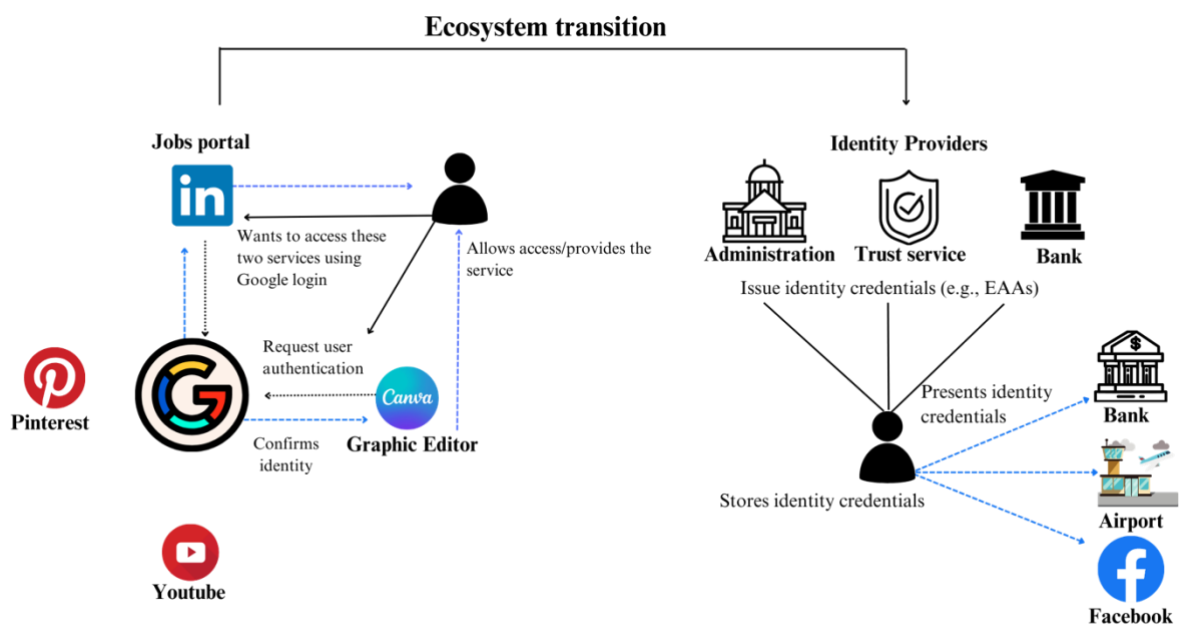
standard from ISO holds significant relevance in the models described and harbors the potential to facilitate a globally interoperable digital identity credential.

Having in mind all the different possibilities for the configuration of these ecosystems, we can state that these have in common at least three fundamental characteristics:

- The role of the IdP is not monopolized by a single entity or a reduced number of entities (public or private).
- The connections within the ecosystem neither rely on nor are controlled by an external entity. The parties can establish direct connections between them.
- The user possesses both awareness of and control over the data being managed, deciding the parties with whom they aim to share their data.

**Figure 11**

Digital Identity Ecosystem Transition



to digital driving licenses. In addition, there are other standards regulating mDL ecosystem, notably 18013-7 and 23220 series.

**2.1.2. New Ecosystems, New Benefits for the Different Stakeholders.** SSI<sup>192</sup> has several advantages over previous digital identity models, especially when compared to federated digital identity. The ecosystem provides benefits to various stakeholders in different ways. From a user's standpoint, the core advantage offered by SSI is digital existence. However, digital existence does not entail complete independence from external entities but rather a user's entitlement to secure the necessary tools for digital presence. The concept of self-attested existence is not practically feasible in either the digital or physical realm<sup>193</sup>, at least in a foundational sense. Yet, the new ecosystems diminish users' dependency on third-party providers, enabling them to control their identity information and establish their own communication channels much like they do in the physical world.

Furthermore, we have noted that one of the other key features of SSI ecosystems is user control. With SSI individuals have control over their personal data, which means that they can decide who can access it and when, as well as manage it by updating, hiding, or deleting it. This control also implies the possibility of accessing and visualizing the data in their wallets or even interacting with the parties in the ecosystem with whom they share data.

Data control and privacy are interrelated, but, in my opinion, these are not the same thing. Depending on the specific design of the wallet and external procedures, varying degrees of privacy may be achieved. Nevertheless, it is indisputable that compared to other forms of digital identity, these models significantly enhance privacy. In these models, the data sharing process is not controlled by external entities, and data sharing only occurs with user authorization<sup>194</sup>, who should also ideally be able to revoke access to their data at any time.

---

<sup>192</sup> We use the term SSI in this section to refer to those ecosystems that fulfill the two criteria noted in the previous section: decentralization of the IdPs and wallet under user control. This term could not be accurate for some readers, but the purpose of this section is not to discuss the definition of this term but to provide the reader with an overview of the benefits provided by these digital identity ecosystems.

<sup>193</sup> At least from the perspective of citizenship.

<sup>194</sup> As it has already been introduced, the authorization model shall not be confused with consent as a legal basis for the data processing according to the GDPR.

In addition, SSI models aim to improve data security, particularly concerning data storage. In the first chapter, we noted that one of the main security issues of current digital identity models is the concentration of data in a single or reduced number of IdPs. With the decentralization of the IdP role, SSI aims to improve data security by eliminating single-point-of-failure scenarios. This is complemented with storage on the user side; that is to say, when possible, data storage will be limited to the user's device.

Furthermore, SSI has the potential to enhance interoperability. By surpassing the "account-model scheme," SSI aims to create a widely interoperable ecosystem with reduced barriers to communication between the different actors. Likewise, SSI could improve user convenience. Digital wallets are conceived as an instrument enabling users to manage their credentials in a user-friendly manner. In addition, the devices are supporting new authentication protocols, eliminating the need for passwords or finding more convenient ways to manage them. Furthermore, this convenience can go even further and support socio-economic inclusion, especially for people in remote areas who can benefit by downloading a digital wallet app.

Although most of the discourse around SSI's benefits has focused on the user, these ecosystems also bring benefits for the other roles/participants. One of the main benefits for organizations is the emergence of new business opportunities. From an Issuer's perspective, a standardized process of issuing credentials to a standardized digital wallet can alleviate burdens from both a technical and administrative standpoint. Furthermore, for RPs, their processes become simpler, and these can instantly verify credentials, thereby eliminating the necessity for time-consuming manual checks. This leads to significant enhancements in efficiency and accuracy within identity verification processes. Furthermore, as proposed by Laatikainen et al. (2022, p.15), the adoption of SSI can foster the formation of strategic alliances, creating competitive advantage and subsequently leading to an expansion of customer possibilities.

Although SSI has many benefits, there are also challenges that need to be addressed. One of these challenges is the difficulty of achieving full interoperability between systems. Difficulties are not only limited to technological interoperability, but these are

notably challenging in the legal and semantic domain. Additionally, organizations need to invest in replacing their traditional digital identity ecosystems in a moment of regulatory uncertainty and change. Furthermore, users will need to adapt to new technologies and processes.

Nevertheless, we are in the midst of a transformative period. The process of transformation will, however, be progressive, involving several stages in the integration of new tools and learning of new patterns. Yet, this transformation seems to be a natural progression of the digital identity ecosystem, which is now even backed by upcoming regulations.

## ***2.2. eIDAS2: within Emerging Digital Identity Ecosystems, but with its Own Unique Features***

The eIDAS2 Regulation creates a unique ecosystem that incorporates some of the central features of SSI while also having its own characteristics. One of the main objectives of eIDAS2 is to avoid power concentration in the IdP role by promoting the decentralization of this role, which now can be assumed by various entities as “issuers of identity credentials.” In addition, eIDAS2 has opened the door to the participation of private entities in this role through the new trust service of Issuers of EAAs, a role that, as previously explained in this chapter, can also be assumed by public entities on the basis of their public powers. Nevertheless, the eIDAS2 ecosystem has a very unique characteristic: all these possibilities ultimately depend on a "foundational identity" guaranteed by the State<sup>195</sup>.

### ***2.2.1. A Digital Identity Landscape integrated by Wallets and Identity Credentials.***

The eIDAS2 Proposal enables a deep transformation in the digital identity ecosystem where public and private entities will now integrate under the form of Issuers of EAAs. As technology advances, it is becoming more common for people to use identity credentials. Therefore, eIDAS2 has taken a sensible approach that recognizes the

---

<sup>195</sup> Perhaps, the closest approach to SSI in its original meaning could be the possibility of generating pseudonyms through the EUDI Wallet.

technological advancements through the creation of the new trust service for Issuers of EAAs, a strategic move timely executed by the EU legislature<sup>196</sup>.

This strategy offers multiple advantages, including a potential boost in efficiency and innovation and the facilitation of customer-centric solutions. At the same time, it ensures appropriate regulation and public oversight through the trust services regulatory regime, particularly regarding security<sup>197</sup>, data protection<sup>198</sup>, transparency and identification<sup>199</sup>, record-keeping<sup>200</sup>, liability<sup>201</sup>, and business continuity. Moreover, qualified trust service providers will be expected to meet associated obligations and those specifically introduced by eIDAS2, as already explained.

Consequently, the eIDAS2 Proposal envisions a unique model by capitalizing on the existing system, more specifically leveraging trust services regulation for the inclusion, in a regulated manner, of private entities in the provision of digital identification services. To a certain extent, the eIDAS2 Regulation establishes a regulated market for identity credentials. These credentials, especially those issued by qualified trust service providers and potentially by public sector bodies, are granted a certain level of trust. At the same time, these might function around a nuclear anchor, the PID, a government-backed identity that will serve as the primary link for all subsequent credentials issued to the EUDI Wallet. This, however, does not necessarily mean that they will need to be presented conjointly in all cases, especially considering that the use and request of the EUDI Wallet is voluntary pursuant to Article 6a paragraph 7a.

---

<sup>196</sup> The new ecosystem follows a similar model to Italy's *SPID* case, where private providers were allowed to provide identification services under the conditions established by the *AgID*. Furthermore, as noted, *SPID* ecosystem already included the role of Attributes Authorities.

<sup>197</sup> Articles 10, 19 eIDAS Regulation refer to the need to take appropriate steps to manage and minimize risks, as well as to notify supervisory bodies of security incidents.

<sup>198</sup> Particularly relevant are the new data protection requirements envisaged in Article 45f of the eIDAS2 Regulation.

<sup>199</sup> Article 20 and 23 eIDAS Regulation, among others.

<sup>200</sup> Article 24 eIDAS Regulation.

<sup>201</sup> Article 13 eIDAS Regulation.

Nevertheless, the idea is to expect a strong interaction between these two. The EUDI Wallet emerges as an anchor piece in the opening of a new ecosystem of identity credentials. A “public-guaranteed” identity with the potential to enable a wide range of opportunities for European citizens in the digital sphere.

**2.2.2. The European Union Digital Identity Wallet as a form of State-backed Digital Identity.** As has already been explained in the first section of this chapter, the EUDI Wallet is more than just a place to store identity credentials; it is an electronic identification means. However, this configuration as electronic identification means demands a complex provisioning process for the EUDI Wallet, requiring a binding between the wallet app and a “foundational credential” known as the PID.

The PID is a term that appears in the ARF. At the time of adoption of the eIDAS2 Proposal, the Commission adopted the Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach toward a European Digital Identity Framework. This Recommendation established that Member States should work together toward the development of a Toolbox to support the implementation of the European Digital Identity Framework and, where relevant, other concerned public and private sector parties.

The purpose of the eIDAS Toolbox was to facilitate collaborative work by Member States on various objectives<sup>202</sup> through the production of the ARF that will serve as a basis for the IAs referred to in the eIDAS2 Proposal, notably in Article 6a paragraph 11. The available version of the ARF defines PID Providers as the entities tasked with verifying the identity of EUDI Wallet users in alignment with LoA high requirements. They are responsible for issuing PID to the EUDI Wallet in a standardized format and providing information to RPs to validate the PID. Nevertheless, the ARF does not delimit the specific entities that might offer these services, recognizing that PID

---

<sup>202</sup> These objectives are: a) A technical architecture and reference framework defining the functioning of the European Digital Identity framework in accordance with the eIDAS Regulation, taking into account the Commission's Proposal for a European Digital Identity framework; b) Common standards and technical specifications; c) Common guidelines and best practices in areas where alignment practices will support the smooth functioning of the European Digital Identity framework.



Providers could either be the current organizations issuing official identity documents and electronic identification means or different entities. Similarly, they may or may not be the same organizations that provide the EUDI Wallet, a key point that will be the subject of discussion in the subsequent chapters.

The ARF stipulates a set of requirements for PID<sup>203</sup>. However, it asserts that the mechanism for generating and providing the PID to the EUDI Wallet is also at the discretion of Member States, constrained only by legal obligations such as LoA high, GDPR, or any other applicable national or EU Law. Nevertheless, in order to ensure a high degree of harmonization between Member States, the ARF has prescribed the specific attributes to be included in the PID, distinguishing between mandatory and voluntary attributes. The mandatory attributes coincide with the ones established in the CIR 2015/1501, with the particularities provided in eIDAS2 concerning the unique and persistent identifier. With regard to additional optional identifiers, it offers the possibility to include the attribute of nationality/citizenship and optional attributes used at the national level, like the tax number or social security number.

Considering that the eIDAS2 Proposal nor the ARF, do not explicitly delineate the roles of PID Provider or EUDI Wallet Provider<sup>204</sup>, it is to be expected that the different approaches to electronic identification in Member States, as presented in the second chapter, will continue to exist in the EUDI Wallet landscape with their necessary adaptations. Each model has its own advantages and limitations. While “public” models often deal with more inefficiency and struggle to keep pace with the advancements in the private sector, these offer better guarantees. On the other hand, “private” models, while more efficient, might not provide the necessary legal safeguards and exclude certain population groups.

---

<sup>203</sup> a) No two people should have the same PID set of mandatory attributes; b) The PID should at least contain the minimum set of attributes specified in CIR 2015/1501 and; c) The mandatory set is limited to the narrow intersection of what all Member States can provide for all natural and legal persons and what is needed for electronic identification purposes.

<sup>204</sup> The ARF previously referred to this role as EUDI Wallet Issuer.

What is clear is that the eIDAS2 Proposal represents an opportunity for the reconsideration of all these factors and learning from previous “mistakes.” To break the ground, the eIDAS2 Proposal lays down a clear mandate directed to Member States for the provision of the EUDI Wallet, emerging as a form of public-guaranteed digital identity. Materializing this obligation presents a lot of challenges in an emerging ecosystem that is essentially complicated and that, as will be discussed in the last chapter of this thesis, will require further legal guidance at national level to detail the specific model each Member State adopts for the EUDI Wallet provision, ensuring individual protection and also clearly define the administrative processes and governance structure of the ecosystem.

### **3. Charting the Course to a New Digital Identity Ecosystem**

The eIDAS2 Regulation has represented one of the first instances of legislative intervention to foster and accompany the transformation of the digital identity landscape. While this regulation targets the EU's territory, some of the modifications could affect the foundations of the Internet. In my opinion, the eIDAS2 Proposal has represented a very audacious step by EU lawmakers, who, acknowledging the progressive transformation that was occurring by technological evolution, have taken the opportunity to intervene, foster the transformation, and, more importantly, prevent the continuation of existing problems.

Transformation within the ICT sector is innate to its nature, manifesting as a gradual process. The transition from Web 1.0 to Web 2.0 was not a single event but rather a series of advancements that took place over several years. This progress was driven by improvements in technology and changes in user behavior and expectations<sup>205</sup>. Similarly, the anticipated transition to Web 3.0 is expected to unfold over time. Yet, it is a significant milestone that regulatory instruments like the eIDAS2 Regulation are already being used to facilitate and, in some cases, even force the transformation of certain sectors.

---

<sup>205</sup> For example, while in Web.1.0. the content was created by a small number of professionals, Web 2.0 allows anyone to create and share content.

The eIDAS2 Regulation is not simpler than its predecessor. It maintains the dual regulatory regime explained in the second chapter but has now introduced, in addition to the identities federation, a new form of harmonized eID means, the EUDI Wallet, and new trust services, notably in what directly concerns the digital identity landscape, the Issuers of EAAs. Consequently, the Regulation requires careful consideration and understanding as these two elements, despite having great potential through their integration, operate separately and with differentiated legal effects.

The eIDAS2 Regulation has been approved at the time I was doing a final review of this section; therefore, its content has been drafted considering the final text currently available of the eIDAS2 Regulation as well as the progress made and publicly available in its implementation, notably in the ARF. In addition, to date, two key public procurement procedures<sup>206</sup> have been undertaken within the framework of the eIDAS Toolbox, the results of which will be worth exploring.

As a result, it is important to keep in mind that this section will have to be updated in the coming months to incorporate the developments in the scope of IAs and results from “EUDI Wallet consortiums.” Nevertheless, despite the potential specifics in its implementation, the eIDAS2 Regulation forces a change in the digital identity ecosystem. In addition to existing models, it offers a new ecosystem where the role of the IdP is at least partially decentralized and gives back users control over their personal data, ensuring more personal autonomy. Furthermore, unlike its predecessor, we appreciate the greater effort made to establish a legal framework for an electronic identification means that goes beyond authentication functionality by including a set of requirements that also allow the "creation" and "storage" of this digital identity by the user.

---

<sup>206</sup> Firstly, a public contract with a smaller budget was aimed at the development of the EUDI Wallet, awarded to a partnership between Netcompany and Intrasoft S.A., along with Scytáles AB. Secondly, a more extensive public procedure has resulted in four consortiums of public and private entities: the EU Digital Identity Wallet Consortium (EWC), which focuses on travel credentials and payments; the Nordic-Baltic eID Wallet Consortium (NOBID), which focuses on payments; the Digital Credentials for Europe Consortium (DC4EU), which focuses on educational and social security credentials; and the Pilots for European Digital Identity Wallet Consortium (POTENTIAL), which focuses on a wide range of uses cases, including access to government services, ePrescription or Mobile Driver Licenses, among others.

However, numerous questions and challenges remain unresolved. Specifically, this Regulation will be directly enforceable in the different Member States, necessitating a series of decisions accounting for the legislative framework and other factors like market and societal challenges. This is, in my opinion, an excellent opportunity and moment to impose a stronger role for legal rules, in the face of mere private self-regulation without public intervention, toward the development of a law capable of regulating intersubjective relations and power relations in a future "Digital Rule of Law State" (Canals Ametller, 2021a, p.65).

## CHAPTER IV

---

### **THE ULTIMATE PUBLIC NATURE OF THE EIDAS2 DIGITAL IDENTITY METASYSTEM**

---

Under eIDAS2, all Member States are now required to notify one electronic identification scheme containing at least one eID means and provide their citizens with a EUDI Wallet. This requirement marks an important milestone in digital identity legislation in the EU because it implies the right for every citizen in the EU to be provided with a digital identity that functions within a specific, but broad, scope, as will be explained in this chapter. The obligation to provide the EUDI Wallet lies with Member States, and lack of compliance could potentially trigger a legal proceeding before the TJEU, initiated either by an individual (who has exhausted all available legal recourse at the national level) or the European Commission.

However, the eIDAS2 Proposal does not prescribe a specific modality for its implementation. Instead, it provides three alternative modalities for the provision of the EUDI Wallet, as stipulated in Article 6a paragraph 2. These three possibilities are not new, but as it has been explained, they were already envisaged in the first version of the eIDAS Regulation, leading to different modalities for its implementation.

Nevertheless, the EUDI Wallet is a very specific type of eID mean, the result of a very specific combination of elements, more specifically, a PID (which can be contained or not in a notified eID means) and a wallet app that enables the EUDI Wallet to fulfill the requirements established in the Regulation. At this point, it is critical to remember that this obligation arises in a context of technological rivalry, with applications such as Apple Wallet or Google Wallet dominating the market and already playing a role in supporting State digital identities beyond EU borders. In addition, “foundational identities” are not provided in the same way in all Member States. Some open the door

to private collaboration, while others directly “delegate” or “outsource” the provision of these digital identities to the private sector.

Whatever approach is adopted, the obligation of guaranteeing the provision of the EUDI Wallet lies with the Member States; adopting, therefore, a similar approach to that of the first version of eIDAS, the new metasystem for the EUDI Wallet is perceived as a public service, independently of the modality for provision adopted. This understanding might require legislative measures at a national scale. Nevertheless, before proceeding with that topic, this chapter aims to explore the significance of the introduction of the obligation to provide the EUDI Wallet from the perspective of Public Law.

## **1. The Mandate for the Provision of the European Union Digital Identity Wallet**

### ***1.1. Is there a Right to a Digital Identity?***

At the moment of writing this thesis, in the legal landscape, a potential right to identity remains intertwined with the right to privacy and data protection. However, privacy, data protection, and identity are different, and even if these are interconnected<sup>207</sup>, each concept holds its own significance. Until now, legal recognition has focused on the right to privacy and data protection, with almost no recognition of the right to identity. The eIDAS2 mandate represents an important change in this regard. However, the mandate for the provision of the EUDI Wallet is limited to the digital domain and constrained by the EU limitations in sovereignty and should not take the place that corresponds to the recognition of a potential Fundamental Right.

***1.1.1. Detaching Identity from Privacy and Data Protection.*** The right to privacy and the right to identity are both considered part of a set of rights known as personality rights, which stem from the broader rights to dignity and self-determination (Gomes de Andrade, 2011, p.99). Although these two concepts share an intrinsic relationship, they are distinct from each other. Sullivan (2016, p.478), in her studies on the differentiation

---

<sup>207</sup> This is particularly evident when considering the affected rights in the event of a cyberattack involving user impersonation that usually leads to unlawful access or utilization of user's data.

between these rights, emphasizes the need for the recognition of a right to identity, particularly in the context of digital identity.

Privacy and data protection are two complementary legal tools for the purpose of controlling and limiting powers. While privacy is designed to ensure non-interference in individual matters, creating a personal zone of non-intrusion (i.e., protecting individuals against interference in their autonomy by governments and private actors), data protection, on the other hand, is a tool of transparency that is not prohibitive by nature, but it operates under the presumption that personal data is in principle allowed to be processed and used, involving the individual's faculty to make use of their own information (*habeas data*) that can be exercised without an existing violation of their privacy (Gutwirth & De Hert, 2006,p.77).

However, according to Sullivan (2016, p.478), the right to privacy alone is insufficient because, while certain aspects of digital identity consist of private information, identity also encompasses predominantly public information. Furthermore, privacy and data protection focus on individuals' control over their personal information (including collection and disclosure). Conversely, the right to identity pertains to autonomy in the sense of being recognized as a unique individual. The right to identity is violated when indicia of identity are falsely or inaccurately employed, and it is conceptualized as a legal entitlement to be recognized and engage in transactions as a distinct individual<sup>208</sup>.

Additionally, there is a lack of clarity regarding which data falls under the realm of privacy and data protection versus those categorized as identity-related data. Gomes de Andrade (2011, p.101) introduces an interesting approach according to which the right to identity is infringed if person A makes use of person's B identity, while the right to privacy is only infringed if actual private facts are revealed to the public. According to this idea, only information that qualifies alethically (in which there is correspondence between the concept of personal data and the set of true objective facts or acts related

---

<sup>208</sup> As a result, the nature of these rights fundamentally diverges, encompassing more than just the ownership or control of data. It extends to the right to participate in transactions and be recognized as a distinct individual.

to the data subject) shall be protected under the right to privacy, whereas personal information that is not necessarily truthful shall be covered by the right to identity. This point of view becomes especially relevant in the context of upcoming metaverses, where the information disclosed may not correspond to reality but still holds personal significance.

Another key point is determining which entities are entitled to the right to identity. According to some theorists, inherent humanity is an essential requirement for true personhood, emphasizing its utmost significance to human beings (Naffine 2003, pp. 357–361). On the contrary, for others, legal identity emerges through the allocation of rights and responsibilities (Naffine, 2003, pp.350–354). Although this consideration may appear superficial, it is particularly relevant in a context where digital identity refers not only to individuals but also to legal entities and even non-living entities.

The rights to privacy and data protection in EU Law have been stipulated in different legal texts. Article 8 of the ECHR states that “everyone has the right to respect for his private and family life, his home and his correspondence,” and this legal provision is supported by Article 6.2 of the TEU 2012, which adds that “the Union shall respect Fundamental Rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to Member States.” Moreover, the right to data protection is expressly stipulated by Article 16 of the TFEU 2012, which states that “everyone has the right to data protection of personal data concerning them.”<sup>209</sup>

Conversely, up until now, the right to identity has not been officially recognized in EU Law. The only legal text that we have identified providing some recognition to the right to identity is the Convention on the Rights of the Child<sup>210</sup>. However, this recognition in the scope of International Law is subject to important limitations, notably the exclusion of the current adult population, as acknowledged by Sullivan (2016, p.480). On the other

---

<sup>209</sup> Numerous case law exists from the ECHR and the EUCJ concerning the protection of the right to privacy. Some of the most relevant rulings from the past years are *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos or Schrems v. Data Protection Commissioner*.

<sup>210</sup> It envisages that "States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name, and family relations as recognized by law without unlawful interference."



hand, the International Convention on Civil and Political Rights has recognized the right to self-determination or to legal recognition by the law in Article 1. While these two rights do not directly recognize a right to identity, these concern various aspects related to personal status and identity.

In EU case law, the ECtHR has recognized the right to identity, but it is only implied in Article 8 of the ECHR. This is supported by various cases such as *Goodwin v. the United Kingdom*<sup>211</sup>, *B v. France* or *Mikulic v. Croatia*<sup>212</sup>. However, these cases mainly focus on recognizing the identity of transgender individuals.

Consequently, as it can be observed, the only formal recognition in the international scope of the right to identity appears in the Convention on the Rights of the Child, while in most cases, it is incardinated in the right to self-determination, legal recognition, or privacy, or at a national level in the right to nationality or registration. Therefore, the right to identity is not formally recognized, and as can be expected, there is no formal recognition of a right to a digital identity. Nevertheless, some examples of recognition, although not in a legally binding manner, can be already identified, such as the *Carta de Derechos Digitales*, where Article 2 provides a right to identity in the digital domain, setting a precedent in recognition of this right, hopefully, in the near future.

***1.1.2. The Inherent Regulatory Limitations of the European Union Digital Identity Wallet Provision Mandate.*** The Proposal for Revision of the eIDAS Regulation marks a significant milestone in digital identity policy and overcomes the absence of a mandate for the provision of digital identity means in the EU scope, as was noted in the first chapter of this thesis. The eIDAS2 Proposal mandates Member States to provide a

---

<sup>211</sup> The Court's assessment paragraph 6 "Nonetheless, the very essence of the Convention is respect for human dignity and human freedom. Under Article 8 of the Convention in particular, where the notion of personal autonomy is an important principle underlying the interpretation of its guarantees, protection is given to the personal sphere of each individual, including the right to establish details of their identity as individual human beings."

<sup>212</sup> Alleged violation of Article 8 of the Convention, letter B number 66 "Accordingly, the inefficiency of the courts has left the applicant in a state of prolonged uncertainty as to her personal identity. The Croatian authorities have therefore failed to secure to the applicant the "respect" for her private life to which she is entitled under the Convention. There has, consequently, been a violation of Article 8 of the Convention."

EUDI Wallet within 24 months after entry into force of the IA provided in Article 6a paragraph 11, and mandates Member States to notify one electronic identification scheme, which includes at least one electronic identification means, according to Article 7.1.

As a consequence, Member States will be obliged to provide citizens with a digital identity that functions within the eIDAS2 scope, acquiring a guarantor role. Such consideration could lead to qualifying the EUDI Wallet as a public-guaranteed electronic identification means, considering that, irrespective of the modality chosen for its provision (that falls within the sovereignty of each Member State), these are required to ensure a supranational form of digital identity.

While the right to obtain a digital identity is there, it is also important, in my opinion, to acknowledge that, from a "strict" legal perspective, the digital identity covered by the mandate (the EUDI Wallet) circumscribes to a very well-defined scope. First, because this digital identity only exists on the basis of a previously issued form of legal identity by the Member State. Secondly, because it does not guarantee any right to an identity beyond the digital realm, and thirdly, because the scope covered by the mandate is that of the EUDI Wallet as an electronic identification means, falling potential extensions through EAAs out of the scope of this obligation and being subject to a different legal regime. Furthermore, the mandate for recognition is, in principle, limited to the cross-border scenario.

Therefore, in my view, the consequences of the eIDAS2 mandate are limited and cannot be considered equivalent to the recognition of a fundamental right to identity, which is called to emerge as a foundational element in current societies that should not always be subsumed in other rights, such as the right to privacy. The need for recognition is also supported by the United Nations General Assembly for Sustainable Development Goal 16.9, which envisages that States must provide legal identity for all, including birth registration, by 2030.

Nevertheless, it can be said that a certain right to a digital identity already emerges with eIDAS2, and it is especially appreciated in the broad acceptance of the EUDI Wallet, which suggests a right to a digital identity for EU citizens. However, I would also like to acknowledge at this point that digital identity is a global topic and that following the statements made by other authors (Sullivan, 2016, p.481), ultimately, a right to identity should be further developed and formally recognized in the domain of International Law. This is logical in the understanding that identity is inherent to human beings living in society. Therefore, it shall be granted global recognition that should not exclusively depend on States' governance models. Yet, this first step would be its recognition, at least in its physical form. Undoubtedly, there is a significant amount of work yet to be done in defining and understanding the right to digital identity, and it is not the objective of this thesis. As acknowledged by Michalkiewicz-Kadziela & Milczarek, (2022, p.5), digital identity differs substantially from the identity formed by individuals in the physical world. Consequently, it constitutes a separate area that explores the unique aspects and implications of digital identity.

### ***1.2. The Provision of the European Union Digital Identity Wallet***

As has already been introduced in the third chapter of this thesis, the EUDI Wallet is not only a place to store credentials, but it is an electronic identification means itself. For its configuration as electronic identification means, the EUDI Wallet requires a process of “binding” between the PID and the wallet app. The PID could be described as the “root identity” or “foundational credential” that enables the EUDI Wallet to function. Consequently, in the EUDI Wallet provision, different roles converge, being all of these roles equally crucial in the success of this public-guaranteed electronic identification means that is called upon “opening” a new ecosystem of identity credentials.

#### ***1.2.1. More than just a Wallet App, but an Electronic Identification Means in Itself.***

The available ARF displays a visual representation of all the roles involved in the ecosystem. We have already referred to the PID Provider in the previous chapter. The PID Providers are entities that verify the identity of EUDI Wallet users, securely

provide PID to the wallet, and offer information to RPs to verify the validity of the PID without receiving any information about its use. These can be organizations that issue official identity documents or electronic identification means, and they may also act as wallet providers.

On the other hand, EUDI Wallet Providers<sup>213</sup> are Member States or organizations either mandated or recognized by Member States, making the EUDI Wallet available for end-users. More specifically, EUDI Wallet Providers make available to users a EUDI Wallet Solution that could be a combination of several products and trust services and which gives the user full control. These are responsible for ensuring compliance with the requirements for the EUDI Wallet established in the eIDAS2 Regulation (notably, Article 6a).

Device manufacturers and related entities are also essential in the ecosystem since the wallet app exists within a specific device/s<sup>214</sup>. This role is not defined per se in the ARF. Instead, it lists the interfaces with the devices they are based on, which may have the following purposes: local storage, online internet access, sensors in the devices, and offline communication channels, which are essential for the EUDI Wallet to function.

It has already been noted that the PID provider plays a crucial role in the eIDAS2 ecosystem. The EUDI Wallet cannot function without a PID. The currently available version of the ARF differentiates between the EUDI Wallet Solution, the complete product or service provided by EUDI Wallet Providers, and Wallet Instance, a personal instance of EUDI Wallet Solution owned and controlled by a user.

---

<sup>213</sup> The last version of the eIDAS2 Proposal replaced the term “issuance” by “provision” of the EUDI Wallet. Yet, there are some references to the term issuance in the context of EUDI Wallet, such as Article 6a paragraph b, “The issuance, use and revocation of the European Digital Identity Wallet...”

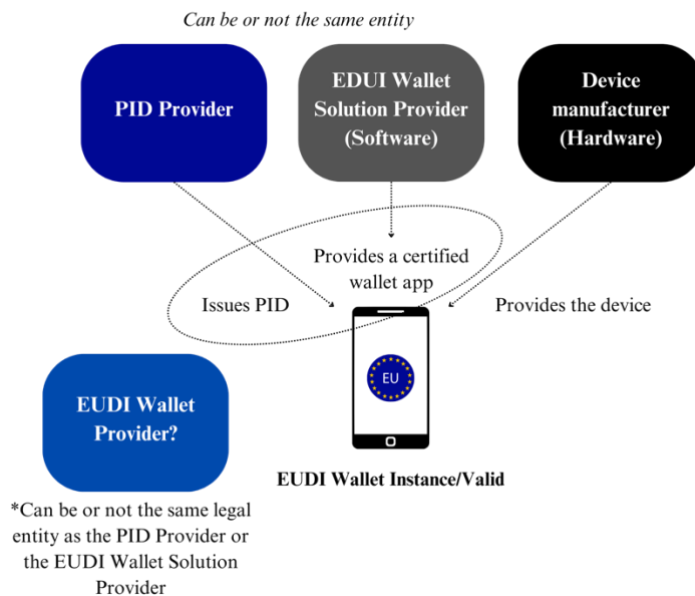
<sup>214</sup> In today's digital world, where public and private sectors intersect, questions arise about whether individuals have the right to access the necessary tools and equipment to participate in digital ecosystems, such as a mobile phone or computer, when these means are being imposed. Until now, alternatives exist to digital means, and the EUDI Wallet is voluntary. Therefore, I think this discussion should be kept for a later moment. The first step, and precisely the topic of discussion, is the right to exist in the digital realm, at least for certain purposes.

Once a EUDI Wallet in a candidate state is certified, a Member State may decide to start providing Instances of the Solution to Users. At this moment, PID might be issued to a EUDI Wallet or a pre-provisioned PID might be used. Once the EUDI Wallet is recognized by the PID Provider and it holds a valid PID set, the EUDI Wallet is considered valid. If, for some reason, the PID expires or is revoked, it becomes a Wallet Instance in an operational state. In the event a EUDI Wallet needs to be suspended, this would lead to the suspended state.

Although the provision of the EUDI Wallet involves various roles, it is the ultimate responsibility of Member States. The definition for EUDI Wallet Provider in the previous versions of the ARF is confusing as it refers to the PID and EAAs, but the last version seems to focus on the provision of a EUDI Wallet Solution. In my opinion, if the EUDI Wallet only exists when there is a process of binding between the wallet app and the PID, hence the role of the EUDI Wallet Provider should include this process of binding. This role, at the same time, implies two other roles: the PID provider and the EUDI Wallet Solution Provider. The EUDI Wallet Solution must fulfill the requirements and criteria established in the Regulation and upcoming IAs but cannot be considered equivalent to the EUDI Wallet insofar as this last one is an electronic identification means itself.

**Figure 12**

EUDI Wallet Provision



If we follow this distinction between EUDI Wallet Provider and EUDI Wallet Solution Provider, then Article 6a paragraph 2 refers to EUDI Wallet Provision, that is to say, the entity in charge of performing the binding between the PID and the EUDI Wallet Solution for the configuration of the EUDI Wallet. This is, however, a very subtle detail. As can be expected, the role of the EUDI Wallet Provider will normally be assumed by the PID Provider or the EUDI Wallet Solution Provider. Nevertheless, understanding the different processes that occur behind the scenes reflects the broad range of possibilities in the provision of the EUDI Wallet by Member States.

Notably, the variety of roles in the process of provision of the EUDI Wallet, combined with Article 6a paragraph 2, allows us to deduce a certain margin for the participation of the private sector. This must also be contextualized in a moment of digital transformation, particularly accelerated after the COVID 19 pandemic, and where digital wallets play a key role in digital exchanges. With the EUDI Wallet, the EU aims to achieve a level of efficiency and usability capable of competing with the advancements in the private sector. Yet, all of this occurs under Member States oversight and responsibility. The EUDI Wallet circumvents the categorization as a mere

product, and instead, it becomes a service that reflects, in my opinion, the exercise of public authority by Member States.

***1.2.2. A Form of Public Intervention to Facilitate Markets and Societal Transformation.*** The EUDI Wallet aims to become a fundamental piece in the transformation of the Digital Single Market. In this regard, the EUDI Wallet is not limited to providing a set of basic functionalities for identification, authentication, and electronic signature, but it is called to enable a whole new ecosystem of identity credentials.

Nevertheless, this ecosystem is structured around the idea of the EUDI Wallet as an “opening door.”<sup>215</sup> This EUDI Wallet Provision, in my opinion, embodies a form of public intervention to facilitate societal and market transformation. This intervention is justified for the broader objective of driving beneficial societal and market change, extending beyond mere correction of potential market failures<sup>216</sup>. However, facilitating transformative changes is a complex endeavor that typically demands robust cooperation, moving beyond the simplistic dichotomy of State versus the market. As argued by Foray et al. (2012, as cited in Mazzucato 2016, p.1), societal challenges require technological, behavioral, and systemic changes<sup>217</sup>. This suggests a more progressive perspective of the public sector, one that is not confined to merely regulating markets. Instead, it involves empowering societal transformations that, in turn, indirectly reshape markets.

---

<sup>215</sup> Nevertheless, keep in mind that although the idea is that the EUDI Wallet and the EAAs work together, both are subject to different regimes and can work independently. Therefore, an EAA does not necessarily need to be issued to a EUDI Wallet.

<sup>216</sup> The rationale behind public intervention typically rests on the understanding that certain goods and services possess unique characteristics that imply a competitive market may not effectively supply them in optimal quantities. This notion is usually supported by the presence of specific properties associated with these goods and services. For example, they might be non-rival in consumption, which introduces the issue of free ridership. Other potential challenges include the presence of externalities, informational asymmetries, or imperfect competition conditions. However, I do not observe that these traditional arguments exist behind the rationale of the EUDI Wallet whose motivations are tied to the new economy of data and digital markets, which have their own unique features.

<sup>217</sup> We can draw valuable insights from mission-oriented achievements such as landing humans on the moon and the development of new general-purpose technologies ranging from the Internet to nanotechnology. It is important to note that these monumental tasks were only accomplished when the public and private sectors collaboratively fostered the creation of new technologies and sectors (Mowery et al. 2010, Ruttan, 2006, as cited in Mazzucato 2016, p.1).

We can identify this line of thought in eIDAS2, which, besides regulating new markets, established an anchor piece or cornerstone, the EUDI Wallet, as a service of guaranteed public provision. The idea is that this can later integrate with other services, notably, the trust services concerning EAAs, in order to empower the user with a vast range of possibilities in the digital realm, including public and private services. At this point, it is worth recalling Article 6db, imposing mandatory acceptance of the EUDI Wallet to public services, but also private sector RPs requiring strong user authentication, as well as very large platforms.

The reasoning behind this imposition is not only “corrective” but also “extensive.” The eIDAS2 Regulation does not only aim to reshape power dynamics among participants in digital identity ecosystems by offering alternative eID means, but it also aims to extend the acceptance and usability of electronic identification means operating under the legal regime of the eIDAS Regulation. Furthermore, the eIDAS Regulation “extends” even beyond basic identification, authentication, and signature through the integration with new trust services, in particular, the EAAs, which create an ecosystem, at least partially regulated, of identity credentials.

The choice of instrument in eIDAS2 reveals the high level of ambition. As the Proposal states, “digital wallets were identified as a main asset for a future-proof solution,” and Recital 4 emphasizes the need for a more harmonized approach to digital identification to strengthen the Single Market and enable everyone to access public and private services relying on improved ecosystems of trust services. For example, we might expect to see the EUDI Wallet replace traditional identification and authentication through usernames and passwords. In the context of online shopping, enabling the user to prove that they are over a certain age. Combining the identification functionality with the electronic signature, the EUDI Wallet can be used to conclude a car rental contract through online means, authenticate payments, or even for in-person authentication at the moment of receiving an online order. Furthermore, combined with the possibilities of EAAs issued by the public and the private sector, other use cases are already envisioned and subject to work, such as academic qualifications or social security credentials.



Figure 13

Scenarios for the EUDI Wallet Implementation



At this point, it is worth advancing that the strict legal interpretation of the eIDAS2 Regulation is that the acceptance of the EUDI Wallet only refers to cross-border scenarios. However, in practice, it can be inferred that the aim of the Proposal goes beyond cross-border use cases and is willing to affect the whole digital ecosystem. This aim is also evident in the integration of the two legal regimes, electronic identification and trust services.

Nevertheless, as it has been introduced in the previous subsection, the provision of the EUDI Wallet is complex and might result in very varied scenarios. Likewise, although the EUDI Wallet and the EAAs might operate separately, the objective behind the Proposal is to leverage their integration. Therefore, the “success” of the EUDI Wallet seems to be a determinant element for the Proposal to achieve its objectives. At this point, Member States can opt for different strategies in the provision of the EUDI Wallet and might decide to leverage or not private sector advancements to achieve increased efficiency and innovation.

Nevertheless, it is essential to acknowledge that while the EU has embarked on the journey to reclaim its digital sovereignty, regulations do not exist in a vacuum; they are influenced by reality, and in this case, the technological reality. Even though the EU might provide alternative identification and authentication options (for instance, to the traditional method of login with Facebook), it is still confronted with the challenge of not possessing a robust technological industry that can effectively compete with international markets. Therefore, I believe that the EUDI Wallet reveals a complex landscape where a collaborative model between the public and private sectors might be necessary to ensure that the EUDI Wallet provision is competitive and efficient, particularly considering the broad range of use cases where it aims to be implemented that might demand efficiency and availability requirements that are not always feasible or reasonable for the public sector.

## **2. A Paradigm Shift in the EU: the Growing Role of Public Intervention in the Digital Age**

### ***2.1. On the Path to Recovering Digital Sovereignty***

Typically, the EU has operated through a combination of public interventionism and market freedom. The European continent has been characterized by its protection of individual rights and freedoms, but it also promotes market competition, notably through the development of the Single Market. The EU maintains more liberal principles insofar as this approach does not result in a detriment of citizens' rights. However, during times of crisis, there is a shift toward public intervention. In the digital sphere, this paradigm shift was triggered by events such as the Snowden revelations and the Cambridge Analytica scandal.

The first regulation materializing this shift in the EU landscape was the GDPR. This regulation has contributed to the evolving concept of digital sovereignty, understood as the control of various layers of the digital sphere, including data, software, standards and protocols, processes, services and infrastructures (Floridi, 2020, pp.370–371). Nevertheless, the GDPR falls short in addressing all challenges in the digital domain,

leading to the emergence of new regulations, such as the eIDAS2 Proposal, but also others, such as the Digital Services legislative package or those aiming for the establishment of a unified European space for data.

**2.1.1. Evolution of the EU's Digital Regulatory Landscape: Consequences for the Digital Identity Sector.** EU policy has shifted recently toward a more public-interventionist regime. Historically, the 1990s saw a minimal regulatory approach, focusing on market-driven solutions that enhanced European competitiveness in the global information society and the new economy created by the Internet. In the 2000s, some regulatory instruments, such as the eCommerce Directive or the Digital Signature Directive, started emerging. However, these are still in the framework of market freedom and focused on content responsibility by media providers, with little regulation, which is mainly left to the specific rules of the Member State where the ISS is established.

Nevertheless, in the mid-2010s to early 2020s, there was a profound change following events like the Arab Spring and Snowden revelations that led the EU to reassert its "digital sovereignty" and independence. GDPR was instituted during this period, although it still maintained a more market-liberal approach based on the country-of-origin principle. A few years later, in the 2020s, situations like the Cambridge Analytica scandal and the COVID-19 pandemic exposed the EU's digital vulnerabilities and perceived security threats from dependence on foreign companies. The situation led to the introduction of the Digital Services package, including the DSA and DMA. These regulations, although retaining some market-liberal principles, incorporated a stronger public-interventionist perspective in digital governance<sup>218</sup>. The eIDAS2 Proposal is also part of the mid-2020s policy shift.

---

<sup>218</sup> Instead of depending on individual Member State competences, which previously led to bottlenecks, the role of the EU Commission has been reshaped. Notably, the DMA established ex-ante regulation, enabling proactive rulemaking to prevent market failures before they materialize. Another example is the EU's changing its approach in cybersecurity governance from Regulatory Capitalism, in which the private sector holds a privileged coregulatory position within the Commission's regulatory efforts, to one of Regulatory Mercantilism in which the Commission positions the private sector as something to be overseen and controlled. Regulatory capitalism is characterised by the increasing desire of active control over the regulatory design, building a secure territory through reducing external dependencies,

Ultimately, these regulations underscore a contest for sovereignty as a form of legitimate control in the digital age. Unlike physical territory, the digital realm is not finite, scarce, rivalrous, or a non-renewable resource. This reality demands a reevaluation of the concept of sovereignty in the digital era. The early decades of this century saw the rise of de facto digital corporate sovereignty. However, this model fails due to a lack of alternatives when corporations inflict harm, and the shortcomings of national approaches suggest that digital sovereignty may need to evolve into a supranational entity. For instance, monetary sovereignty has, in some cases, become supranational when Member States adopt the euro. Similarly, digital sovereignty may need to be executed at both national and supranational levels<sup>219</sup> (Floridi, 2019, p.8).

This is, in my opinion, the approach taken by the EU with the amendment of the eIDAS Regulation. Given the unique competences implicated by this Regulation, fostering cooperation among Member States on a matter intrinsically tied to their national sovereignty, thereby promoting the development of a digital identity at the EU level. The regulation is grounded in the establishment of necessary competition rules for the internal market's functioning (Article 3 TFEU). However, interestingly, identification is not expressly included in any of the EU's competences, implying it is reserved for Member States, which means that the EU digital identity created through the EUDI Wallet must be understood as an addition to national digital identification means.

This transition from the exclusive responsibility of Member States to the importance of developing a strong digital identity policy for the progress of the EU's internal market can also be seen in other areas, such as cybersecurity. Cybersecurity was initially configured as an internal policy related to security and prevention of cybercrime, to its evolution as a transversal policy, key for the Digital Single Market and with a strong international profile. Indeed, cybersecurity, as part of national security, was considered the exclusive responsibility of Member States, with a complementary role for the

---

accumulating data resources within that territory and using this accumulation of power to set norms internally and, it is hoped, externally (Farrand & Carrapico, 2022, p.436).

<sup>219</sup> Experience shows that digital data sovereignty is more achievable and effective at the EU level, as evidenced by GDPR. The discourse on digital sovereignty is not about replacing traditional national sovereignty but augmenting it with a supranational, digital counterpart.

European institutions. However, the growing importance of digital services in European economies and the increase in the number of incidents and computer attacks have motivated the development of a cybersecurity policy that focuses less on the prevention of cybercrime and more on the importance of secure cyberspace for the development of the EU's internal market (Piernas López, 2020, p.189).

Furthermore, eIDAS2 emerges in a moment of change, with the adoption of several regulations by the EU affecting the digital landscape. In this line, the DMA is particularly important. Among the content of this regulation is the designation of gatekeepers and the introduction of a series of obligations. The modification introduced by the Council to the eIDAS2 text means interaction with these concepts, implying that EUDI Wallets Providers and issuers of notified electronic identification means acting in a commercial or professional capacity and using core platform services for the purpose or in the course of providing EUDI Wallet services and electronic identification means to end-users, are business users.

Their consideration as business users implies that gatekeepers will be required to ensure, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware, or software features that are available or used in the provision of its own complementary and supporting services. This provision is essential as the EUDI Wallet already needs to be built, at least on the operating systems of the different devices (e.g., iOS, Android). Article 6.7 DMA requires gatekeepers to allow business users and providers of ancillary services (which includes identification services pursuing Article 2.15) to access hardware or software features, such as secure elements in smartphones, and to interoperate with them through the EUDI Wallet or Member States notified electronic identification means.

In addition, as already noted, eIDAS2 leverages the definition of very large platforms introduced in Article 33 DSA, which identifies these with those with a number of recipients in the Union equal to or higher than 45 million. These platforms will fall under the scope of mandatory acceptance of the EUDI Wallet.

Furthermore, we identify other interesting regulations that are emerging or have emerged in recent years. For example, the Data Governance Act has defined the prerequisites for establishing a regulated environment for data sharing within the EU. This regulation presents a number of possibilities, one of which is the voluntary sharing of data by individuals or businesses for the common good. This provision aligns with the principle that users should have the ability to control and decide on the use of their personal data. On the other hand, in the financial landscape, there exists a specific version for data sharing within financial ecosystems, the Proposal on a Framework for Financial Data Access or FIDA<sup>220</sup>. Additionally, the Proposal for a Regulation for Payment Services explicitly references the EUDI Wallet. This Regulation refers in its Recital 111 to the utility of the EUDI Wallet in supporting identification and authentication in payment processes and its value for the development of a pan-European payment system.

From this brief analysis, I aimed to show that we are currently undergoing a transition toward an era marked by important public intervention. Emerging regulations must be considered conjointly to understand the overall purposes of this transition. Upcoming legislative pieces tend to have in common at least three objectives or patterns: the enhanced protection of EU citizens, the regulation of digital spaces, marked by continuous data flows in all sectors, and the position of the user at the center of the ecosystem, who must be able to exercise control over their information. By putting these regulations together and understanding them from a “higher” perspective, we can visualize the EU's objectives on the path to recovering digital sovereignty and creating a new, more efficiently regulated digital ecosystem.

---

<sup>220</sup> The Proposal on a Framework for Financial Data Access refers to the obligation to provide customers with an interface that allows them to authorize the sharing of data (permissions dashboard) in Article 5.3 letter d, which, in my opinion, could raise questions as to whether this could be integrated with the functionalities of the EUDI Wallet or whether we are talking about two separate tools. This discussion is led by Prof. Dr. Carmen Pastor Sempere, who coordinates the LegalCripto research project, in which one of the topics studied is the identification of the person in control of digital assets, following the UNIDROIT principles. More information available in BAES Blockchain Lab. (n.d). *LegalCripto by BAES*. Retrieved 12 February, 2024 from <https://www.baeslegalcripto.eu/>

**2.1.2. Public Sector Leadership versus Market Dominance: A Comparison of EU and US Strategies in Digital Identity.** Government intervention directly influences the promotion of technological innovation, as noted by Utomo and Dodson (2001, as cited in Seeman & O’Hara, 2007, p.3). In the process of technological innovation, technological standards play a crucial role in facilitating the widespread adoption of a certain technology. However, standards can evolve in different ways: these can be set either through regulatory measures or established via negotiated agreements, complemented by market-driven forces that aim to achieve compatibility<sup>221</sup>.

Technological standards are called to play a determinant role in the adoption of the EUDI Wallet. The legislator has established a set of requirements for the EUDI Wallet in the eIDAS2 Proposal. However, these are high-level requirements that, for the purpose of maintaining the technological neutrality that is required by the Regulation, do not point out to any technological standard. However, the Regulation has envisaged the development of these requirements in form of IAs. The responsibility for further refining these requirements to enable practical implementation has been entrusted to a dedicated expert group. This group is responsible for producing the previously mentioned ARF<sup>222</sup>, the main objective of which is to develop an interoperable EUDI Wallet Solution based on common standards and best practices. The ARF must prepare the content of the IA referenced in Article 6a paragraph 11, that is, the one developing the features and requirements for the EUDI Wallet. The IAs are a specific legislative instrument. Consequently, the EU’s approach toward standardization in digital identity ecosystems will still be the “imposition” of certain standards through regulatory instruments. Nevertheless, at the present moment, the latest version of the ARF is not

---

<sup>221</sup> For example, in the case of wireless communications standards the US. government did not designate a specific standard. Instead, it opted to let market forces determine the standards. The EU, on the other hand, relied on the collective efforts of the European Community and ETSI) to develop and establish a single, uniform cellular standard (Seeman & O’Hara, 2007, p.7).

<sup>222</sup> The first version of the ARF provided an outline or a first description of the requirements of the EUDI Wallet. In particular, it distinguished between the objectives of the EUDI Wallet, roles in the ecosystem, and functional and non-functional requirements in the EUDI Wallet. The European Commission published a second version of the ARF, considered to be the first complete version, in January 2023. Successive versions have been published recently during the month of March 2024 in the GitHub repository.

yet available, nor is the IA. Therefore, it will have to be re-assessed later the level of “imposition” based on the final drafting and the number of alternatives provided by it.

The US approach to digital identification has historically diverged from that of the EU. In the US, the role of the public sector in identity policy is less relevant<sup>223</sup> than in Member States within the EU. In the scope of digital identity, instead of implementing a centralized, government-led initiative, the US government has traditionally relied on the private sector to provide the necessary credentials to authenticate citizens when they use federal websites. The reliance on the private sector for tasks where there is a public interest at stake is complex and, in the case of the US, led to the development of a common risk methodology. To this end, the Federal Office of Management and Budget issued the first memorandum (M-04-04) in 2003, which required agencies to review new and existing electronic transactions to ensure compliance with the appropriate level of assurance. This document established and detailed four levels of identity assurance for electronic transactions that required authentication, thereby providing a basis for assessing credential service providers on behalf of federal agencies. In 2019, the same office issued a second memorandum (M-19-17), establishing that agencies must implement the guidelines laid out in the NIST Special Publication 800-63-3 and any subsequent versions. Note at this point that the risk methodology presents an important resemblance with the LoAs in eIDAS, which is again an indicator that, although eIDAS implementation has predominantly resulted in State-owned formulas, the methodology is open to different modalities.

As we navigate the current technological transition, the US approach differs significantly from that of the EU, particularly in the absence of a dedicated regulatory framework like in the EU. Yet, the US has a legislative proposal named the Improving Digital Identity Act; however, more than two years after this Proposal was first

---

<sup>223</sup> Already, the US has not issued a national identification document. The first instance of establishing a minimum set of requirements at a federal level in the U.S. can be traced back to the Real ID Act. This legislation, which was passed by Congress in 2005, put in place minimum security standards for the issuance of licenses. Moreover, it prohibits certain federal agencies from accepting driver's licenses and identification cards from states that fail to meet the Act's standards. This law became mandatory in May 2023. Consequently, only State-issued driver's licenses and identification cards that fully comply with the Real ID Act are accepted for official federal government purposes, such as entering secure federal buildings or boarding domestic flights.



introduced, there have not been significant advancements in the legislative procedure, and it may never enter into force. This regulatory proposal is less comprehensive than the eIDAS2 Regulation. Nevertheless, it is interesting that it introduces the concepts of identity credentials and identity attributes, setting up the basis for a new ecosystem. Furthermore, it proposes the establishment of a Task Force whose purpose would be to orchestrate a government-wide effort to develop methods to improve access and bolster the security of both physical and digital identity credentials, spanning all levels of governance: federal, state, local, tribal, and territorial.

However, even in the absence of an approved and well-defined regulatory framework, there exist observable responses by industry; notably, a wave of new mobile apps has emerged over the last three years. In this context, we can categorize these emerging solutions into three types: State-owned proprietary apps, the Apple Wallet, and other wallet apps, most of which have been developed through established public-private partnerships<sup>224</sup>. From a legal perspective, for the recognition of third-party wallet apps, States have entered into agreements with the providers of these wallets. The case of Apple is particularly noteworthy, whose latest agreements with some States have allowed residents to store their driver's licenses or State IDs digitally in their Apple wallets. In addition, Apple exerts a standardization role by requiring States to comply with the ISO standards for mDL, a standard in which Apple itself has actively participated in developing.

While the approach taken by these States seems to be efficient, it also raises important concerns. Already, various observers have noted the excessive control that Apple can exert over the whole digital identity process. For instance, quality testing is mandated to align with Apple's certification requirements, and any marketing efforts are subject

---

<sup>224</sup> The LA Wallet, a Digital Driver's License app, was formulated in collaboration of a private company with the Louisiana Office of Motor Vehicles. LA Wallet. (n.d.). *Official Louisiana Digital Driver's License - LA Wallet*. LA Wallet. Retrieved October 18, 2023 from <https://lawallet.com/> The Mississippi app appears to be a product of a partnership with IDEMIA. Mississippi Department of Public Safety. (n.d.). *MISSISSIPPI MOBILE ID*. MS Driver Services Bureau. Retrieved October 18, 2023 from <https://www.driverservicebureau.dps.ms.gov/mobile-id/>; and myColorado app is the outcome of a joint venture between the State of Colorado and various software companies. State of Colorado. (n.d.). *Home*. myColorado. Retrieved October 18, 2023 from <https://mycolorado.state.co.us/>

to Apple's prior review and approval. Furthermore, Apple shifts responsibility to the State, and the choice to finance this initiative via taxes is also subject to debate, as it only serves those who use Apple products (Roth, 2021).

Even though this is an entirely different scenario, I believe that the US context can offer valuable insights into the EU landscape, specifically regarding best practices and pitfalls to avoid when engaging with private providers of wallet apps. On the contrary, the US can gather some lessons from the EU background, especially in coming up with federal laws to help develop a uniform governance framework for identity credentials ecosystems in all States.

Broadly speaking, the EU approach provides greater stability and regulatory certainty, and it gives the public sector a key role in this transition, which must lead it and make it possible. However, unlike the US, the EU has yet to integrate with the industry, particularly with technology giants. These companies are expanding at an extraordinarily fast pace, taking advantage of the regulatory design period. Furthermore, a robust alliance with technology could foster a quicker and more efficient rollout of transformative changes. Consequently, it is clear that the regulatory climates vary, as do societal needs and values; however, both models face the shared pressure of advancing technology; in both ecosystems, there is no unique authority, and both can learn from each other's unique experiences and approaches.

## ***2.2. Services of General Interest and Their Applicability in the Digital Sphere***

The provision of the EUDI Wallet to citizens will fulfill a fundamental function in digital societies. Its potential impact extends far beyond the scope of public services, fostering business development and driving economic growth. Although eIDAS2 has now introduced a clear mandate directed to Member States, the functionalities that the EUDI Wallet is called to offer are essential for the development and participation of citizens in current digitized societies, which, in my opinion, evidences the existence of a general interest<sup>225</sup> in its provision.

***2.2.1. Digital Society's Advancements Highlight the General Interest in a Digital Identity Layer.*** The EUDI Wallet has emerged at a moment where it was necessary to provide citizens with “better” means that guarantee their existence over digital channels. As explained in previous sections, the EUDI Wallet aims to “revolutionize” the way we traditionally access public and private, cross-border and, hopefully, national services. This is also justified by the fragmented landscape that was presented in the first chapter of this thesis, as well as the excessive reliance on poorly regulated private providers of electronic identification means.

The EUDI Wallet arrives to change this situation, and the fundamental value it incardicates is, in my opinion, “access to digitalization,” where a general interest exists. The EUDI Wallet aims to ensure equal opportunities for all persons in the digital era and protect digital rights and privacy. Furthermore, it encompasses the broader societal benefits and advancements that digitalization can bring, such as economic growth, innovation, or increased efficiency, involving policies that foster digitalization or promote digital innovation. These are the objectives behind the rationale of the EUDI Wallet, which precisely justify the intervention of the legislator. The EUDI Wallet is a

---

<sup>225</sup> I have not identified a clear distinction between these two terms (general interest and public interest), and general interest is sometimes identified as public interest or even common good. Some authors describe it as those outcomes best serving the long-run survival and well-being of a social collective constructed as a public (Bozeman, 2007, p.17). In my opinion, these two concepts overlap to a certain extent, with the particularity that general interest usually refers to a broader societal or collective welfare and well-being that encompasses the interests of the entire community or society.

clear policy option for better protection of citizens' rights and freedoms in digital means as well as to foster digitalization.

Appreciating the existence of general interest involves certain obligations for the State in the protection of the service at stake through various legal forms, traditionally grouped under the term “public services.” Nevertheless, given the variety of definitions<sup>226</sup> for public services at the national level, the EU Law has adopted its proper terminology and identified them with the term SGIs. SGIs, public services, or essential services, as some authors call them, aim to satisfy the vital needs of citizens. These services are characterized by the fact that these are, in principle, reserved to the State, leading to more “restrictive” legal regimes. Nevertheless, this should be the exemption, notably when it is possible to provide it under a regime of free competition (Laguna de Paz, 2022, p.240). As Barrio Andrés notes (2017, p.53), these services are configured around the idea of the State as a guarantor of the functioning and quality of the services, which is a reflection of the abandonment of a “State owner of the service” or “State provider of the service” in favor of a “State guarantor,” as Esteve Pardo adds (2023, p.35), a recent doctrinal and conceptual elaboration in line with the latest evolution of the State when scientific and technological knowledge is in the hands of private operators, and so the leading role in public service management.

SGIs are a supporting pillar of the European social model and a social market economy. Three categories of SGIs are traditionally distinguished: economic, non-economic, and social (Leanerts, 2012, p.1261), although some authors refer to only two categories: economic and social (Laguna de Paz, 2022, p.240) and the Commission Communication in 2011 is limited to distinguish economic and non-economic services. The delimitation between the different types of SGIs, or even between normal economic services and SGEIs, is very complex in practice<sup>227</sup>. However, for the purpose of distinction between

---

<sup>226</sup> Despite the differences articulated around the term of public services, as Wollmann's note (2010, p.3), it can be identified by the government acknowledging that certain essential collective needs must be met, and cannot be solely achieved through market supply and demand. The government, whether central, local, or European, may vary in their interpretation of what is considered essential and the level of coverage they guarantee. However, these variations do not alter the core of what a public service is.

<sup>227</sup> Piernas López provides a very illustrative example (2017, pp. 122–123) where the Commission rejected the construction of an airport as an SGEI. Although the Commission acknowledges that it would have a positive impact on local economic development, this cannot be considered sufficient to qualify as

the different types of SGIs, the idea is that while economic services are those carried out for profit, social services respond to the needs of vulnerable citizens and are based on the principles of solidarity and equal access. Both categories imply a title for public intervention, not a delineated legal regime. However, in the case of social services, public intervention is usually more intense.

The debate over SGIs arises precisely because of the tension over how far the market involvement in the provision of basic services through the private sector (privatization and liberalization) needs to be regulated and controlled to ensure that the general interest is guaranteed. However, as it can be inferred from the previous classifications, not all types of SGIs imply privatization or market liberalization. In this sense, SGIs of a non-economic nature tend to be identified with those services that the State does not want to delegate or even allow for private participation (normally because they are intrinsically tied to the State's prerogatives), such as police or justice; these services operate under the principle of solidarity and are subject to public control, or that service implies the exercise of State prerogatives and the fulfillment of State responsibility toward the population. Conversely, SGEIs are characterized by the economic nature of their activity and, notably, the provision of these services in exchange for financial compensation.

The distinction between the different types of services can, however, be thin, in particular, considering that these services are not defined in EU Law, and their references in the legal texts are limited<sup>228</sup>. Some authors note that SGEIs must be distinguished from those activities that are connatural to the State, such as police, justice, and defense, or that might imply the exercise of public powers (Laguna de Paz, 2009, p.5), in my opinion, a fragile criterion nowadays, considering that there already exist private actors that exercise public authority. In practice, the delimitation has a

---

an SGEI. Conversely, the construction of an airport in an isolated area where no other airports or means of transport are readily available could be considered an SGEI.

<sup>228</sup> The term SGEI appears in Article 14 TFEU and Article 36 of the Charter of Fundamental Rights, while the term SGI appears only for the first time in Protocol no.26 annexed to the Treaty of Lisbon. These limited mentions are probably an attempt to provide close definitions, given Member State's power of decision in their identification. Discretion that on the other hand is reconducted by the EUCJ case law.

casuistry nature. The author notes some case law where the ECJ considered the service of a social nature due to the link with prerogatives that traditionally correspond to the State, the impossibility of separating the activities with an economic nature, and the aim of the State to provide the service to all its population<sup>229</sup>. In addition, other criteria, such as the question of whether a market exists for certain services, may depend on the way those services are organized by Member States and may vary from one Member State to another. In other words, due to political choices or economic developments, the classification of a given activity can change over time, and what is not an economic activity today may become an economic activity in the future.

The application of these ideas to the provision of the EUDI Wallet can be approached in various ways. Firstly, it is important to acknowledge that it shall be clarified whether the provision of the EUDI Wallet implies the exercise of public authority and to whom this authority corresponds. In addition, the eIDAS2 Regulation, as it has been repeatedly noted, allows for a variety of implementation options, so Member States have the flexibility to either directly or indirectly provide the service or even to regulate a corresponding market. In addition, contrary to other identification means, the EUDI Wallet is voluntary and is composed of at least two elements: a PID and a wallet app.

Nevertheless, the EUDI Wallet is only provided when there is a convergence of all the necessary elements, implying the provision of electronic identification means and making the connection with public powers more apparent. In addition, in most European nations, there is no dedicated market for these services<sup>230</sup>. Even in scenarios like that of Norway, there is no market in a strict sense for these services. Additionally, the EUDI Wallet's use is free for natural persons, which consequently narrows the potential for market profits. According to Gallo (2022, p.15), remuneration is a crucial element in achieving the prospect of generating profit independently, without State interference.

---

<sup>229</sup> Laguna de Paz and other authors, such as Lenaerts (2012, p.1250), cited in this regard Case C-364/92 SAT Fluggesellschaft (1994) ECR I-43, paragraph 30, concerning the control and supervision of air space, and Case C-343/95 Diego Calí & Fligi (1997) ECR I-1547, paragraphs 22-23 concerning anti-pollution surveillance of the maritime environment.

<sup>230</sup> This aspect would need to be restudied in detail in the scope of the EUDI Wallet.

Moreover, another factor to consider is the eIDAS liability model that has been sustained thus far, with Member States at its core<sup>231</sup>.

For these reasons: the intrinsic connection with public powers, the absence of a dedicated market, and the inability to generate remuneration, I would suggest that the provision of the EUDI Wallet is likely to be classified as a non-economic SGI. However, this classification would be strictly limited to the provision of the EUDI Wallet and does not imply that the service can only be provided by the public sector, but private participation will be possible insofar as these private operators comply with the obligations required by SGIs. In addition, there might exist other services associated with the EUDI Wallet that might fall in the category of SGEIs or even the EUDI Wallet for legal entities, which, in principle, will not be provided for free.

In conclusion, in this moment of technological and regulatory evolution, I believe it is also important to bring back basic legal constructs such as the concept of SGIs. This moment of change presents a unique opportunity to reevaluate digital services that will be crucial if we aim for digitalization to be inclusive rather than erecting additional barriers. If we do not seize this chance to challenge traditional ideas and infrastructures, we are at risk of perpetuating inequalities and exclusions or even exacerbating these disparities, given the broad reach and impact of digital means.

---

<sup>231</sup> The eIDAS introduces a tripartite liability system, with Member States at its heart. Essentially, Article 11 states that the notifying Member State is responsible for any intentional or negligent damage caused due to non-compliance with its obligations under Article 7, points (d) and (f), in cross-border transactions. This means the Member State must ensure the uniqueness of person identification data and the availability of free online authentication for services provided by public sector bodies. They also can't impose any disproportionate technical requirements on parties intending to authenticate, if such requirements obstruct the interoperability of the notified electronic identification schemes. Additionally, the eIDAS Regulation holds the issuer of the electronic identification means, which may be a party other than the Member State, liable for any damage caused due to failure in compliance with obligations specified in Article 7, point (e), in cross-border transactions (as per Article 11.2). The party operating the authentication process is also liable for damage caused due to incorrect operation of the authentication as per Article 7, point (f), in cross-border transactions.

**2.2.2. Conceptualizing the European Digital Identity Wallet as a Service of General Interest.** As already introduced above, the distinction between SGIs and SGEIs is complex in practice and ultimately decided on a case basis. Furthermore, the qualification depends on the specifics of the Member State or territory and might vary over time. Nevertheless, some common rules apply to all SGIs, irrespective of the economic nature, notably non-discrimination, freedom of movement, and application of public procurement rules. In the event of qualification of the SGI as economic, the rules on internal market and competition law apply.

Considering the EUDI Wallet as an SGI implies a certain degree of public intervention to guarantee adequate service provision. This is particularly relevant in a scenario where the participation of private providers is possible. Such consideration is not something new, but several sectors already exist (some very related to the subject of discussion) where regulation has been adopted to ensure the availability and affordability of high-quality services, as is the sector of telecommunications<sup>232</sup> or access to the Internet and digital services<sup>233</sup>.

There is no closed list of obligations for providers of SGIs, but these vary depending on the specific country or region, as well as the intrinsic features of the service provided and its economic or non-economic nature. Nevertheless, as noted above, we can identify a set of basic or core obligations, usually common to all SGIs, that I will try to summarize in this section in the context of the EUDI Wallet provision.

From the perspective of the “user of the service,” SGIs have associated a set of key obligations usually grouped under the term “universal service obligations.” These obligations imply that the service is available to all citizens, independently from their location or income, at a reasonable price (in case of an economic nature) and quality. Shelling out this term, we identify an obligation of availability that requires that the

---

<sup>232</sup> For example Article 27 of the *Ley 11/2022, de 28 de junio, General de Telecomunicaciones*, in Spain

<sup>233</sup> For example the *Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia*, in Spain, or the *Loi pour une République numérique*, in France.



service is available in all areas, including remote or rural areas. However, availability also implies that the service is affordable<sup>234</sup> to citizens and, in the context of digital services, accessible. In the scenario of the EUDI Wallet, these obligations would imply that the EUDI Wallet is easily available for people living in rural areas, which might, in turn, translate into easy online onboarding processes. Likewise, even if the service is non-economic, it is essential that certain groups of the population do not get excluded from it, as it could happen in a scenario where PID provision depends on the banks.

Additionally, in my opinion, availability in the digital sphere has a strong connection with digital literacy. From the perspective of digital literacy, the EUDI Wallet should be made “technically available” to all people, irrespective of their age and technical knowledge, which might be achieved through dedicated learning programs or other policy strategies. The availability requirement is also intrinsically connected with the principle of non-discrimination; therefore, these services shall not discriminate based on personal characteristics, ensuring equal access to all persons. Nevertheless, considering that the EUDI Wallet is provided on the basis of a legal identity issued by Member States, these must define the categories of citizens that shall be able to obtain the EUDI Wallet, as will be explored in the next chapter.

Another key obligation in SGIs is the continuity of the service. This requirement implies that the service is consistently available to all citizens, including on weekends, holidays, and during emergencies. In the scenario of the EUDI Wallet, it is essential to guarantee its continuous functioning, particularly given the nature of the use cases where it aims to be implemented. For instance, in the scenario of payment authentication, the impossibility of using the EUDI Wallet could result in the user not being able to pay for a certain service. Such considerations bring important challenges or questions concerning the regime for the provision of the EUDI Wallet, questioning whether a model of public provision is suitable for a service that might require 24-hour assistance.

---

<sup>234</sup> Affordability is also a key obligation of SGIs, traditionally applicable to the scope of SGEIs. The goal is to prevent any discrimination or exclusion based on financial means, therefore ensuring service availability. Article 6a, paragraph 6b of the eIDAS Regulation envisages that the issuance, use, and revocation of the EUDI Wallet shall be free of charge, at least for natural persons. This provision has been modified in the last text of the eIDAS2 Proposal, making it clear that no price can be charged in the processes related to the issuance and use of the EUDI Wallet.

Another dimension of this obligation in the EUDI Wallet could be the “continued ability to obtain the EUDI Wallet,” which is a topic up for debate and strongly linked to the onboarding process. Finally, linked to the continuity obligation is also its counterpart, the possibility of suspending the service, which, in turn, requires delimited and reasonable causes for its suspension, as could be the case of a security breach.

SGIs must be provided under certain quality standards that ensure citizens receive reliable and satisfactory services. As it could be inferred, assessing the quality of public services is not a trivial matter. In the scope of the EUDI Wallet, the eIDAS2 Regulation has already advanced a high number of requirements that ensure the quality of the service. These requirements will be further refined in the upcoming IAs, particularly concerning security, privacy, and user interface. However, there is a remaining margin of decision for Member States in the actual quality of the provision of these services. In this regard, the quality of the EUDI Wallet will not be exclusively related to the technology deployed but also to organizational and administrative aspects, such as the ease of their use or available assistance.

Finally, accountability is another key obligation in the provision of SGIs. A service must be accountable to ensure compliance with the previous obligations, making it transparent to citizens as well as effective and efficient in its provision. The eIDAS2 Regulation has introduced a governance framework in Article 46a that requires Member States to designate one or more supervisory authorities in their territory that must supervise providers of the EUDI Wallet and take actions if necessary. This requirement will need to be refined at the national level, appointing the concrete entity assuming this role and taking account of the specific modality for the EUDI Wallet provision. We cannot go into more detail here, but the resulting governance framework at the national level from the eIDAS2 Regulation may deserve the contributions and conclusions of another research work. For now, we will just note the topic and include some mentions in the next chapter in the hope that someone else is already working on it<sup>235</sup> or that I will revisit it in the near future.

---

<sup>235</sup> In this regard, I strongly encourage you to read Alexandre Amard's research paper titled “Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Decisions.” Amard, A., Hartwich, E., Hoess, A., Rieger, A, Roth, T., & Fridgen, G. (2024). Designing Digital Identity Infrastructure: A

The purpose of this section was to provide some guidance on the expected key obligations in the provision of the EUDI Wallet in its consideration as an SGI. Some of these obligations are already included or can be derived from the eIDAS2 text. Consequently, the aim of this section was to abstract the concept of the EUDI Wallet from the eIDAS Regulation and to connect it with basic concepts in European and Administrative Law. By doing so, we get more pieces that help to complete the puzzle of the EUDI Wallet, where even if eIDAS2 is bound to be the key regulation on digital identity in the EU, it has to be integrated with other regulations, especially at the national level, that ensure the success of the service provision.

### **3. The Public Sector is Bound to Play a Crucial Role in the Development and Guarantee of a Digital Identity Layer, at least in Europe**

Digital identity is becoming a fundamental service in today's modern societies. Its significance extends far beyond interactions with governments and public entities, being at the core of all exchanges that take place in our daily lives. The eIDAS2 Proposal arrives at a key moment to redefine the digital identity landscape and try to remedy previous shortcomings, notably due to the fragmentation of digital identities used in different services which resulted in a poor protection of the citizens which might be left without any means for communication in the digital sphere. The mandate for the provision of the EUDI Wallet is undoubtedly a commendable step; however, as it has been presented in this chapter, it is also important to take into account that the EUDI Wallet is limited by the specificities of EU legislation. This does not imply that the EUDI Wallet cannot achieve the level of success that is inferred from the Proposal, affecting all sorts of services in the national and European scope. However, from a strict legal perspective, legal obligations are limited in the Regulation; the rest will rely on the political will of the Member States or the voluntary adoption by the different stakeholders in the ecosystem.

---

Taxonomy of Strategic Governance Decisions. Proceedings of the 57th Hawaii International Conference on System Sciences, 2151-2161. <https://hdl.handle.net/10125/106646>

Likewise, a curious aspect that wanted to be brought to the readers' attention is the lack of a standalone identity right. When I started this thesis around four years ago, digital identity was usually confused with privacy and data protection. Indeed, there is a very important dimension in digital identity that concerns privacy and data protection, but it goes far beyond that. For this reason, the unique nuances associated with a right to a digital identity deserve an extensive examination, with the goal of defining a specific right.

In the context of eIDAS2, the EUDI Wallet emerges as the cornerstone of the new digital identity ecosystem. This EUDI Wallet, although it opens the door to new markets, emerges as a public-guaranteed service, in line with the latest EU policies and regulations emerging in the digital era that are opting for a more intense public intervention to lead a transformative change. This is also the result of the changes in the development of the cyberspace, initially conceived as an ideal means for anarchy, to the need to claim a strong public control, coexisting with private control, over the activities carried out in the cyberspace (Barrio Andrés, 2017, p.55). However, these transformations are complex and normally do not result in a unique solution. In the scope of digital identity services, we have seen very varied modalities for implementation within EU borders and, beyond European territory, completely different approaches that are resulting in diverse evolutions of the digital identity ecosystem.

In this context, where very various implementations are possible and what is more, that I suggest considering in order to achieve a high level of efficiency in the provision of the EUDI Wallet, I would like to recall that the eIDAS2 is a Regulation with a strong public guarantee. The provision of the EUDI Wallet must be guaranteed by Member States, a core obligation clearly stated in the Proposal, and the consideration of EUDI Wallet as an SGI will imply that irrespective of the entity who provides it, will need to comply with certain obligations, partially completing the puzzle of guarantees and obligations for the EUDI Wallet Providers started by the eIDAS2 Proposal.

However, I also believe that, beyond eIDAS2, the obligation of the public sector to guarantee a functional digital identity could have also been inferred from the general interest that exists nowadays in a digital identity layer that ensures citizens' access and participation in digitized societies. I believe this reasoning is in line with the proposals of Barrio Andrés (2017, p.167) on the need to recognize a Fundamental Right of access to the Internet insofar as this becomes the vehicle for exercising other rights of active participation in contemporary societies, which I find is also very much predictable for a digital identity layer as an “essential” component of this vehicle to enable this effective participation. Such a consideration may, therefore, require a reconsideration of the fundamentals of the Internet, as noted at the beginning of this thesis, which was initially built on a privatized infrastructure, demands now a digital identity layer that falls within the scope of public services.



## CHAPTER V

---

### UNKNOWN IN THE EIDAS2 REGULATION AND THE CALL FOR NATIONAL REGULATORY DEVELOPMENTS

---

The eIDAS2 Regulation, in its purpose of providing an EU-level strategy for harmonizing electronic identification means to drive digital transformation, sets out a list of well-defined mandates and objectives; however, it does not specify the means to achieve them, leaving an important margin for national intervention by Member States. It is curious that we are referring to national intervention in the context of a Regulation<sup>236</sup>, which, as it is well known, is directly applicable in all Member States. However, due to the nature of the subject covered by the eIDAS2 Regulation and the delimitation of competences between the EU and Member States, the need for national intervention is more than evident. Even in other sectors where the need for national intervention might not be that clear, such as in privacy and data protection, we identify various national laws emerging post-GDPR approval, including Spain, Germany, France, and Italy<sup>237</sup>. In the eIDAS scope, we already identify supplementing laws, such as in the case of Spain<sup>238</sup>.

Consequently, the choice of instrument does not preclude the possibility of national intervention. However, the role of Member States is different in the sense that these are not required to transpose the totality of the regulation but rather complement those areas

---

<sup>236</sup> EU legislation has been recently evolving toward more regulations instead of directives. While the traditional differentiation between these two instruments has been the necessity for national intervention, nowadays, this perspective is challenged by the dominance of regulations, which are, in some cases, complemented by national legislation.

<sup>237</sup> *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de derechos digitales, Bundesdatenschutzgesetz, Loi Informatique et Libertés and Codice in materia di protezione dei dati personal*, respectively.

<sup>238</sup> *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza*.

that are left for national discretion or development. eIDAS2 embodies a complex balance between the EU's competence in the development of the Single Market and Member States' exclusive competence concerning their national sovereignty. The eIDAS2 Proposal effectively blends with this national self-determination by offering flexibility in the provision of the EUDI Wallet and leaving the specifics of its implementation to Member States. These specifics include determining the entities authorized to provide the EUDI Wallet, the categories of citizens or other entities that may receive it, as well as the guarantees, rights, and obligations associated with its provision and use.

This final chapter aims to identify areas for national supplementation by Member States, with a focus on two key topics: the provision of the EUDI Wallet and the statute of guarantees, rights, and obligations of the various participants within the ecosystem. For the purpose of making the conclusions more concrete, I will refer to the Spanish case and laws. Nevertheless, I believe this analysis can provide important value to other European countries, but keep in mind that it will need to be adapted and refined in the context of different national laws, especially when it comes to referring to concepts as abstract and complex as administrative authority.

## **1. The Provision of the European Union Digital Identity Wallet from A Public Law Perspective**

### ***1.1. The Provision of the European Union Digital Identity Wallet as a Manifestation of the Exercise of Public Powers***

The question of who will provide the EUDI Wallet remains one of the main uncertainties within the eIDAS2 Proposal. Various arguments exist, particularly advocating for the opening of the market to private wallets, given the potential increased efficiency these may offer. However, the eIDAS2 Proposal entrusts this decision entirely to the Member States' discretion. Thus, the selection of the EUDI Wallet Provider is ultimately a political decision.



However, independently of the model chosen, we anticipate that it will require the adoption of certain safeguards in the process of provision. Likewise, the provision of the EUDI Wallet, as an electronic identification means aiming to create legal effects for third parties, constitutes, in my opinion, an exercise of public authority that must adhere to the relevant legal requirements under Public Law.

***1.1.1. The Attribution and Exercise of Administrative Authority.*** Some authors have abandoned the attempt to translate the concept of administrative<sup>239</sup> powers or administrative authority due to the complexities that this concept entails. Gamero Casado (2021, p.27) opts to maintain the term *potestad administrativa* in Spanish to avoid potential confusion or ambiguities and make the concept as precise as possible. In our case, given that the purpose of this work is not to offer additional conclusions on the notion of administrative authority but rather to study a very specific subject, I believe that we can keep the concept of administrative authority or administrative powers in order to make this work accessible to a wider audience. Nevertheless, the concept of administrative authority has a very specific and unique meaning in each legal framework, which is inherently tied to the concept in the respective language.

The definition of administrative powers is notoriously complex. As some authors suggest, these are often recognized by their unique characteristics, especially when compared to other legal constructs. Gamero Casado (2015, pp.22 and following), citing Romano (1965, p.299), sheds light on some of these specific features. He points out that administrative authority does not arise from a prior legal relationship but is bestowed by the legal system, with specific legal rules enabling its holder. This recognition may be embedded in Constitutional rules or in law and can be acknowledged either explicitly or implicitly. Furthermore, administrative powers are imprescriptible, meaning they are not exhausted through their exercise or over time. Additionally, the legal object upon which the authority is vested is generic (not specific or for a particular case) and has a

---

<sup>239</sup> It is important to note that the term "administrative" is not as commonly used in English as it is in Spanish to refer to matters of the Public Administration and is often substituted for "public." Nevertheless, I believe that the concept of administrative authority is more accurate insofar as it refers to an entity's role in the administration, execution, and enforcement of laws and policies.

functional character. In other words, they are conditionally granted to achieve a specific purpose, surpassing the exclusive interest of the subject.

Indeed, administrative authority as a form of exorbitant power is usually justified by the need to satisfy a general interest, and they must be used for that end (Rivero Ysern & Rodríguez, 2015, pp.23 and following). General interest, however, is one of those notions undefinable from an objective perspective (Gonzalez Gil, 2021, p.18) or that might not even be advisable to define (Gamero Casado, 2015, p.16). Nevertheless, it was already noted in the previous chapter that the interest in a digital identity layer concerns the common good of citizens. In a context where digital identity is emerging as a necessary starting point for all interactions in a society that is becoming more and more digital, the general interest is, in my opinion, obvious and will become more obvious every day.

If we claim that there exists a general interest in a digital identity layer, we can deduce, as was suggested in the previous chapter, that in the EUDI Wallet, which attempts to be a more harmonized and cross-operational electronic identification means (to a certain extent, a first attempt for a “digital identity layer”), there exists a general interest. Appreciating a general interest in the provision of a service may justify the existence of administrative power for its provision. In addition, this perspective shall be integrated with the direct mandate to the Member States included in the eIDAS2 Regulation, who are ultimately responsible for providing the EUDI Wallet.

Furthermore, I would like to insist on the fact that the EUDI Wallet goes beyond the mere provision of technical services; its provision, as electronic identification means, gives rise to specific legal effects for third parties. However, I would also like to point out that the final version of the ARF is not yet available, and therefore, the roles in the EUDI Wallet may be subject to some changes. Nevertheless, in the configuration of the EUDI Wallet as an electronic identification means, it was previously noted that regardless of whether this role is subsumed in other roles or not, there will be a provider of the EUDI Wallet as an electronic identification means. This process of configuring a EUDI Wallet Solution as electronic identification means is what produces legal effects

before third parties and what, in my opinion, could be considered to imply the exercise of administrative authority.

This conclusion brings a set of consequences, notably the need to allocate administrative authority through legal provisions<sup>240</sup>. Insofar as public authority does not arise from a previous legal relationship, this must be directly attributed by the law<sup>241</sup>. It could be said that eIDAS2 "attributes" public power to the Member State in the form of legislative power to decide and regulate the provision of the EUDI Wallet. Subsequently, the legislation will establish the administrative authority for the provision of the EUDI Wallet. Such reasoning does not imply that the EUDI Wallet can only be provided by the public sector, but the participation of public sector entities with private law forms, or even directly of private entities, is still possible. As Gamero Casado (2021, p.59) conveniently notes, although this manifestation of power is always attributed to the public sector, its exercise may be entrusted to other public sector bodies governed by Private Law, as well as to strictly private persons.

However, its consideration as a manifestation of administrative authority triggers the application of Administrative Law, which might have different manifestations in line with the modality finally chosen by Member States. In the first modality of provision of the EUDI Wallet, there is no delegation in the exercise of administrative authority, but instead, the public sector opts to provide the service itself (i.e., *gestión directa* in Spanish Administrative Law). However, this choice still demands a specific allocation of competence unless it falls within already established administrative powers and competences. Similar reasonings could be reached with regard to the second modality, "under the mandate of a Member State," as it is necessary to know which specific entity

---

<sup>240</sup> In this context, Gamero Casado observes (2015, p.48), referencing Articles 9.3 and 103.1 of the Spanish Constitution, as well as the judgments from the Spanish Supreme Court (*STS* 20/12/94): "There is no administrative power without authorization from the legal system. Therefore, every administrative action, to be valid, must have the appropriate authorization. Specific administrative powers can be identified whose coverage is provided by the law."

<sup>241</sup> In this regard the Spanish Supreme Court Judgement of 20 December 1994, appeal 322/1993 stated that: "There is no *potestad administrativa* without conferral by law. Therefore, all administrative action, in order to be valid, must contain the due attribution (...)."

has the authority to outsource the task through public procurement procedures<sup>242</sup>. Finally, the third modality might be the one presenting more particularities, requiring first the attribution of the administrative authority to the public sector and, secondly, the configuration of a concrete mechanism or legal regime enabling its exercise by other parties.

**1.1.2. Provision by the Public Sector.** The first modality for the provision of the EUDI Wallet is its direct provision by Member States. This drafting seems to suggest that, under this modality, the EUDI Wallet is provided by a public sector entity without involving a public procurement procedure or similar techniques, which under Spanish Administrative Law falls within the model of *gestión directa*. Nevertheless, this modality requires allocating the administrative authority by determining the public sector body competent for the provision of the EUDI Wallet.

The most straightforward approach would be to consider that the *Dirección General de Policía* is competent for the provision of the EUDI Wallet based on the extension of the authority for the issuance of the national identification document<sup>243</sup>. However, in my opinion, the EUDI Wallet goes beyond merely serving as a tool for citizen identification in the context of public order because the acquisition and use of the EUDI Wallet are entirely voluntary. Secondly, because the EUDI Wallet transcends the mere identification function, opening, as suggested in the previous chapter, a vast array of possibilities in a new ecosystem of identity credentials which might lead to perceiving the EUDI Wallet as closer to the scope of public services than identification or police State's function<sup>244</sup>.

---

<sup>242</sup> It may be worth considering including other forms of "under the mandate of a Member State", but the amendment made by the Parliament's compromise text suggests that this provision is primarily intended for public procurement scenarios. Nevertheless, this reference to public procurement has not been maintained in the final text and could potentially open the door to other modalities that may exist within the scope of Member States' national law.

<sup>243</sup> This competence is established in Article 10 of the *Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana*.

<sup>244</sup> The EUDI Wallet is not primarily designed to identify and monitor citizens within national borders. Instead, its purpose is to offer citizens new avenues for accessing both public and private services, in principle, in a cross-border context. We propose viewing the EUDI Wallet not merely as a means of national identification. Its use extends beyond that, facilitating access to a range of services, both in the

If the administrative authority for the provision is not determined analogically, and, in fact, I suggest avoiding this approach, implementing the eIDAS2 Proposal, even under this first modality, demands a previous exercise of competences delimitation, which in the case of Spain, is contained in the Constitution. As can be expected, the Spanish Constitution does not contain any legal rule where the EUDI Wallet provision can be easily allocated. Nevertheless, my conclusion is that the State retains legislative competence supported by several reasons: first, because the EUDI Wallet, even if we assert that it must be distinguished from national identification tools, can only be provided on the basis of previous valid legal identity issued by a Member State (Article 149.1.2 *Constitución Española*); secondly, the EUDI Wallet has international implications as its scope of use is in principle international or cross-border (Article 149.1.3 *Constitución Española*); thirdly, the EUDI Wallet must provide an electronic signature functionality, which, even if not explicitly mentioned, can be inferred to fall under certain sections. For instance, section 24 pertains to the State's exclusive competence over "customs and tariff regimes; foreign trade," and section 25 discusses the "fundamental legal framework of Public Administrations." Since electronic signatures have ramifications in cross-border trade and interactions with the government, these sections could be applicable. The same reasoning can also be extended to the functionality of electronic identification and authentication of the EUDI Wallet. Finally, it could be said that a connection exists with the telecommunications sector on multiple fronts, notably in communication infrastructure, mobile authentication, security, confidentiality, and interoperability (Article 149.1.2 *Constitución Española*).

Nevertheless, the State's exclusive legislative competence for the provision of the EUDI Wallet should not preclude, in principle, the possibility of execution by territorial entities (*Comunidades Autónomas*). In this line, we identify case law from the *Tribunal*

---

public and private sectors. This broad usability suggests that the EUDI Wallet might be considered a service itself.

*Constitucional*<sup>245</sup> and is already evident in sectors such as electronic signatures where the *Comunidades Autónomas* hold executive competences to establish systems, platforms, and procedures that utilize electronic signatures in their administrative procedures or even in the area of electronic identification means in the access to public services according to Article 9 Law 39/2015 and its addition “any other that the Public Administrations consider as valid.”<sup>246</sup>

For these reasons, my point of view is that the EUDI Wallet could theoretically be provided at different territorial levels. However, the final decision will be strongly dependent on the national perception of the EUDI Wallet. If it is perceived as analogous or complementary to the national identification document in the scope of the State's police function, it is very likely that the authority for its provision will, in principle, remain at a centralized State level. On the contrary, if the EUDI Wallet is perceived as an innovative “tool” that is more in line with public services, there will be less resistance to its implementation by the *Comunidades Autónomas*.

At present, important works are being conducted by the *Secretaría General de Administración Digital (SGAD)* in developing a national identity wallet aligned with the requirements established in the eIDAS2 Proposal<sup>247</sup>. The *SGAD* is a public organism dependent on the *Ministerio de Transformación Digital*. Nevertheless, within this first modality of provision, it is also conceivable, in my opinion, that the public sector entity designated for the provision of the EUDI Wallet recurs to other entities within the public

---

<sup>245</sup> In this sense, various judgements from the Spanish Constitutional Court (*STC* 227/1988, dated 29<sup>th</sup> of November 1988, *STC* 13/1992 dates of 6<sup>th</sup> of February, *STC* 18/2011 of 3<sup>rd</sup> of March, among many others).

<sup>246</sup> For instance, when considering identification services for accessing Public Administration, several judgments have challenged the adherence to the Constitutional distribution of powers (*competencias*) between the State and the *Comunidades Autónomas*. Even though the law was amended before the Constitutional Court's judgment (*STC* 60/2023, dated 24th May 2023), it highlighted the absence of a clear mandate to recognize electronic identification methods from the State exclusively. This leaves room for the *Comunidades Autónomas* to introduce other electronic identification means as they exercise their powers of self-organization.

<sup>247</sup> For more information on the developments of the national identity wallet in Spain by *SGAD*, please view the presentation given by Ángel Martín Bautista during the Conference “*La Nueva Regulación sobre Identidad Digital en la Unión Europea*” held at the University of Murcia on November 2023. Martín Bautista, A. (2023). La propuesta de Reglamento eIDAS2 : contexto y visión general. [Video]. tv.um.es <https://tv.um.es/video?id=148290>

sector, such as the *Instituto Nacional de Ciberseguridad (INCIBE)* or dependent on it. For that purpose, the *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público* regulates in Article 11 the legal construct of *encomienda de gestión*, which would enable the possibility to delegate the exercise of the administrative authority to a separate entity falling within the category referred to as *medios propios personificados*<sup>248</sup>, potentially allowing entities such as the *Fábrica Nacional de Moneda y Timbre*<sup>249</sup> to be vested with the exercise of the administrative authority for the provision of the EUDI Wallet. Another option is the *convenio de colaboración*, as provided in Article 47 of Law 40/2015. This provision also facilitates cooperation between different Public Administrations or between a Public Administration and an entity associated with it.

Finally, it is also worth noting that it is possible that the Public Administration decides to rely on a private sector operator for the development of the technology (i.e., the EUDI Wallet Solution), which will normally imply a public procurement procedure. Nevertheless, insofar as the role of the private operator is limited to the development of the technology, it would still be the case of *gestión directa*, which also explains why the mention of “public procurement” in the second modality of provision established in the eIDAS2 Regulation, “under the mandate of a Member State,” has been removed in the final text.

In conclusion, the keynote in the first modality for the provision of the EUDI wallet is that it remains within the public sector entities or is dependent on them. Following the

---

<sup>248</sup> Pursuing Article 32 of Spain's Public Sector Contracts Law, an entity to be considered a "personified own means" must meet several criteria. The Public Administration should exercise over it a control akin to its own services; the entity should predominantly carry out its activities for the controlling Public Administration; it should not have direct private capital participation; and when operating in the market, it should not seek profit and doesn't operate under normal competition conditions.

<sup>249</sup> In fact, the *Fábrica Nacional de Moneda y Timbre* published its modified statutes in February 2023 to include among its functions (Article 4 letter g) “The provision of security services in communications through electronic, IT, and telematic techniques and means, as well as electronic identification services and trust for electronic transactions, enabled electronic addresses and electronic notifications, scanning, deposit, and custody of documents in any format, and the issuance, manufacturing, and supply of user titles or certificates, in digital format or on a card; the provision of blockchain services and the issuance and verification of decentralized credentials, and the development and provision of digital services for the digital transformation of public administrations, in accordance with the terms established by national, community, or international legal provisions.”

principle of legality contained in the Spanish Constitution (Article 103.1), the attribution of the administrative authority for the provision of the EUDI wallet can only be made by law. Taking into account this requirement, together with the developments proposed in the second part of this chapter toward the configuration of a statute of guarantees, rights, and obligations for the participants of the EUDI Wallet ecosystem, it can already be perceived the relevance of a specific law at the national level for the implementation of the EUDI Wallet.

### ***1.2. Possibilities for the Provision of the European Union Digital Identity Wallet by the Private Sector: Public Procurement and The Act of "Recognition."***

Private entities will also have the possibility to provide the EUDI Wallet, as it is explicitly established in the eIDAS2 text. However, the Regulation is only limited to set two very generic formulations, "under the mandate" and "independently but recognized," that will need to be concretized in the scope of national law. Furthermore, if we maintain the hypothesis that the provision of the EUDI Wallet, as electronic identification means, represents an exercise of administrative authority, then the various legal constructs for the application of Public Law to private entities that exercise administrative authority in their functions apply. This matter is not pacific in the doctrine and raises some challenges, particularly in countries with a strong separation between public and private spheres.

***1.2.1. The Delegation of the Exercise of Administrative Authority to the Private Sector.*** The exercise of administrative powers by entities other than public sector bodies, particularly private sector entities, is discussed in the Spanish doctrine, particularly in view of the latest complexities raised by technological advancements. The topic even concerns the possibility of exercising this function by civil servants (*personal funcionariado*) or another type of personnel at the service of the Public Administration. However, I will not dig into the specifics and will be limited to offering a more generic view, considering that the objective of this thesis is not to provide new conclusions on this topic but notably to connect the subject of study with potentially applicable core notions of Public Law.



The possibility of private operators performing functions involving administrative authority has been well-studied by Canals Ametller. The author notes that the doctrine does not have a unified opinion on the topic. Following the author's studies (2021, p.331), while some authors consider that it would go against the constitutional guarantees of Administrative Law (Martínez López-Muñiz, 2017, p.27), other authors agree with the idea to apply core Administrative Law guarantees and principles when an entity exercise administrative powers, even by private law entities (Gamero Casado, 2015, p.192 and following, García-Andrade Gómez, 2019, pp.175–208, p.17–56, Mir Puigpelat, 2017, p.52).

In this thesis, we adopt this second perspective for logical reasons. Otherwise, the hypothesis we are sustaining in understanding the EUDI Wallet provision as a manifestation of administrative authority, letters b and c of Article 6a paragraph 2 eIDAS2, would be inapplicable in the Spanish regulatory landscape. However, even if we understand that it is possible to enable market operators to exercise public authority, this cannot be let exclusively to private sector rules regulating the legal business, but Public Law shall apply to those acts that imply the exercise of administrative powers (Canals Ametller, 2021, p.325–327). A clear example of this extension of Public Law is the case of SGEIs discussed in the previous chapter. Even if Private Law and market competition rules apply to the provision of these services, these also integrate the principles that constitute the legal regime of public services, ensuring a set of guarantees in their provision, as already explained.

From a purely legal perspective, the possibility of delegating the exercise of administrative authority, particularly those functions involving public authority, is typically prohibited by Spanish Administrative Law. In this regard we identify such prohibition in Article 17 of the *Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público*, but also in Article 113 of the *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público*. However, in practice, we observe examples where private operators assume functions involving the exercise of administrative powers. Such assumption is usually justified by the complexities of the tasks, requiring specialized qualified personnel, and is common in sectors such as industrial security, vessel

inspection, or environmental verification, to name a few. Although the specific functions these entities perform can vary, they often revolve around authorization, inspection, or even the drafting of technical regulations.

As an example of the exercise of administrative authority by private operators, the case of technical inspection of vehicles (*ITVs*) is commonly cited. According to the judgment of the CJEU on the 22<sup>nd</sup> of October 2009, their activity is organized in two phases. The first phase of inspection is purely technical and does not imply the exercise of administrative powers. However, this conclusion cannot be maintained in the second phase insofar as the certification of the technical inspection implies a set of legal effects derived precisely from the technical inspection. This conclusion is also sustained by the judgment of the Spanish Supreme Court on the 13<sup>th</sup> of October 1997, as well as the judgment from the Superior Court of Justice of Catalonia on the 11<sup>th</sup> of July 1990, stating that it cannot be accepted that the fact that a public function is exercised by a private entity distorts its nature, as the public attribution of the function is not thereby lost<sup>250</sup>.

Other examples of the exercise of tasks involving administrative authority can be found in the functions of control and inspection, notably in the inspection of credit institutions (Canals, Ametller, 2021, p.334). The common note of the scenarios where the exercise of the administrative authority is authorized to other entities different from the Public Administration is the technical complexity, which raises excessive difficulties for it to offer the service in adequate conditions of efficiency or other guarantees. This also justifies that private entities are not merely engaged for technical assessments; they also derive the legal implications stemming from these assessments, which in turn affect third parties (Cantero Martínez, 2010, p.297). Even if there were an intervention by a public sector officer as a last step to provide the act with public effects, insofar as these personnel would not be qualified enough, the content of the act would have been previously decided by the private operator.

---

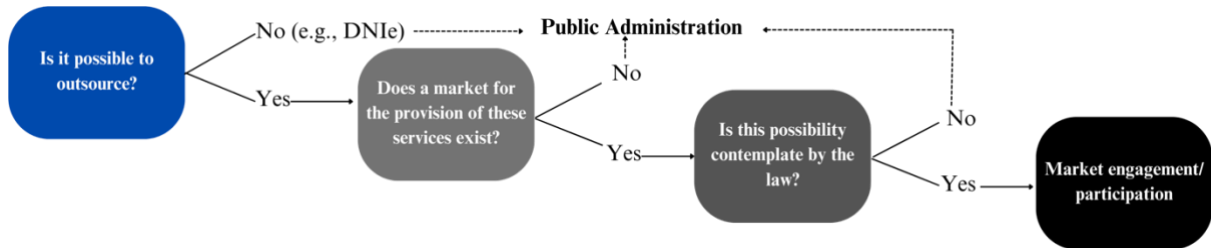
<sup>250</sup> A detailed explanation of this matter and case law is contained in the analysis of Canals Ametller, D. (1999). La jurisprudencia ante el ejercicio de control técnico por razones de seguridad. *Revista del Poder Judicial*, (56), 459-479.

Nevertheless, the possibility of private entities exercising administrative authority does not imply that they must do it in an indiscriminate way. As Canals Ametller already noted (2003, p. 300), “just as the Public Administration must necessarily be enabled by law to exercise public powers and prerogatives, private individuals must also be authorized by law to perform the same functions.” This requirement is logical if we consider that in the same way a law requires the attribution of the administrative authority to the public sector, another law should enable the delegation of its exercise to a private operator, becoming an appropriate instrument for this transfer of authority and prerogatives insofar as their exercise implies consequences for citizens and might even represent a burden, either because it implies a power of intervention in relation to third parties or because it in some way alters the legal positions of other citizens, it requires formal authorization (Sáinz Moreno, 1983, p. 177).

The provision of the EUDI Wallet is bound to produce legal effects before third parties. Consequently, I posit that if the State chooses to delegate the exercise of the public authority implied in the provision of the EUDI Wallet, the law shall contemplate that possibility. Yet, the decision to authorize the exercise of administrative authority requires at least a triple judgment. First, the identification of functions that can be or not be outsourced or delegated and the analysis of the repercussions. Secondly, the existence of a market capable of performing the task with a quality superior to the one that can perform the Public Administration. Thirdly, the existence of a law that precisely makes possible the outsourcing or recognition of administrative powers. Such analysis, as the reader can infer, would need to be adapted to each Member State and their specific Administrative Law, as well as market development in the sector.

**Figure 14**

Outsourcing of Administrative Authority



**1.2.2. Between Public Procurement and the Incorporation of the eIDAS2 "Recognition of Independent European Union Digital Identity Wallets" Option into National Law.**

The eIDAS2 Regulation brings two possibilities that enable the provision of the EUDI Wallet by private operators. Concerning the first one, “under the mandate of a Member State,” this possibility refers, in my view, to a case of public procurement that enables an indirect provision of the service (*gestión indirecta*). That is to say, there exists a contract between the public sector entity and the private provider, but the private operator provides the service under their name and responsibility. Note that this scenario does not exclude the requirement we noted in the previous subsections. It is first necessary to determine the specific Public Administration attributed with the administrative authority for the provision of the EUDI Wallet, and secondly, contemplate the possibility of outsourcing the exercise of this administrative authority.

Well-developed studies in the public procurement sector exist, but we are not going to reproduce here for the same reasons exposed in the previous section. In the case of Spain, the transposition of Directives of the European Parliament and of the Council 2014/23/EU and 2014/24/EU, of February 26 2014, took place through the *Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público*. As a first note, this Law explicitly excludes service contracts in the scope of defense and national security, except service concessions, which are not directly excluded. On the other hand, as noted before, Article 17 excludes the possibility of delegating public authority in service concessions. If the EUDI Wallet is considered relevant in the context of national security, which could occur if seen as analogous to a national electronic identification means, the possibilities of outsourcing would be excluded, except for service

concessions. However, in principle, at least from a strictly legal perspective, outsourcing administrative authority in service concessions is impossible. These two points might be considered as another incentive to view the EUDI Wallet closer to the scope of a public service than an identification tool.

The Law 9/2017 covers different types of procurement, each with its own unique characteristics. Determining the specific procedure to follow can be a relevant aspect, in particular, given the complexities associated with the provision of the EUDI Wallet, that might suggest a restricted procedure (*procedimiento restringido*) or even innovative procedures such as the competitive dialogue (*diálogo competitivo*), instead of the traditional open procedure (*procedimiento abierto*). Nevertheless, I will not go into detail on this point, and I will just refer to the excellent work conducted by Alfonso Sánchez García<sup>251</sup> on electronic public procurement.

An interesting topic in the event of a public procurement procedure for the provision of the EUDI Wallet is the design of the contractual mandate. The eIDAS2 Regulation already contains a set of requirements that would be directly applicable, such as the obligation to contract with a separate legal entity when the EUDI Wallet is provided by a private entity or the requirement for physical and logical separation of personal data. Beyond the requirements envisaged in the eIDAS 2 Regulation, the concrete Member State might take the opportunity to extend these requirements or even include new ones (e.g., interoperability with a broad spectrum of services, universal accessibility to the enrollment process, or the existence of specific backup and recovery plans). As we have observed in the US, certain issues emerge from the contractual agreements that have been concluded with companies like Apple. During a public procurement process, the State can leverage its position to define the boundaries and conditions of service provision explicitly.

---

<sup>251</sup> The author has published extensive work in the area, but I would strongly recommend his first monography titled “La transformación electrónica de la contratación pública. De la digitalización a la automatización.” Sánchez García, A. (2022). *La transformación electrónica de la contratación pública. De la digitalización a la automatización*. Tecnos.

Nevertheless, various challenges might arise in this scenario. A potential topic of discussion is the confinement to a certain operating system, as it occurs in the US. Another important issue to consider is the possibility of excluding foreign entities from public procurement procedures on the EUDI Wallet<sup>252</sup>. Although the 2014 Directives on Public Procurement aim for equal access to public procurement in the EU, there are circumstances where exemptions can be made, especially if the contract is linked to national security. Consequently, due to the sensitivity and critical nature of the service provided, it may be prudent to incorporate the mandates of eIDAS into national law or even develop new ones.

On the other hand, there is a last modality for the provision of the EUDI Wallet where this is provided “independently but recognized by that Member State.” The act of “recognition” comes from EU Law, in this case, the eIDAS2 Regulation, and requires it to be interpreted in national law in the context of available legal constructs. In this scenario, the State is not the owner of the service; neither is it provided directly or indirectly. Spanish Administrative Law immediately leads us to those constructs that enable private operators' participation in regulated sectors or functions traditionally reserved for Public Administration: service concessions and administrative authorizations.

A service concession is defined as an agreement in which one party entrusts another with the operation of a public service, with compensation determined by the financial outcomes of the operation (Bon, 2005, p.2). Service concessions are a form of public contract governed by Law 9/2017 in Spain and at the EU level by Directive 2014/23/EU. The process of awarding these contracts typically follows a public procurement procedure<sup>253</sup>, which could potentially include this figure in the second modality for the

---

<sup>252</sup> Bearing in mind that EU public procurement procedures function on the principle of non-discrimination among Member States, an exemption to this general rule would normally have to be established, justified either by a clear public interest or by the value it brings to national security.

<sup>253</sup> Specific circumstances included in Law 9/2017 exist that can potentially surpass the need for a public procurement procedure. For example, Article 118 pertains to minor contracting; Articles 168 and 169 refer to the negotiated procedure without publicity, especially for reasons of exclusivity; and Article 120 discusses emergency contracting. There are also provisions for scenarios where previous open or restricted procedures have been declared void. Yet, these require the justification of specific reasons to apply.

EUDI Wallet provision included in the eIDAS2 Proposal as a service concession transcends the “mere recognition” and grants exclusive rights to an organization to manage a service. However, various aspects challenge the provision of the EUDI Wallet under this legal construct. First, Article 17 of the *Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público* prohibits service concessions from transmitting administrative authority to the concessionaire. Secondly, because a concession typically involves a right to exploitation. As the EUDI Wallet must be provided free of charge, what constitutes the exploitable right? Could it be the ability to penetrate the market and impose charges for additional services? Could it be the ability to charge private providers who decide to rely on the EUDI Wallet? This is a complex question to answer for the discrimination it could generate.

Besides service concessions in Spanish Administrative Law, it is also common to refer to administrative authorizations like licenses or permits<sup>254</sup>. Licenses are administrative acts which, in exercising authority legally attributed to the Public Administration, allow private operators to undertake an activity when compliance with legal norms has been verified to protect the public interest at stake. Therefore, the core difference with concessions is that authorizations do not attribute a right to the private operator but just confirm compliance with the requirements that enable their exercise. Consequently, the exercise of the right without authorization does not infringe a prohibition, but the legal mandate to exercise it without previous authorization (Arancibia Mattar, 2020, p.7). The imposition of a regime of authorization requires it to be justified by the existence of a general interest, and it must also be proportional. These regimes are usually regulated by specific laws<sup>255</sup>, and authorizations are granted by either the State or the *Comunidades Autónomas* based on the distribution of competences.

---

<sup>254</sup> Administrative permits do not differ significantly from licenses. These are not regulated in a single law, but they are included in laws on diverse matters. The distinction between these two concepts normally derives from the involvement of fewer requirements and a more temporary character. Furthermore, the use of one or another in the market has usually been made depending on the willingness to establish a *numerus clausus*.

<sup>255</sup> Examples could be health licenses for activities related to health, regulated under the *Ley 14/1986, de 25 de abril, General de Sanidad*, or for specific sectors like pharmacies, the *Ley 29/2006 de garantías y uso racional de los medicamentos y productos sanitarios*.

Alternatives such as *declaración responsable* or *comunicación* have gained predominance in recent years. However, the suitability of all of these legal constructs to the subject of study is debatable as they might be considered too lenient for ensuring the public interest at stake. Consequently, my suggestion would be to consider the development of new legal constructs. This is justified because, first, in the case of Spanish Administrative Law, despite the examples in practice, the possibility of exercising administrative powers that imply authority functions is still a topic of debate<sup>256</sup>. As noted by Cantero Martínez (2010, p.325), in other countries, there exist legal forms that enable the transmission of authority functions, like in Italy, the legal construct of *Munera*, or in Germany, *Belihene*. Secondly, it is necessary to consider the specifics of digital identity services and take as reference the examples studied in this context, like the case of Italy or France. In the first one, the *Codice dell'Amministrazione Digitale* establishes in Article 64.3 ter that digital identity managers within the SPID ecosystem are recognized as “public service managers.” In the second one, *Le Code des postes et des communications électroniques* expressly included the legal construct of “provider supplying an electronic identification means” (*prestataire fournissant d'un moyen d'identification électronique*) in Article L102. While the first concept is tailored to a specific context, notably the *SPID* circuit explained in the second chapter of this thesis, the second mirrors the principles of trust services, emphasizing both a required level of assurance and a shift in the burden of proof.

Nevertheless, in addition to the existing models, at the time of the final review of this thesis, specific legislation concerning the EUDI wallet, *the Decreto-Legge de 2 de marzo 2024, n.19*. Article 20 of the Decree introduces a new article in the *Codice Amministrazione Digitale* (the Article 64.4) that includes the possibility of provision of the Wallet by the public sector or private operators prior accreditation by *AgID* complying with defined procedures and requirements listed in paragraph 3 of this Article (e.g., technical requirements, type of services available, procedures for accreditation before *AgID*, technical standards for interoperability...). Consequently, a

---

<sup>256</sup> At least, it seems that it would require that a public authority appears as ultimate responsible according to the Supreme Court ruling 870/2016 of 21<sup>st</sup> of April 2016 that incorporate the ECJ ruling of 15<sup>th</sup> October 2015 (case C-168/14). Case law cited by Canals Ametller (2021, p.363).



new ecosystem for the EUDI Wallet seems to be built on the *SPID* model, with the *AgID* as the governing body.

In the case of Spain, adopting this third modality for the provision of the EUDI Wallet would require something more than administrative authorizations, particularly in support of the idea that the provision of the EUDI Wallet represents an exercise of administrative authority attributed to the Public Administration. Yet, it is also true that implementing the third modality for the EUDI Wallet might require an “operational” regime resembling administrative authorizations more than public procurement procedures. Consequently, it would be wise to use the chance to draft a specific law that goes beyond merely setting the criteria for “authorization” issuance, considering the vital importance of the service and the need for strong public sector involvement, notably in a scenario where Member States hold the ultimate responsibility. A dedicated law should ideally establish the requirements for these entities and their personnel, requirements in the documentation of their processes, and specific requirements they must uphold<sup>257</sup>, established in the eIDAS2 Regulation or national legislation. Furthermore, it should identify the Public Administration in charge of overseeing their operations and potentially responsible for claims that are not satisfactorily resolved.

This approach would imply an active effort by the public sector to create a framework that facilitates the development of a dedicated “market,” or at least, ecosystem. If we do not seize the opportunity to lead regulatory developments, it is also possible that evolution occurs in the opposite sense, leading to a phenomenon of “regulated self-regulation” as noted by Esteve Pardo (2023,p.78) or “interiorization,” implying that the legislator attributes private powers with public effects (Canals Ametller, 2021, p.236), a phenomenon that already exists in the digital identity sector through the recognition of electronic certificates as a valid means for electronic identification in public relationships (Canals Ametller, 2021, p.371). Ultimately, as already pointed out by Alamillo Domingo (2018, p.158), the possibility of enabling private participation might

---

<sup>257</sup> It could be said that such an approach would be in line with the idea of a “law” applying to a determined category of operators, notably justified in the risks created by their operation. These are rules that apply to the operators but also to any person who interacts with them (Esteve Pardo,2023, pp.70–73).

be the one that makes possible more innovative solutions and is more adapted to the Internet's nature, characterized by the intervention of numerous intermediaries.

## **2. A Defined Statute of Guarantees, Rights, and Obligations for Participants in the eIDAS2 Digital Identity Ecosystem**

### ***2.1. The Provision of the European Union Digital Identity Wallet***

The provision of the EUDI Wallet represents a key process in the configuration of the eIDAS2 ecosystem. In its conceptualization as an exercise of public authority, the specific Public Administration attributed with the administrative authority for its provision must be determined in the law and whether its exercise can be delegated. However, legal requirements in the provision of the EUDI Wallet are not limited to determining the entity in charge or authorized for its provision, but I believe it is also crucial to formulate a comprehensive framework of rights, guarantees, and obligations that govern its provision. While the eIDAS2 Regulation includes certain guarantees, some aspects are left to national discretion. Notably, eIDAS2 only distinguishes between natural persons and legal entities, but it does not specify the categories of natural persons entitled to receive the EUDI Wallet. Likewise, the provisioning process is crucial to prevent undesirable outcomes, particularly those impacting individuals' privacy.

This section aims to shed some light on the adaptation of some traditional rights or the emergence of new ones inherent to this very specific and crucial cyberspace sector. As of the time this section was drafted, the various IAs alluded to within the eIDAS2 Proposal were not available, and it is possible that these guarantees could be integrated within these IAs. However, should they not be, it would be recommendable to incorporate them into national legislation.

#### ***2.1.1. Guarantees from the Perspective of the Provisioning Process and the Provider.***

To ensure a high level of guarantees in the provision of the EUDI Wallet, specific obligations shall be imposed on EUDI Wallet Providers. These obligations vary in

nature. Some pertain to the technical requirements for the EUDI Wallet, while others address the unique processes and structures associated with EUDI Wallet Providers. Additionally, it can be said that the provision of the EUDI Wallet entails two separate and well-defined processes. The first involves a process of ID Proofing at a LoA high pursuing the CIR 2015/1502. The second involves a process of binding between the user's PID and, typically, a specific wallet app<sup>258</sup>.

Concerning the first process, as already explained in the third chapter, the EUDI Wallet must achieve a LoA high. According to currently available legislation, the CIR 2015/1502, the EUDI Wallet will likely involve the processing of biometric data, particularly for the purpose of ensuring this LoA high in in-person scenarios where physical comparison will be required. Although the GDPR does not prescribe specific measures for processing special categories of personal data under Article 9 (instead, it delegates these details to national legislation), it typically prohibits such processing unless it meets the conditions established in paragraph 2. The immediate question that surfaces pertains to the legal basis for this data processing. Although the EUDI Wallet is voluntary, I do not believe that consent would be the applicable legal basis for the data processing; instead, it will be the exercise of public authority, which is also consistent with what has been presented in the previous section; therefore, a public mission covered under Article 6.1 letter e GDPR. Consequently, the processing of biometric data, classified as a special category of personal data, would fall under the scope of Article 9.2 letter g GDPR.

As it is well-known, the GDPR has been developed by national laws in several Member States, and in the case of Spain, when the fulfillment of a public mission justifies the processing of special categories of personal data, Article 9.2 of the *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de derechos digitales* requires a regulation with the status of law to legitimize data processing.

---

<sup>258</sup> It is important to note that the EUDI Wallet should not be confined to a single device and operate in a cross-device context. This point has been raised by John Erik Setsaas and might require the application of cloud-technologies.

Taking as the point of departure the necessity of a law, I believe that this law can be leveraged to further specify the conditions for the processing. The eIDAS2 Regulation already mandates a series of protections, such as the mandate to keep the data both physically and logically separate from any other data and the establishment of a separate legal entity when the EUDI Wallet is provided by a private provider. In addition, it expressly forbids the EUDI Wallet Provider from gathering any personal data that is not necessary for the EUDI Wallet's provision. However, along with these measures, national legislation could further stipulate the specific conditions for data processing, including mandates such as the requirement for the data not to be reused for other purposes, the use of robust encryption algorithms or storage in secure data centers. These are just some examples, as it is evident this is a topic that deserves a complete and separate study by experts in privacy and data protection.

The second key process or step in the provision of the EUDI Wallet is the binding of the user's PID to a specific wallet app. How this process is articulated is essential due to the potential for user traceability it enables. The eIDAS2 Regulation, in Article 6a paragraph 7, mandates that the EUDI Wallet Provider shall not collect any data about the wallet's use that is not necessary for providing wallet services. The final text has incorporated some additional privacy requirements regarding the technical framework to enable privacy-preserving techniques and prevent traceability, but without imposing "strict" mandates as the Parliament's text did<sup>259</sup>. Such a "smoothing process" in the legislative text is justified, in my opinion, to avoid confining the EUDI Wallet to concrete technological solutions and to opt for proportional options in cases where traceability might be justified and beneficial.

However, this does not imply that the EUDI Wallet should enable user traceability. In most cases, the EUDI Wallet will have to adopt technologies and procedures that prevent traceability. A key process in this scope is the verification or validation of the

---

<sup>259</sup> The Parliament's text mandated that the technical architecture of the EUDI Wallet should prevent the EUDI Wallet Provider, any Member State, or any other parties from collecting or obtaining electronic identification means, attributes, electronic documents contained in the EUDI Wallet, and information about the user's use of the EUDI Wallet.

electronic identification means. This process should resort to measures that do not require checking the validity of the EUDI Wallet with the providing entity every time the user recurs to the EUDI Wallet as a means for identification or authentication. The solutions at this point emerge at two complementary levels. On a technological level, the task of investigating privacy-preserving technologies has been assumed by the eIDAS Toolbox and, more specifically, the production of the ARF, which contains or at least prepares the IA referred to in Article 6a paragraph 11. The available version of the ARF offers important insights in this respect. These measures would pertain to presentation protocols. At present, and as my knowledge allows me to understand, only the OIDC4VC<sup>260</sup> and EACv2 protocols can prevent traceability. Moreover, privacy could also be enhanced with respect to data formats, particularly concerning the generation of signatures during the provisioning phase. While both mDL and AnonCreds/W3C VCs allow for selective disclosure, depending on the signature used (for instance, CL signature), collusion prevention could be achieved when the signature is partially generated by both the provider and the wallet. Recommended alternatives for more privacy-preserving solutions could include the availability to download periodically updated revocation lists gathered by RPs (device retrieval) or even exploring the possibilities of decentralized trust registries.

Considering this is a very technical matter and to avoid mistakes, I will refer to technical experts well-known in the sector who will provide more detailed explanations than I can offer<sup>261</sup>. At this point, I would just like to note concerning the interaction between technical and legal norms that IAs are binding regulations under EU Law; however, the technique of *renvoi*, applicable to the EUDI Wallet technologies as per Article 6a paragraph 11, could potentially present some challenges. The direct *renvoi* technique ensures a more uniform application as it becomes a directly applicable technical norm. However, it lacks flexibility. Any update must be explicitly detailed in a new IA,

---

<sup>260</sup> OpenID for Verifiable Credentials is a hybrid approach that integrates the OpenID Connect protocol with the Verifiable Credentials Data Model. When combined, OpenID for VCs allows users to present verified credentials within their OpenID Connect identity token, providing a more secure identity verification process and breaking the connection with the IdP.

<sup>261</sup> We can cite the research work of Peter Lee Altmann (<https://www.researchgate.net/profile/Altmann-Peter>) and Johannes Sedlmeir (<https://www.researchgate.net/profile/Johannes-Sedlmeir-2>).

resulting in a rigid legal instrument that could lead to inconsistencies over time. Conversely, the indirect *renvoi* technique has the issue of being voluntarily adhered to with the presumption of compliance it implies. This means that a technical standard might occupy the space typically reserved for legal developments<sup>262</sup>.

Nevertheless, beyond technical particularities, the law shall prescribe key mandates that will have to be respected irrespective of the technology finally adopted. I believe that there is a pressing need to mandate EUDI Wallet Providers to abstain from accessing, even when technically possible, any data within the EUDI Wallet or related to its use and from using this data for other purposes. We discussed the theme of surveillance in the initial chapter of this thesis, and while an obligation of this nature can be deduced from the GDPR<sup>263</sup> and other cited legal instruments<sup>264</sup>, the absence of a defined mandate against traceability has resulted in practical challenges. The current legislative text has only incorporated this requirement in the scope of EAAs. Therefore, I would suggest crystalizing this mandate into a concrete privacy requirement of non-traceability for EUDI Wallet Providers with justifiable exceptional circumstances<sup>265</sup>. This mandate, insofar as it does not prescribe technological impossibility, leaves a broad margin of interpretation and, hopefully, proportional solutions. This requirement is also particularly relevant in the case of a third-party service, a proxy, that connects the EUDI Wallet with the RPs.

---

<sup>262</sup> Alamillo Domingo (2018, p.431) already noted the dangers of this technique. "Using the indirect referral technique, the European Commission is empowered to establish technical standards through implementing acts. These standards, produced by standardisation bodies (essentially, the industry) imply compliance with corresponding legal requirements when adopted by the Commission and adhered to voluntarily. This presumption is binding on national supervisory bodies. This regulatory approach places emphasis on technical standards, filling the role traditionally reserved for regulatory developments."

<sup>263</sup> Although the GDPR does not specifically mention "non-traceability," several of its principles and obligations imply protection against undesired traceability. These include the data minimisation principle, which limits data collection to the bare minimum; purpose limitation, which confines data use to specific intents; and the emphasis on individual consent. Moreover, rights like access, rectification, and erasure safeguard against unauthorized tracking. Lastly, the GDPR advocates for privacy by design and by default, suggesting a pro-privacy configuration in all data processing activities.

<sup>264</sup> For example, in the case of Spain Article 18.4 CE as well as several case law from the EU we noted in the first chapter of this thesis.

<sup>265</sup> In multiple discussions, John Erik Setsaas has expressed concerns regarding the balance between user privacy and their inclination toward external surveillance to enhance the security of their actions.

Depending on the specific model adopted for the provision of the EUDI Wallet, the requirements, guarantees, and safeguards can also vary. It is expected that the Commission's IA will cover an important part of the requirements for the security and privacy safeguards that shall be adopted in the EUDI Wallet provision. However, considering the necessity, at least in the Spanish legal framework, of a legislative provision for the processing of biometric data, I suggest taking the opportunity to delineate concrete safeguards according to the ecosystem designed at national scale<sup>266</sup>. In addition, this national law could potentially specify what available electronic identification means (if any) could be used for the provision of the EUDI Wallet as well as the specific measures that will be adopted in Member State to ensure cross-border identity matching, in particular in those Member States that do not rely on a unique persistent identifier.

To conclude, we can identify other obligations, such as the duty to provide technical assistance and education to EUDI Wallet users during the provision of the EUDI Wallet. However, since these guarantees are not limited to the provisioning process, we will consider them in the following subsection.

**2.1.2. Guarantees, Rights, and Obligations from the User Perspective.** The first right for the user that emerges from the eIDAS2 Regulation is the right to obtain a EUDI Wallet. This right stems directly from the mandate in Article 6a paragraph 1. However, this mandate does not specify the legal status required by natural persons to acquire the EUDI Wallet. Considering that the EUDI Wallet is provided on the basis of a previous legal identity issued by the Member State, it is expected that its availability will notably depend on the issuing country's regulations. Drawing from the logic applied in the issuance of electronic identification documents, it is likely that these documents will be made available to citizens, permanent residents, and certain categories of immigrants, such as refugees or asylum seekers.

---

<sup>266</sup>For instance, in the case of adoption of the third model, providers of the EUDI Wallet might be subject to specific obligations, such as conformity supervision by regulatory authorities, or other types of obligations according to the designed ecosystem. In *SPID*, *AgID* plays a key role in overseeing these providers to ensure they comply with established standards and provide quality service to users.

It seems logical that nationals are included among those entitled to the provision of the EUDI Wallet. Under Spanish law, nationality is defined by the *Código Civil*<sup>267</sup>; however, there exist other additional scenarios that warrant consideration. It is the case, for example, of long-term residents, whose rights and obligations are governed by the *Ley 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social* and the *Real Decreto 557/2011, de 20 de abril, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, sobre derechos y libertades de los extranjeros en España y su integración social, tras su reforma por la Ley Orgánica 2/2009*. In Spain, foreign individuals intending to stay for a period exceeding six months and who do not possess other permits, such as a residence visa or temporary work authorization, are required to obtain a foreigner's identification number, known as the *NIE*. This requirement is stipulated in Article 4 of the Law<sup>268</sup>, with the specific conditions elaborated in Article 206 of the Royal Decree<sup>269</sup>.

The immediate question is whether the existing timeframes<sup>270</sup> and conditions should be analogously applied to the EUDI Wallet, if distinct requirements should be instituted, and if specific conditions should be imposed in the provisioning process for foreign individuals. Likewise, there might be special categories, such as refugees or stateless individuals, which might require particular consideration. In addition, it should be noted that the process of provision of the EUDI Wallet could potentially affect the Fundamental Rights of natural persons<sup>271</sup>, which raises the question of whether an

---

<sup>267</sup> The Spanish Civil Code (Articles 17-26) defines nationality based on various criteria. It can be acquired by origin, such as when one of the parents is Spanish, or by birth in Spanish territory under certain conditions. There are also options to acquire it, such as nationality by residence or by special grant. However, it is possible to lose nationality through voluntary renunciation, voluntary acquisition of another nationality, or by judicial decision in exceptional cases, such as treason against Spain.

<sup>268</sup> Article 4.1: "Foreigners who are in Spanish territory have the right and the duty to keep the documentation that proves their identity, issued by the competent authorities of the country of origin or of departure, as well as the documentation that proves their situation in Spain."

<sup>269</sup> Article 406.3 provides the possibility of obtaining this number provided that the following requirements are met: a) They are not in Spain in an irregular situation. b) They communicate the reasons for which they request the assignment of said number.

<sup>270</sup> Although it should be noted that the Law on Foreigners establishes a mandatory timeframe for the obtention of the *NIE* (a period of more than 6 months), while the EUDI Wallet would be voluntary.

<sup>271</sup> The EUDI Wallet involves the processing of personal data, thereby potentially impacting the Fundamental Right to personal and family privacy (*intimidad personal y familiar*) envisaged in Article



ordinary law can govern these aspects or if it precises the implementation of an organic law.

In the determination of the categories of natural persons entitled to the provision of the EUDI Wallet, another scenario that warrants consideration is the case of minors. Determining the age at which minors can obtain the EUDI Wallet intersects various aspects, from the capacity of identification and signature to the protection of personal data. Article 1 of the *Real Decreto por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica* stipulates that the *DNI* can be obtained after the age of 14, although it can also be acquired earlier. In the case of the *DNIe*, the Royal Decree specifies that for minors, it will only contain the capability for electronic identification, not for signature. Lastly, the *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de derechos digitales* sets the age limit at 14 years old, as per Article 7. Therefore, the analogical application of these laws could result in the provision of the EUDI Wallet for minors after the age of 14, potentially limiting the electronic signature functionality.

Furthermore, although we have focused on the idea of providing the EUDI Wallet to natural persons, it is essential to note that the EUDI Wallet will also be available for legal entities and non-human entities. The precise process of provision, as well as eligible legal entities for obtaining the EUDI Wallet, will need to be clearly delineated<sup>272</sup>. However, we will not delve into this particular aspect in this section due to the specific nuances it may entail. For instance, it may not necessarily involve the processing of personal data.

On the other hand, the GDPR is directly applicable to the eIDAS2 Proposal; however, I believe it might also be worth contextualizing GDPR rights in the scope of the EUDI Wallet, particularly some aspects that might not have been explicitly addressed in the

---

18 CE. Likewise, the right to equality and non-discrimination (*igualdad*) envisaged in Article 14 CE could also potentially be affected.

<sup>272</sup> In this context, it is worth noting that the EU research project ERATOSTHENES explicitly envisions the potential for non-human entities to acquire a wallet and employ it for identification and authentication purposes. For instance, it can serve as proof of a specific vehicle's status as an emergency vehicle.

eIDAS2 Regulation, such as a potential “authorization right” that surpasses GDPR consent. In this regard, the EUDI Wallet is expected to operate under an authorization model in which users are required to authorize the disclosure of their personal data and any other actions executed via the EUDI Wallet. This authorization can be adapted to the specific circumstances<sup>273</sup> but at least shall involve proof of will and presence of the user.

Despite not being legally binding, the *Carta de Derechos Digitales* provides valuable insights into the delimitation and determination of rights in the EUDI Wallet. The Charter already acknowledged a right to digital identity (*derecho a la identidad en el entorno digital*) that must be managed securely and cannot be controlled or manipulated by third parties. This digital identity must be understood in a broad sense, including attributes and certifications; however, it must also be possible to prove the legal identity with a high level of assurance, which in turn implies that the State guarantees the provision and use of electronic means for the identity accreditation.

Nevertheless, besides the “digital identity right,” other rights could be extrapolated from this document. For instance, in line with the non-traceability requirement that we discussed in the previous section, it might be necessary to define a user's right not to be located and profiled, as contemplated in Article V of the *Carta de Derechos Digitales*, which implies that it is not an absolute right, but it might be possible in those scenarios where it is legally permitted and with the necessary guarantees.

Article VI on Digital Rights provides a right to cybersecurity. Cybersecurity in the EUDI Wallet is a topic already covered in the eIDAS2 Regulation, among other aspects,

---

<sup>273</sup> A clear distinction should be made between cases where explicit authorization is required and where a simple “click-through” would suffice. For example, the authorization level might depend on the sensitivity of the shared data. Likewise, online and offline scenarios may be distinguished for authorization purposes, as in offline scenarios, the user is acting in a presumably “trusted environment,” and the authorization could be understood as the action of unlocking and showing the device to the appointed person (if it is an attended use cases) or machine (unattended use case) to initiate the data flow. The EUDI Wallet might also enable authorization choices (authorization may be given before each transaction or may be configured to cover types of transactions) that will be stored by the RPs as well as in the EUDI Wallet for future transactions. It shall also be possible to withdraw authorization for future transactions that shall not be confused with consent withdrawal under GDPR (which would have implications in processing personal data when no other legal basis applies).

by requiring a LoA high, but also in the mandate of security-by-design that has been incorporated in the final text of the Proposal. However, as it is well known, the user plays a key role in maintaining security, which raises the question of whether a certain degree of user diligence in the management of the EUDI Wallet should be expected. The eIDAS2 Proposal remains silent on this point; however, the PSD2, for example, addresses liability by considering the user's diligence.

The introduction of a diligence requirement in the management of digital tools raises significant concerns, especially when dealing with the elderly population or people with disabilities. This concern is also intrinsically related to the accessibility of the EUDI Wallet, a requirement that has been introduced in the final text of eIDAS2, more specifically in Article 15. Yet, this requirement opts for a generic formulation that will need to be concretized in light of the United Nations Convention on the Rights of Persons with Disabilities, as well as the Annex I of Directive (EU) 2019/8821. For instance, adopted measures could result in specific onboarding processes, educational and assistance programs, and ultimately, a limitation by the design of functionalities.

Besides, we could envision other user rights that could potentially emerge in the context of the management of the EUDI Wallet. The user must be able to understand the functioning of the EUDI Wallet, especially when it involves the processing of personal data, which brings into play the fundamental principles of fairness and transparency as delineated in the GDPR but also somewhat indirectly envisioned in Article 6a paragraph 7 of the eIDAS2 Proposal by requiring the user to be in full control of the EUDI Wallet. Beyond the obvious requirement to limit any external control that this implies, the full control of the user can only be achieved through the adequate understanding of the user, which might, in turn, imply that the EUDI Wallet Provider facilitates detailed explanations or potentially offers educational courses, as well as that it provides technical assistance, which results in the user's possibility to request support through various means when needed.

Additionally, the final text of the eIDAS2 Proposal has included several mentions to the possibility of generating pseudonyms, which appears to indicate a certain right to

pseudonymity when permitted. Article 5 of eIDAS2 states that the use of pseudonyms in electronic transactions shall not be prohibited; however, it seems to delegate its implications to national and Union law, which might imply the need to provide in the scope of other laws, national and Union law, a more explicit description of the specific contexts where these pseudonyms can be used, along with their corresponding legal effects (e.g., purchases performed through the use of pseudonyms when a claim aims to be interposed). In this regard, national intervention can opt for innovating or introducing a functional equivalence principle<sup>274</sup> to provide an effect that nowadays does not exist in paper means (Alamillo Domingo, 2018, p.427).

Tied to the voluntary nature of the EUDI Wallet and the right of issuance is the right to revoke or deactivate the Wallet. This is not explicitly included in the eIDAS2 Regulation, indicating that national legislation should address this issue by defining the specific procedure for deactivation as well as its consequences. In addition, it would be advisable to specify GDPR safeguards in the processes, for instance, concerning the erasure of personal data.

This list does not aim to be comprehensive but rather to provide a brief summary of some of the user rights that we could envision directly for the EUDI Wallet. Like the other sections in this final chapter, it requires a thorough analysis that cannot be fully addressed in this thesis. Finally, it is worth noting that one of the main rights that emerges for the user in the provision of the EUDI Wallet is its possibility of being used as an electronic identification means. In this regard, there is a clear right for the user to opt for its use in those services that are mandated to accept it, but it also implies the right to opt for other electronic identification means, as it has been pertinently included in the final eIDAS2 text, following the Parliament's text modifications.

---

<sup>274</sup> For example, the use of a valid pseudonym shall have the same legal effects as the person's identification through name and surname.

## ***2.2. The Acceptance of the European Union Digital Identity Wallet and Possibilities for a Comprehensive Digital Identity***

Besides the user, the EUDI Wallet ecosystem is integrated by two other key participants: the providers of identity credentials (Issuers of EAAs, which can be considered as the new form of IdPs in the eIDAS2 ecosystem) and the RPs. The providers of identity credentials in the new eIDAS2 ecosystem are integrated by at least two different categories that correspond to different legal regimes, as will be explained in the second subsection. On the other hand, the RPs on the EUDI Wallet can be observed from at least a double perspective: those RPs that are mandated to accept the EUDI Wallet and those that might decide to accept the EUDI Wallet voluntarily. The border between these two is not static, but it might change by the influence of national laws that could potentially extend mandatory acceptance of the EUDI Wallet.

In addition, besides the obligations that might result from the application of the corresponding legal regime, the different parties must have the right to participate in the ecosystem under defined procedures and guarantees.

***2.2.1. Obligation and Possibilities for Reliance on the European Union Digital Identity Wallet and Registration Procedure.*** The success of eIDAS2 strongly relies on the acceptance of the different stakeholders. We already noted in the second chapter that one of the main drawbacks of the eIDAS Regulation has been the limited mandatory acceptance of notified eID means to cross-border public services. As explained in the third chapter, the eIDAS2 Proposal mandates selected categories of RPs to accept the EUDI Wallet and defines a registration procedure for all RPs intending to accept the EUDI Wallet. Both points are, however, described at a very high level and demand to be concretized in the respective Member State.

Concerning the first aspect, the limitation of the eIDAS2 Regulation to cross-border scenarios implies that, in national processes, these RPs are not required to accept the EUDI Wallet. The only exemption, as already noted, is the case of very large platforms that appear delimited by the DSA. However, for other RPs, the eIDAS2 Regulation

would not, in principle, impose mandatory acceptance in the national scope. This is consistent with the delimitation of competences between the EU and the Member States insofar as the EU does not have the competence to regulate national electronic identification means. The consequence is that the decision to accept the EUDI Wallet in national processes depends on Member States. Some authors challenge this perspective insofar as they do not identify grounds in the eIDAS2 text that reflect a limitation of the EUDI Wallet to the cross-border scope<sup>275</sup>. While I agree with this view, in particular, in a scenario such as the one discussed in the paper (payments), a strict legal interpretation of the eIDAS2 Proposal, conjointly with the foundational Treaties of the EU, could challenge this conclusion.

To avoid potential inconsistencies, the solution might pass by recurring to national law to mandate the acceptance of the EUDI Wallet in national processes. Such modification could be driven by a dedicated law that specifically mandates the acceptance of the EUDI Wallet or by introducing concrete amendments to existing Regulations, such as Article 9 of the *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*<sup>276</sup>. In the case of private providers, at the present moment, there is no legislation mandating the acceptance of the EUDI Wallet; therefore, it could be an opportunity to introduce legal provisions in this regard<sup>277</sup>.

On the other hand, to rely on the EUDI Wallet, both parties, those obliged to accept it as well as those that voluntarily decide to accept it, are required to undergo a registration procedure. The registration procedure is only defined at a very high level on the eIDAS2 Proposal, missing essential details such as whether all RPs are required to follow the same procedure, potential causes for exclusion (e.g., RPs that pose a high risk, as indicated by criteria such as previous GDPR fines) or the entity in charge of deciding

---

<sup>275</sup> In this regard, review the paper “Why the acceptance of the EU Digital Identity Wallet for SCA will be mandatory under eIDAS2”. Lange-Hausstein, C. & Kremer, T. (2023). *Why the acceptance of the EU Digital Identity Wallet for SCA will be mandatory under eIDAS2*. (Digitallabor Discussion Paper). <https://rb.gy/yvgc3t>

<sup>276</sup> And potentially Article 40 of the *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público* if Public Administrations, as legal entities, also see the EUDI Wallet as means for identification.

<sup>277</sup> This could potentially raise questions concerning user rights, such as the possibility of using the EUDI Wallet free of charge to access national services.

on the outcome of the registration procedure, as well as potential guidelines to be used in the decision process. Clearly, the personal data aimed to be requested by the applying RP will be key in the decision on admitting the reliance on the EUDI Wallet, demanding guidelines that could be developed by national or EU data protection authorities<sup>278</sup>.

In decentralized States, as is the case of Spain, it might be necessary to determine whether the communication process is at the national or *Comunidad Autónoma* level. This decision could be very much linked to the decision on the provision of the EUDI Wallet that was presented in the first part of this chapter. Also, practical examples that are currently seen in other sectors, such as public procurement, where decentralization challenges the interoperability mandated by EU Law, even in the national scope, might encourage the adoption of a more centralized model unless it is proved that the necessary safeguards to prevent these inconsistent results are adopted. The registration procedure concludes with a decision, an appealable decision. Given the expected nature of the process, this will imply that standard administrative appeals procedures apply<sup>279</sup>.

Once an RP has registered, it can interact with the EUDI Wallet. The registration process is essential insofar as mutual authentication is one of the key requirements in the EUDI Wallet, and under Article 6b paragraph 2, Member States are obliged to provide common mechanisms for the authentication of RPs. A potential enhancement not currently foreseen in the eIDAS2 Regulation could be the structuring of the RPs' registry based on data domains, which would ensure that specific data requests are only permitted from their respective authorized domains.

The eIDAS2 Proposal anticipates that the European Commission will detail the technical and operational specifications concerning these processes; thus, it is reasonable to expect that Member States should base their national developments on

---

<sup>278</sup>This might also include potential involvement of data protection experts in evaluating the data protection elements. In addition, in alignment with the Parliament's amendment, if special categories of data are to be processed, the law should identify the authority responsible for authorizing that processing.

<sup>279</sup>In Spain, various administrative remedies are available for individuals to challenge decisions made by public authorities. These remedies include the *Recurso de Reposición* (a review by the same authority that made the decision), the *Recurso de Alzada* (an appeal to a higher authority), the *Recurso de Sustitución* (an appeal to a different authority), and the *Recurso Contencioso-Administrativo* (a legal action before administrative courts).

these IAs. Nevertheless, beyond the registration process, other areas might require legislative development, as in the case of services requiring “strong user authentication.” At the moment and considering that the definition of strong user authentication” is identical to the definition of “strong customer authentication” contained in the PSD2, and that article 6db is limited to citing categories of services without an exhaustive aim, it is unclear, in my opinion, the specific services that will be mandated to accept the EUDI Wallet, which could demand further delineation at national or even EU level.

**2.2.2. The Opportunity for a Dynamic, Rich Digital Identity through Electronic Attestations of Attributes.** From the beginning of this thesis, we have maintained that identity shall be understood from a broader perspective, encompassing more than legal identity but including all forms of attributes that could be potentially associated with that person. This idea is maintained in the eIDAS2 Proposal, creating an ecosystem where the user might decide to extend their identity. However, the different pieces or fragments of the user's identity operate under separate legal regimes.

In this identity landscape, it can be said that the EUDI Wallet Provider could be identified as the “initial” or “foundational” IdP, which facilitates the “first” electronic identification means, aiming to act as the cornerstone of the rest of the eIDAS2 digital identity ecosystem. It is true that before the EUDI Wallet, there must be a PID provider, but, in my opinion, this could be considered as a “pre-foundational” identity that enables the setting up of the EUDI Wallet, being this last one, a new digital identity itself. The EUDI Wallet is an electronic identification means that operates under a Public Law regime falling within the “part” of the eIDAS Regulation that concerns electronic identification means<sup>280</sup>.

However, the eIDAS Regulation also has a second “part” that is precisely the one that regulates trust services. Although the intervention of Public Law is justified by the guarantees these services must comply with, particularly qualified ones, these services

---

<sup>280</sup> Although under different legal provisions than those concerning electronic identification means. For instance, as it has been noted, it operates under a certification regime instead of peer review.



also operate under the rules of the free market. The new trust service of Issuers of EAAs falls within this second category, which implies that the EAAs will not be granted mandatory acceptance<sup>281</sup> in concrete services, but instead, a principle of functional equivalence is established for qualified EAAs and those issued by or on behalf of the public sector body responsible for an authentic source that shall have the same legal effect as lawfully issued attestations in paper form (Article 45a paragraph 2).

Furthermore, although the idea is that the EUDI Wallet and the EAAs interact with each other to unlock the maximum potential for digital identity in the EU, from a legal perspective, there is no mandate in the eIDAS Regulation that requires the possession of a EUDI Wallet to receive EAAs. Therefore, it shall be possible to receive these insofar as the “container” complies with the interoperability requirements. Clarified this point, it is still worth noting that there is a potential “third legal regime” in the recognition in the final text of the eIDAS2 Proposal of the possibility of issuing EAAs by public entities responsible for authentic sources. The final text has included a specific legal effect according to Article 45a paragraph 3a that requires them to be recognized as such (issued by or on behalf of a public sector responsible for an authentic source) in all Member States. The interaction of these three elements enables the creation of a broad digital identity landscape for the citizens, where they also have a choice in its configuration and extension.

A topic already introduced in the second chapter of this thesis is the poor regulation of non-qualified trust services. In the eIDAS2 ecosystem, although the new provision is expected to increase the business opportunities of qualified trust services providers drastically, it is still reasonable to expect that the user will be managing a wide range of identity credentials that are not issued by qualified trust services providers, and therefore, in principle could fall under the realm of non-qualified EAAs<sup>282</sup>. The poor or almost non-existent regulation for non-qualified trust services might call for additional

---

<sup>281</sup> An exemption to this could be the case of public services when the Member State decides to accept qualified EAAs pursuing Article 45b.

<sup>282</sup> As noted by Delgado Báidez, J.M. (2023) “the attribute provider does not necessarily need to be a public entity, nor a qualified trust service provider, and therefore the probative effects will be uneven.”

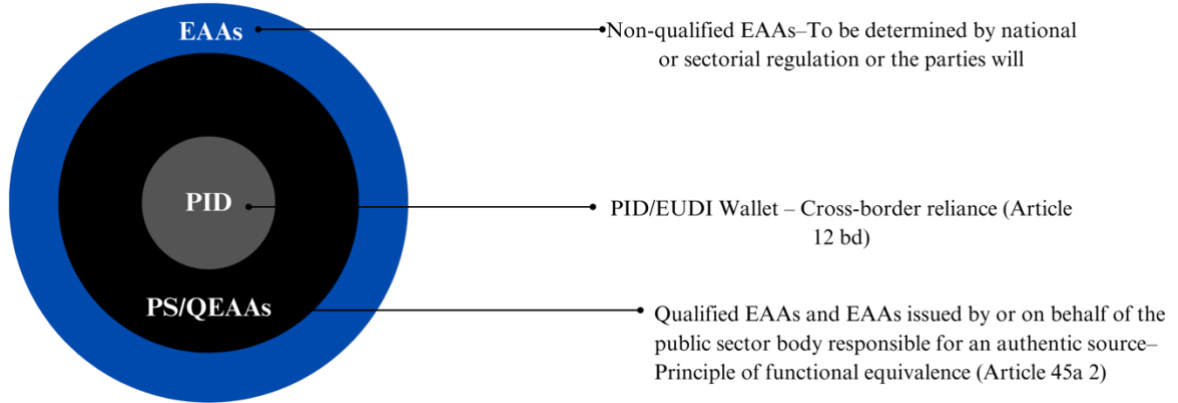
developments at the national or EU scopes, potentially delimiting further the requirements of certain types of identity credentials that are expected to fall under the form of non-qualified EAAs but still offer potential for European interoperability. More specifically, Member States can establish their legal effects from a general perspective or in the concrete sector or could not establish any specific rule, but these cannot deny all legal effects for those EAAs that are not qualified or limit their admissibility as probatory means, leaving space to the will of the parties and Private Law rules.

At the end of the day, one of the key modifications introduced by the eIDAS2 Regulation has been the decentralization of the IdP role; the new scenario is integrated with a high number of IdPs of different types that are subject to different legal regimes. The user, in the center of the ecosystem, might decide to interact with all or some of them, deciding on the final configuration of their digital identity in a dynamic way. Furthermore, what is particularly noteworthy has been the ability of the EU to configure a digital identity landscape capable of functioning at the Union level but still respecting the sovereignty of Member States and without imposing an excessive burden or complexity on RPs that keep a certain margin on the decision on accepting claimed identity attributes; a potential scenario of interest in the configuration of the global interoperable digital ecosystem as it gets closer each day.

Finally, the eIDAS Regulation does not prohibit other types of instruments from interacting with the EUDI Wallet insofar as these do not violate or go against the regime established in eIDAS2, but this will need to be defined at the national or sector level or under a contractual regime.

**Figure 15**

Layered Digital Identity in eIDAS2 & Legal Effects



**3. Further Regulatory Developments will be Key in Determining the Success of the eIDAS2 Regulation**

The eIDAS2 ecosystem combines public and private entities in the role of the IdP; however, the foundation of the ecosystem is essentially of a public nature. The EUDI Wallet as a public-guaranteed good involves the exercise of administrative authority in its provision insofar as it is bound to produce effects before third parties, at least in the international scope. The allocation of that administrative authority requires a law that attributes it to a concrete public entity and, if desired, authorizes the delegation of its exercise to private providers.

The second and third modalities for the provision of the EUDI Wallet bring more complexities linked to the limits and concerns in the exercise of administrative authority by non-public operators. Notably, the third modality of provision demands the existence of a Public Law regime that translates the act of “recognition” into national law. The ease of integration of this EU concept into national law will depend on existing legal constructs in Administrative Law; however, I also suggest considering the sensitive nature of digital identity services at this point, which might require a new dedicated legal regime. In the early days of electronic Public Administration, Martín Delgado

(2009, p.358) pointed out that applying new technologies to Administrative Law presents a twofold challenge. Firstly, there is a technological challenge in developing programs and systems that comply with legal and normative requirements. Secondly, there is a legal challenge in adapting legal requirements to the framework of new technologies, which may involve either adapting existing legal constructs or creating new ones.

This suggestion is also sustained by other authors, notably Canals Ametller (2021, p.64), for whom the generation of new legal constructs seems to be essential in the adaptation of the democratic State under the rule of law, where its traditional powers seem to be wavering under the specifics of the digital domain. In this ecosystem, the principles and traditional concepts of the various branches of law are currently undergoing, and will in the future, undergo important corrections in their adaptation, not only to adapt to emerging or disruptive technologies but also to their expansion and impact in predominantly unknown cyberspace. This thesis notes this need for adaptation in a very concrete scenario.

Either way, deciding on what model is best is not the task in this thesis, but just to reflect, from a legal perspective, on the necessary requirements for its implementation. It might be possible and even desirable to opt for a combination of various models, notably the first and the third model: while the public sector might provide its own EUDI Wallet, other private operators are also allowed to provide their own. This combination might be particularly beneficial to guarantee the provision of the service, especially considering that, in principle, no direct economic exploitation from the EUDI Wallet provision to natural persons is possible.

On the other hand, although the eIDAS2 Regulation has extensive content, introducing a broad range of provisions that affect the different roles in the digital identity scenario, it does not address all the particularities and nuances. Among the particularities that need to be further delineated, we identify the process for the provision of the EUDI Wallet, which demands robust safeguards for the sensitivity of the data that are processed and the potential for surveillance that it enables. Moreover, it is essential to

delimit the subjects entitled to obtain the EUDI Wallet according to national law, and it is also possible to further refine existing stipulations in the eIDAS2 Regulation, affecting other parties participating in the eIDAS2 ecosystem, notably RPs and Issuers of EAAs. Although, until now, the configuration of legal norms, opting for principles and high-level norms was the first step in the attempt to regulate technologies, as Valero Torrijos (2022, p.34) has noted, in my opinion, in some cases, leaving a lot of leeway, brings important drawbacks and might demand to start concretizing these general principles in very specific sectors in order to facilitate their effectiveness and enforcement.

The eIDAS2 Regulation reflects a complex balance between EU and Member States' sovereignty, improving its predecessor from a dual perspective. From the perspective of electronic identification, it includes the EUDI Wallet, opting for a Public Law regime. On the other hand, it expands the sector of trust services to include digital identity services that can operate independently, but that should ideally work in conjunction with the EUDI Wallet to achieve its maximum potential. In conclusion, the law is expected to play a key role in fostering a transformation of the digital identity ecosystem; however, the eIDAS2 Regulation is only the first step of many. National law will still play a key role in the good implementation and broad adoption of the new digital identity model, which could potentially result in a phenomenon of Europeanization as a consequence of the interaction between national and European law and, as Martín Delgado notes (2017, pp.115–117) the transformation of national law through the imposition of European law, where the phenomenon affects not only the law but also ideas, identities, and behaviors, and ultimately culture.



## CONCLUSIONS

**FIRST. The imperative for a digital identity layer is undeniable in today's digital era. As processes become increasingly digitized, digital identity becomes a fundamental cornerstone for citizens to exercise their rights and participate in society effectively. To date, approaches to digital identity have been insufficient to cover actual demands.**

Until now, the provision of digital identity services has been characterized by a fragmented regulatory framework, distinguishing, as suggested in this thesis, between those digital identities provided and used in the scope of public services, private services, or the special case of financial services. However, irrespective of the sector, we have identified a common drawback to all of them: the absence of a clear mandate for the provision of digital identity. The direct consequence of the absence of a mandate of provision is the exclusion of individuals from essential services such as financial transactions, cross-border public services, or everyday commerce.

Today, in an increasingly digital society, the relevance of digital identity is crucial. I advocate for the recognition of the existence of a general interest in a digital identity layer that should be more unified, including different types of services. This is the approach taken by the eIDAS2 Regulation, which creates a sovereign digital identity layer that shall function across the digital sphere in all Member States. The eIDAS2 Regulation establishes a digital identity metasystem that aims to operate across Member States while respecting their different approaches to digital identity but ultimately guarantees the “existence” of the natural person in the digital sphere.

On the other hand, although beyond the scope of this thesis, the EU as an international organization can take a proactive role in developing a globally interoperable digital identity strategy, a space that is otherwise likely to be taken up by private operators. From a legal perspective, a globally interoperable digital identity layer raises important challenges.

The question of the possibility of a global law has come to the fore with the quick proliferation of technologies affecting all regions in the world; however, a very characteristic feature of such a global law would be the need to abandon a "Kelsian approach," where the interaction between different types of rules is clearly defined, in order to accept an ecosystem characterized by the interconnection of different norms and legal systems. Although it is clear that such an approach is unlikely to lead to a well-defined legal system, the reality so far is that, in the absence of regulatory initiatives, technological standards, usually in the form of self-regulation, occupy a space that could be better filled by some form of regulation, where at least there is a certain degree of protection of public interests.

I am aware that it may sound complicated to devise a global form of regulation, but I would like to insist here again on the need to think about new approaches. EU Law has taken such an approach, opting for a regulatory model based on an extension of the sovereignty of the States, with the particular notes of the European Union, resulting in a legal framework that will be able to harmonize States with completely different cultures and traditions. Consequently, taking as the point of departure that digital identity is a national matter, the possibility of reaching a certain level of agreement between nations, at least in the digital sphere, for example, through sectorial harmonization, with a strong focus on concrete use cases, or the conclusion of international agreements, may not be too far away.

**SECOND. eIDAS2 substantially changes the state of affairs in digital identity services by proposing that digital identity, at least for natural persons, must be a public service where Member States must ensure it is provided and that it is done in accordance with established requirements and guarantees.**

The increasing importance of reliable digital identities, united with the issues identified due to the unregulated evolution of the market in these services, has been a call of attention for European legislators. Among the different possibilities, eIDAS2 has taken the most ambitious one, the introduction of the EUDI Wallet. Beyond the specifics around the requirements in its design and provision, the introduction of the EUDI Wallet



contains a strong message, that is, digital identity for natural persons cannot be left to the market or self-regulation; instead, the importance of this service requires a strong intervention of the State.

The EUDI Wallet, as the core element in the eIDAS2 Proposal, aims to become the cornerstone of an ecosystem of identity credentials and provides identification and authentication functionalities to the natural person. Nevertheless, the most relevant note is that the EUDI Wallet emerges as a service whose provision, as well as that it takes place according to established requirements, is guaranteed by Member States. Until now, timid steps had been taken, notably in regulating electronic identification means to public services and the acceptance of a “pseudo market” participated by private providers. However, the insufficiency of this approach, as evidenced in this thesis, demanded a change in the paradigm, and the EUDI Wallet emerged as an electronic identification means of mandatory acceptance for public and private services.

This change is not at all something trivial, but it shows the willingness of States to exercise their sovereignty in the digital sphere and, more notably, the Internet, until now, a space dominated by private operators where the delimitation and exercise of some forms of sovereignty by Member States was at the very least challenging. The eIDAS2 Regulation overcomes the approach of merely imposing new requirements to existing players but, instead, intervenes in the infrastructure of the Internet, notably in the digital identity layer for natural persons, which acquires a public nature independently of the modality for provision.

Furthermore, although out of the scope of this research, it is important to acknowledge that artificial intelligence has come to change the rules of the game, offering notable opportunities but also increasing risks. Its arrival, in my opinion, highlights even more the need for public control of digital identity as an “Internet’s control infrastructure” that ultimately imposes strong guarantees.

**THIRD. The accelerated pace of technological development, combined with the dominance of major digital players, highlights the need to reevaluate possible innovative public-private collaborations, especially through the enforcement of public service obligations. The implementation of the eIDAS2 Proposal represents a fresh avenue for innovation, offering a chance to incorporate insights gathered from various existing models.**

The public nature of the digital identity layer for natural persons does not imply that it can be exclusively provided by the public sector, but instead, as it has been repeatedly noted during this thesis, the entity that provides it will have to do it respecting public service obligations.

This thesis has provided an overview of the implementation of the eIDAS Regulation in various Member States for the purpose of demonstrating the different possibilities for implementation. Notably, the differences between these countries have been articulated around the participation or lack thereof of private entities in the provision of digital identity services. The upcoming application of the eIDAS2 Proposal aims to reopen these considerations by introducing the possibility for Member States to reconsider their digital identity strategies.

In this process, I encourage integrating the lessons learned from various countries, as well as different modalities and strategies deployed to enable the private sector's participation in the ecosystem. While countries that have enabled the participation of private providers have generally achieved a higher level of usability of their digital identity services, allowing the participation of private providers without proper regulation in place also results in denying essential services to citizens. Therefore, lessons and experiences learned from other countries are now relevant in the implementation of the EUDI Wallet. Although the EUDI Wallet has a very specific nature as it is conceived as an electronic identification means, it cannot be ignored that it is bound to offer "digital wallet functionalities." In this context, it is essential to be aware of the current industry pressure by dominant wallet providers and the approaches taken in other countries, such as the US.

Public service obligations could enable the participation of private providers in digital identity services. Yet, as already exposed, the sensitivity of the sector may require additional public control mechanisms, particularly in nations where these functions are traditionally viewed as critical and assumed by the State. For these reasons, I insist on the potential to incorporate new legal constructs at the national level to enable the participation of private entities in the EUDI Wallet provision, which might not only be advisable but necessary to cover the necessities demanded by the specific use cases where it aims to be implemented. I recall once again the example of the *SPID* ecosystem, where private providers are recognized as “public service managers,” a specialized agency oversees these providers, and a comprehensive suite of procedures exists for their integration and participation within the ecosystem. A comparable approach, as the Italian’s legislation has already suggested, might be suitable for the EUDI Wallet landscape, ensuring that citizens have access to multiple EUDI Wallets provided by either the public or private sector.

I believe that the convergence of digital identity models will be almost inevitable for the development of more unified digital ecosystems where public and private services coexist. In fact, convergence can be beneficial to leverage advantages associated with both models: from the private or hybrid models it can be leveraged the potential of technology advancements and the interest of the private sector in the efficient delivery of the service; conversely, from the public model, we extract the emphasis on regulation, especially in ensuring that advancements in technology are used in a way that preserves the rights and guarantees for the citizens.

**FOURTH. The public nature of the EUDI Wallet, which emerges as a “public-guaranteed” electronic identification means that it is bound to produce effects before third parties, will likely demand the application of Administrative Law in regulating its provision.**

The provision of the EUDI Wallet is a key process in the configuration of the eIDAS2 ecosystem but is also subject to important complexities due to its innovative nature and the requirements it might imply for Member States within the different modalities for

provision. We have posited that the provision of the EUDI Wallet transcends the mere offer of technical services and implies, at least in the case of Spanish Law, the exercise of administrative authority, which triggers the application of requirements established in Administrative Law for its attribution and exercise. In Spain, the attribution of the administrative authority for the provision of the EUDI Wallet should be grounded in the law. Therefore, if there is no allocation of administrative authority derived from the analogous application of another norm, a new specific legal provision is required to allocate this authority.

However, one thing is the allocation of the administrative authority, and another is its exercise. The EU Law is limited to introducing the concept of “recognition,” but it precises adequate translation into national law. In Spanish Administrative Law, despite the controversies on the possibility of delegating the exercise of administrative authority to private entities, examples already exist in practice. However, I want to seize the opportunity in the conclusions of this thesis to encourage again the development of more sophisticated and dedicated legal constructs or even ecosystems that open the door to private participation but ensure adequate protection of the public interest at stake.

Additionally, the role of legislation must transcend the “enabling law” purpose and incorporate essential safeguards within the provisioning process. In Spain's context, there must be a specific law in place that oversees the processing of biometric data when it takes place in the framework of the exercise of administrative powers. Likewise, it is essential that the legal framework includes guarantees, rights, and obligations for the participants in the ecosystem. While part of these contents are already included in the eIDAS2 Regulation, Member States' Public Law is essential for the implementation of the EUDI Wallet at the national level, filling the gaps intentionally left open in the eIDAS2 Proposal to afford Member States some flexibility, but also due to the pure delimitation of competences between the EU and Member States.

**FIFTH. In this time of technological change, eIDAS2 represents a concerted effort to create a cohesive regulatory framework for digital identity services. However, it is essential that these regulatory initiatives go beyond the international dimension and take root at the national level.**

The eIDAS2 Regulation has marked a crucial shift in digital identity policy, emerging as the first attempt for a more comprehensive regulatory framework for digital identity services, aiming, among other objectives, to reduce the fragmentation between the public and the private sectors. The EUDI Wallet, as the anchor piece of the eIDAS2 ecosystem falls within the “part” of the eIDAS regulation concerning eID means, and, as repeatedly noted throughout this thesis, the EUDI Wallet framework is, in principle, thought for the cross-border context.

It cannot be ignored that technological advancements have been the driving force behind the changes and the transformation of the digital identity ecosystem. However, the objective now is that the transition occurs in a “regulated” manner, and the law encourages those processes that reshape the ecosystem’s traditional power dynamics and communication flows, as well as facilitate trust. While the eIDAS2 Regulation sets the basis for this transformation to occur in a regulated manner, due to the pure limitations of EU Law and the distribution of competencies between Member States and the EU, it is not sufficient from a strict regulatory standpoint to fully reshape the digital identity landscape. Thus, there is a pressing need for national-level regulatory frameworks that either mirror or, ideally, integrate with this Regulation, going beyond the interoperability objective at the core of the eIDAS Regulations in favor of the development of a more comprehensive digital identity layer that is not limited to the cross-border domain.

**SIXTH. The eIDAS2 Regulation reshapes power dynamics and offers a digital identity model that aligns closely with the SSI framework. However, unlike the more purist interpretations of SSI, it inherently ties to a Member State's legal identity. The extent to which this model is realized depends on future developments in the ecosystem, emphasizing the need to prevent undue barriers that could hinder providers' participation.**

The eIDAS2 Proposal is expected to lead to a transformative change in the ecosystem that impacts prevailing power dynamics. The ecosystem created by the eIDAS2 Proposal shares some features in common with SSI models. On the one hand, there is an emphasis on user control, and on the other hand, the Proposal aims for a decentralization of power hubs. However, the eIDAS2 Regulation has its very own and singular features. Conversely to purist interpretations of SSI, the eIDAS2 Proposal is inherently tied to a Member State's legal identity and strongly advocates for the public sector's leading role in providing digital identity (independently of the model finally adopted, that might welcome the participation of the market). Nevertheless, the eIDAS2 Regulation is not limited to the introduction and regulation of the EUDI Wallet, but it opens a whole new landscape for the participation of private entities in the provision of identity services under the new trust service of Issuers of EAA, ultimately, forcing a decentralization of the role of the IdP by leveraging, among other factors, the natural development of the market.

However, it is important to note that the eIDAS2 Regulation is limited to setting the basics for the emerging ecosystem and that the degree of decentralization will strongly depend on the final implementation of the Regulation. In this regard, the model chosen for the provision of the EUDI Wallet already influences the power dynamics between the user and the EUDI Wallet Provider and, eventually, even between the State and the EUDI Wallet Provider. Furthermore, while it is true that the new trust service of Issuers of EAAs opens the door to the decentralization of digital identity services, the degree of decentralization will strongly depend on the number of these and the correct distribution of the market.

In addition, although we have not gone into detail in this thesis, there could be more ambitious implementations of the eIDAS2 Regulation by merging the new ecosystem with the power of DLTs. The new trust service of Electronic Ledgers enables the decentralization, in a regulated manner, of key services in the digital identity landscape. Among the services that could benefit from this decentralization, we could identify the verification or validation of identity attributes. However, other implementations are possible, such as the generation of DIDs, and efforts in this direction already exist, as is the case of EBSI.

As a result, the eIDAS2 Regulation establishes the basic rules for the evolving landscape, ensuring at least a certain degree of decentralization. However, it will depend on further developments at the national or EU level to maximize the possibilities of decentralization and the affectation of traditional power dynamics. In this regard, it is essential to ensure that no unnecessary barriers are introduced and that market opportunities remain open to prevent monopolization. Ultimately, it is important to opt for a configuration that widens the range of options available for citizens, prevents power concentration, decreases the risk for traceability, and eliminates single points of failure.

**SEVENTH. While the eIDAS2 Regulation lays the foundation for the ecosystem, it does not detail the rights and obligations of the various parties involved. At a minimum, a tripartite framework of rights and obligations should be considered for the EUDI Wallet Provider, the User, and the RPs.**

The eIDAS2 Regulation provides a number of rights and obligations for the different participants in the ecosystem that shall apply in all Member States. However, this framework of rights and obligations demands further specification at the national level. This is particularly evident insofar as Member States are expected to opt for a modality for the provision and delineate the process. Delineating this process implies introducing the necessary safeguards and obligations for EUDI Wallet Providers but also clarifying the user position, particularly those individuals that, according to domestic laws, are entitled to obtain the EUDI Wallet.

Additionally, it is possible for Member States to enhance the rights outlined in the eIDAS2 Regulation. However, such modifications must not go against the rights and obligations stated in the Regulation or cause an unreasonable burden. In other words, Member States may extend the protection provided by the eIDAS2 Regulation as long as it is reasonable and does not conflict with the Regulation's primary principles. In my opinion, considering that the user is going to face an innovative tool, a key point in its success is to ensure it has the right to obtain the necessary resources in its proper management, as well as a clear regime of liability that determines the level of diligence required, particularly considering that the EUDI Wallets will become a vector of attack for cybercriminals. In some cases, the “extended protection” granted by some Member States already by application of the national regulations, such as those that prohibit the existence of unique persistent identifiers, will require further legislative developments, especially the process for cross-border identity matching in their respective countries.

Furthermore, for the user to use their EUDI Wallet in a high number of RPs, it is necessary that there exist defined processes for RPs to rely on the EUDI Wallet and potential causes for exclusion. The definition of the processes to rely on the EUDI Wallet is also determinant in the adequate use of the EUDI Wallet insofar as parties will have communicated the intended use and data to be processed.

While national developments will need to consider the content included in the IAs and the eIDAS2 Proposal, in this thesis, I would like to advise keeping in mind that technological requirements cannot wholly substitute a framework of rights and guarantees for the various parties within the ecosystem. Therefore, a well-defined framework of rights and obligations for the different key roles in the eIDAS2 digital identity ecosystem could be essential to guard against abusive practices and avert an unregulated environment that might perpetuate the current challenges faced in the digital identity landscape.



**EIGHTH. The right to identity merits recognition within the scope of International Law. Nevertheless, with accelerated digitalization and societal changes, there is a need to re-evaluate and fortify our Fundamental Rights and guarantees. While eIDAS2 represents a first form of a digital identity right for EU citizens, this should be further articulated, perhaps initially within national legislation.**

Until now, the protection of the right to identity has been commonly articulated through the extension of other rights, particularly the right to privacy and data protection. However, these two rights have different content insofar as they are designed to protect different goods. In this regard, an infringement of the right to identity does not automatically imply a breach of the right to privacy, and vice versa. As already mentioned in this thesis, when I started my research, I was immediately referred to privacy and data protection. However, at the moment of the conclusion of this thesis, it is hard for me to understand why, given its significance to individual and social development, this right has largely been overlooked in legal frameworks, with only a few mentions in legal texts.

At this moment, we can state that digital identity involves more than privacy matters and deserves its own dedicated regulatory framework. In this regard, it is challenging to advocate for a right to digital identity without a pre-existing recognition of the right to identity in legal texts. I believe that the first right should be established as a foundation before defining its digital counterpart. Once this right is established, it is essential to recognize that while digital identity and traditional identity share foundational elements, they are distinct in nature. Typically, one's real-life identity serves as the basis for a digital identity; however, as noted in this thesis, identity can have multiple dimensions, and in the case of digital identity, its function as a means to access electronic services is particularly pronounced.

The right to identity as a component intrinsically linked to human beings seems to deserve recognition in International Law, particularly within the realm of Human Rights. Conversely, the right to a digital identity remains more debatable at present. While the eIDAS2 Proposal is a pioneering effort in this direction and marks a crucial

milestone, in my opinion, efforts should not stop at this point, and broad recognition of a right to digital identity might require further developments, as noted before, in the scope of national regulatory frameworks. Indeed, such recognition could take place, at least initially, through national instruments, such as enacting or making legally binding documents of the type of the *Carta de Derechos Digitales* in Spain. Such an approach would only be a temporary legal remedy; as society evolves, there is a pressing need to adapt our Fundamental Rights and Freedoms to accommodate them to an increasingly digitized society. The right to digital identity essentially refers to the right to exist in the digital domain and stands out among these emerging rights. However, as we enter further into the digital age, other existing rights may need re-evaluation, and new ones may emerge. This presents a vast area for legal research in the coming years.

**NINTH. Privacy and cybersecurity are foundational pillars of our digital landscape. General regulations, however, often fall short in addressing the specific challenges that arise within concrete domains. This study in the digital identity sector demonstrates that sometimes it is necessary to incorporate dedicated privacy and cybersecurity provisions directly within targeted regulations to ensure effective legislative measures in specific contexts.**

The introduction of privacy and cybersecurity regulations within the EU has undeniably influenced how data is managed and protected, even beyond the EU's borders. However, in recent years, these regulations have sometimes been perceived as ineffective due to their inability to foresee and address all potential issues in a rapidly evolving digital society. As discussed in this thesis on digital identity, the focus sometimes is not merely on how data is processed but also on who has the capacity to process it, thereby affecting the entire power dynamic of participants in the ecosystem. From this perspective, the principle of privacy by design is not just about ensuring data is processed securely but making certain data “unprocessable by design.”

Nevertheless, achieving this ideal is not always feasible, as it can sometimes lead to excessively complex technologies and ineffective processes. This is where regulations notably step in, providing clarity by including dedicated privacy requirements. The

eIDAS2 Regulation is particularly noteworthy in this regard by introducing specific privacy requirements for all participants, along with concrete cybersecurity provisions. In the sector of digital identity, one of the main limitations of the GDPR was, as presented at the beginning of this thesis, its inefficiency in preventing surveillance practices. The latest dramatic events, such as the Cambridge Analytica scandal, have made the whole community rethink its importance, and a non-traceability requirement has been directly stated in the scope of the eIDAS2 Regulation for the scenario of Issuers of EAAs. I suggested in the last chapter that this requirement could also be crystalized for EUDI Wallet Providers, even if justified exemptions are admitted. To draw a parallel that might perhaps result illustrative to the reader, the GDPR does not establish an absolute prohibition to profiling, but it does mandate safeguards. Similarly, traceability, by its importance, should have its protective measures as it usually represents the previous step in the enablement of profiling.

On the other hand, although we could not explore in detail the topic of cybersecurity, I would just like to note that while there are expectations for cybersecurity requirements to be fulfilled by mandating a specific LoA for the EUDI Wallet, there is no perfect overlap between NIS2 and EUDI Wallet Providers. This discrepancy indicates the potential need for national cybersecurity obligations specific to this role, regardless of the entity that assumes it. This would also be in line with the paradigm shift we have been suggesting along this thesis of recognizing the cruciality of digital identity services themselves and not only depending on the entity that provides them.

In conclusion, there was a pressing need to define cybersecurity and privacy requirements within the sector of digital identity. We have suggested that these requirements could be further developed at the national level, but it must also be said that the eIDAS2 Regulation has already established a very valuable precedent that could be replicated in other areas. Specifically, I support the idea that, in concrete sectors, there is value in defining privacy and cybersecurity requirements rather than leaving them vague and open to interpretation, which often results in ineffective practical implementation.

**TENTH. The evolving paradigm in personal data processing now places the user at the forefront. This challenges the traditional concept of data controller, potentially limiting its access to data and relegating its role to technology provision.**

Traditionally, the data controller has been responsible for the physical processing of the data it oversees. However, with new tools like the EUDI Wallet, this idea is changing, as the emphasis is now on retaining as much data as possible within the device itself, exclusively controlled by the user. This paradigm shift poses questions about responsibility for the processing occurring within these devices. In the context of data protection, the actual access to the data is not necessarily the defining factor for determining the role of a data controller; instead, it is the determination of the purposes and the means for the processing. This raises important questions about the role of technology providers and whether these could effectively assume the data controller role, even for data these cannot access or directly control in real-time (e.g., influencing the control could potentially require a modification of technical parameters in software).

The question becomes even more complicated when we integrate these scenarios with other requirements, such as the GDPR certification. Although, as explained in this thesis, this requirement has been finally eliminated from the scope of the EUDI Wallet, it was included in the Commission's Proposal and mutated throughout the different compromise texts. This is a requirement in which I have personally worked in the scope of my consultant role, and the first question that arose was whether, according to the current definition of GDPR certification, it is possible to certify data processing activities where the data controller does not exercise direct control over them and whether a GDPR certification could be limited to adherence to technical standards that ensure compliance with privacy by design principles.

Besides, the eIDAS2 Regulation is characterized by a complex data processing landscape involving multiple parties. In this regard, we identified some challenges in scenarios where the entity in charge of the provision of the EUDI Wallet is not the one who has developed the wallet app (e.g., think in a scenario where commercial wallets are admitted but still the binding process is performed by the public entity issuing the

PID, therefore acting as EUDI Wallet Provider). In addition, while it is true that developers play a crucial role in the definition of the technical parameters of the wallet, holding interpretative control that translates into actionable decisions, the user also retains some level of control, particularly, they might decide to share certain personal data even if the wallet app flags it as unsafe.

I believe that raising these concerns is relevant given the prevailing trend of moving toward enhanced user control over personal data and minimizing processing by external entities. For the moment, this requirement, given its inherent complexities, has been eliminated from the final text of the eIDAS2 Proposal. However, it might be a pertinent moment to start re-evaluating traditional GDPR concepts.

**ELEVENTH. The EUDI Wallet aims to empower users with control over their data. The terms “user authorization” or “permission” should be differentiated from GDPR consent or any other legal basis for data processing under Article 6 of GDPR. The relationship between user authorization/permission and other legal basis distinct from consent under GDPR needs to be clarified.**

The EUDI Wallet is designed to handle personal and non-personal data, ensuring users are always informed about how their data are processed. When sharing their data, users can authorize their use by external parties. However, in my opinion, this authorization should be differentiated from the obligation to provide consent under the GDPR.

The EUDI Wallet is designed to manage all sorts of data, which might include personal and non-personal data; therefore, GDPR consent might not be applicable to all scenarios. Furthermore, as it is well-known, consent is not the only legal basis for the processing of personal data, but Article 6 of GDPR provides various legal bases, such as the data processing mandated in a legal obligation or that is carried out for the fulfillment of a contract.

In principle, the idea is that when using the EUDI Wallet, the user will be required to provide authorization, which will be requested regardless of the applicable legal basis,

to ensure that the user is aware of the data being processed in all scenarios. However, the configuration of authorization in the strictest sense could raise challenges when the legal basis differs from user consent and, notably, in scenarios where the processing of certain data is imposed on RPs by a legal obligation. Although this is a topic that deserves more detailed exploration, a possible solution could be to differentiate between scenarios where user authorization aligns with GDPR consent (and could potentially merge) and those where it serves to make the user more aware (e.g., to proceed with this service, we will need to process the following data). Yet, it cannot result in a notice every time the user is going to use the service, especially if the EUDI Wallet aims to be implemented in areas such as recurrent payments, which may just require a first authorization valid for a set of transactions.

**TWELFTH. The challenge of authentication persists. Ensuring that the correct individual is "behind the screen" is crucial to the success of digital identity. While authentication methods have evolved, they seem to have primarily focus on improving convenience for now. It might be worthwhile to consider integrating diverse authentication procedures within a wallet app to enhance both security and user-friendliness.**

Authentication remains one of the main challenges in the digital identity sector, standing as a crucial process to ensure a lawful exercise of rights. At the present time, while authentication methods have certainly advanced, they still fall behind the level of certainty achievable through physical comparison.

Among the latest methods for authentication, the spread of one of them has been particularly significant. Biometrics have emerged as a game-changer in the process of authentication. While it is undeniable that biometrics can achieve a higher degree of certainty in the authentication process, these typically limit the processing of the data to the device itself. Therefore, in most cases, the comparison is limited to biometric features configured by the user, which can belong to the device's owner or someone else. Moreover, biometrics often works in conjunction with a fallback measure, reducing its security to these default measures. Initiatives such as FIDO have brought

advancements by integrating biometrics with device-based authentication, and progress has also been made in the “binding” of identity credentials. Nevertheless, its effectiveness still strongly relies on the authentication performed in the device.

With the arrival of the EUDI Wallet, there is an urgent need to reconsider the topic of authentication and potentially introduce novel measures, particularly because the EUDI Wallet aims to be used in a broad range of use cases requiring different assurance and guarantees. To achieve a higher degree of certainty, methods such as real-time identity verification can be especially pertinent, or, when available, innovative possibilities such as the comparison of a user's biometric data against the biometrics embedded within a specific identity credential.

However, I am aware that we are very far from offering an answer to the challenge of authentication; therefore, my purpose was exclusively to suggest a diversification of authentication methods. The EUDI Wallet should be able to offer diverse authentication processes based on the scenario's demands. The choice of which authentication process to use could be determined by factors detailed in technical regulation and based on the category of the RP requiring the authentication or even the categories of data being processed. I believe this adaptability could offer a better balance between security and user experience tailored to specific scenarios.

**THIRTEENTH. Emerging digital ecosystems attempt to return control over data and processes to users. However, the complexities of certain digital tools introduce new layers of risk, emphasizing the need for substantial support in their management to prevent a natural return of control.**

One of the main features of emerging digital identity landscapes is giving control back to the users over their data. While the latest years have been characterized by the loss of control over our data, we must be cautious now about the specific way this power is restored in order to avoid being perceived as a burden. There are already examples of this “excessive burden,” such as the inundation of cookie policies during web browsing,

illustrating how an overload of information can ironically lead to misinformation or confusion.

We have already emphasized the need to implement accessibility requirements for the EUDI Wallet through concrete measures, such as dedicated training programs or specific assistance, to ensure that users have a clear understanding of the digital tools they are utilizing and are willing to use them, rather than perceiving them as a burden. Security by design also plays a key role in facilitating the acceptance of the EUDI Wallet and making the user feel more protected from external menaces.

However, this effort also concerns legal experts, who often design complex procedures to protect users, which ironically can have the opposite effect. We already have examples of "simplification" of legal requirements, such as in the GDPR's layered approach to consent. Analogous strategies could be adopted for the EUDI Wallet, especially when dealing with aspects like "user authorization" within the EUDI Wallet or other digital services, such as data sharing within the financial sector. Similarly, as mentioned in a previous conclusion, requiring user authorization for very recurrent transactions, for example, could be perceived as burdensome, and while the user may have read the first "framework authorization," they may not read each individual authorization.

In addition, it is crucial to be prepared for situations where users are unable or unwilling to manage their EUDI Wallet or other digital tools, which might lead to the emergence of new assistance services, which, in turn, can imply a detriment to user's privacy and require adequate regulatory provisions. Nevertheless, it is clear that this is not the desired outcome and that since the EUDI Wallet is a voluntary choice, the balance between user empowerment and usability is essential, with convenience and user-friendliness as crucial values for widespread acceptance and success.



**FOURTEENTH. Digital ecosystems highlight the necessity for synergies between the public and private sectors. It may be necessary to shift our perspective on regulation and view it not merely as a set of limitations, but rather as a gateway to new opportunities. Under this new paradigm, the regulatory framework would aim to encourage innovation and growth, while still prioritizing the public's interests and protection.**

To date, while digital regulation can be considered one of the most significant advancements of EU Law that has extended its effects even beyond the EU's borders, its effectiveness has also been limited when dealing with concrete scenarios. In particular, regulations might sometimes be ineffective in solving problems linked to inherent power dynamics, as explained at the beginning of this thesis. Moreover, the EU's regulations have been shaped by the absence of a well-developed technological industry within the EU, and this situation has not been an exemption even for the latest regulations.

The GDPR is, in my opinion, a very illustrative example; while this Regulation has brought very positive changes to the processing of personal data, its limitations are evident nowadays, calling for adaptation. Emerging regulations, such as the eIDAS2 Regulation, have already taken a different approach where the intervention transcends merely implementing more or new prohibitions. Stakeholders' interest in this regulation was therefore perceived not only from the perspective of another "obligation" to be met but also from the perspective of business opportunities they could exploit in the new ecosystem, as well as a potential improvement of their traditional processes.

In addition, we must also recognize that we are navigating unprecedented times where technological advancements are unfolding at such a rapid pace that keeping abreast becomes a challenge. These innovations, whether regulated or not, are becoming integral to our society. For instance, artificial intelligence advancements have gained prominence and have been integrated into various sectors even in the absence of regulatory frameworks just relying on the different actors' applicable obligations (e.g., privacy and data protection, contractual requirements, general interest defense...).

Therefore, I believe that a different regulatory approach is needed in this evolving digital landscape. While I do not want to deny the value of more traditional forms of regulation, I also believe in the need to adopt more innovative approaches; in particular, rather than waiting for an ecosystem to show its problems, we need to lead the development and design of the ecosystem. I think the eIDAS2 Regulation, which was explained in this thesis, is a very good example. The Proposal has not been limited to being a new version of the eIDAS Regulation, just with some regulatory provisions aimed at solving the problems that we have described in the first chapter of this thesis. Instead, this Regulation has enabled a change in the ecosystem where, besides solving the problems identified in the previous model, new opportunities are created for different stakeholders who can ultimately benefit from their participation, leading to a more natural redistribution of power.

**FIFTEENTH. Innovative ideas have the potential to challenge established legal norms. We are currently facing an unprecedented era where the existing structures are bound to undergo transformation. This may require us to re-evaluate deep-rooted legal concepts. While upholding the rule of law is important, it is equally crucial to avoid hastily fitting new ideas into old frameworks.**

In line with my previous conclusion, I believe that the eIDAS2 Proposal proves that, occasionally, a radical legal review is imperative to reshape foundational ecosystems, an approach that might serve as a valuable blueprint for other regulations. Besides potential regulations in other sectors, which, at the present moment, I do not have enough knowledge to identify and provide valuable conclusions, I think that, at the very least, this transformative nature of the eIDAS2 Regulation must be taken into account in the EU and national legislative developments on digital identity.

In what concerns EU legislative developments, my opinion is that these shall maintain the aim of the core text of the Regulation, further specifying how the legal stipulations must be implemented. However, as has been discussed in the last chapter of this thesis, Member States now have a big responsibility to ensure that the objectives of the eIDAS2 Regulation are achieved. Although I am aware that we cannot draw general conclusions insofar as national law can present important variations from one country to another, at

least in the scope of Spanish Administrative Law, what I have identified is the need to adopt a proactive attitude, which might imply modifications to existing regulations, or even the approval of a new law especially dedicated to cover the topic of digital identity, which I think has more than enough relevance nowadays.

However, it is very important that these emerging laws do not attempt to hastily fit new ideas or roles into existing legal constructs, as these might not be adequate and could potentially prevent them from achieving the final objective of the Regulation. In the same way that EU legislation has been very courageous in the introduction of new tools, new roles, new forms of business, and even new forms of exercise of administrative authority, the national legislation should not now limit its powers and must develop new legal constructs if necessary.

In this regard, I want to insist that the process of re-evaluation should not be limited to technology but also concern established norms. Otherwise, as it is very common nowadays, regulations are just perceived as a limitation for development and change. Just to note a simple example: is it essential to know a person's gender for all their procedures? Perhaps, with the rise of technology, it is time to re-examine matters like this from a legal perspective. Ultimately, it is essential to realize that digital processes are merely traditional procedures in a digital format. If transformation is the goal, then the foundational, traditional procedure must first be transformed.

I hope this thesis can at least serve to bring these considerations to public discussion and, notably, encourage others to continue their legal studies in the sector of technology regulation. I believe that this task precises well-formed legal scholars and practitioners aiming to step out of their comfort zones working in interdisciplinary groups that ultimately lead to proposing new ideas that steer society in the right direction. Historically, while the law has often trailed societal changes, we now have the opportunity to challenge this viewpoint, so the law is perceived as a powerful instrument to initiate and conduct beneficial societal shifts. Furthermore, as technology continues to influence every aspect of our lives, we have a brand-new opportunity to create a fairer and more inclusive society with abundant opportunities for everyone, regardless of their

location or background. By doing so, we might be able to guarantee that the digital era brings meaningful and widespread progress.

## REFERENCES

### Scholarly Journal Articles

- Alauzen, M. (2019). L'État plateforme et l'identification numérique des usagers. *Réseaux*, 213(1), 211-239. <https://doi.org/10.3917/res.213.0211>
- Albrecht, K. & Citro, B. (2020). Data Control and Surveillance in the Global TB Response: A Human Rights Analysis. *Law, Technology and Humans*, 2(1), 107-123. <https://doi.org/10.5204/lthj.v2i1.1487>
- Allmer, T. (2013). Critical Internet privacy studies. *Fast Capitalism*, 10(1), 71-80. [https://fastcapitalism.uta.edu/10\\_1/allmer10\\_1.html](https://fastcapitalism.uta.edu/10_1/allmer10_1.html)
- Alpár, G., Hoepman, J.-H., & Siljee, J. (2011). The Identity Crisis: Security, Privacy and Usability Issues in Identity Management. *ArXiv Business, Computer Science, Mathematics*. <https://arxiv.org/pdf/1101.0427.pdf>
- Andraško, J. (2017). Mutual recognition of electronic identification means under the eIDAS Regulation and its application issues. *Ad Alta: Journal of Interdisciplinary Research*, 7(2), 9–13. [https://www.magnanimitas.cz/ADALTA/0702/papers/A\\_androsko.pdf](https://www.magnanimitas.cz/ADALTA/0702/papers/A_androsko.pdf)
- Aparajita, P. & Jatinderkumar R. (2012). An Investigation of challenges to online federated identity management systems. *Int J Eng Innov Res IJEIR*, 1(2), 104-108. <https://rb.gy/vda25>
- Arancibia, J. (2020). Las autorizaciones administrativas: bases conceptuales y jurídicas. *Revista de Derecho Administrativo Económico*, (32), 5-36. [10.7764/redae.32.1](https://doi.org/10.7764/redae.32.1)
- Arner, D. W., Zetsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. *European Business Organization Law Review*, 20, 55-80. <https://doi.org/10.1007/s40804-019-00135-1>
- Avellaneda O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K.H., Maler, E. Reed, D., & Sporny, M. (2019). Decentralized Identity: Where Did It Come From and Where Is It Going? *IEEE Communications Standards Magazine*, 3(4), 10-13. [10.1109/MCOMSTD.2019.9031542](https://doi.org/10.1109/MCOMSTD.2019.9031542)

- Backhouse, J. (2006). Interoperability of identity and identity management systems. *Datenschutz und Datensicherheit (DuD)*, 30, 568–570. <https://doi.org/10.1007/s11623-006-0145-y>
- Baistrocchi, P. (2003). Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce. *High Technology Law Journal*, 19 (1), 111-130. <https://digitalcommons.law.scu.edu/htlj/vol19/iss1/3/>
- Baldoni, R. (2012). Federated Identity Management systems in e-government: the case of Italy. *Electron. Gov. an Int. J.*, 9 (1), 64-84. <https://www.inderscienceonline.com/doi/abs/10.1504/EG.2012.044779>
- Bender, J., Kügler, D., Margraf, M., & Naumann, I. (2020). Privacy-friendly Revocation management without unique chip identifiers for the German national ID card. *Computer Fraud & Security*, (9), 14-17. <https://rb.gy/1ejlb>
- Bon, P. (2005). El Régimen de las Concesiones Administrativas. *Revista de Derecho Administrativo Económico*, (15), 1-15. <https://redae.uc.cl/index.php/REDAE/article/view/4864>
- Cameron, A. & Grewe, O. (2022). An Overview of the Digital Identity Lifecycle (v2). *IDPro Body of Knowledge*, 1(7). <https://doi.org/10.55621/idpro.31>
- Camp, L. J. (2004). Digital identity. *IEEE Technology and Society Magazine*, 23(3), 34-41. <https://doi.org/10.1109/MTAS.2004.1337889>
- Canals Ametller, D. (1999). La jurisprudencia ante el ejercicio de control técnico por razones de seguridad. *Revista del Poder Judicial*, (56), 459-479.
- Canals Ametller, D. (2013). Principios, reglas y garantías propias del derecho público en la prestación privada de servicios económicos de interés general: el caso emblemático del sector de las comunicaciones electrónicas. *Revista Española de Derecho Administrativo*, (158),127-155.
- Cantero Martínez, J. (2010). La incidencia del fenómeno de la externalización en la Administración General del Estado. ¿Existe algún límite? *Documentación administrativa*, (286-287), 297-334. <https://revistasonline.inap.es/index.php/DA/article/view/9673>

- Casciaro, T. & Piskorski, M. J. (2005). Power Imbalance, Mutual Dependence, and Constraint Absorption: A Closer Look at Resource Dependence Theory. *Administrative Science Quarterly*, 50(2), 167-199. <http://www.jstor.org/stable/30037190>
- Cavoukian, A. (2010). Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society (IDIS)*,3, 247-251. <https://doi.org/10.1007/s12394-010-0062-y>
- Chen J., Edwards L., Urquhart L., & McAuley D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law*, 10 (4), 279-293. <https://doi.org/10.1093/idpl/ipaa011>
- Chevallier, J. (2018). The state as a platform strategy? *Revue Francaise d'Administration Publique*, 167 (3),627-637. <https://doi.org/10.3917/rfap.167.0627>
- Clemons, E. K., & Madhani, N. (2010). Regulation of digital businesses with natural monopolies or third-party payment business models: Antitrust lessons from the analysis of Google. *Journal of Management Information Systems*, 27(3), 43-80. <https://doi.org/10.2753/MIS0742-1222270303>
- Cuijpers, C. M. K. C. & Schroers, J. (2014). eIDAS as guideline for the development of a pan European eID framework in FutureID. *GI-Edition Lecture Notes in Informatics*, 2015, 2014, 23-38. <https://research.tilburguniversity.edu/en/publications/eidas-as-guideline-for-the-development-of-a-pan-european-eid-frames>
- Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law and Security Review*, 44. <https://doi.org/10.1016/j.clsr.2021.105636>
- Dhamija, R. & Dusseault, L. (2008). The seven flaws of identity management: usability and security challenges. *IEEE Security & Privacy*, 6(2), 24-29. [10.1109/MSP.2008.49](https://doi.org/10.1109/MSP.2008.49)
- Donnelly, M. (2016). Payments in the digital market: Evaluating the contribution of Payment Services Directive II. *Computer Law and Security Review*, 32(6), 827-839. <https://doi.org/10.1016/j.clsr.2016.07.003>

- Delgado Báidez, J.M. (2023). La Cartera de Identidad Digital Europea y el principio de “solo una vez” en Derecho español. *Revista de Privacidad y Derecho Digital*, (32), pp.19-73.
- Eaton, B., Hedman, J., & Medaglia, R. (2018). Three different ways to skin a cat: Financialization in the emergence of national e-ID solutions. *Journal of Information Technology*, 33(1),70-83. <https://doi.org/10.1057/s41265-017-0036-8>
- Farrand, B.& Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31 (3), 435-453. <https://doi.org/10.1080/09662839.2022.2102896>
- Finck, M. & Pallas, F. (2019). They who must not be identified- Distinguishing Personal from Non-Personal Data under the GDPR. *Max Planck Institute for Innovation and Competition Research Paper Series*, (19-14),1-47. <http://dx.doi.org/10.2139/ssrn.3462948>
- Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33(3), 369-378. <https://doi.org/10.1007/s13347-020-00423-6>
- Furnell, S. & Zekri, L. (2006). Replacing passwords: In search of the secret remedy. *Network Security*, 2006(1), 4-8. [https://doi.org/10.1016/S1353-4858\(06\)70321-X](https://doi.org/10.1016/S1353-4858(06)70321-X)
- Galán Galán, A. & Prieto Romero, C. (2008). El ejercicio de funciones públicas por entidades privadas colaboradoras de la Administración. *Anuario de Derecho Municipal*, (2), 63-104. [https://repositorio.uam.es/bitstream/handle/10486/664240/ADDM2\\_2.pdf?sequence=1](https://repositorio.uam.es/bitstream/handle/10486/664240/ADDM2_2.pdf?sequence=1)
- García-Andrade Gómez, J. (2019). El «sector público» como referente actual del derecho administrativo. *Revista de Administración Pública*, (209), 175-208. <https://doi.org/10.18042/cepc/rap.209.05>
- González Ríos, I. (2023). Servicios Públicos Digitales: naturaleza jurídica y garantías para el ciudadano. *Revista de Administración Pública*, (221), 11-54. <https://doi.org/10.18042/cepc/rap.221.01>
- Grawemeyer, B. & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, 23(3), 256–267. <https://doi.org/10.1016/j.intcom.2011.03.007>



- Gutwirth, S. & de Hert, P. (2022). Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. *Direito Público*, 18(100), 500-549. <https://doi.org/10.11117/rdp.v18i100.6200>
- Halperin, R. & Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the Information Society (IDIS)*, 1, 71-87. <https://doi.org/10.1007/s12394-008-0004-0>
- Heidebrecht, S. (2023). From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. *Journal of Common Market Studies*, 62(1),1-9. <https://doi.org/10.1111/jcms.13488>
- Hemming, R. & Mansoor, A. M. (1998). Is Privatization the Answer? *Finance & Development September 1998*, 25(3),31-33. <https://www.elibrary.imf.org/view/journals/022/0025/003/article-A009-en.xml>
- Jim. I. & Mina.J. H. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8),56-59. [10.1109/MC.2018.3191268](https://doi.org/10.1109/MC.2018.3191268)
- Kerikmäe, T. & Särav, S. (2015). Legal impediments in the EU to new technologies in the example of e-residency. *Baltic Journal of Law & Politics*, 8(2), 71-90. <https://doi.org/10.1515/bjlp-2015-0019>
- Koops, B.J. & Leenes, R. (2006). Identity Theft, Identity Fraud and/or Identity-related Crime. *Datenschutz und Datensicherheit (DuD)*, 30 (9), 553-556. <https://doi.org/10.1007/s11623-006-0141-2>
- Laatikainen, G., Agrawal, R., Wang.X., & Abrahamsson, P. (2022). The state of self-sovereign identity in spring 2021: Results of a survey. *JYU Reports*, 1(16). <https://doi.org/10.17011/jyureports/2022/8>
- Lamer, W. (2017). From sleepwalking into surveillance societies to drifting into permanent securitisation: Mass surveillance, security and human rights in Europe. *Global Campus Human Rights Journal*, 1 (2),393-413. <http://dx.doi.org/10.25330/1465>
- Leanerts, K. (2012). Defining the concept of Services of General Interest in light of the checks and balances set out in the EU Treaties. *Jurisprudencija: Mokslo darbu žurnalas*, 19 (4),1247-1267. <https://philpapers.org/rec/LENDTC>

- Leibbrandt, G. & Goldscheider, D. (2022). Building a global digital identity infrastructure. *Journal of Payments Strategy & Systems*, 16(1), 68-74.  
<https://rb.gy/626p7>
- Lyon, D. (2014). Surveillance, Snowden and Big Data: Capacities, Consequences, Critique. *Big Data & Society*, 1(2).  
<https://journals.sagepub.com/doi/epub/10.1177/2053951714541861>
- Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, 11, 824-842.  
<https://ijoc.org/index.php/ijoc/article/view/5527/1933>
- Mahnkopf, B. (2008). Privatisation of public services in the EU: an attack on social cohesion and democracy. *Work Organisation, Labour & Globalisation*, 2(2), 72-84. <https://rb.gy/ail38>
- Martín Delgado, I. (2009). La administración electrónica como problema actual para la investigación y la docencia en el derecho administrativo. *Revista Aragonesa de Administración Pública*, (11), 355-375.
- Martínez Martínez, R. (2005). El derecho fundamental a la protección de datos: perspectivas. *IDP: revista de Internet, Derecho y Política*, (5), 47-61.  
<https://dialnet.unirioja.es/servlet/articulo?codigo=2372613>
- Martínez Martínez, R. (2020). Tecnología de verificación de identidad y control en exámenes online. *Revista De Educación Y Derecho*, (22).  
<https://doi.org/10.1344/REYD2020.22.32357>
- Maziarz, A. (2016). Services of General Economic Interest: Towards Common Values? *European State Aid Law Quarterly*, 15(1), 16-30.  
<https://www.jstor.org/stable/26689558>
- Mazzucato, M. (2016). From market fixing to market-creating: a new framework for innovation policy. *Industry and Innovation*, 23 (2), 140-156.  
[10.1080/13662716.2016.1146124](https://doi.org/10.1080/13662716.2016.1146124)
- Michalkiewicz-Kadziela, E. & Milczarek, E. (2022). Legal boundaries of digital identity creation. *Internet Policy Review*, 11(1).  
<https://doi.org/10.14763/2022.1.1614>

- Murray, D. & Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*, 52 (1), 31-60. <https://doi.org/10.1017/S0021223718000304>
- Neil M., R. (2013). The Dangers of Surveillance. *Harvard Law Review*, 126 (7), 1937-1965. <https://rebrand.ly/harvardlawreview>
- Ngaire, N. (2003). Who are Law's Persons? From Cheshire Cats to Responsible Subjects. *ModernLawReview*, 66 (3). <https://doi.org/10.1111/1468-2230.6603002>
- Noack, T. & Kubicek, H. (2010). The introduction of online authentication as part of the new electronic national identity card in Germany. *Identity in the Information Society (IDIS)*, 3, 87-110. <https://doi.org/10.1007/s12394-010-0051-1>
- Nuñez, D. & Agudo, I. (2014). Blind IdM: A privacy-preserving approach for identity management as a service. *International Journal of Information Security*, 13, 200-201. <https://doi.org/10.1007/s10207-014-0230-4>
- Plana Arnaldos, M.C. (2021). Economía de los datos y propiedad sobre los datos. *Revista de educación y derecho*, (24). <https://dialnet.unirioja.es/servlet/articulo?codigo=8103852>
- Piernas López, J.J. (2017). La definición de servicio de interés económico general en la Unión Europea... ¿de qué margen disponen los Estados Miembros? *Revista Española de Derecho Europeo*, (61), 101-128. [https://www.revistasmarcialpons.es/revistaespanoladerechoeuropeo/article/download/128\\_definicion\\_servicio\\_interes\\_economico\\_general\\_ue/145/432](https://www.revistasmarcialpons.es/revistaespanoladerechoeuropeo/article/download/128_definicion_servicio_interes_economico_general_ue/145/432)
- Piernas López, J.J. (2022). La Unión Europea como actor internacional en material de ciberseguridad. *Cuadernos de derecho trasnacional*, 14(2), 712-736. <https://doi.org/10.20318/cdt.2022.7202>
- Sáenz, J. E. (2020). Enfoque jurídico penal de los delitos transnacionales según la legislación penal panameña. *Revista Metropolitana de Ciencias Aplicadas*, 3(3), 141-148. <https://remca.umet.edu.ec/index.php/REMCA/article/view/320>
- Sagar, S. & Hoffmann, T. (2021). Intermediary Liability in the EU Digital Common Market – from the E-Commerce Directive to the Digital Services Act. *IDP: revista de Internet, derecho y política*, (34), 1-12. <https://dialnet.unirioja.es/descarga/articulo/8398827.pdf> .

- Sauter, W. (2008). Services of General Economic Interest and Universal Service in EU Law. *European Law Review*, (2), <https://ssrn.com/abstract=1136105>
- Sedlmeir, J., Smethurst, R., Rieger, A. & Fridgen G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, 63, 603-613. <https://doi.org/10.1007/s12599-021-00722-y>
- Seeman, E.D., O'Hara, M.T., Holloway, J., & Forst. A. (2007). The impact of government intervention on technology adoption and diffusion: the example of wireless location technology. *Electronic government: EG; an international journal*, 4(1), 1-19. [10.1504/EG.2007.012176](https://doi.org/10.1504/EG.2007.012176)
- Six P., Raab C., & Bellamy C. (2005). Joined-up government and privacy in the UK part I: managing tensions between data protection and social policy. *Part I. Public Administration*, 83(1), 111-133. <http://doi.org/10.1111/j.0033-3298.2005.00440.x>
- Srnicek, N. (2017). The challenges of platform capitalism: Understanding the logic of a new business model. *Juncture*, 23 (4), 254-257. <https://doi.org/10.1111/newe.12023>
- Stockburger, L., Kokosioulis, G., Mukkamala, A., Rao Mukkamala, R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, 2(2). <https://doi.org/10.1016/j.bcra.2021.100014>
- Sullivan, C. (2009). Is Identity Theft Really Theft? *International Review of Law, Computers Technology*, 23 (1-2), 77-87. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2379249](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379249)
- Sullivan, C. (2009a). Digital identity - The legal person? *Computer Law and Security Review*, 25(3), 227-236. <https://doi.org/10.1016/j.clsr.2009.03.009>
- Sullivan, C. (2016). Digital citizenship and the right to digital identity under international law. *Computer Law and Security Review*, 32(3), 474-481. <https://doi.org/10.1016/j.clsr.2016.02.001>
- Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. *Computer Law and Security Review*, 34(4), 723-731. <https://doi.org/10.1016/j.clsr.2018.05.015>

- Valero Torrijos, J. (2019). Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista Catalana de Dret Públic*, (58), 82-96.  
<http://dx.doi.org/10.2436/rcdp.i58.2019.3307>
- Wang, F. & de Filippi, P. (2020). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, 2. <https://doi.org/10.3389/fbloc.2019.00028>
- Wheeler, C. (2013). The Public Interest Revisited - We know it's important but do we know what it means? *Australian Institute of Administrative Law Forum*,(48).  
<https://www5.austlii.edu.au/au/journals/AIAdminLawF/2006/2.pdf>
- Willer, R. (2009). A status theory of collective action. *Altruism and Prosocial Behavior in Groups (Advances in Group Processes)*, 26, 133-163.  
[https://doi.org/10.1108/S0882-6145\(2009\)0000026009](https://doi.org/10.1108/S0882-6145(2009)0000026009)
- Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: empirical results. *Security & Privacy Magazine IEEE*, 2 (5), 25-31.  
[10.1109/MSP.2004.81](https://doi.org/10.1109/MSP.2004.81)
- Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, 24(5), 1816-1836. <https://doi.org/10.1016/j.chb.2008.02.012>

### **Working Papers**

- Cole, M. D. & Schmitz, S. (2019). *The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape* (University of Luxembourg Law Working Paper 2019-017), SSRN. <http://dx.doi.org/10.2139/ssrn.3512093>
- Coveri, A., Cozza, C., & Guarascio, D. (2021). *Monopoly Capitalism in the Digital Era* (Working Papers in Public Economics, 209. University of Rome La Sapienza, Department of Economics and Law), IDEAS.  
<https://ideas.repec.org/p/sap/wpaper/wp209.html>
- Lange-Hausstein, C. & Kremer, T. (2023). *Why the acceptance of the EU Digital Identity Wallet for SCA will be mandatory under eIDAS2*. (Digitallabor Discussion Paper). <https://rb.gy/yvgc3t>

## Conference Proceedings

- Ali, M. A. & Mann, S. (2013). The inevitability of the transition from a surveillance-society to a veillance-society: Moral and economic grounding for surveillance. *International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmented Reality in Everyday Life*, 243-254. <https://doi.org/10.1109/ISTAS.2013.6613126>
- Amard, A., Hartwich, E., Hoess, A., Rieger, A., Roth, T., & Fridgen, G. (2024). Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Decisions. *Proceedings of the 57th Hawaii International Conference on System Sciences*, 2151-2161. <https://hdl.handle.net/10125/106646>
- Bharosa, N., Lips, S., & Draheim, D. (2020). Making e-Government Work: Learning from the Netherlands and Estonia. In Hofmann, S., Csáki, C., Edelman, N., Lampoltshammer, T., Melin, U., Parycek, P., Schawabe, G. Tambouris, E. (Eds.) S, *Electronic Participation* (pp. 41-53). Springer. [https://doi.org/10.1007/978-3-030-58141-1\\_4](https://doi.org/10.1007/978-3-030-58141-1_4)
- Bhonsle, M. V., Poolsappasit N., & Madria S. K. (2013). ETIS -- Efficient Trust and Identity Management System for Federated Service Providers. *2013 IEEE 27th International Conference on Advanced Information Networking and Applications*, 219-226. [10.1109/AINA.2013.13](https://doi.org/10.1109/AINA.2013.13)
- Braun, W. & Arendt, D. (2011). AusweisApp and the eID Service/Server – Online Identification Finally more Secure. In Pohlmann, N., Reimer, H., & Schneider, W. (Eds) *ISSE 2010 Securing Electronic Business Processes* (pp.374-384). Springer. [https://doi.org/10.1007/978-3-8348-9788-6\\_36](https://doi.org/10.1007/978-3-8348-9788-6_36)
- Clarke, R. (2009). A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation. IDIS 2009-The *2nd Multidisciplinary Workshop on Identity in the Information Society*. Roger Clarke's website. <http://www.rogerclarke.com/ID/IdModel-090605.html>
- Engelbertz, N., Erinola, N., Herring, D., Somorovsky, J., & Mladenov, V. (2018). Security analysis of eIDAS—the cross-country authentication scheme in Europe. *12th USENIX Workshop on Offensive Technologies WOOT 18*. USENIX Association. <https://www.usenix.org/conference/woot18/presentation/engelbertz>

- Fett, D., Kusters, R., & Schmitz, G. (2017). The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines. *Proceedings - IEEE Computer Security Foundations Symposium*, 189-202. <https://doi.org/10.1109/CSF.2017.20>
- Gentili, M. (2001). Italian Electronic Identity Card - principle and architecture. *Very Large Data Bases Conference*. [http://www.dia.uniroma3.it/~vldbproc/072\\_629.pdf](http://www.dia.uniroma3.it/~vldbproc/072_629.pdf)
- Gomes de Andrade, N. (2011). Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. In Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., & Zhang, G. (Eds.) *Privacy and Identity Management for Life* (pp.90–107). Springer. [https://doi.org/10.1007/978-3-642-20769-3\\_8](https://doi.org/10.1007/978-3-642-20769-3_8)
- Jensen, J. (2012). Federated Identity Management Challenges. *2012 Seventh International Conference on Availability, Reliability and Security*, 230-235. [10.1109/ARES.2012.68](https://doi.org/10.1109/ARES.2012.68)
- Mainka, C., Mladenov, V., Schwenk, J., & Wich, T. (2017). SoK: Single Sign-On Security - An Evaluation of OpenID Connect, *Proceedings - 2nd IEEE European Symposium on Security and Privacy*, 251-266. <https://doi.org/10.1109/EuroSP.2017.32>
- Moreno, R. T., Bernabe, J. B., Skarmeta, A., Stausholm, M., Frederiksen, T.K., Martínez, N., Ponte, N., Sakkopoulos, E., & Lehmann, A. (2019). Towards oblivious identity management for private and user-friendly services. *Global IoT Summit, GIOTS 2019 – Proceedings*, 1-6. <https://doi.org/10.1109/GIOTS.2019.8766357>
- Nielsen, M.M. (2017). E-Governance and online service delivery in Estonia. *Proceedings of the 18th Annual International Conference on Digital Government Research*, 300-309. <https://doi.org/10.1145/3085228.3085284>
- Pattakou, A., Mavroeidi, A., Kalloniatis, C., Diamantopoulou, V., & Gritzalis, S. (2018). Towards the design of usable privacy by design methodologies. *Proceedings - 2018 5th International Workshop on Evolving Security and Privacy Requirements Engineering*, 1-8 . <https://doi.org/10.1109/ESPRE.2018.00007>
- Reible, V. & Braunmandl, A. (2011). The eID Function of the nPA within the European STORK Infrastructure. In Pohlmann, N., Reimer, H., Schneider, W. (Eds) *ISSE 2010 Securing Electronic Business Processes* (pp. 392-398) Springer Link. [https://doi.org/10.1007/978-3-8348-9788-6\\_38](https://doi.org/10.1007/978-3-8348-9788-6_38)

- Rocha, J. (2021). Spanish and Portuguese eIDAS node evolution for electronic identification of European citizens. *Proceedings of the 10th Euro-American Conference on Telematics and Information Systems*, artículo 60, 1-5. <https://doi.org/10.1145/3401895.3402094>
- Scholl, H.J. (2005). Interoperability in E-government: more than just smart middleware. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 123-123. <https://doi.org/10.1109/HICSS.2005.336>
- Tian, M. & Xin Yi, Z. (2021). Platform Monopoly and Regulatory Measures. In Wang, J., Achour, B., & Huang, C.Y. (Eds). *Proceedings of the 7th International Conference on Humanities and Social Science Research* (pp.776-779). Atlantis Press. <https://doi.org/10.2991/assehr.k.210519.155>
- Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems. *ARES' 21: Proceedings of the 16th International Conference on Availability, Reliability and Security*, artículo 132, 1-9. <https://doi.org/10.1145/3465481.3469207>
- Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). Which authentication method to choose. A legal perspective on user-device authentication in IoT ecosystems. *ARES' 21: Proceedings of the 16th International Conference on Availability, Reliability and Security*, artículo 83, 1-6. <https://doi.org/10.1145/3465481.3470068>
- Valero Torrijos, J. & Sánchez Martínez, D. (2006). Protección de datos personales, DNI-e y prestación de Servicios de certificación: ¿un obstáculo para la e-Administración? *IX Jornadas sobre Tecnologías de la Información para la Modernización de las Administraciones Públicas*, comunicación 122. [https://administracionelectronica.gob.es/pae/Home/pae/Biblioteca/pae/Tecnimap/pae/TECNIMAP\\_2006\\_-\\_SEVILLA.html](https://administracionelectronica.gob.es/pae/Home/pae/Biblioteca/pae/Tecnimap/pae/TECNIMAP_2006_-_SEVILLA.html)
- Wollmann, H. (2012). Public Services Provision in European Countries from Public/Municipal to Private Sector – and back to municipal? *Symposium on Neither Public nor Private: Mixed Forms of Service Delivery around the Globe*. <http://www.ub.edu/graap/Final%20Papers%20PDF/Wollmann%20Hellmut.pdf>



**Books**

- Alamillo Domingo, I. (2010). Identidad electrónica, robo de identidad y protección de datos personales en la red. In *Robo de Identidad y Protección de Datos en la red* (pp.17-34) Thomson Reuters Aranzadi (Ed.).
- Alamillo Domingo, I. (2020). El régimen jurídico de la Administración digital: aspectos tecnológicos, plataformas y servicios de intermediación. In Martín Delgado, I. (Dir.), *El procedimiento administrativo y el régimen jurídico de la Administración Pública desde la perspectiva de la innovación tecnológica* (pp.225-276). Isutel.
- Almeida Cerrada, M. (2017). Una breve aproximación al proceso de construcción de un Derecho Administrativo Europeo Común. In Martín Delgado, I., Almeida Cerrada, M. & di Lascio, F. (Coord.) *La europeización del Derecho Administrativo. Una evaluación desde el ordenamiento español* (pp.21–31). Andavira.
- Alonso García, R. (1989). *Derecho Comunitario, Derechos nacionales y Derecho común europeo*. Civitas.
- Arroyo Amayuelas, E. (2022). Las Nuevas Directivas sobre Digitalización del Derecho de Contratos. In Arnau Raventos, L. (Dir.), *La digitalización del derecho de contratos en Europa* (pp. 19-46). Atelier.
- Barrio Andrés, M. (2017). *Derecho Público en Internet: la actividad administrativa de regulación de la Red*. Instituto Nacional de Administración Pública.
- Barrio Andrés, M. (2020). *Fundamentos del Derecho de Internet* (2ª ed.). Centro de Estudios Políticos y Constitucionales.
- Bozeman, B. (2007). The Privatization of Public Value. In *Public Values and Public Interest: Counterbalancing Economic Individualism* (pp.1-21). Georgetown University Press. <http://www.jstor.org/stable/j.ctt2tt37c>
- Brener, A. (2019). Payment Service Directive II and Its Implications. In Lynn, T., Mooney, J., Rosati, P. & Cummins, M. (Eds.), *Disrupting Finance* (pp.103-119). Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Pivot, Cham. [https://doi.org/10.1007/978-3-030-02330-0\\_7](https://doi.org/10.1007/978-3-030-02330-0_7)

- Canals Ametller, D. (2021). El ejercicio de potestades administrativas por operadores privados en régimen de mercado. In Gamero Casado, E. (Dir.), *La Potestad Administrativa Concepto y alcance práctico de un criterio clave para la aplicación del Derecho administrativo* (pp.320–385). Thomson Reuters Aranzadi.
- Canals Ametller, D. (Dir.). (2021a). La seguridad en el entorno digital. In *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales* (pp.61-88). Wolters Kluwer.
- Cox, J. (2021). *APA 7TH EDITION. Formatting Guide*. Churchgate Publishing House.
- Darnaculleta I Gardella, M.M. (2020). La producción de normas en un mundo global. In Arroyo Jiménez, L., Martín Delgado, I., & Meix Cereceda, P. (Dirs.), *Derecho Público Global. Fundamentos Actores y Procesos* (pp.245-273). Isutel
- Davies, J. & Szyszczak, E. (2011). Universal Service Obligations: Fulfilling New Generations of Services of General Economic Interest. In Szyszczak, E., Davies, J., Andenæs, M., & Bekkedal, T. (Eds.), *Developments in Services of General Interest. Legal Issues of Services of General Interest* (pp.155-177). T.M.C. Asser Press.
- De Hert, P. & Gutwirth, S. (2003). Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence. In Clements, B., Maghiros, I., Beslay, L., Centeno, C., Punie, Y., Rodríguez, C., & Masera, M. (Eds.), *Security and Privacy for the Citizen in the Post 11 D* (pp. 111-162) IPTS-Technical Report Series, EUR 20823 EN. <ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf>
- Esteve Pardo, J. (2023). *Principios de Derecho regulatorio: Servicios económicos de interés general y regulación de riesgos* (2ª ed.). Marcial Pons.
- Gamero Casado, E. (2015). *Desafíos del Derecho Administrativo ante un mundo en disrupción*. Comares.
- Gamero Casado, E. (Dir.). (2021). Potestad Administrativa: The Concept of Administrative Public Power in Spanish Law. In *Administrative Public Power: Comparative Analysis in European Legal Systems* (pp.25-94). Thomson Reuters Aranzadi.
- Gallo, D. (2022). *Public Services and EU Competition Law; The Social Market Economy in Action* (pp.9-30). Routledge.

- González Gil, D. (2021). El interés general, presupuesto de atribución y ejercicio de la potestad administrativa. In Gamero Casado, E. (Dir.), *La Potestad Administrativa Concepto y alcance práctico de un criterio clave para la aplicación del Derecho administrativo* (pp.153-229). Thomson Reuters Aranzadi.
- Gutwirth, S. & De Hert, P. (2006). Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In Claes, E., Duff, A., & Gutwirth, S. (Eds.) *Privacy and the Criminal Law*, (pp. 61–104). Intersentia, Antwerp.
- Harcourt, B. (2015). *Exposed: Desire and disobedience in the digital age*. Harvard University Press.
- Koltay, A. (2019). *New media and freedom of expression. Rethinking the constitutional foundations of the public sphere*. Hart Publishing.
- Laguna de Paz, J.C. (2009). *Servicios de Interés Económico General* (pp.33-49). Thomson Reuters Aranzadi.
- Laguna de Paz, J.C. (2022). *Tratado de Derecho Administrativo General y económico*. Thomson Reuters Aranzadi.
- Hansen, M., Obersteller, H., Rannenberg, K., & Veseli, F. (2015). Establishment and Prospects of Privacy-ABCs. In Rannenberg, K., Camenisch, J. & Sabouri A. (Eds.), *Attribute-based Credentials for Trust* (pp.345-360). Springer.  
[https://doi.org/10.1007/978-3-319-14439-9\\_11](https://doi.org/10.1007/978-3-319-14439-9_11)
- Khatchatourov, A., Laurent, M., & Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption. In Tambouris, Janssen, M., Jochen Scholl, H., Wimmer, Maria A., Tarabanis, K., Gascó, M., Klievink, B., Lindgren, I., & Parycek, P. (Eds.), *Electronic Government* (pp.273-290). Springer.  
[https://doi.org/10.1007/978-3-319-22479-4\\_21](https://doi.org/10.1007/978-3-319-22479-4_21)
- Kirkpatrick, C., Minogue, M., & Parker, D. (2004). Competition, regulation and regulatory governance: An overview. In Cook P., Colin Kirkpatrick, C., Martin Minogue M., & Parker, D. (Eds.), *Leading Issues in Competition, Regulation and Development* (pp.3-35). Edward Elgar Publishing.

- Martín Delgado, I. (2010). Identificación y autenticación de los ciudadanos. In Gamero Casado, E. & Valero Torrijos, J., *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* (pp. 463–536). Thomson Reuters Aranzadi.
- Martín Delgado, I. (2012). Identificación electrónica de los ciudadanos y profesionales en el ámbito de la justicia. In Gamero Casado, E. & Valero Torrijos, J., *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio* (pp.503-560). Thomson Reuters Aranzadi.
- Martín Delgado, I. (2017). La europeización del Derecho Administrativo Español: un comentario al estudio de Andrés Boix Palop. In Martín Delgado, I., Almeida Cerredá, M., & di Lascio, F., *La europeización del Derecho Administrativo. Una evaluación desde el ordenamiento español* (pp.109–136). Andavira.
- Martínez López -Muñiz, J.L. (2017). El contexto y los principios inspiradores de las Leyes 39 y 40/2015. In Velasco Ruiz, C.I. (Dir.) *Reflexiones sobre la reforma administrativa de 2015. Análisis crítico de las leyes de procedimiento administrativo común y de régimen jurídico del sector público* (pp.9-30), Marcial Pons.
- Mir Puigpelat, O. (2017). Veinte años no es nada: la oportunidad perdida con la nueva Ley 39/2015 del procedimiento administrativo común. In Tornos, J. (Coord.), *Estudios sobre las leyes 39/2015 del procedimiento administrativo común de las administraciones públicas y 40/2015 del régimen jurídico del sector público* (pp.49-60). Atelier Libros Jurídicos.
- Särav, S. & Kerikmäe, T. (2017). E-residency: a Cyberdream Embodied in a Digital Identity Card? In T. Kerikmäe, T. & Rull, A. (Eds.), *The Future of Law and eTechnologies* (pp.57-79). Springer. [https://doi.org/10.1007/978-3-319-26896-5\\_4](https://doi.org/10.1007/978-3-319-26896-5_4)
- Piernas López, J.J. (2020). *Ciberdiplomacia y ciberdefensa en la Unión Europea*. Thomson Reuters Aranzadi.
- Preukschat, A. & Reed, D. (Eds.) (2021). Why the Internet is missing an identity layer— and why SSI can finally provide one. In *Self-Sovereign Identity, Decentralized digital identity and verifiable credentials* (pp.1-19). Manning Publications Co.

- Pfutzmann, B. & Waidner, M. (2005). Federated Identity-Management Protocols. In B. Christianson, B. Crispo, J.A. Malcolm, & M. Roe (Eds.), *Security Protocols 2003* (pp. 153-174). Springer. [https://doi.org/10.1007/11542322\\_20](https://doi.org/10.1007/11542322_20)
- Salvador, I. (2010). Identidad electrónica, robo de identidad y protección de datos personales en la red. In *Robo de Identidad y Protección de Datos en la red* (pp.221-238). Thomson Reuters (Ed.).
- Sánchez García, A. (2022). *La transformación electrónica de la contratación pública. De la digitalización a la automatización*. Tecnos.
- Stanley, J., & Steinhardt, B. (2014). Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society. In Sandler, R.L. (Ed.), *Ethics and Emerging Technologies*. Palgrave Macmillan. [https://doi.org/10.1057/9781137349088\\_18](https://doi.org/10.1057/9781137349088_18)
- Valero Torrijos, J. (2022). Los derechos en la era digital. In Rodríguez Ayudo, J.F. (Ed.) *Nuevos retos en materia de derechos digitales en un context de pandemia: perspectiva multidisciplinar* (pp.25-45). Thomson Reuters Aranzadi.
- Van der Sloot, B. (2016). Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities. In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Data Protection on the Move. Law, Governance and Technology Series* (pp.411-436). Springer. [https://doi.org/10.1007/978-94-017-7376-8\\_15](https://doi.org/10.1007/978-94-017-7376-8_15)
- Rivero Ysern, E. & Rodríguez-Arana Muñoz, J. (2014). *Con miras al interés general*. Derecho Público Global-INAP-Bubok Publishing
- Wood, A.F. & Smith, M.J. (Eds.) (2005). *Online Communication* (2<sup>nd</sup> ed., pp.51-75). Lawrence Erlbaum Associates.
- Wollmann, H., & Marcou, G. (Eds.) (2010). Introduction. In *The Provision of Public Services in Europe: Between State, Local Government and Market* (pp.1-14). Edward Elgar Publishing

### **Governmental Reports/Documents/Sites**

- Agencia Española de Protección de Datos. (2014). *Dictamen 05/2014 sobre técnicas de anonimización*. <https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf>

- Agencia Española de Protección de Datos. (2018). *Guía práctica para las evaluaciones de Impacto en la protección de los datos sujetas al RGPD*. <https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>
- Agencia Española de Protección de Datos. (2019). *Guía para la privacidad desde el diseño*. <https://www.aepd.es/documento/guia-privacidad-desde-diseno.pdf>
- Agencia Española de Protección de Datos. (2023). *Informe 0048/2023*. <https://www.aepd.es/documento/2023-0048.pdf>
- Agencia Española Protección Datos. (2023). *Orientaciones para la Evaluación de Impacto en el Desarrollo Normativo* (versión septiembre 2023). <https://www.aepd.es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>
- Alamillo Domingo, I. (2020). SSI eIDAS Legal Report. *How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*. European Commission. [https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI\\_eIDAS\\_legal\\_report\\_final\\_0.pdf](https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf)
- Article 29 Working Party. (2014). *Opinion 05/2014 on Anonymization Techniques*. [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)
- Article 29 Working Party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*. [https://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](https://ec.europa.eu/newsroom/document.cfm?doc_id=44137)
- Ceccanti, C., di Legge, A., Eichholtzer, M., Kuhl, A., McNally, P., Ongono Pomme, A., Van der Peljl, S., & Walsh, C. (2021). *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation): final report*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/evaluation-study-regulation-no9102014-eidas-regulation>
- Centro Criptológico Nacional. (2017). *PILAR-Manual de Usuario* (v 6.2). Ministerio de la Presidencia y de las Administraciones Territoriales. <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/2133-ccn-stic-470-h1-manual-de-la-herramienta-de-analisis-de-riesgos-pilar-6-2/file.html>

- Data Protection Commission. (2019). *Guidance on Anonymisation and Pseudonymisation*. <https://www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf>
- Department for the Economy. (n.d.). *Services of General Economic Interest*. Department of Economy. Retrieved August 21, 2023 from <https://www.economy-ni.gov.uk/articles/services-general-economic-interest>
- De Streel, A. & Husovec, M. (2020). *The e-commerce Directive as the cornerstone of the Internal Market*. IMCO Committee Study. European Parliament. [https://www.europarl.europa.eu/thinktank/en/document/IPOL\\_STU\(2020\)648797](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)648797)
- European Banking Authority. (2019). *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* (EBA-Op-2019-06). European Banking Authority. <https://rb.gy/bnj4vf>
- European Commission. (2018, December 10). EU Negotiators Agree on Strengthening Europe's Cybersecurity, Press Release. *European Commission, Press corner*. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_18\\_6759](https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6759)
- European Commission, Directorate-General for Communications Networks, Content and Technology. (2018). *Study on eID and digital on-boarding : mapping and analysis of existing on-boarding bank practices across the EU : final report*. Publications Office of the European Union. <https://data.europa.eu/doi/10.2759/94773>
- European Commission. (2020, April 21). Belgium's mobile eID scheme is all you need to access online services – thanks to European standards and solutions. *European Commission Digital Building*. <https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=533365191>
- European Commission. (2022). *Payment services – review of EU rules*. [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_en)
- European Commission. (2022). Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation. *Digital Europe Programme*. <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-deploy-02-electronic-id>

- European Commission, Directorate-General for Communications Networks, Content and Technology. (CONNECT) (2022). Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Digital Identity Wallet. *TED: Tenders Electronic Daily*.  
<https://ted.europa.eu/udl?uri=TED:NOTICE:309685-2022:TEXT:EN:HTML&src=0>
- European Commission. (2023). *Services of General Interest*. European Commission.  
[https://commission.europa.eu/topics/single-market/services-general-interest\\_en](https://commission.europa.eu/topics/single-market/services-general-interest_en)
- European Commission. (2023, May 23). *EU Digital Identity:4 projects launched to test the EUDI Wallet*. Retrieved from: <https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet>
- European Commission. (n.d.). *What is EBSI?* European Commission. Retrieved 2023, October 21 from <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi>
- European Credit Sector Associations. (2023). *European Credit Sector Associations call for removing payments from the scope of the Digital Identity Regulation*.  
[https://www.wsbi-esbg.org/wp-content/uploads/2023/04/ECSAs-Public-Statement\\_final-1.pdf](https://www.wsbi-esbg.org/wp-content/uploads/2023/04/ECSAs-Public-Statement_final-1.pdf)
- European Data Protection Supervisor. (2019). *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725*.  
[https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint\\_en](https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint_en)
- European Trade Union Confederation. (2007). *Public Services & Services of General Economic Interest (SGEIs)*. Syndicat European Trade Union.  
<https://www.etuc.org/en/public-services-services-general-economic-interest-sgeis>
- European Union Agency for Fundamental Rights. (2015). *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume I: Member States' legal frameworks*. Publications Office of the European Union.  
<https://doi.org/10.2811/55040>
- European Union Agency for Fundamental Rights. (2022). *Bias in algorithms: artificial intelligence and discrimination*. Publications Office of the European Union. <https://data.europa.eu/doi/10.2811/25847>



- Federal Office for Information Security. (2017). *German eID based on Extended Access Control v2, Overview of the German eID system*. [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German\\_eID\\_Whitepaper.pdf?\\_\\_blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf?__blob=publicationFile&v=1)
- Garbasso, G., Bianchini, D., Tortis, M., Gori, M., Van Eecke, P., De Roucke, F., Genchini, R., Manaila, V., Sel, M., & Tancioni, M. (2021). *Study to support the impact assessment for the revision of the eIDAS regulation : final report*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/study-support-impact-assessment-revision-eidas-regulation>
- Gobierno de España. (2021). *Carta de Derechos Digitales*. Ministerio de Asuntos Económicos y Transformación Digital. <https://derechodigital.pre.red.es/>
- Pedroli, M., O'Neil G., Fravolini A., & Marcon L. (2021). *Overview of Member States' eID Strategies*. European Commission. <https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/National+Strategies>
- Ritcher, M. (2020). *Nine-point plan for a digital Germany: Priorities of the Federal Government Commissioner for Information Technology*. Federal Government Commissioner for Information Technology. [https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/EN/9-point-plan.pdf;jsessionid=E864D46013BA35F102A870924716AF92.1\\_cid287?\\_\\_blob=publicationFile&v=1](https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/EN/9-point-plan.pdf;jsessionid=E864D46013BA35F102A870924716AF92.1_cid287?__blob=publicationFile&v=1)
- Tennessee Department of Safety & Homeland Security. (n.d.). *What Is REAL ID?* Department of Safety & Homeland Security. Retrieved October 4, 2023 from <https://www.tn.gov/tnrealid/what-is-real-id.html>
- United States Senate Committee Commerce, Science, and Transportation. (2013). *Office of Oversight and Investigations, Majority Staff, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*. Office of Oversight and Investigations Majority Staff. <https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577>
- Vandystadt, N. & Waldstein, J. (2018). *EU negotiators agree on strengthening Europe's cybersecurity*. European Commission. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_18\\_6759](https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6759)

### **International Organizations/ Research Institutions/ Corporate Reports**

Becker, P. (2007). *Privatizing Public Enterprises in the European Union- The Impact of European Integration on European Water Markets*. Research Unit EU Integration. <https://rebrand.ly/qd4ned2>

Christl, W. (2017). *Corporate Surveillance in Everyday life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Cracked Labs. <https://crackedlabs.org/en/corporate-surveillance>

Clark, J., Dahan, M., Desai, V., Lenco, M., de Labriolle, S., Pellestor, J.P., Reid, K., & Varuhaki, Y. (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper*. The World Bank Group, GSM and Security Identity Alliance. <https://secureidentityalliance.org/publications-docman/public/4-july-2016-report-digital-identity/file>

Deloitte. (2021). *Digitalization of public services*. Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/FoDT-Digitalization-public-services.pdf>

Echikson, W. (2020). *Europe's digital identification opportunity*. Centre for European Policy Studies. [https://www.ceps.eu/wp-content/uploads/2020/06/TFR\\_Europe-Digital-Identification-Opportunity.pdf](https://www.ceps.eu/wp-content/uploads/2020/06/TFR_Europe-Digital-Identification-Opportunity.pdf)

EPN Services Group. (2007). *Services of General Interest: Glossary and Terms Explained*. EAPN Services Group. <https://www.eapn.eu/images/stories/docs/services-glossary-en.pdf>

Feld, H. (2019). *The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms*, Roosevelt Institute. <https://rooseveltinstitute.org/publications/the-case-for-the-digital-platform-act-market-structure-and-regulation-of-digital-platforms/>

Financial Action Task Force. (2020). *Appendix A. In Guidance on Digital Identity*. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Appendice%20A.pdf>

Harbitz, M. & Tamargo, M.C. (2009). *The Significance of Legal Identity in Situations of Poverty and Social Exclusion*. Inter-American Development Bank. <https://crvssystems.ca/significance-legal-identity-situations-poverty-and-social-exclusion>

International Civil Aviation Organization. (2018). *ICAO TRIP Guide on Evidence of Identity*. <https://rb.gy/rtrii>

International Telecommunication Union. (2018). *Digital Identity Roadmap Guide*. International Telecommunication Union. <https://handle.itu.int/11.1002/pub/81215cb9-en>

Jorna P., Smith R., & Norman K. (2020). *Identity crime and misuse in Australia: Results of the 2018 online survey*. Australian Institute of Criminology. <https://doi.org/10.52922/sr04169>

Langaker, E.M; Wunderlich, F., Thaulow, H.G., & Kasch, K.C. (2021). *Federated e-IDs as a value driver in the banking sector based on experience from Nordics markets*. Arkwright. <https://resources.signicat.com/federated-eids-arkwright>

Smith, M. (2020). *Enforcement and cooperation between Member States*. IMCO Committee Study, European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648780/IPOL\\_STU\(2020\)648780\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648780/IPOL_STU(2020)648780_EN.pdf)

Timmers, P. (2022). *Digital-Industrial-Policy-for-Europe*. Centre on Regulation in Europe. <https://cerre.eu/wp-content/uploads/2022/12/Digital-Industrial-Policy-for-Europe.pdf>

World Bank Group. (2019). *ID4D Practitioner's Guide: Version 1.0*. World Bank Group. <https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

World Economic Forum. (2018). *Identity in a Digital World: A new chapter in the social contract*. Insight Report. [https://www3.weforum.org/docs/WEF\\_INSIGHT\\_REPORT\\_Digital%20Identity.pdf](https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf)

## Technical Standards/Documentation

- Grassi, P.A., García, M.E, & Fenton, J.L. (2017). *NIST SPECIAL PUBLICATION 800-63-3, Digital Identity Guidelines*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63-3>
- European Commission. (The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework) (2022). *The European Digital Identity Wallet Architecture and Reference Framework* (Outline February 2022). [https://digital-strategy.ec.europa.eu/es/library/european-digital-identity-architecture-and-reference-framework-outline#:~:text=Framework%20%E2%80%93%20Outline%20\(.pdf\)-.Descargar%C2%A0,-Temas%20relacionados](https://digital-strategy.ec.europa.eu/es/library/european-digital-identity-architecture-and-reference-framework-outline#:~:text=Framework%20%E2%80%93%20Outline%20(.pdf)-.Descargar%C2%A0,-Temas%20relacionados)
- European Commission (The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework). (2023). *The European Digital Identity Wallet Architecture and Reference Framework* (V. 1.0.0. January 2023). <https://ec.europa.eu/newsroom/dae/redirection/document/93678>
- European Commission (The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework). (2024). *The European Digital Identity Wallet Architecture and Reference Framework* (V. 1.2.0. November 2023). <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/>
- European Commission (The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework). (2024). *The European Digital Identity Wallet Architecture and Reference Framework* (V. 1.3.0. March 2024). <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases>
- International Organization for Standardization. (2019). *Information technology -- Security techniques -- A framework for identity management (ISO/IEC 24760-1:2017)*. <https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en>
- International Standardisation Organization. (2021). *Personal identification–ISO-compliant driving license–Part 5: Mobile driving License (mDL) application*. (ISO/IEC 18013-5:2021). <https://www.iso.org/standard/69084.html>
- World Wide Web Consortium. (2019). *Verifiable Credentials Data Model 1.0* (Recommendation). <https://www.w3.org/TR/vc-data-model/>

World Wide Web Consortium. (2022). *Decentralized Identifiers (DIDs) v1.0* (Recommendation). <https://www.w3.org/TR/did-core/>

World Wide Web Consortium. (2023). *Universal Wallet* (Editor's Draft 22 February 2023). <https://w3c-ccg.github.io/universal-wallet-interop-spec/>

### **EU Legislation/ Documents in the scope of Legislative Processes**

Commission communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM (2011) 942. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0942&from=en>

Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. *Official Journal of the European Union*, L 69/23. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389>

Commission Implementing Decision (EU) 2016/650 of 25 April 2016 on the security of communication and information systems in the European Union. *Official Journal of the European Union*, L 107/53. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D0650&from=EN>

Commission Implementing Regulation (EU) 2015/1501 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union*, L 235/1. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1501>

Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union*, L 235/7. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502>

Commission Recommendation (EU) 2014/478 of 14<sup>th</sup> July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from online gambling. *Official Journal of the European Union*, L 214/38. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014H0478>

Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity. *Official Journal of the European Union*, L 210/51. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021H0946&from=EN>

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Quality Framework for Services of General Interest in Europe, COM (2011) 900. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0900>

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). *Official Journal of the European Union*, L 178/1. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031>

Directive 2005/36/EC on the recognition of professional qualifications. *Official Journal of the European Union*, L 255/22. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0036&from=EN>

Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. *Official Journal of the European Union*, L 141/73. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>

Regulation (EU) no 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*, L 257/73. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910>

Regulation (EU) 2017/2018 on cross-border portability of online content services in the internal market. *Official Journal of the European Union*. L 168/1. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1128&qid=1696341990735>

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. *Eur-Lex Access to European Union law*. [https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF)

Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010. *EUR-Lex Access to European Union law*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0367>

Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). *Eur-Lex* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767>

Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (2021/0136 (COD)) Council's Consolidated text - Compromise Amendments. Interinstitutional File: 2021/0136(COD). <https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/en/pdf>

Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554. *Eur-Lex*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0360>

Report on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. Report - A9-0038/2023. [https://www.europarl.europa.eu/doceo/document/A-9-2023-0038\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.html)

### **National legislation (Spain)**

Ley 21/1992, de 16 de julio, de Industria. *Boletín Oficial del Estado*, 176, de 23 de julio de 1992. <https://www.boe.es/buscar/act.php?id=BOE-A-1992-17363>

Ley 29/2003, de 19 de diciembre, de firma electrónica. *Boletín Oficial del Estado*, 304, de 20 de diciembre de 2003. <https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399>

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. *Boletín Oficial del Estado*, 312, de 29 de diciembre de 2007. <https://www.boe.es/buscar/act.php?id=BOE-A-2007-22440>
- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia. *Boletín Oficial del Estado*, 252, de 17 de octubre de 2014. <https://www.boe.es/buscar/pdf/2014/BOE-A-2014-10517-consolidado.pdf>
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. *Boletín Oficial del Estado*, 236, de 2 de octubre de 2015. <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10565-consolidado.pdf>
- 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. *Boletín Oficial del Estado*, 272, de 9 de noviembre de 2017. <https://www.boe.es/buscar/act.php?id=BOE-A-2017-12902>
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. *Boletín Oficial del Estado*, 298, de 12 de noviembre de 2020. [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2020-14046](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-14046)
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones. *Boletín Oficial del Estado*, 155, de 29 de junio de 2022. <https://www.boe.es/buscar/doc.php?id=BOE-A-2022-10757>
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 281, de 24 de noviembre de 1995. <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>
- Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. *Boletín Oficial del Estado*, 10, de 12 de enero de 2010. <https://www.boe.es/buscar/act.php?id=BOE-A-2000-544>
- Ley Orgánica 4/2015, de 30 de marzo, de protección de seguridad ciudadana. *Boletín Oficial del Estado*, 77, de 31 de marzo de 2015. <https://www.boe.es/buscar/act.php?id=BOE-A-2015-3442>
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 294, de 6 de diciembre de 2018. <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>



Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *Gaceta de Madrid*, 260, de 17 de septiembre de 1882. [https://www.boe.es/eli/es/rd/1882/09/14/\(1\)](https://www.boe.es/eli/es/rd/1882/09/14/(1))

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. *Gaceta de Madrid*, 206, de 25 de julio de 1889. <https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763>

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. *Boletín Oficial del Estado*, 307, de 24 de diciembre de 2005. <https://www.boe.es/buscar/act.php?id=BOE-A-2005-21163>

Real Decreto 557/2011, de 20 de abril, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, sobre derechos y libertades de los extranjeros en España y su integración social, tras su reforma por Ley Orgánica 2/2009. *Boletín Oficial del Estado*, 103, de 30 de abril de 2011. Available: <https://www.boe.es/eli/es/rd/2011/04/20/557/con>

Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. *Boletín Oficial del Estado*, 2021, 77, de 30 de marzo de 2021. <https://www.boe.es/buscar/act.php?id=BOE-A-2021-5032>

### **National legislation (Belgium)**

Loi 18 juillet 2017 relative à l'identification électronique. Service public Federal Strategie et Appui, *Numac 2017020539*, de 9 août 2017. [https://www.ejustice.just.fgov.be/cgi/article\\_body.pl?language=fr&caller=summary&pub\\_date=17-08-09&numac=2017020539](https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=17-08-09&numac=2017020539)

### **National legislation (France)**

Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'Etat. (2018). *Journal Officiel*, 0264, du 15 novembre 2018. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037611479>

Code des postes et des communications électroniques. *Légifrance*. [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006070987/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070987/)

Code des relations entre le public et l'administration. *Légifrance*.

[https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000031366350/2021-01-21/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000031366350/2021-01-21/)

Code pénal. *Légifrance*.

[https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006070719/](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/)

Décret n° 2021-387 du 2 avril 2021 relatif à la lutte contre l'anonymat des actifs virtuels et renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme. *Légifrance*.

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043328577>

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. *Journal Officiel*, 0235, du 8 octobre 2016.

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746/>

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *Journal Officiel*, de 7 janvier 1978.

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460>

### **National legislation (Italy)**

Codice in materia di protezione dei dati personali. Normattiva. *Gazzetta Ufficiale*, 174, de 29 luglio 2003. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196>

Decreto Legislativo marzo 2005, n.82 (Codice Amministrazione Digitale), *Gazzetta Ufficiale*, 112, del 15 maggio 2005. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82>

Decreto-legge 16 luglio 2020, n.76. Misure urgenti per la semplificazione e l'innovazione digitale, *Gazzetta Ufficiale*, 178, del 16 luglio 2020.

<https://www.gazzettaufficiale.it/eli/gu/2020/07/16/178/so/24/sg/pdf>

Decreto-Legge 2 marzo 2024, n.19 Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza, *Gazzetta Ufficiale*, 52, del 2 marzo 2024.

<https://www.gazzettaufficiale.it/eli/id/2024/03/02/24G00035/sg>

Presidenza del Consiglio dei Ministri (2014). Regolamento recante le Regole Tecniche. *Agenzia per l'Italia Digitale*.

[https://www.agid.gov.it/sites/default/files/repository\\_files/circolari/spid-regole\\_tecniche\\_v1.pdf](https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regole_tecniche_v1.pdf)

Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico. *Gazzetta Ufficiale*, 277, del 25 novembre 1999 [https://www.uaipit.com/uploads/legislacion/files/0000000182\\_F1-IS-Ec-IT-Decr437-19991022.htm](https://www.uaipit.com/uploads/legislacion/files/0000000182_F1-IS-Ec-IT-Decr437-19991022.htm)

### **National legislation (UK)**

Fraud Act 2006 (c. 35). *legislation.gov.uk*  
<https://www.legislation.gov.uk/ukpga/2006/35/contents>

### **National legislation (US)**

Improving Digital Identity Act of 2023 (Proposal). *Billtrack*. Introduced on the 12<sup>th</sup> of July 2023. <https://www.billtrack50.com/billdetail/1609681>

### **Case Law**

ECJ. SAT Fluggesellschaft mbH v Eurocontrol. January 19<sup>th</sup>, 1994.  
<https://curia.europa.eu/juris/liste.jsf?num=C-364/92>

ECJ. Diego Calì & Figli Srl v Servizi ecologici porto di Genova SpA (SEPG). March 18<sup>th</sup>, 1997. ECLI:EU:C:1997:160

ECJ. Commission of the European Communities v. Portuguese Republic, October 22<sup>nd</sup>, 2009. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62008CJ0438>

ECJ. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, April 8<sup>th</sup>, 2014. ECLI:EU:C:2014:238

ECJ. Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, May 13<sup>th</sup>, 2014. ECLI:EU:C:2014:317

ECJ. Sotiris Papasavvas versus O Fileleftheros Dimosia Etaireia Ltd and others, September 11<sup>th</sup>, 2014, ECLI:EU: C:2014:2209

ECJ. Maximilian Schrems v. Data Protection Commissioner, October 6<sup>th</sup>, 2015, ECLI:EU:C:2015:650

ECJ. Grupo Itevelesa, S.L., y otros v. Oca Inspección Técnica de Vehículos, S.A., y Generalidad de Cataluña, October 15<sup>th</sup>, 2015. ECLI:EU:C:2015:685

ECJ. Jehovan todistajat, July 10<sup>th</sup> 2018. ECLI:EU:C:2018:551

ECJ. Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, July 29<sup>th</sup> 2019. ECLI:EU:C:2019:629

ECtHR. Case of Klass and Others v. Germany, September 6<sup>th</sup>, 1978, Application no.5029/71. <https://hudoc.echr.coe.int/eng?i=001-57510>

ECtHR. Case of Marckx v. Belgium, June 13<sup>th</sup>, 1979, Application No. 6833/74. <https://hudoc.echr.coe.int/fre?i=001-57534>

ECtHR. Case of Dudgeon v. The United Kingdom, October 22<sup>nd</sup>, 1981, Application No. 7525/76. <https://hudoc.echr.coe.int/eng?i=001-57473>

ECtHR. Case of Norris v.Ireland, October 26<sup>th</sup>, 1988, Application no.10581/83. <https://hudoc.echr.coe.int/eng?i=001-57547>

ECtHR. Case of B. v. France, March 25<sup>th</sup> 1992, Application no. 13343/87. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57770%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57770%22]})

ECtHR. Case of Roman Zakharov v. Russia, December 4<sup>th</sup>, 2015, Application no.47143/06. <https://hudoc.echr.coe.int/fre?i=001-159324>

ECtHR. Case of Christine Goodwin v. the United Kingdom, July 11<sup>th</sup>, 2022, Application No. 28957/95. <https://hudoc.echr.coe.int/fre?i=001-60596>

ECtHR. Case of Mikulic v. Croatia, September 4<sup>th</sup>, 2022, Application No. 53176/99. <https://hudoc.echr.coe.int/fre?i=001-60035>

STC 227/1988, de 29 de noviembre. BOE núm. 307, de 23 de diciembre de 1988. <https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/1168>

STC 13/1992, de 6 de febrero. Recursos de inconstitucionalidad acumulados núms. 542/1988 y 573/1989. BOE de 3 de marzo de 1992. [https://www.congreso.es/constitucion/ficheros/sentencias/stc\\_013\\_1992.pdf](https://www.congreso.es/constitucion/ficheros/sentencias/stc_013_1992.pdf)

STS de 20 de diciembre de 1994. Recurso de casación 322/1993. <https://vlex.es/vid/202673427>

STC18/2011, de 3 de marzo de 2011. Recursos de inconstitucionalidad acumulados 838-1998, 867-1998 y 997-1998. BOE núm. 75, de 29 de marzo de 2011.  
<https://www.boe.es/buscar/doc.php?id=BOE-A-2011-5704>

STC 60/2023, de 24 de mayo de 2023. Recurso de inconstitucionalidad 762-2020. BOE núm. 150, de 24 de junio de 2023.  
<https://www.boe.es/buscar/doc.php?id=BOE-A-2023-14928>

STS 870/2016, de 21 de abril de 2016.  
[https://www.poderjudicial.es/stfls/TRIBUNAL%20SUPREMO/DOCUMENTOS%20DE%20INTER%20C3%89S/sentencia%20itv%20Catalunya%20\(1\).pdf](https://www.poderjudicial.es/stfls/TRIBUNAL%20SUPREMO/DOCUMENTOS%20DE%20INTER%20C3%89S/sentencia%20itv%20Catalunya%20(1).pdf)

### **Thesis/ Dissertations**

Alamillo Domingo, I. (2018). Identificación Electrónica y Confianza en las Transacciones Electrónicas: la Regulación Jurídico-Administrativa de las Instituciones de Acreditación de la Actuación Electrónica. [Tesis doctoral, Universidad de Murcia].  
<https://digitum.um.es/digitum/bitstream/10201/61019/6/Ignacio%20Alamillo%20Domingo%20Tesis%20Doctoral.pdf>

Arocha Vinagre, S.B. (2017). *Ciberdelincuencia: problemas en la determinación de la jurisdicción y competencia de los tribunales del orden penal*. [Trabajo de Fin de Grado, Universidad de la Laguna]. <https://rebrand.ly/ciberdelincuencia>

Arredondo, Solís, C. (2018). *L'usurpation d'identité numérique sur Internet : Etude comparée des solutions françaises, mexicaine et nord-américaines*. [Thèse de doctorat, l'Université Paris-Saclay]. <https://www.theses.fr/2018SACL5023>

Castro Lucas Da Silva, J. (2022). *The antithesis between KYC practices and the increasing presence of cryptocurrencies*. [Master's Thesis, Nova School of Law].  
[https://run.unl.pt/bitstream/10362/141157/1/LucasdaSilva\\_2022.pdf](https://run.unl.pt/bitstream/10362/141157/1/LucasdaSilva_2022.pdf)

L.Rosner. (2014). *Identity Management Policy and Unlinkability: A comparative study of the US and Germany*. [PhD Thesis, University of Nottingham].  
[https://eprints.nottingham.ac.uk/14358/1/Full\\_Draft\\_v4.1.4.2\\_FINAL\\_post-viva\\_corrections.pdf](https://eprints.nottingham.ac.uk/14358/1/Full_Draft_v4.1.4.2_FINAL_post-viva_corrections.pdf)

Nikolopoulou, A. (2018). *The Directive on security of network and information systems (NIS Directive) from a practical view-Challenges for the Aviation Industry*. [Master's Thesis, International Hellenic University].

<https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/29357/NISDirective.pdf?sequence=1>

Nilsson, A. (2018). *An increase in safety for payment services?*. [Master's Thesis, Lund University].  
(<https://lup.lub.lu.se/luur/download?func=downloadFile&recordId=8965762&fileId=8970334>)

Van Alsenoy, B. (2016). *Regulating Data Protection: The allocation of responsibility and risk among actors involved in personal data processing*. [PhD Thesis, KU Leuven]. [https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1711667&context=L&vid=Lirias&search\\_scope=Lirias&tab=default\\_tab&lang=en\\_US&fromSitemap=1](https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1711667&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1)

### Websites/ Blogs

Adams, T.S. (2023, August 16). *What is Anonymous Authentication*. EasyTechJunkie. <https://www.easytechjunkie.com/what-is-anonymous-authentication.htm>

Adobe. (2022, August 10). *Electronic Signature Laws & Regulations-Germany*. Adobe. <https://helpx.adobe.com/legal/esignatures/regulations/germany.html>

AgID. (n.d.). *Carta Nazionale dei Servizi*. AgID. Retrieved August 15, 2023 from <https://www.agid.gov.it/it/piattaforme/carta-nazionale-servizi>

AgID. (n.d.). Agreement for adhesion to the public digital identity management system [Template], AgID. <https://www.agid.gov.it/>

Allen, C. (2022, December 13). *Musing of a Trust Architect: Progressive Trust*. Blockchain Commons. <https://www.blockchaincommons.com/musings/musings-progressive-trust/>

Allen, C. (2023, August 9). *Origins of Self-Sovereign Identity*. Blockchain Commons. <https://www.blockchaincommons.com/musings/origins-SSI/>

Amsler, S. & Shea, S. (n.d.). *RFID (radio frequency identification)*. TechTarget. Retrieved August 23, 2023 from <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification>

- api.gouv.fr. (n.d.). *Authentifier des personnes et des organisations*. République Française. Retrieved August 15, 2023 from <https://api.gouv.fr/guides/authentification>
- api.gouv.fr. (n.d.). *FranceConnect et les API FranceConnectées*. République Française. Retrieved August 15, 2023 from <https://api.gouv.fr/les-api/franceconnect>
- Apple. (2022, March 23). *Apple launches the first driver's license and state ID in Wallet with Arizona*. Apple. <https://www.apple.com/newsroom/2022/03/apple-launches-the-first-drivers-license-and-state-id-in-wallet-with-arizona/>
- Arampatzis, A. (2023, April 28). *Homomorphic Encryption: What Is It and How Is It Used*. Venafi. <https://venafi.com/blog/homomorphic-encryption-what-it-and-how-it-used/>
- Arana, J. (2017, November 26). *¿Es residual el uso del DNI electrónico?*. Administración Electrónica, Universidad de Zaragoza. <https://administracionelectronica.unizar.es/es-residual-el-uso-del-dni-electronico>
- aruba.it. (n.d.). *Price list*. aruba.it. Retrieved August 15, 2023 from <https://www.aruba.it/en/spid-price-list.aspx>
- ascens. (2011, July 29). *Sólo el 4,7% de los españoles hacen uso del DNI electrónico. A qué esperamos para hacer crecer ese porcentaje?* ascens blog. <https://rebrand.ly/6po0kuu>
- BAES Blockchain Lab. (n.d.). *LegalCripto by BAES*. Retrieved February 12, 2024 from <https://www.baeslegalcripto.eu/>
- belga news agency. (2023, March 28). *Itsme reaches 6.7 million Belgian users, app is now profitable*. belganewsagency. <https://www.belganewsagency.eu/itsme-ziet-aantal-gebruikers-stijgen-tot-67-miljoen-en-is-voor-eerst-winstgevend>
- Blocks. Retrieved August 15, 2023 from. <https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=533365191>
- Bodoni, S. (2021, July 30). *Amazon Gets Record 888 Million EU Fine Over Data Violations*. Bloomberg. <https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach>

Borroy, A. (2012, July 18). *Estadísticas de uso (real) del DNI electrónico en España*. Programming and So. <https://angelborroy.wordpress.com/2012/07/18/estadisticas-de-uso-real-del-dni-electronico-en-espana/>

Brook, C. (2022, December 28). *Google Fined 57M by Data Protection Watchdog Over GDPR Violations*. *Digital Guardian's Blog*. Frotra. <https://www.digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations>

Burt, C. (2021, November 15). *States to bear digital ID costs without income from Apple Wallet contracts*. Biometricupdate.com. <https://www.biometricupdate.com/202111/states-to-bear-digital-id-costs-without-income-from-apple-wallet-contracts>

CNIL. (2019, October 17). *L'anonymisation des données, un traitement clé pour l'open data*. CNIL. <https://www.cnil.fr/fr/lanonymisation-des-donnees-un-traitement-cle-pour-lopen-data>

*Data deduplication*. (2023, July 7). In Wikipedia. [https://en.wikipedia.org/wiki/Data\\_deduplication](https://en.wikipedia.org/wiki/Data_deduplication)

Digital Berry. (n.d.). *Electronic archiving system*. Digital Berry. Retrieved August 18, 2023 from <https://www.digitalberry.fr/en/expertise/electronic-archiving-system/>

Etherum org. (2023, September 21). *What are zero-knowledge proofs?* Ethereum org. Retrieved August 14, 2023. <https://ethereum.org/en/zero-knowledge-proofs/>

EU Digital Wallet Consortium. (n.d.). Home - EUDI Wallet Consortium. EWC. Retrieved August 18, 2023 from <https://eudiwalletconsortium.org/>

Fábrica Nacional de la Moneda y Timbre. (n.d.). *Documentos de Identificación*. Real Casa de la Moneda. Fábrica Nacional de Moneda y Timbre. Retrieved August 14, 2023 from <https://www.fnmt.es/institucion>

Federal Ministry of the Interior and Community. (2023). *What is the Online Access Act*. Federal Ministry of the Interior and Community. Retrieved August 14, 2023 from <https://www.onlinezugangsgesetz.de/Webs/OZG/EN/home/home-node.html>

Finnish Social Science Data Archive. (n.d.). *Anonymisation and personal data*. Finnish Social Science Data Archive. Retrieved January 24, 2024 from <https://www.fsd.tuni.fi/aineistonhallinta/en/anonymisation-and-identifiers.html>



- GDPR.EU. (n.d.). *What is a privacy notice?* GDPR.EU. Retrieved August 8, 2023 from <https://gdpr.eu/privacy-notice/>
- German identity card*. (2023, September 25). In Wikipedia. [https://en.wikipedia.org/wiki/German\\_identity\\_card](https://en.wikipedia.org/wiki/German_identity_card)
- Global Legal Entity Identifier Foundation. (n.d.). *Introducing the Legal Entity Identifier (LEI)*. GLEIF. Retrieved August 23, 2023 from <https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei>
- Goodman, J.B. & Loveman, G.W. (1991). Does Privatization Serve the Public Interest? *Harvard Business Review*. <https://hbr.org/1991/11/does-privatization-serve-the-public-interest>
- Goudet, J.L. (2010, February 3). *Idénium : la fausse bonne idée du gouvernement français*. Furtura. <https://www.futura-sciences.com/tech/actualites/internet-idenium-fausse-bonne-idee-gouvernement-francais-22487/>
- Group-IB. (2024, February 15). *Face Off*. <https://www.group-ib.com/blog/goldfactory-ios-trojan/>
- Hakoune, R. (2021, October 20). *How digital platforms are changing the way we work*. mondayblog. <https://monday.com/blog/project-management/digital-platforms/>
- Heath, N. (2019, February 19). *How Estonia became an e-government powerhouse*. TechRepublic. <https://www.techrepublic.com/article/how-estonia-became-an-e-government-powerhouse/>
- Heller, N. (2017, December 11). *Estonia, the Digital Republic*. The New Yorker. <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>
- Hendrickson, L. (2023, January 30). *The Ultimate Guide to Self-Sovereign Identity (SSI)*. Identity.identity. [https://www.identity.com/self-sovereign-identity/#The\\_Benefits\\_of\\_Self-Sovereign\\_Identity\\_SSI](https://www.identity.com/self-sovereign-identity/#The_Benefits_of_Self-Sovereign_Identity_SSI)
- IDnow. (n.d.). *Anti-Money Laundering Directive (AMLD)*. IDnow. Retrieved August 8, 2023, from <https://www.idnow.io/glossary/anti-money-laundering-directive->
- invest in estonia. (n.d.). *e-identity*. Invest in Estonia. Retrieved August 14, 2023 from <https://investinestonia.com/business-opportunities/cyber-security/e-identity/>

- IPv6. (2023, September 28). In Wikipedia. <https://en.wikipedia.org/wiki/IPv6>
- it Developers Italia. (n.d.). *CIE Electronic Identity Card*. Dipartimento per la Trasformazione Digitale + AgID. Retrieved August 15, 2023 from <https://developers.italia.it/en/cie/>
- itsme. (2023). *Get started with itsme. Itsme*. Retrieved August 15, 2023 from <https://www.itsme-id.com/en-BE/get-started>
- jewelbai. (2022, September 10). *DINUM extends FranceConnect experimentation. Technology News*. <https://trends.akashtdr.com/dinum-extends-franceconnect-experimentation/>
- Kaspersky. (n.d.). *What is Biometrics? How is it used in security?* Kaspersky. Retrieved August 23, 2023 from <https://www.kaspersky.com/resource-center/definitions/biometrics>
- Kokumai, H. (2018, August 1). *Assurance by our own volition and memory Part 1*. Payments Journal. <https://www.paymentsjournal.com/identity-assurance-by-our-own-volition-and-memory-part-1>
- Kokumai, H. (2019, September 30). *Passwords made of unforgettable images*. Payments Journal. <https://www.paymentsjournal.com/passwords-made-of-unforgettable-images>
- Kokumai, H. (2020, April 28). *'Easy-to-Remember' is one thing, 'Hard-to-Forget' is another*. Payments Journal. <https://www.paymentsjournal.com/easy-to-remember-is-one-thing-hard-to-forget-is-another/>
- LA Wallet. (n.d.). *Official Louisiana Digital Driver's License - LA Wallet*. LA Wallet. Retrieved October 18, 2023 from <https://lawallet.com/>
- Leyden, J. (2003, April 18). *Office workers give away passwords for a cheap pen*. The Register. [https://www.theregister.com/2003/04/18/office\\_workers\\_give\\_away\\_passwords/](https://www.theregister.com/2003/04/18/office_workers_give_away_passwords/)
- Libération. (2022, September 1). *Cyberattaque. Piratage de FranceConnect: ce que l'on sait*. Libération. <https://rb.gy/b4kfgj>
- Lorette, K. (2019, March 12). *Code of Business Conduct. Small Business*. Chron.com. <https://smallbusiness.chron.com/code-business-conduct-2732.html>

- Mastercard. (2020). *Digital Identity: Our Service*.  
<https://idservice.com/content/dam/public/mastercardcom/idservice/pdf/digital-identity-our-service.pdf>
- Mastercard. (n.d.). *Digital Identity Services*. Mastercard. Retrieved August 9, 2023 from <https://idservice.com/en/home.html>
- Mcleod, S (2023, October 5). *Social Identity Theory In Psychology (Tajfel & Turner, 1979)*. SimplyPsychology. <https://www.simplypsychology.org/social-identity-theory.html>
- Meta for Developers. (n.d.). *Facebook Login*. Facebook. Retrieved August 8, 2023 from <https://developers.facebook.com/docs/facebook-login/>
- Mississippi Department of Public Safety. (n.d.). *MISSISSIPPI MOBILE ID*. MS Driver Services Bureau. Retrieved October 18, 2023 from <https://www.driverservicebureau.dps.ms.gov/mobile-id/>
- National identity number. (Norway)* (2023, July 31). In Wikipedia.  
[https://en.wikipedia.org/wiki/National\\_identity\\_number\\_\(Norway\)](https://en.wikipedia.org/wiki/National_identity_number_(Norway))
- NIST. (n.d.). *Identity Assurance Level (IAL)*. NIST Computer Security Resource Center. Retrieved August 8, 2023 from [https://csrc.nist.gov/glossary/term/identity\\_assurance\\_level](https://csrc.nist.gov/glossary/term/identity_assurance_level)
- Nikel, D. (2022, January 27). *BankID: Norway's Digital ID System Explained*. Life in Norway. <https://www.lifeinnorway.net/bankid-norway/>
- Norge. No. (n.d.). *Electronic ID*. Norge. No. Retrieved August 15, 2023 from <https://www.norge.no/en/digital-citizen/electronic-id>
- Oberlo. (2023). *US Smartphone Market Share: Statistics & Facts*. Oberlo.  
<https://www.oberlo.com/statistics/us-smartphone-market-share>
- Office for the Protection of Competition. (n.d.). *Services of General Economic Interest*. UOHS. Retrieved August 21, 2023 from <https://www.uohs.cz/en/state-aid/services-of-general-economic-interest.html>
- Onfido. (n.d.). *Digital identity made simple*. Onfido. Retrieved August 21, 2023  
<https://onfido.com/>

- Pettinger, T. (2019, May 19). *Private Sector vs Public Sector*. Economics Help. <https://www.economicshelp.org/blog/2634/economics/private-sector-vs-public-sector/>
- Pettinger, T. (2019, November 28). *Government Intervention in Markets*. Economic Help. <https://www.economicshelp.org/microessays/equilibrium/govt-intervention/>
- Portal de la Administración Electrónica. (n.d.). *Sistema de identificación electrónica notificados*. Portal Administración Electrónica. Retrieved August 14, 2023 from [https://administracionelectronica.gob.es/pae/Home/pae/Estrategias/pae/Identidad\\_y\\_firmaelectronica/Nodo-eIDAS/Sistemas-de-identificacion-electronica-notificados.html](https://administracionelectronica.gob.es/pae/Home/pae/Estrategias/pae/Identidad_y_firmaelectronica/Nodo-eIDAS/Sistemas-de-identificacion-electronica-notificados.html)
- Raymond, N. (2022, December 23). *Facebook parent Meta to settle Cambridge Analytica scandal case for 725 millions*. Reuters. <https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/>
- République Française. (n.d.). *FranceConnect simplifie les démarches de plus de 40 millions de personnes* Retrieved August 14, 2023 from <https://franceconnect.gouv.fr/>
- Roth, E. (2021, November 14). *Apple is reportedly relying on states to pay for digital ID rollouts*. The Verge. <https://www.theverge.com/2021/11/14/22781570/apple-making-states-pay-digital-id-service>
- State of Colorado. (n.d.). *Home*. myColorado. Retrieved October 18, 2023 from <https://mycolorado.state.co.us/>
- Smertnik, H. (2020, June 4). *Confusing biometric ID experiences at a young age: voices from Thailand*. Medium. <https://medium.com/caribou-digital/confusing-biometric-id-experiences-at-a-young-age-voices-from-thailand-abe6579ff45b>
- Spid. (n.d.). *How to choose between digital identity providers AGID*. Retrieved August 15, 2023 from <https://www.spid.gov.it/en/what-is-spid/how-to-choose-between-digital-identity-providers/>
- Swan, Z. (2020, April 27). *What is an Industry Code of Practice?* Lawpath. <https://lawpath.com.au/blog/what-is-an-industry-code-of-practice>

TechTarget. (2015) *Pseudonymity*. WhatIs.com. Retrieved August 8, 2023 from <https://www.techtarget.com/whatis/definition/pseudonymity#:~:text=Pseudonymity%20is%20the%20near%2Danonymous,in%20a%20generally%20anonymous%20way.>

TechTerms. (n.d.). *GUID*. TechTerms. Retrieved January 12, 2023 from <https://techterms.com/definition/guid>

TechTerms. (n.d.). *UUID*. TechTerms. Retrieved January 12,2023 from <https://techterms.com/definition/uuid>

Thales. (2017). *June 2017: New German ID cards are “switched on”*. Thales. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/eid-in-germany>

The Bulletin. (2022, June 28). *Belgian government plans official alternative to ItsMe*. The Bulletin. <https://www.thebulletin.be/belgian-government-plans-official-alternative-itsme>

Tinianow, A. (2024, January 29). *The EU Lays The Techno-Legal Tracks For Its Rising Digital Ecosystem*. Forbes. <https://www.forbes.com/sites/andreatinianow/2024/01/29/the-eu-lays-the-techno-legal-tracks-for-its-rising-digital-ecosystem/>

United Nations. (n.d). *The 17 Goals*. United Nations. Retrieved October 18,2023 from <https://sdgs.un.org/goals>

Validated ID. (n.d.). *Remote signature*. Validated ID. Retrieved August 18, 2023 from <https://www.validatedid.com/en/remote-signature>

### **Project Deliverables/Documentation**

Alamillo Domingo, I., Timón López, C., Valero Torrijos, J., Frederisken, T., Stausholm, M., Bernal, J., Rodríguez, J., & Torres, R. (2020). *D3.2 Security and Privacy-aware OLYMPUS Framework Impact Assessment*. OLYMPUS Project. [https://olympus-project.eu/wp-content/uploads/2020/02/Olympus\\_pu\\_d3\\_2\\_v1\\_0.pdf](https://olympus-project.eu/wp-content/uploads/2020/02/Olympus_pu_d3_2_v1_0.pdf)

Bauer, M., Meints, M., & Hansen, M. (Eds.). (2005). *D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems*. FIDIS.

[http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview\\_on\\_IMS.final.pdf](http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf)

Ponte, N., Timón López, C., Alamillo Domingo, Valero Torrijos J., Martínez Alonso, N., Martins, N., Marques, N. Esteban, F., Sakkopoulos, V., & Sourla, G. (2020). *D5.3 OLYMPUS support for extended eID models*. OLYMPUS Project. [https://olympus-project.eu/wp-content/uploads/2020/10/Olympus\\_pu\\_d5\\_3\\_v1\\_0.pdf](https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d5_3_v1_0.pdf)

Schaarup Andersen, M., Stausholm, M., Sourla, G., Timón López, C., Alamillo Domingo, I., Valero Torrijos, J., Ponte, N., Martins, N., Conceição, F.C., García Rodríguez, J., & Martínez Alonso, N. (2021). *D6.3 Final Pilot deployment and evaluation of User experience and GDPR compliance*. OLYMPUS Project. [https://olympus-project.eu/wp-content/uploads/2021/10/Olympus\\_pu\\_d6\\_3\\_v1\\_2.pdf](https://olympus-project.eu/wp-content/uploads/2021/10/Olympus_pu_d6_3_v1_2.pdf)

Stausholm, M., Frederiksen, T., Gargía J., Torres, R., Bernal, J. Skarmenta, A., Sourla, G., Hesse, J., & Lehman, A. (2020). *D3.3 OLYMPUS Blueprint*. OLYMPUS Project. [https://olympus-project.eu/wp-content/uploads/2020/10/Olympus\\_pu\\_d3\\_3\\_v1\\_0.pdf](https://olympus-project.eu/wp-content/uploads/2020/10/Olympus_pu_d3_3_v1_0.pdf)

Timón López, C. & Skarmeta Gómez, A. (2022). *Allocating controllership in the European Digital Identity Wallet*. CyberSecurity4Europe. <https://cybersec4europe.eu/wp-content/uploads/2023/02/wallet.pdf>

### **Other resources**

De Felcourt, G. (2020). *L'identité numérique aujourd'hui. Cours d'enseignement supérieur, Société e identité numérique* [ Unpublished manuscript].

Martín Bautista, A. (2023). *La propuesta de Reglamento eIDAS2 : contexto y visión general* [Video]. tv.um.es <https://tv.um.es/video?id=148290>

Pfitzmann, A. & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management* [Terminology]. [http://dud.inf.tu-dresden.de/literatur/Anon\\_Terminology\\_v0](http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0). 34.

Setsaas, J.E. (2021). *eID in the Nordics* [PowerPoint presentation].

Schwalm, S., & Canela, S. (2023). *Mesa 2. eIDAS 2 and the role of identity standards: an outlook of current activities/ La arquitectura de referencia (ARF) del eIDAS 2* [Video]. tv.um.es <https://tv.um.es/video?id=148292>

Panizo Plaza, J.M. & Ariño Martín, L.A. (2023). *Mesa 3. La iniciativa European Blockchain Services Infrastructure/ El piloto de gran escala DC4EU* [Video]. tv.um.es <https://tv.um.es/video?id=148293>





# ANNEX A

## THE DATA PROTECTION IMPACT ASSESSMENT IN “LAYERS”: A METHODOLOGY FOR EVALUATING TECHNOLOGICAL PROPOSALS

### Ensuring Privacy at the Foundational Stages of Technological Innovation

The adapted methodology for the DPIA was produced as part of my first research work in the scope of the research project OLYMPUS. The task that triggered the proposed adaptations of the DPIA methodology was the requirement to conduct a DPIA in the context of a research project, where no concrete implementation scenarios are foreseen, but rather a proposal for a technological architecture and a high-level description of use cases.

The DPIA is a tool specifically designed to ensure compliance with data protection principles and obligations in situations where personal data processing takes place. The DPIA's intended purpose is to keep the specific stakeholders informed about the concerned environment by identifying affected entities, as well as the resultant data processing and its risks, and evaluate proposed measures to mitigate or eliminate them. The DPIA becomes an obligation in the cases cited in Recital 84 of the GDPR, “where processing operations are likely to result in a high risk to the rights and freedoms of natural persons,” and Article 35, “where a type of processing, in particular, using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk (...).”

Although there is no official methodology for the DPIA, some guidelines can be found in different texts. The GDPR provides some basic content in Article 35.7<sup>283</sup>. However,

---

<sup>283</sup> The assessment shall contain at least: a) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b) An assessment of the necessity and proportionality of the processing operations in

in practice, it is necessary to refer to other instruments such as the ISO 29134:2017, the National Data Protection guidelines, or the A29 WP Guidelines on Data Protection Impact Assessment.

Based on these texts, it can be agreed that the DPIA involves four main phases: 1) Inventory and description; 2) General privacy safeguarding requirements; 3) Identification and evaluation of privacy risks; and 4) Proposals for safeguards. Furthermore, to accurately assess pertinent privacy risks, Recital 76 of the GDPR stipulates that risk evaluation should consider the likelihood and severity of potential harm to the data subject's rights and freedoms, taking into account the nature, scope, context, and intent of the data processing activities. After identifying potential threats, risks should be categorized based on their likelihood and potential consequences.

However, the main concern emerging with this methodology is its applicability only in specific contexts, wherein data processing activities are well-documented, and the type and volume of data being processed are clearly defined. However, this contrasts with the situations encountered in research projects like OLYMPUS and, more recently, ERATOSTHENES. In these cases, the technologies being developed are still in their nascent stages, and the potential applications are not yet fully defined. This situation is not only limited to academic fields but is also common in technology companies.

The importance of considering privacy as part of a system's development process is widely accepted as an essential aspect of the development of privacy-aware systems (Pattakou et al., 2018, p.1). Ontario Privacy Commissioner Ann Cavoukian stated that Privacy by Design is achieved by building fair information practice principles or the seven foundational principles into information technology, business practices, and physical design and infrastructures<sup>284</sup>. These principles have been incorporated into EU

---

relation to the purposes; c) An assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and d) The measures envisaged addressing the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

<sup>284</sup> Firstly, the principle of Proactive not Reactive requires having the mechanisms to observe and resolve privacy issues before they turn into problems. These mechanisms must also envisage Privacy by Default in such a way that if the individual does not take any action, their privacy remains intact because it is

Law in Article 25 GDPR, mandating data protection by design and by default and listing the elements the controller must consider when determining the measures for a specific data processing operation<sup>285</sup>.

The Spanish Data Protection Agency has also referred to the concept of privacy engineering as the process for the implementation of privacy in the lifecycle of those information systems where the processing of personal data takes place. Privacy engineering involves a set of phases: 1) Determination of the properties and functionalities in terms of privacy that a system must fulfill so its implementation will be possible; 2) The design of the architecture and implementation of the elements in the system that cover the privacy requirements previously defined; and 3) Confirmation that privacy requirements have been correctly implemented and satisfy expectations and needs.

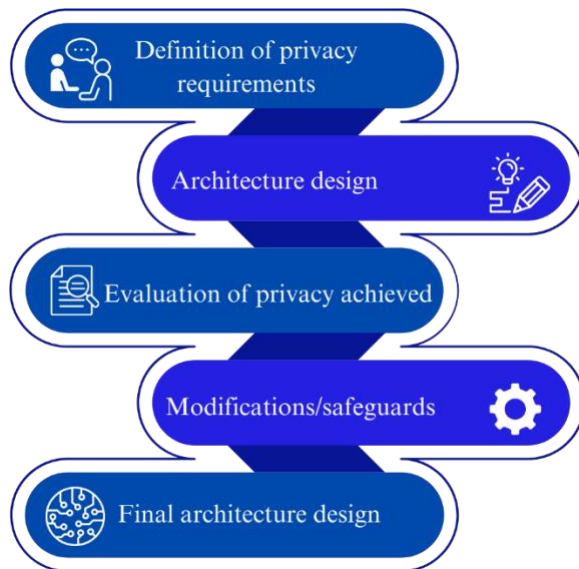
---

built into the system by default. Likewise, Privacy is integral to the system without diminishing functionality; that is to say, Privacy is Embedded into the Design. Furthermore, privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, assuring Full Functionality and avoiding false dichotomies. Privacy by design must also cover all lifecycle; hence, for example, in the case of digital identity management, the whole lifecycle of digital identities must be protected through End-to-End Security. Finally, privacy by design seeks to assure Visibility and Transparency thus all stakeholders operate according to the stated promises and objectives, subject to independent verification, as well as to Respect Users Privacy, keeping the solution user centric.

<sup>285</sup> The state of the art, costs of implementation, nature, scope, context and purpose of the processing.

Figure A.1

Privacy Engineering Phases



*Note.* Adapted from “Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems” by Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). *ARES’ 21: Proceedings of the 16<sup>th</sup> International Conference on Availability, Reliability and Security*, 132, (p.4).

The goal is to integrate privacy considerations directly into the system design, ensuring that privacy requirements are articulated as tangible properties and functionalities from the outset. This approach allows the system to proactively address any privacy risks that are identified and is also in line with current efforts toward developing technology solutions that are inherently privacy-centric, protecting privacy and eliminating or reducing unnecessary or undesired processing of personal data without compromising the functionality of the information system (i.e., Privacy Enhancing Technologies).

However, one of the main concerns when developing new technologies is how to evaluate them before they are implemented. This is where a DPIA can be useful. Although the DPIA is a tool designed for context-based scenarios, it can also be adapted for the analysis of technological solutions before their implementation. We referred to

this adaptation as “DPIA in layers” and was published in a research paper titled "Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems". The paper was published as part of the ARES Conference proceedings in 2021. The key ideas are summarized in this Annex.

### **DPIA in “layers”: Steps and an Example of the Adapted Methodology**

The first step in the development of a DPIA is the description of the subject of study. This description should contain at least an explanation of the technological proposal and its main differences or improvements concerning existing technologies. Once the characteristics of the technology are explained, the data flows must be described. The data flows refer to the transfer, exchange, storage, or modification of data that takes place in the use or performance of operations involving the processing of personal data. In the case of digital identity systems, the data flows refer to the lifecycle of digital identities, that is to say, how enrollment, authentication, and digital identity management will be performed in this specific system.

By way of example, we provide a summarized version of the description of the scope of the DPIA performed as part of the OLYMPUS research project.

**Description of the technology:** OLYMPUS is a digital identity system developed in the scope of the EU research program OLYMPUS in the framework of Horizon 2020. It proposes a digital identity system in the paradigm of delegated digital identity.

#### **Main innovations:**

- OLYMPUS distributes the task of the IdP among several IdPs (which conform the virtual IdP) by means of novel cryptographic approaches applied to digital identity technologies and allows the user’s password “fragmentation.”
- OLYMPUS has included a possibility for privacy-preserving authentication, at least in offline scenarios, thanks to the deployment of cryptographic techniques that prevent the IdP’s traceability.

- OLYMPUS has included “key-resharing,” which consists of a cryptographic technique that allows the change/refresh of the secret key material (or fragment of password) in established periods of time.

**Data flows:**

- a) Enrollment: the user requests to enroll in OLYMPUS. Credentials are username and password. Password information is disaggregated among the partial IdPs that conform the virtual IdP. The user can attach attributes to their account. ID proofing is out of the scope. Attributes are encrypted and stored. To access these data the user has to perform authentication.
- b) Authentication: the user requests the information to be shared with the SP. Each partial IdP among the virtual IdP will validate whether required attributes can be satisfied by information stored in their databases linked to the user's account. If so, they generate a partial signature, whose combination will result in an authentication token or credential (depending on whether it is an online or offline scenario).
- c) Account management: the user can manage their account (i.e., deletion, modification, update, or data transfer) by authenticating in OLYMPUS.

Furthermore, it would also be recommended to include a graphical (and adapted) representation of the architecture's design to make technology easily understandable and to highlight the main differences introduced.

Before proceeding with the DPIA, it is advisable to analyze at least one prior issue. With the latest advancements in cryptography and techniques that aim to achieve data anonymity, the first thing to consider is whether the processed data can be categorized as "personal data" and thus falls under the scope of GDPR. In order to determine whether the data processed can be qualified as personal data, we have to refer to the definition contained in Article 4(1) of the GDPR, “any information relating to an identified or identifiable individual. An identifiable natural person is one who can be identified directly or indirectly (...).” Conversely, when data does not relate to an

identified or identifiable natural person, data must be considered anonymous and does not fall under the scope of GDPR principles and obligations (Recital 26).

Nevertheless, determining which data can be considered anonymous is a complex task in practice. This is because it requires a deep understanding of the techniques deployed and their reversibility possibilities. Moreover, the GDPR and A29 WP have provided different approaches, making it more challenging to determine which data can be deemed anonymous. Pursuing Recital 26 GDPR, “data is anonymous if it is reasonably likely<sup>286</sup> that it cannot be linked to an identified or identifiable natural person” (risk approach). Conversely, the A29 WP Opinion on Anonymization Techniques states that “anonymization results from the processing of personal data in order to irreversibly prevent identification.” To assess whether this risk of identification exists, A29 WP provides three criteria: 1) The possibility to isolate records that identify the individual in a dataset (singling out); 2) The possibility to determine that at least two data sets contain information about the same data subject (linkability); and 3) The possibility to deduce, the value of an attribute from the values of other sets of attributes (inference). Additionally, A29 WP introduces a time frame to be considered during data processing. This includes taking into account both the current state-of-the-art technology as well as the potential for technological advancements during the period in which the data will be processed or is expected to be processed. Following the examples provided by Finck & Pallas (2019, p.9), the national authorities have expressed opinions on both approaches<sup>287</sup>.

---

<sup>286</sup> To determine what is reasonably likely, for example, the British Data Protection Authority (ICO) proposes the “motivated intruder test.” The motivated intruder is taken to be a person who starts without prior knowledge but who wishes to identify the individual. This approach states that it must also be considered the possible attractive of the data for potential intruders, such as the existence of nefarious or personal reasons, financial gain, political or activist purposes.

<sup>287</sup> For example, for the Irish Supervisory Authority or the Spanish Data Protection Agency it is not necessary to prove that it is impossible for the data subject to be identified, while for the *CNIL* and the Finnish Social Science Data Archive, to fall within the scope of anonymized data, re-identification must be nearly impossible. Despite the different approaches in determining whether a data should be included in the category of personal data, it is concluded that in practice a risk approach is adopted. By way of example, the *CNIL* in its opinion *L’anonymisation des données, un traitement clé pour l’open data*, recalls its conception of anonymization as the impossibility of re-identification, but it also introduces anonymization as an obligation in the *Code des relations entre le public et l’Administration*.

Finally, in the process of determining whether data is anonymous, it must be analyzed for which parties the re-identification is no longer possible. In this point, we also identify two different approaches. A relative approach where data must be anonymous from the perspective of the data controller, and an absolute approach in which data must also be anonymous from the perspective of third parties. The Spanish Data Protection Agency has stated that the anonymization process must also guarantee that reidentification is impossible for the data controller. Regarding third parties, opinions differ<sup>288</sup>.

In our specific technological proposal, we needed to determine for which parties the data would remain anonymous. To determine this, we can identify the parties involved and assess the risks that could potentially make them identifiable. In the case of a digital identity system, there are three main parties involved, and we suggested considering the following risks.

**Table A.1**

Parties and Risks of Reidentification

<b>Third unauthorized parties</b>	For example, in the case of information leaks or identity theft attacks
<b>SPs</b>	Linkability risks among services
<b>IdPs</b>	Possibilities of having knowledge of user’s attributes, to identify the data subjects and trace their activity

*Note.* Adapted from “Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems” by Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). *ARES’ 21: Proceedings of the 16<sup>th</sup> International Conference on Availability, Reliability and Security*, 132, p.5.

---

<sup>288</sup> According to Advocate General Campos Sánchez-Bordona in Breyer 17: “It would never be possible to rule out with absolute certainty that there is no third party in possession of additional data which may be combined with other information, and therefore capable of revealing a person’s identity.”



By applying these criteria to the OLYMPUS example, we obtained the following results:

**Table A.2**

Degree of Anonymization of Data Processed in OLYMPUS

Party	Analysis	Degree of anonymization
Third unauthorized parties	Conversely to the case of identity theft, information leaks do not require all the partial IdPs to be compromised.	Medium
SPs	The possibility of using different pseudonyms before each SP reduces the risks of linkability.	High
IdPs	Although the technology aims to blind the IdP in the authentication process, the data are not encrypted for the multiple IdPs.	Low

*Note.* Adapted from “Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems” by Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). *ARES’ 21: Proceedings of the 16<sup>th</sup> International Conference on Availability, Reliability and Security*, 132, p.5.

From this analysis, we concluded that OLYMPUS would process personal data. The possibility of using different pseudonyms will reduce the risk of linkability, but pseudonymized data still falls under the scope of personal data pursuing Recital 26 GDPR. On the other hand, the IdPs (who will likely act as data controllers or joint controllers when identity management is not provided as a service) will have knowledge of the data.

Once it is determined that personal data are processed, the next step in the DPIA is the evaluation of risks. Risk management is necessary to determine the potential damages

or risks to which an activity is exposed. From the perspective of data protection, the analysis focuses on those threats that affect the rights and freedoms of individuals. In order to provide this analysis, we should differentiate threats depending on the risk source<sup>289</sup>:

**Table A.3**

Threats and Risk Sources

<b>Risks relating to the particularities of the service: identity management</b>	Identity theft, data theft, alteration of personal data...
<b>Risks relating to the architecture system components</b>	Malware diffusion, hardware and software failure, software manipulation...
<b>Risk relating to users</b>	Social engineering, extortion...

*Note.* Adapted from “Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems” by Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). *ARES’ 21: Proceedings of the 16<sup>th</sup> International Conference on Availability, Reliability and Security*, 132, p.5.

Each risk source materializes on a set of threats of likelihood and impact variable that determines a specific risk resulting thereof. Risk sources can include threats that materialize in risks that are not necessarily privacy risks, such as the availability [A] of the service. Therefore, we consider risks that affect the integrity [I], confidentiality [C], and authenticity [Auth] of the data. By way of example, we refer again to the analysis deployed in the project OLYMPUS.

**Risks relating to the service:** we found a contradictory result. Due to OLYMPUS distributed authentication mechanisms, the risk of masquerading identity is reduced.

---

<sup>289</sup> These examples of threats and risks sources have been extracted and adapted from the information management tool PILAR.

Nevertheless, the distributed modus operandi is not foreseen for the purpose of data encryption/decryption, increasing the risks of information leaks or unauthorized access to the data. This risk is higher than normal if we consider that the user's information would be stored in each partial IdP.

**Table A. 4**

Risks Relating to the Service

Threat	Likelihood	Impact	Risk
System /Security administration errors	Unlikely	Limited [A, I, C]	Negligible [A, I, C]
Accidental alteration of information	Unlikely	Negligible [I]	Negligible [I]
Information leaks	Relevant	Maximum [C]	Very critical [C]
Masquerading identity	Unlikely	Substantial [I, C, Auth]	Low [I, C, Auth]
Deliberate alteration of information	Unlikely	Limited [I]	Negligible [I, Auth]

*Note.* Adapted from “D3.2 Security and Privacy-aware OLYMPUS Framework Impact Assessment” by Alamillo Domingo, I., Timón López, C., & Valero Torrijos, J. (2020). *OLYMPUS Project*, p. 52.

**Risks concerning architecture system components:** the security measures implemented in the OLYMPUS design mean that even in cases where the impact on integrity and confidentiality is medium, the risk is almost negligible since the possibility of these threats materializing is minimal. However, we noticed that an increase in the number of IdPs also led to an increase in the potential spread of malware.

**Table A.5**

Architecture System Components Risks

Threat	Likelihood	Impact	Risk
Malware diffusion	Relevant	Limited [A, I, C]	High [I, C]
Software vulnerabilities	Unlikely	Substantial [I, C]	Low [I, C]
Software manipulation	Unlikely	Substantial [I, C]	Low [I, C]

*Note.* Adapted from “D3.2 Security and Privacy-aware OLYMPUS Framework Impact Assessment” by Alamillo Domingo, I., Timón López, C., & Valero Torrijos, J. (2020). *OLYMPUS Project*, p. 53.

**Risks concerning hardware components:** considering that data are encrypted for third parties, they will mainly involve risks with regard to the availability of the service. Therefore, hardware does not imply a privacy risk since the attacker will still need to decrypt information.

**Risks with regard to the connections:** OLYMPUS had foreseen the implementation of TLS connections. Hence, although risks for data privacy exist, the possibility of threat materialization is nearly negligible, and the resulting values remain low.

**Risks relating to the user:** the architecture design hampers those attacks targeting the IdP, but the resilient architecture might favor attacks on the user. In many cases, it would be enough for the user to reveal their password to lose control over their data and enable their impersonation.

Considering the results offered in the risk analysis, the final step would be the proposal of safeguards. Once the time for the implementation of safeguards has concluded, it should be reevaluated whether the technology has solved relevant risks.

In the case of OLYMPUS, we proposed with urgency two safeguards:

1. To avoid the storage of users' attributes in each partial IdP.

2. To include additional measures/ mechanisms that protect the user against social engineering techniques.

After this analysis, OLYMPUS implemented two measures to improve privacy. First, user attributes are decrypted in a distributed manner involving all partial IdPs. This enhances protection against information leaks. Second, OLYMPUS introduced multifactor authentication to overcome the limitations of using passwords as the sole authentication method.

In this phase, it must be concluded whether the technology fulfills the minimum requirements (or achieves an adequate level of privacy by design and by default) for its deployment in further scenarios, still requires modifications or safeguards, or will never achieve an adequate level of privacy.

Nevertheless, it should be noted that privacy is not an absolute value and will have to be considered conjointly with the nature and the scope of the data processed. In this sense, regarding the risks obtained from this first DPIA, it might be concluded that certain technology is suitable for processing certain types of data but not for others, which might imply a higher risk. For example, in OLYMPUS, prior to the introduction of the proposed safeguards, there was a higher risk of data theft; therefore, it might have been adequate for identification operations that do not involve the processing of sensitive information. That reasoning is precisely what makes the “second layer” necessary, a more legal analysis focusing on ensuring compliance with GDPR principles.

This second analysis should include at least the following elements. First, the lawfulness of the processing must be studied, that is to say if it is based on consent or any of the other circumstances provided in Article 6 of the GDPR. In those cases where the data processing is based on consent, the data controller shall be able to demonstrate that the user has consented and that this consent is voluntary and informed. The same would apply to the procedure to withdraw their consent. On the other hand, for those cases where the processing will not be based on user consent, the data processing must be

justified according to any of the other causes listed in Article 6.1 GDPR or whether specific regulations might be applicable (e.g., the Directive EU 2016/680 with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties).

Once the lawfulness of the data processing has been determined, other circumstances must be considered. In this sense, the data minimization principle implies processing the strictly necessary data for justified purposes, as well as limiting the storage to the strictly necessary term. In the risk analysis, examples of threats of lack of compliance with the data minimization principle could be excessive data collection or an excessive period of storage. Likewise, proportionality in the data processing must be analyzed. From this perspective, it is necessary to evaluate if the aim pursued with the data processing can be achieved by other means that imply a lower risk.

The evaluation of the proportionality in a data processing activity does not refer to a single threat, but it requires considering the specific characteristics of the data processing. A good example of these cases is, as mentioned in this thesis, the implementation of biometric authentication. Biometric data are qualified as a special category of personal data, and they present a high risk because once compromised, they will be compromised forever. However, biometric data also represent important advantages in the process of binding identity during authentication, and it is extremely convenient for end users. Consequently, in the case of implementing a technology involving the use of biometrics, in this "second layer," it would need to be justified that the technology chosen is balanced for the concrete scenario.

In addition, accuracy, integrity, transparency, and confidentiality in data processing must be studied. Pursuing Article 5.1. GDPR, accuracy in the data processing requires data to be accurate in order to assure a correct fulfillment of requests and rights, as well as the possibility of the user demanding the correction of inaccurate data, as stated in Article 16 of the same text. On the other hand, transparency in data processing can be considered from different perspectives. It means that the data subject can access their

data at any moment with no need to provide special justification, but also that the data processing must be carried out in a way that enables and facilitates eventual controls by Law Enforcement Authorities. To conclude, the confidentiality of the data implies that data must remain unknown before non-authorized parties; thus, it requires appropriate mechanisms to ensure that the person accessing the data is the authorized user. Besides, in this second assessment, we will normally have additional information, such as the staff in charge of providing the service or specific security measures adopted that could modify the initial result of our DPIA.

In the case of the OLYMPUS technology, we noted that: a) It increased the amount of data processed as it replicates the user's attributes in each partial IdP without introducing a conjoint decryption mechanism; b) It was exclusively based on passwords. The proposed safeguards mitigate the risk highlighted, leading to modification of the likelihood of information leaks and social engineering attacks in our first DPIA. Yet, the proposed architecture will replicate the user's attributes, leading to an increase in the data processed.

In this second assessment, we are referring to concrete use cases. In the research paper explaining this adapted methodology, we proposed the following invented<sup>290</sup> use case: "OLYMPUS technology is implemented to provide services of identification and identity management (identity as a service) in the context of authentication for streaming services. In this case, the data collected will be the name and surname of the user as well as their age and email address. User consent is obtained in a comprehensible and informed way. These data will be exclusively used to provide identification services and will be erased when the user decides to delete their account. The user can access their account and visualize their data at any moment. Financial information (i.e., credit card information) remains on the side of the SP. The IdP does not receive/store any information about the content visualized."

---

<sup>290</sup> The OLYMPUS projects had two very specific pilots. However, due to their complexity and given that the objective of this Annex is to provide an overview of the methodology, we have opted to maintain the invented use case we proposed in the research paper. Nevertheless, the documentation of the project can be consulted at <https://cordis.europa.eu/project/id/786725/results>

**Table A.6**

Risk Analysis in the "Second Layer"

Threat	Likelihood	Impact	Risk
Problems related to the lawfulness of data collection and processing	Unlikely	Significant	Low
Problems related to the transparency of the processing	Unlikely	Limited	Low
Problems related to excessive data collection	Unlikely	Limited	Low
Problems related to accuracy of the data	Unlikely	Significant	Low
Problems related to the retention period of the data	Unlikely	Limited	Low
Problems related to the rights of the interested subject: access, rectification, cancellation and opposition	Unlikely	Significant	Low
Unauthorized access to personal data	Relevant	Limited	Negligible
Impersonation of the user	Unlikely	Maximum	Medium
Profiling	Limited	Limited	Negligible

*Note.* Adapted from “Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems” by Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). *ARES’ 21: Proceedings of the 16<sup>th</sup> International Conference on Availability, Reliability and Security*, 132, (p.8).

Considering that financial information remains on the SP’s side (the streaming service), the nature of the data processed by the IdP limits the impact of unauthorized access. Conversely, user impersonation would enable access to financial information and the content visualized; hence, in case of materialization of this threat, the impact would be maximum. Nevertheless, the resulting risk of impersonation must be considered as medium thanks to OLYMPUS distributed architecture that reduces the likelihood of this risk in common IdPs.



This analysis can be repeated in different use cases where the OLYMPUS technology aims to be implemented. The process will be easy as the previous analysis performed with regard to the technological proposal for digital identity management has already identified and corrected drawbacks, when possible, or identified the concrete risks tied to the technological proposal.

In conclusion, this proposed methodology seeks to pre-emptively evaluate the extent to which privacy is integrated into technology. This type of approach is increasingly needed in today's landscape, where privacy risks are often embedded within technological frameworks, leading to detrimental effects on user rights. In some instances, these risks have precipitated the market withdrawal of technologies, which could have been mitigated with foresight and corrective measures. Our methodology offers a necessary adaptation, providing an early-stage analysis that can enhance the responsible deployment of technology while safeguarding user privacy.



# ANNEX B

## THE ROLE OF THE DATA CONTROLLER IN USER-CENTRIC TECHNOLOGIES: THE IDENTITY WALLETS

### Scenario Overview and Analysis

The study on the role of the data controller was triggered by the demand of the research project OLYMPUS, where the topic of data controllership had already been considered in the scope of distributed architectures. With the occasion of the publication of the eIDAS2 Proposal, we considered that it was necessary to extend this study to the scenario of identity wallets. In addition, this question was raised again in the scope of the consulting projects developed at the time of conducting this thesis. This research was published as part of a project deliverable (OLYMPUS-D6.3 Final Pilot Deployment and Evaluation of User Experience and GDPR Compliance) as well as a policy recommendation in the framework of the project CyberSecurity4Europe.

As it has been repeatedly stated in this thesis, eIDAS2 sets the legal basis to enable a transition toward new models for digital identity, placing the user at the center of the ecosystem and limiting the power of the role of IdPs. In this context, the EUDI Wallet emerges as a key piece to empower users in the control of their personal data, enabling identification and authentication processes through the request and sharing of credentials with SPs. However, this new ecosystem also displaces the IdP's responsibility in the authentication process to the wallet, insofar as, for privacy and user control reasons, the EUDI Wallet Provider should not actively participate nor have control of these processes.

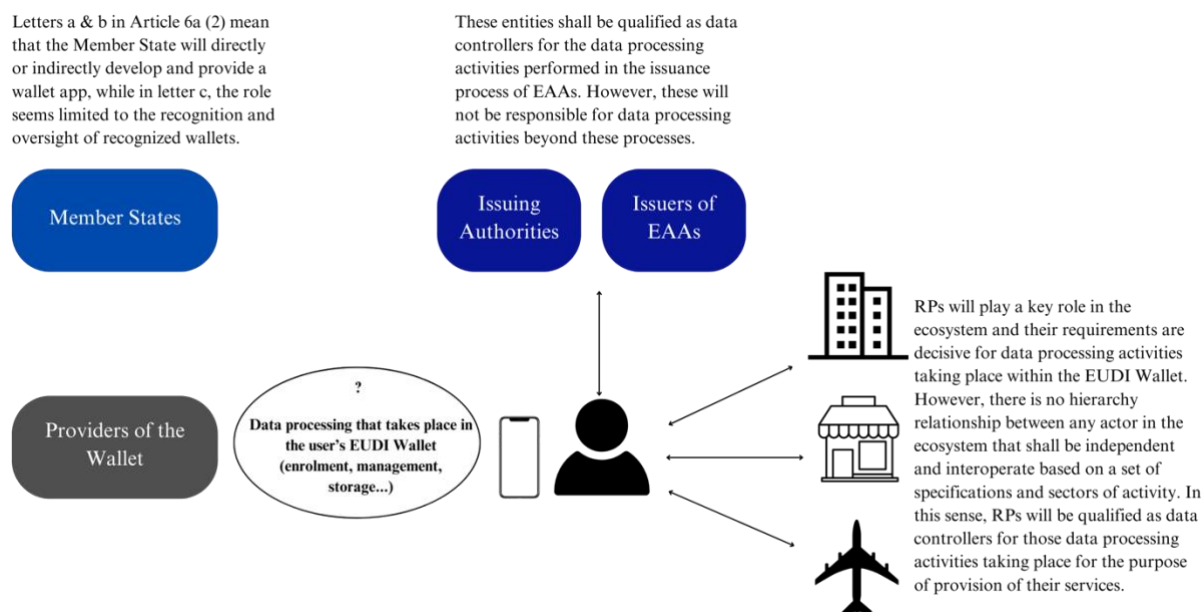
While this approach, for the reasons well-discussed in this thesis, is extremely needed nowadays, technologies involving the processing of personal data and exclusively managed under user control can challenge traditional legal notions of data controller and data processor according to the GDPR (Article 4. (7) & (8)), which are, in principle, thought for a scenario where there is a physical control of the data processed by the controller.

The EUDI Wallet ecosystem is complex and encompasses different entities holding various roles and performing a set of data processing activities with separate purposes that are necessary or contribute to the overall functioning of the ecosystem. As we have repeatedly discussed, Article 6a paragraph 1 of the eIDAS 2 Regulation establishes that “each Member State shall provide a European Digital Identity Wallet”; however, paragraph 2 of this Article provides three different possibilities for the provision of the EUDI Wallet, allowing the independent provision by private entities recognized by that Member State. Considering that the data controller qualification is purpose-based, in those scenarios where there is a direct or indirect provision by the Member State, it seems clearer that, insofar as this has the obligation and, therefore, the interest to provide it, the public entity attributed with the administrative authority that we were explaining in the last chapter of this thesis will hold a data controller role. However, this conclusion is less clear in the scenario of recognition of wallets by the Member States.

In addition, I would like to recall at this point the double nature of the EUDI Wallet, which, besides serving as an electronic identification means, would also enable the user to request, store, manage, and present very varied EAAs. At this point, we could agree that credential providers (i.e., Issuers of EAAs) shall be qualified as data controllers for the processing required in the issuance of the credential but not for the processing once the credentials have been stored in the EUDI Wallet. Similar reasonings could apply with regard to RPs, who will be responsible for the data processed in the provision of their services but not for the data processing strictly taking place in the scope of the EUDI Wallet.

Figure B.1

## Data Controller Role in the EUDI Wallet Scenario



*Note.* Adapted from “Allocating Controllorship in the European Digital Identity Wallet” by Timón López, C. & Skarmeta Gómez, A. (2021). *Cybersecurity4Europe*, (p.1).

I would like to emphasize that this is a very contextual scenario and that not all the scenarios involving an identity wallet raise these problems. In fact, in my opinion, these concerns are particularly relevant nowadays in the attempt to develop a more unified digital identity landscape with a core tool under exclusive user control. For example, we could have a scenario in which company X develops digital identity software for company Y that generates a set of specific credentials stored in a concrete wallet app. In this case, as the credentials' possibilities of use and storage are limited, it seems more logical to think that company Y could be qualified as a data controller since it is this company that has the ultimate purpose in the provision of the service. However, the case of the EUDI Wallet is different, transitioning from a mere user-centric ecosystem to a decentralized landscape where this intermediary disappears, and the tech company, as legal entity A, provides the software directly to the user in the form of a wallet app, while many entities will provide the credentials stored in the wallet that the user will

decide to share with different RPs, being these processes, out of the wallet’s provider overview and control.

## **Conclusions and Recommendations**

In this new digital identity ecosystem, I believe that the main discussion on the data controller role is articulated around the provider of the digital wallet and the user, as both subjects exercise a respective form of control over the wallet. Considering the lack of dedicated guidelines at the present moment, for the purpose of offering some light on this topic, we answered the questions proposed in the “EDPS Guidelines on the concepts of controller, processor, and joint controllership under Regulation (EU) 2018/1725” in the context of the digital identity wallet<sup>291</sup>.

---

<sup>291</sup> Please note that we are referring to a digital identity wallet in the sense of a wallet app to store identity documents, not to the EUDI Wallet precisely for the additional considerations the specific role would imply, and that could deserve more extensive research.

**Table B.1**

## Assessing the Data Controller Role in a Wallet Scenario

<b>Who has decided the purpose or outcome of the processing?</b>	The outcome of the processing is in fact decided by the designers of the wallet, who, by means of specifying its technical features, are determining the final purpose of the data processing.
<b>Who is determining the essential elements of the data processing?</b>	This is not clear in this model. The wallet designer has a limited control, also shared with the aim of the user, that is to say, the specific services in which the user authenticates and the access requirements demanded by these services.
<b>Who has a direct relationship with the data subject?</b>	The interface shown to the user, in this case, will be the wallet, which is used to access different services. In the process of accessing different services, the user might see different SP's interfaces. Nevertheless, prior data collection and management will take place in the wallet.
<b>Do users have autonomy in the processing of personal data? Or they follow the instructions of the designer of the wallet?</b>	It will depend on the margin of freedom left by the digital wallet. For example, whether we can make use of different procedures for storage or authentication, or if the users of the wallet are strictly limited by the designers thereof.
<b>Who is responsible for justifying the legal basis of the data processing?</b>	Although the user will be the one in control of their data, the designer of the wallet is the one responsible for obtaining user consent before storing user's data in the wallet.
<b>Who is interested in the result of the processing?</b>	In this case, the main interested is the user, who will be able to authenticate before the RPs. Nevertheless, the designer of the wallet, by designing the wallet for the purpose of storing and managing user data in authentication processes, is also interested in this stage of the data processing.

Note. Adapted from “D6.3 Final Pilot deployment and evaluation of User experience and GDPR compliance” by Schaarup Andersen, M., Stausholm, M, Sourla, G., Timón López, C., Alamillo Domingo, I., Valero Torrijos, J., Ponte, N., Martins, N., Conceição, F.C., García Rodríguez, J., & Martínez Alonso, N. (2021). *OLYMPUS Project* (p.83).

Considering answers provided to these questions, it seems very likely for the wallet app provider to assume a data controller role with regard to the data processing taking place in and through the wallet<sup>292</sup>. Indeed, as noted in the last question, the entities developing

<sup>292</sup> In the EUDI Wallet scenario, this aspect will strongly rely on the policy option taken by Member States, particularly in cases where the development of the wallet is outsourced to a private entity but is still under the control of the Member State.

the wallets are concerned with the final purpose of the wallet, and although the user will hold a certain control (e.g., with which parties they want to share their data), this management will ultimately rely on the application created by the developer of the wallet.

We are aware that the user has been considered to exercise a key control and, therefore, hold a data controller role in some scenarios, such as in the scenarios where they submit their transactions in blockchain because they are determining the purposes of recording a specific transaction and also the means by using that blockchain platform. Furthermore, the French Authority on Data Protection, the *CNIL*, has also recognized that where the household exemption does not apply because the purpose of the transaction is professional or commercial, users of a given blockchain can be considered to be controllers. Nevertheless, in my opinion, these reasonings cannot be applied to the scenario described because the personal data managed in the wallets will, in principle, relate to the data subject<sup>293</sup> and, depending on the purposes of the data processing, the household exemption applies (i.e., accessing social networks might be considered covered by this exemption). On the other hand, due to the inherent nature of the data subject rights, a right to information or the obligation to consent would not make sense anymore. Furthermore, the fact that the data subject authorizes the disclosure of personal information within a certain context merely signifies their agreement toward the processing, but it does not exclude the presence of another entity that determines the purposes and means of processing this data. As Van Alsenoy states (2016, p.308), “even where the individual has the ability to control the release of their personal data, and might decide the medium to be used, this does not alter the role of the collectors or handlers of the individual’s data.”

Looking for some comparatives that could potentially bring some light to the scenario discussed, we encountered some reflections made with regard to the developers of smart home devices. In this case, the authors acknowledge (Chen et al., 2020, p.285) that they

---

<sup>293</sup> A different scenario will be of minors or persons under legal guardianship. In this case, the possible role of data controller of the user of the wallet with regard to personal data relating to others must be restudied.



may well fall within the definition of controllership as they are the ones defining in technical terms how smart home data are collected and for what potential purposes. More specifically, the authors propose a classification of different types of control exercised in smart home device scenarios that we summarize in the following table:

**Table B.2**

Types of Control in Smart-Home Devices

<b>Developers of device's software</b>	Schematic control	Determine the structure and protocols mandating the communications between the components of the system
<b>Device manufactures</b>	Input control	Determine how data are collected and transmitted through network
<b>Developers of apps</b>	Interpretative control	Determine how data can be translated into actionable decisions
<b>Users</b>	Operation control	Determine what components or functionalities are enabled

*Note.* Table created from “Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption” by Chen J., Edwards L., Urquhart L., & McAuley D. (2020) *International Data Privacy Law*, 10 (4), (p.290).

If we apply this typology to the scenario subject of discussion, it can be said that the developers of the app, or in this case, the wallet, hold the biggest control over the determination of the purposes in the data processing as they transform this data into real actions or facts. It might seem questionable, though, how an entity can assume a data controller role without having actual access to the data; however, European case law has already supported this possibility<sup>294</sup>, stating that it is irrelevant whether a concerned party has actual access to the data when it comes to ascertaining its controllership. Additionally, contrary to the case of users, it is very unlikely that manufacturers of the devices or developers of the software benefit from the household exemption since there is a clear commercial involvement (regardless of their non-/for-profit status) and

<sup>294</sup> In this sense, paras. 69 & 82 in Case Fashion ID and para. 69 in Case Jehovan Todistajat.

because these manufacturers or developers are not natural persons but rather organizations.

Nevertheless, some aspects are still very challenging. Indeed, it is not clear how GDPR rights will be exercised in such a scenario or how wallet developers could comply with all GDPR obligations. At the same time, it might be argued whether imposing these obligations in such conditions is fair. On this basis, the following recommendations are proposed: 1) The European Data Protection Supervisor should issue an Opinion clarifying the application of the data controller role to the scenarios described for the issuance of the EUDI Wallet in Article 6a section 2 of the eIDAS 2 Regulation. 2) Support and provision of funding to conduct research on the impact of innovative technologies in EU regulatory frameworks.

The scenario presented above is not unique, and technologies are challenging the way traditional legal concepts are understood. It would be worth investigating more in-depth the application of traditional GDPR administrative roles (data controller/processor) to the scenarios raised by new technologies, like the EUDI Wallet, but also others, such as artificial intelligence or DLTs. Such studies would be crucial to understanding if traditional legal concepts remain applicable to new technological developments and might suggest rethinking these concepts to cover upcoming advances.

# ANNEX C

## **CURRENT ADVANCEMENTS IN THE IDENTITY OF OBJECTS: A REFLECTION ON DEVICES' IDENTIFIERS**

### **Project Description**

Although the main focus of this thesis has been the digital identity of natural persons, as part of my research labor, I conducted some additional work concerning the identity of objects in the scope of the research project ERATOSTHENES. The objective of my research was, in the framework of a DPIA, to analyze the implications of the proposed architecture for personal data and, therefore, the potential reidentification of natural persons.

The project ERATOSTHENES proposed the development of an architecture falling in the scope of Zero Trust Architectures for the secure and privacy-respectful management of interconnected devices. Its main objective was to increase trust, which indirectly enhances the security and privacy in the operation of the devices. In simple words, the increased trust is achieved through the calculation of a "trust score" at the point of enrollment and during subsequent periods via routine security checks, as well as black-or-white lists of authorized actions for a specific device. These functionalities are integrated with the potential of DLTs to record "trust levels" as well as other relevant events, enabling different parties within an organization, or even different organizations (inter-domain DLT), to verify them.

As can be easily inferred, the identification of objects or devices plays a crucial role in the operation of the architecture. The project's architecture relies on the generation of identifiers for the interconnected devices and even contemplates the possibility of issuing credentials that will be stored in the device's wallet. In principle, this identity is limited to the device itself, framed by the particularities associated with the "identity of

objects” that we suggested in the introduction of this thesis. Nevertheless, as it is known nowadays, it is more complex to separate the identity of things and natural persons, and in some cases, it might be beneficial to establish this link. At present, the main focus of digital identity has been on identifying natural persons; however, it is a natural progression to extend digital identity management to objects or things. Research on digital identity in this specific area is currently underdeveloped and deserves extensive study. Nevertheless, in this section, we aim to offer a brief overview of the key aspects that are relevant when dealing with scenarios where identity management is concerned only with objects or things.

### **Are Device Identifiers Personal Data?**

The architecture proposed in the ERATOSTHENES project, in principle, does not deal with the identities of natural persons but instead focuses on identifying objects and forming connections with the identity of legal entities (e.g., manufacturer, seller...). The identity of objects, as discussed in this thesis, is usually subject to fewer limits and constraints than the identity of natural persons. In the context of some emerging technologies, such as the DIDs, their suitability to be used for the identification of natural persons is debatable insofar as their record on a DLT could result in the impossibility of erasing personal data; however, these technologies can be particularly beneficial in the scenario of the identity of objects.

In the ERATOSHENES scenario, various identification technologies were proposed, including a physical unclonable function (PUF) acting as a digital fingerprint for the devices and the assignment of DIDs to the devices, which enable their traceability through the DLTs. Until now, we have exclusively referred to the identification of devices, which implies that, in principle, these shall not be considered personal data. However, a device does not enroll itself in a network, requiring someone, a natural person, to perform this task, associating certain data concerning this introducer or the person actually in possession of the device.

In this regard, it is possible that the introducer's certificate is exclusively limited to the identification of the legal entity (e.g., indicating that a specific smart thermometer belongs to the University of Murcia); however, it could also contain personal data, leading to two possible scenarios. In the first one, the owner and the introducer are not the same person, but it becomes necessary to reidentify the specific individual within an organization who has enrolled the device (e.g., Maria, a manager at Company X, has enrolled Device Y). In the second scenario, the owner and the introducer of the device are the same person (e.g., Mark has enrolled his own iPhone). In both scenarios, the processing of personal data will require the implementation of suitable safeguards; however, the implications are more significant in the second scenario as the identification of the individual could lead to the traceability of all actions performed by a specific individual using that device. Conversely, in the first scenario, the data processing would be "internal" and justified by the security measures and controls that are implemented within a company's policy.

Furthermore, although it might be seen as trivial, the device's identifier, by itself, should not include personal data (e.g., Maria's iPhone could easily identify the owner of the device), and its design should consider the context in which it is used (e.g., if other data are collected or could potentially be accessed and could ease identification).

My suggestion to assess this aspect was to take as a point of departure the idea that a device's identifier should not be qualified as personal data, provided certain conditions are met. These conditions refer to A29 WP criteria on the qualification of anonymous data:

- a) The device's identifier does not single out or allow singling out data that could potentially identify the user; that is to say, the device's identifiers type Maria's UMU iPhone are not used, and no additional information that could enable identification is collected. Furthermore, the device's identifiers are anonymized/pseudonymized (e.g., a MAC address is not collected directly, but it goes through a process of anonymization/pseudonymization).
- b) The device's identifier does not enable one to infer that two data sets contain information about the same individual. For instance, from the device identifier

XYZ used for workout purposes, we cannot associate it with the user's height or weight.

- c) The device's identifier does not permit deducing, with a high probability, the value of other attributes. For example, from the device identifier XYZ, one cannot deduce that the owner is 28 years old.

Therefore, my conclusion was that a device identifier does not necessarily entail the processing of personal data. However, this qualification will need to be obtained in a specific scenario once the concrete data to be processed are determined, assessing the indicated criteria one by one.

### **A Case-by-Case Analysis**

Taking as the point of departure that a device's identifier does not necessarily imply a link with the identity of a natural person nor the direct processing of personal data, I evaluated the different use cases proposed in the scope of the ERATOSTHENES project of which, I briefly summarize the key ideas here<sup>295</sup>.

The objective of the first pilot (Connected Vehicles) was to explore the potential benefits of the ERATOSTHENES security architecture within the automotive industry. More specifically, the use cases have as their core objective to ensure the security and trustworthiness of the vehicle when it interacts with other vehicles, but also with external roadside elements or even with IT infrastructure for the purpose of updating the vehicle's software. The crucial question that arises in this concrete use case is whether the vehicle's identifier could potentially identify the vehicle's driver or owner, which could result in a significant privacy risk by enabling the traceability of the individual.

To determine that the vehicle's identifier is not personal data, it is essential that the identifier used for the vehicle does not identify the natural person. In addition, by applying the A29 WP criteria:

---

<sup>295</sup> For a more detailed content, please review the ERATOSTHENES Project documentation: <https://eratosthenes-project.eu/>

- a) The vehicle's identifier should be designed to avoid singling out individuals, which could be potentially achieved by opting for a random combination of numbers and letters without including any potentially personal information.
- b) The vehicle identifier does not facilitate or enable the identification of other data sets belonging to the same individuals. Given the random mix of numbers and letters, it would be impossible to determine if other potential data sets belong to the same person.
- c) The vehicle identifier does not permit the inference of additional data. With a random combination of letters and numbers, no other data about the individual seems to be possible to infer (unless the assignation of numbers and letters correspond to known criteria, in which case, fulfillment of these criteria might need to be reconsidered).

All of these criteria were fulfilled in the scenario studied; therefore, I consider that the vehicle's identifier is not personal data. However, this is a very contextual conclusion in which we are considering a factual separation of data; that is to say, the vehicle's identifier is not linked to a concrete user account that the provider might be aware of and, from a temporary perspective, the entity responsible for enrolling the vehicle in ERATOSTHENES is the manufacturer (hence, a legal entity) prior to being owned by an individual and been provided with a registration plate. Furthermore, the type of data that could typically be processed within the ERATOSTHENES framework for digital identity management purposes might be restricted to the type of vehicle, such as its qualification as an emergency vehicle.

This conclusion, however, could not be maintained in the second pilot (Smart Health). The second pilot use cases focus on the domain of smart health to establish reliable management of devices within the ecosystem, particularly to ensure an automatic and reliable enrolment of devices, but also to enable these to interact with external devices or services by assessing their level of trust and therefore potential sharing of personal data.

From the perspective of data protection, this pilot presented a key difference compared to the previous one, that is, the association between the device's identifier and the user

account, making it very unlikely its qualification as anonymous data. This association is simply justified by the logic of the use cases and the benefits it implies. However, such classification as personal data implies the application of the GDPR, necessitating compliance with its principles.

The third pilot (Disposable IDs in Industry 4.0) leads us again to the opposite conclusion. The different use cases envisaged as part of this pilot concentrated on the industrial environment. More specifically, its objective was to create “disposable IDs,” which serve as temporary identifiers of industrial machines associated with specific permissions or authorizations. However, we are exclusively referring to the identification of concrete industrial components, so this identifier does not refer to a natural person, nor can a natural person be indirectly identified through this identifier and would not be qualified as personal data.

These conclusions are only a first step in managing the identity of objects but do not cover the whole assessment of the ecosystem. In this context, the processing of personal data could take place through the data shared by the devices themselves. However, today, it seems that the possibility that the identifier of a particular device could identify the natural person is crucial. We are currently experiencing the benefits of device identification, which in many cases make our lives easier (e.g., recovering a lost device to claiming the warranty of a certain product). However, we must also be aware that while there are benefits, there are also major risks to traceability, which require careful assessment of the likelihood of a device's identity matching or leading to a person's identity and, if necessary, who has access to it.



## ACKNOWLEDGMENTS

As I conclude this thesis, I am deeply grateful for the opportunity to conduct this research. When I started this work right after my master's degrees, I could hardly imagine how profoundly it would change my thinking. In my personal experience, I would remark two aspects of this journey. First, conducting this research has helped me to develop the ability to grasp and engage with new and complex ideas. The essence of research lies in its endless exploration, and the ability to navigate uncertainty is also crucial, especially in innovative fields, which require thinking beyond established boundaries and design novel concepts. This has taught me the importance of raising challenging questions and adopting a perspective that looks beyond the superficial to uncover deeper insights. Second, I believe this experience has sharpened my resilience. A Ph.D. is like a roller coaster, with moments of satisfaction but also periods of challenge and frustration. It truly tests your resolve and requires a high level of self-discipline. Learning that some things require time, even when you do not see the results in the short term, has been key in my personal growth. In a world where things have become essentially immediate, the lesson of patience stands out as a virtue.

I would like to thank everyone who has accompanied me on this journey. I do not have enough space to list all the names of the people who have contributed to this thesis, but I want you to know that I remember you all and that I will be eternally grateful to you. In particular, I would like to thank John Erik Setaas, Arthur van der Wees, Guy de Felcourt, Hitoshi Kokumai, Dr. Gilad Rosner, my colleagues at the University of Murcia and in the research projects, my colleagues at Explicit Selection and at the European Commission, the organizers of the research sprint at the Berkman Klein Center for Internet and Society, and all the speakers in the weekly sessions of the research sprint. On a personal level, I would like to thank all the people who have been with me during this period of my life: my family, close friends, and especially those who helped me realize that I need to be brave to show what I can do, as well as those who have had infinite patience with me as I complete this phase of my career.

As it could not be otherwise, I would especially like to thank my Ph.D. coordinators, Dr. Ignacio Alamillo Domingo and Prof. Julián Valero Torrijos, I am still impressed by their knowledge and the depth of their reflections. I would also like to thank Prof. Antonio Skarmeta Gómez for making this research possible and the opportunity he provided me to learn. Personally speaking, I also feel that I could not have been more fortunate. The quality they have as human beings and educators is simply impeccable and was decisive for me to complete this thesis. Therefore, if there is one thing I take away from this, it is that education has immense value, and when I look back from this moment, at 28 years old, I can see my parents, all the teachers, professors, mentors, and any form of educators, who have had a decisive influence in making me the person I am today. So, thank you to all the people who dedicate their lives and time to education; you have truly impacted my life. Second, thank you to all the people who are dedicated to the research journey; you are essential to changing this society for the better.