UNIVERSIDAD DE MURCIA

FACULTAD DE INFORMÁTICA

Development of a Security and Privacy Framework for the Internet of Things

Desarrollo de un Framework de Seguridad y Privacidad Aplicado al Internet de las Cosas

D. José Luis Hernández Ramos

2016

UNIVERSIDAD DE MURCIA

FACULTAD DE INFORMÁTICA

Development of a Security and Privacy Framework for the Internet of Things

Desarrollo de un Framework de Seguridad y Privacidad aplicado al Internet de las Cosas

D. José Luis Hernández Ramos

2016

Universidad de Murcia

Facultad de Informática

Desarrollo de un Framework de Seguridad y Privacidad Aplicado al Internet de las Cosas

Tesis Doctoral

Presentada por:
José Luis Hernández Ramos

Supervisada por:
Dr. Antonio Fernando Skarmeta Gómez

Murcia, Julio de 2016

University of Murcia

Faculty of Computer Science

Development of a Security and Privacy Framework for the Internet of Things

Ph.D. Thesis

Authored by:
José Luis Hernández Ramos

Supervised by:
Dr. Antonio Fernando Skarmeta Gómez

Murcia, July 2016

A Vosotros tres

Agradecimientos

Como toda tesis doctoral, ésta también es deudora de personas que me han acompañado de un modo u otro para su consecución.

A mi familia, por darme el equilibrio, por haberme apoyado siempre incondicionalmente, por su cariño, comprensión y paciencia, y por compartir cada momento de este camino conmigo.

A mi director de tesis, Antonio, por haberme dado la oportunidad de trabajar en este grupo, y por la confianza transmitida en este tiempo. Siendo un ejemplo de esfuerzo y dedicación, gracias a él, hoy tengo la posibilidad de escribir estas líneas.

A todos los compañeros que, de un modo u otro, han colaborado en el día a día desde que empecé, como Pablo, David, Jara, Leandro, Victoria, Jorge, Dan, Fábio,... para que esto sea hoy realidad.

Tampoco me quiero olvidar de Gabi, con quien me adentré hace ya unos años en este apasionante *mundillo*, así como al grupo de *IT Security* de AGT, en especial a Mario, con quienes tuve el placer de colaborar, y sobre todo de aprender, al inicio de esta etapa.

"Lo que no se empieza hoy nunca se termina mañana". Johann Wolfgang von Goethe

Contents

Capítulo 1

Resumen

1.1. Motivación y objetivos

En los últimos años, el *Internet de las Cosas* (IoT) [4] se ha convertido en un término ampliamente usado para designar una red global de objetos inteligentes interconectados, cuyos escenarios derivados promete transformar la forma en que vivimos. El concepto de IoT fue por primera vez mencionado por Kevin Ashton (cofundador del Auto-ID Center del *Massachusetts Institute of Technology* (MIT) en 1999. Sin embargo, la materialización del IoT ha sido posible en los últimos años, debido a la confluencia de diferentes avances en computación pervasiva y comunicación inalámbrica. Estos desarrollos están posibilitando que objetos físicos cotidianos sean habilitados con capacidades para detectar, procesar y enviar información, convirtiéndose en *Objetos Inteligentes* [45] que empiezan a componer nuestro entorno. Mientras que existen distintas proyecciones sobre su impacto, el IoT ha sido identificado como uno de los principales paradigmas emergentes en el ámbito de las *Tecnologías de la Información y la Comunicación* (TIC), como es indicado por la prestigiosa compañía Gartner en su último *Hype Cycle for Emerging Technologies*, que es mostrado en la Figura 1.1. En este sentido, diferentes previsiones apuntan a que esta tendencia continúe en los próximos años, hasta alcanzar la interconexión de entre 50 y 100 billones de dispositivos en 2020 [60].

El IoT posee la capacidad de desarrollar servicios innovadores basados en su naturaleza ubicua, como resultado de la visión integrada de objetos inteligentes conformando nuestra esfera personal. Sin embargo, mientras que existe una convergencia entre academia e industria sobre la necesidad de iniciativas hacia la materialización del paradigma IoT, existen numerosos aspectos divergentes sobre cómo esa consecución debe ser impulsada. Esto ha motivado la creación de diferentes iniciativas a nivel mundial, con el objetivo primordial de ofrecer un marco común que favorezca el diseño y desarrollo de estos servicios, así como su despliegue en el ámbito de las Ciudades Inteligentes [84]. En Europa, la *Alliance for Internet of Things Innovation* (AIOTI) ha sido iniciada recientemente por la Comisión Europea, como una ambiciosa iniciativa para apoyar el diálogo e interacción entre instituciones de diferentes sectores e industrias. AIOTI, impulsada por el trabajo previo del *IoT Research Cluster* (IERC), reparte sus esfuerzos en diferentes grupos de trabajo abordando diversos ámbitos del IoT, con el principal propósito de construir un ecosistema dinámico a nivel europeo.

El despliegue de escenarios IoT promete una revolución transversal a todos los ámbitos de nuestra vida cotidiana. Sin embargo, la naturaleza del IoT necesita de enfoques multidisciplinares con el fin de consensuar un entendimiento común sobre sus implicaciones. Particularmente, con el fin de desbloquear su enorme potencial y maximizar sus beneficios, es necesario minimizar los riesgos asociados derivados de sus implicaciones. En este sentido, la seguridad y la privacidad se mantienen como las principales barreras para el despliegue de IoT a gran escala [82] [29]. Por un lado, esto es debido a la necesidad de conciliar los requisitos de seguridad y privacidad de los diferentes actores del ecosistema IoT, como

[1] http://3.bp.blogspot.com/-kQnFFHP4QcI/Vd9V-az-DQI/AAAAAAAAzEc/DOEMH_7Ygjc/s640/emerging-tech-hc.png

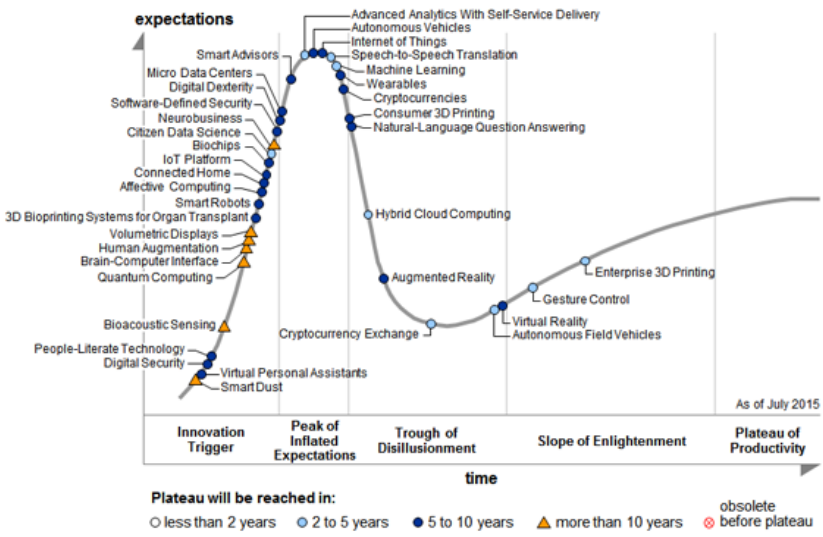

Figura 1.1: Hype Cycle de Gartner para Tecnologías Emergentes (2015)[1]

ciudadanos, gobiernos, compañías, fabricantes de dispositivos o cuerpos de regulación. Estos requisitos, contrapuestos en muchas ocasiones, son abordados generalmente mediante enfoques parciales que son acomodados a las necesidades de un escenario o caso de uso particular. Por otro lado, gran parte de los obstáculos para la adopción del IoT surge de la necesidad de acomodar las tecnologías de seguridad y privacidad actuales para ser integradas en escenarios emergentes. Estas soluciones, principalmente desarrolladas en los últimos años para entornos Web o Cloud, necesitan ser adaptadas con el fin de adecuarse a entornos donde un gran número de objetos inteligentes con alto grado de heterogeneidad estarán habilitados para intercambiar información.

Las necesidades mencionadas exigen que las preocupaciones de seguridad y privacidad en IoT sean abordadas mediante enfoques transversales y multidisciplinares, que requieren de exigentes esfuerzos desde diferentes ámbitos. Desde el punto de vista social y legal, el IoT demanda de enfoques que abarquen las necesidades de seguridad y privacidad desde diferentes perspectivas, bajo la integración de un marco legal que las soporte. Este proceso es fundamental con el fin de introducir a los ciudadanos en el ecosistema IoT, mientras que su seguridad y privacidad no estén en entredicho. Esto ha motivado la aparición de la "*Opinion 8/2014 on the Recent Developments on the Internet of Things*"[2], basada en la actual directiva "*Data Protection Directive 95/46/EC*"[3], que regula el procesamiento de datos personales dentro de la Unión Europea. Dicho documento subraya la necesidad de la aplicación de los fundamentos de *Privacidad por Diseño* (PbD) [47] en escenarios IoT, mediante la aplicación de los principios de *minimización de datos* y *limitación de propósito*. Adicionalmente, la UE ha acordado recientemente un nuevo marco legal de protección de datos bajo la *General Data Protection Regulation* (GDPR)[4], con el fin de fortalecer los derechos de privacidad de los ciudadanos, y cuya aplicación, prevista para 2018 (aunque ya vigente), derogará la anterior directiva sobre protección de datos. Desde el punto de vista técnico, el IoT requiere de enfoques de seguridad y privacidad holísticos que sean flexibles para soportar escenarios con dispositivos heterogéneos (sensores, actuadores, gateways o servidores backend), haciendo frente a los requisitos inherentes con respecto a escalabilidad, interoperabilidad y usabilidad durante todo el ciclo de vida del objeto inteligente. En este sentido, el "IoT Standardisation"Working Group (WG03) de AIOTI ofrece una lista exhaustiva de "*Organiza-*

[2]http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[3]http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[4]http://ec.europa.eu/justice/data-protection/reform/index_en.htm

ciones desarrollando estándares IoT"(SDOs), y Alianzas, como un primer paso para la definición de una Arquitectura IoT de alto nivel. Por su parte el *Internet Engineering Task Force* (IETF) ha creado grupos de trabajo (WGs) específicos con el fin de acomodar tecnologías y protocolos de seguridad y privacidad ampliamente desplegados en la actualidad, a los requisitos que son derivados de escenarios IoT.

El conjunto de requisitos y desafíos descritos anteriormente ha estimulado doblemente el desarrollo de esta tesis doctoral. En primer lugar, a pesar de las iniciativas mencionadas, la carencia de una visión unificada sobre las consideraciones de seguridad y privacidad en el paradigma IoT, ha motivado el **Diseño de un Framework Arquitectónico que abarca las principales necesidades de Seguridad y Privacidad durante el Ciclo de Vida de los Objetos Inteligentes**. En segundo lugar, la necesidad de considerar los requisitos inherentes en despliegues IoT, ha motivado el **Diseño y Desarrollo de Mecanismos de Seguridad y Privacidad y su Despliegue en diferentes escenarios IoT**, como resultado de la Instanciación de la arquitectura definida.

Asimismo, para hacer frente a las necesidades descritas, los principales objetivos que han marcado el desarrollo de esta tesis son descritos a continuación:

- O1. Análisis e identificación de los requisitos de seguridad y privacidad asociados a las diferentes fases del ciclo de vida de un objeto inteligente.
- O2. Propuesta de un framework arquitectónico para capturar las principales necesidades de seguridad y privacidad de los objetos inteligentes a lo largo de su ciclo de vida.
- O3. Análisis de propuestas existentes en la literatura abordando el problema del control de acceso en escenarios IoT para la identificación de sus limitaciones y restricciones.
- O4. Propuesta de un modelo de control de acceso distribuido y flexible mediante la consideración de aspectos dinámicos de autorización, para ser instanciado y desplegado en entornos IoT.
- O5. Propuesta de mecanismos de preservación de la privacidad y su integración en el modelo de control de acceso propuesto.
- O6. Instanciación, validación, y despliegue del modelo de control de acceso y sus extensiones en diferentes entornos IoT con el fin de demostrar su viabilidad.

El conjunto de objetivos descrito ha guiado la línea de trabajo a seguir para la consecución de esta tesis doctoral. En particular, las tareas previas de análisis y estudio sobre los requisitos de seguridad y privacidad en entornos IoT, determinaron la necesidad de diseñar una arquitectura con el fin de ofrecer una visión unificada de esta problemática. En este sentido, el framework arquitectónico diseñado se basa en el *Modelo de Referencia Arquitectónico* (ARM) derivado del proyecto europeo IoT-A [5], representando una instanciación funcional centrada en los aspectos de seguridad y privacidad a ser abordados por los objetos inteligentes durante su ciclo de vida. Asimismo, la definición de las etapas de este ciclo de vida se basa en la propuesta presentada por [35], donde las etapas de *arranque*, *operación* y *gestión* (o mantenimiento) ya son identificadas. Adicionalmente, una fase intermedia, conocida como *registro/descubrimiento* ha sido añadida con el fin de enfatizar la necesidad de infraestructuras de resolución de nombres que permitan a los objetos inteligentes ser direccionables y descubiertos por otros dispositivos para operar entre sí. Por otra parte, este análisis previo puso de manifiesto las limitaciones de los modelos de control de acceso actuales para ser desplegados en entornos IoT, así como la carencia de enfoques holísticos permitiendo la integración de mecanismos que soporten la gestión de credenciales de seguridad, considerando aspectos adicionales de privacidad. El diseño, desarrollo y despliegue de estos mecanismos representan, a su vez, el fruto de la instanciación del framework propuesto, como parte de los resultados alcanzados en esta tesis, y que son descritos en la siguiente sección.

1.2. Resultados

La consecución del conjunto de objetivos planteados al inicio de esta tesis ha dado lugar a diferentes contribuciones que han sido presentadas en diversas publicaciones recogidas en revistas, conferencias y capítulos de libro. Estas contribuciones reflejan gran parte del conjunto de resultados alcanzados durante el desarrollo de esta tesis, que son resumidos en la Tabla 1.1.

Nro.	Resultado	Objetivo	Publicación
1	Análisis y propuesta de extensión de las fases del ciclo de vida de un objeto inteligente, así como de las principales necesidades de seguridad y privacidad a ser abordadas durante cada fase identificada.	O.1	[99], [96], [92]
2	Diseño de una instanciación de un modelo de referencia de arquitectura con el fin de capturar los principales requisitos de seguridad y privacidad en cada fase del ciclo de vida.	O.2, O.3	[96], [88], [98]
3	Diseño e implementación de mecanismos de gestión de credenciales para el soporte de las necesidades de seguridad y privacidad durante la operación de los objetos inteligentes.	O.3, O.4	[96], [92], [91]
4	Diseño e implementación de un modelo de autorización distribuido y flexible a ser desplegado en entornos IoT	O.4	[93], [94]
5	Diseño e implementación de extensiones al modelo de autorización propuesto para considerar aspectos dinámicos durante el control de acceso.	O.4	[90], [89]
6	Diseño e implementación de mecanismos que preserven la privacidad durante el acceso a servicios IoT, e integración con el modelo de autorización inicialmente propuesto	O.5	[91]
7	Instanciación y validación del modelo de autorización, y sus extensiones, en diferentes casos de uso y escenarios IoT	O.6	[95], [93], [87], [91]

Tabla 1.1: Resumen de los resultados alcanzados asociados a los objetivos abordados y las publicaciones donde son recogidos

La materialización de los resultados mostrados ha sido guiada por diferentes etapas de análisis, diseño y desarrollo durante el transcurso de este trabajo. En una fase inicial, se llevó a cabo un proceso de identificación de los principales requisitos de seguridad y privacidad en entornos IoT [99], en términos de escalabilidad, interoperabilidad, flexibilidad y ligereza. Esta descripción fue entonces enriquecida posteriormente en [96], donde algunas de estas necesidades son abordadas en el caso de las fases de arranque y operación del ciclo de vida. Adicionalmente, el trabajo presentado en [98] ofrece un enfoque integrador de estos requisitos, considerando además una extensión del ciclo de vida de los objetos inteligentes propuesto por [35], mediante la inclusión de la etapa de registro/descubrimiento, previamente mencionada. El diseño inicial del framework propuesto es descrito en [88], donde se identifican los principales componentes, abarcando un subconjunto de la funcionalidad necesaria para abordar los diferentes requisitos de seguridad y privacidad de los objetos inteligentes. Asimismo, las interacciones requeridas en las etapas de arranque y operación son descritas e instanciadas en [96], como parte de las fases del ciclo de vida consideradas. Además, el trabajo propuesto en [98] recoge las principales relaciones e interacciones entre los componentes identificados, así como su intervención durante las diferentes fases del ciclo de vida.

Asimismo, el proceso de análisis de requisitos inicial evidenció la carencia de modelos de control de

acceso considerando los requisitos inherentes de entornos IoT, en términos de flexibilidad, escalabilidad y ligereza. Esto motivó la propuesta de un mecanismo de control de acceso basado en credenciales de autorización, cuya descripción es recogida en [94] [93]. El trabajo propuesto en [96] extiende este mecanismo mediante su integración con un enfoque de autorización basado en políticas, como un primer paso para automatizar el proceso de obtener tales credenciales. La propuesta presentada en [95] hace hincapié en este proceso de obtención y gestión de credenciales, presentando una instanciación en el ámbito de *edificios inteligentes*. Asimismo, el trabajo presentado en [92] ofrece una propuesta de extensión de mecanismos de bootstrapping para la obtención de tales credenciales por parte de objetos inteligentes.

La necesidad de considerar aspectos dinámicos durante el proceso de control de acceso entre objetos inteligentes es abordada en [97], donde se ofrece una visión de cómo información contextual puede ser usada por otros componentes del framework propuesto, con el fin de adaptar las decisiones de seguridad y privacidad en concordancia. Esta visión es instanciada en [90] considerando la información de localización como un factor adicional durante el proceso de control de acceso. Adicionalmente, el trabajo presentado en [89] integra el mecanismo propuesto con un modelo de confianza y reputación multidimensional basado en lógica difusa. Esta integración representa, a su vez, una instanciación del credencial de autorización inicialmente diseñado, considerando valores de confianza asociados con los objetos inteligentes, y que son comprobados dinámicamente en el instante de permitir o denegar el acceso. Adicionalmente, el trabajo presentado en [91] proporciona el diseño y desarrollo de diferentes mecanismos de preservación de la privacidad en el proceso de demostración del credencial diseñado. El diseño de estos mecanismos es planteado como una instanciación del framework propuesto donde diferentes técnicas son analizadas y comparadas cualitativamente.

Finalmente, la validación del modelo de control de acceso, así como sus extensiones previas, es descrita en las diferentes publicaciones referenciadas. Sin embargo, cabe destacar que el trabajo desarrollado durante esta tesis ha sido adicionalmente instanciado y desplegado en el ámbito de dos proyectos europeos, cuyo foco es el diseño y desarrollo de soluciones de seguridad y privacidad en escenarios IoT. En particular, el modelo de autorización propuesto en esta tesis doctoral, junto con los mecanismos de gestión de credenciales previamente descritos, han sido integrados bajo el amparo del proyecto SMARTIE[5]. Adicionalmente, una instanciación de este modelo ha sido desarrollada durante el proyecto SocIoTal[6] [87], con el fin de acomodar los mecanismos propuestos para su integración con diferentes componentes de la plataforma FI-WARE[7].

La descripción de estos resultados proporciona una visión general de las principales líneas de trabajo abordadas durante esta tesis doctoral. Esta visión es extendida de forma más detallada en el Capítulo 3, que ofrece una descripción pormenorizada de los principales procesos involucrados en la materialización de los resultados descritos.

1.3. Conclusiones y Trabajos Futuros

El paradigma IoT representa el siguiente paso de la era digital, en el que el diseño y desarrollo de nuevas aplicaciones y servicios debe abordar los requisitos derivados de la inclusión de objetos físicos en la infraestructura de Internet. El enorme potencial del ecosistema resultante puede verse amenazado si las preocupaciones de seguridad y privacidad no son acometidas por enfoques holísticos, que aborden tales necesidades durante todo el ciclo de vida de los objetos inteligentes conformando estos escenarios.

Esta problemática ha sido abordada en esta tesis doctoral mediante la Definición de un Framework Arquitectónico para la gestión de aspectos de Seguridad y Privacidad durante el Ciclo de Vida de los Objetos Inteligentes. El diseño de esta arquitectura es el resultado del análisis teórico y revisión bibliográfica de los principales aspectos de seguridad y privacidad a ser abordados en el paradigma

[5] http://www.smartie-project.eu/
[6] http://www.sociotal.eu/
[7] http://www.fiware.org/

IoT. El framework resultante está basado en el *Modelo de Referencia de Arquitectura* (ARM) del proyecto IoT-A[8], representando una instanciación de arquitectura de referencia con un fuerte énfasis en dichos aspectos. En este sentido, este framework puede ser, a su vez, instanciado por otras iniciativas abordando escenarios o casos de uso concretos, donde los aspectos de seguridad y privacidad deban ser tratados durante las principales fases del ciclo de vida.

De hecho, partiendo de este análisis teórico, la instanciación del framework propuesto ha resultado en la definición de distintos mecanismos de seguridad y privacidad, como parte de los resultados obtenidos en esta tesis doctoral. En particular, las necesidades de un modelo de control de acceso que aborde los requisitos de escalabilidad, ligereza e interoperabilidad en entornos IoT, han motivado el desarrollo de un mecanismo de autorización considerando aspectos y tecnologías concretas para su adecuación a tales escenarios. Este mecanismo se basa en la definición de credenciales de autorización ligeros y ha sido integrado con enfoques de control de acceso basados en políticas. Los resultados derivados de la validación de este mecanismo no son solamente recogidos en diferentes publicaciones, sino que provienen de su desarrollo y despliegue en el ámbito de dos iniciativas europeas centradas en aspectos de seguridad y privacidad en IoT: SocIoTal y SMARTIE, en las que ha participado el Grupo de Sistemas Inteligentes y Telemática de la Universidad de Murcia.

A partir de este modelo de control de acceso propuesto, diferentes extensiones han sido planteadas con el fin de abordar cuestiones transversales a este problemática. En particular, el proceso de gestión de los credenciales de autorización ha sido acometido mediante la propuesta de extensión a protocolos de acceso a la red, para posibilitar la obtención de dichos credenciales por parte de un objeto inteligente. En particular, la extensión propuesta para el protocolo *Protocol for Carrying Authentication for Network Access* (PANA) está siendo actualmente desplegada en el proyecto SMARTIE, que tiene el propósito de ofrecer un enfoque para la gestión de la seguridad y la privacidad durante las etapas de arranque y operación de un objeto inteligente. Asimismo, el modelo inicialmente propuesto ha sido extendido mediante la consideración de dos líneas de trabajo complementarias. Por un lado, la inclusión de aspectos dinámicos que pueden ser usados durante el procedimiento de control de acceso, ha motivado la necesidad de considerar información contextual como un factor en el momento de permitir o denegar el acceso a un determinado servicio. Así, este modelo de control de acceso ha sido integrado con un sistema de localización basado en medidas de campo magnético para ser usado en edificios habilitados con capacidades IoT. Por otro lado, las necesidades de privacidad han sido abordadas mediante la integración de este modelo con diferentes mecanismos para la demostración de posesión del credencial, mientras la privacidad del objeto solicitante es preservada. En concreto, estos mecanismos se basan en el uso de criptografía basada en identidad, criptografía basada en atributos, y sistemas de credenciales anónimos, que son planteadas como opciones alternativas y comparadas en diseño y rendimiento.

La consecución de los objetivos planteados al inicio de esta tesis a partir de los resultados conseguidos, y su despliegue bajo el amparo de dos proyectos europeos, demuestra la viabilidad, aplicabilidad y practicidad de los mecanismos desarrollados durante esta tesis doctoral. Asimismo, la instanciación del framework propuesto determina un excelente punto de partida para el diseño y desarrollo de futuros trabajos que ahonden en diversas cuestiones, que son derivadas de la necesidad de considerar un enfoque holístico para la gestión de aspectos de seguridad y privacidad abarcando todo el ciclo de vida de los objetos inteligentes.

En particular, una de las principales líneas de trabajo futuro nace de la integración del modelo de control de acceso propuesto en una infraestructura de resolución de nombres global, con el fin de permitir un descubrimiento selectivo de los servicios ofrecidos por los objetos inteligentes. Este mecanismo puede ser visto con un nivel adicional de autorización previo al control de acceso. Mientras que otras iniciativas previas, como el proyecto IoT6[9], propusieron la aplicación de enfoques de resolución de nombres en entornos IoT, actualmente existe una carencia de soluciones que tengan aspectos de seguridad y privacidad durante los procesos de registro y descubrimiento de objetos inteligentes, como fases fundamentales de su ciclo de vida.

[8] http://www.iot-a.eu/public
[9] http://iot6.eu/

Por otra parte, dada la escala y el dinamismo de los escenarios IoT, la aplicación de mecanismos de seguridad y privacidad involucrando grupos de objetos inteligentes se mantiene como un aspecto desafiante en la actualidad. Esta problemática ya es reflejada en la arquitectura propuesta, en la que se ha definido un componente funcional específicamente implicado en los aspectos de seguridad y privacidad para la gestión de grupos de entidades. Estos grupos pueden ser adicionalmente creados de forma oportunista, por ejemplo, basándose en proximidad física y mediante el uso de tecnologías de comunicación de corto alcance. De hecho, este componente ya ha sido instanciado en el ámbito del proyecto SocIoTal mediante la aplicación de criptografía basada en atributos, en el caso de smartphones, cuyo desarrollo ha sido integrado con otros componentes de la plataforma europea FI-WARE. En este sentido, el principal desafío subyacente proviene de la extensión de estos mecanismos de grupos en el caso de dispositivos con restricciones de recursos, cuya materialización ha despertado el interés de diferentes grupos de trabajo del IETF como el *Constrained RESTful Environments* (CoRE) o el *Authentication and Authorization for Constrained Environments* (ACE).

Finalmente, otra prometedora línea de investigación nace de la necesidad de considerar la información contextual como parte fundamental de los aspectos de seguridad y privacidad en IoT. En tales escenarios, los objetos inteligentes son desplegados físicamente en entornos cuyas condiciones son cambiantes, y por consiguiente, la información percibida de su entorno puede permitir al objeto inteligente la aplicación de mecanismos de seguridad y privacidad adaptativos a tales condiciones. Aunque durante el desarrollo de esta tesis se ha integrado información de localización, como parte de esta información contextual, para enriquecer el modelo de control de acceso propuesto, surge la necesidad de considerar otros factores de contexto que ayuden los objetos inteligentes a tomar de decisiones de seguridad y privacidad más efectivas de forma automatizada.

1.4. Estructura de la Tesis

La presentación de esta tesis doctoral se enmarca dentro del modelo de compendio por publicaciones. Con el fin de satisfacer los requisitos de la normativa vigente establecida para este tipo de tesis doctorales, el capítulo actual presenta un resumen en castellano de los principales aspectos motivadores, así como una visión general de cómo los objetivos planteados al inicio han sido alcanzados mediante el conjunto de resultados descrito. Asimismo, por ser una tesis doctoral con mención de doctorado internacional, el Capítulo 2 ofrece una versión en inglés del resumen presentado en este capítulo. Por su parte, el Capítulo 3 tiene el propósito de ofrecer una visión más detallada de la arquitectura propuesta, así como de los mecanismos diseñados y desarrollados como resultado de la instanciación de dicha arquitectura. Además, una descripción pormenorizada de estos mecanismos es proporcionada en el Capítulo 4, donde se recogen las publicaciones componiendo esta tesis doctoral, y que son resumidas a continuación:

El artículo con título *DCapBAC: embedding authorization logic into smart things through ECC optimizations* describe la necesidad de dotar de mecanismos de autenticación y autorización en dispositivos con restricciones en recursos, debido a la integración de este tipo de dispositivos en la infraestructura de Internet. Tras la descripción de las limitaciones y restricciones del trabajo relacionado en esta área, se detalla el modelo de autorización propuesto para ser desarrollado en escenarios del IoT. Además, este modelo es integrado con una versión optimizada de criptografía de curva elíptica, proporcionando resultados prácticos y realistas en dispositivos restringidos.

El artículo *A soft computing based location-aware access control for smart buildings* presenta la necesidad de considerar aspectos físicos en la toma de decisiones de control de acceso, ante la naturaleza ubicua planteada en escenarios del IoT. Para ello, este trabajo presenta una extensión del trabajo previo, con el fin de diseñar un mecanismo de control de acceso, cuyas decisiones de autorización están basadas en datos de localización y credenciales de acceso. Específicamente, este mecanismo hace uso de un sistema de localización basado en medidas de campo magnético, que es combinado con credenciales de autorización para ser desplegado en el contexto de edificos inteligentes. Adicionalmente, este sistema es evaluado en un edificio de la Universidad de Murcia, validando la precisión del sistema

de localización, así como el tiempo de procesamiento durante el acceso.

El trabajo *SAFIR: Secure access framework for IoT-enabled services on smart buildings* presenta los requisitos de seguridad que deben ser tenidos en cuenta en el ámbito de edificios inteligentes. Además, se describe la necesidad de considerar arquitecturas abstractas que sean capaces de capturar los requisitos de seguridad y privacidad en estos escenarios. En este sentido, este trabajo presenta el diseño de un framework de seguridad y privacidad que se abstrae de las tecnologías subyacentes, y que es instanciado en el contexto de edificios inteligentes que son habilitados con tecnologías del IoT. En particular, esta instanciación se basa en el uso de mecanismos de descubrimiento de objetos inteligentes dentro de un edificio, así como su integración con procesos para la obtención y uso de credenciales de autorización en el acceso a dichos dispositivos.

Por último, el trabajo titulado *Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things* presenta la necesidad de integrar mecanismos que preserven la privacidad durante el control de acceso en escenarios IoT, así como los requisitos derivados de tal integración. Para ello, el modelo de autorización propuesto inicialmente es extendido con diferentes mecanismos de preservación de la privacidad, que son comparados cualitativamente, así como en rendimiento. Adicionalmente, estos mecanismos son enmarcados en la arquitectura abstracta de seguridad y privacidad presentada en trabajos previos, y son presentados como una instanciación de tal arquitectura.

Adicionalmente, el Capítulo 5 incluye las referencias bibliográficas que son usadas en este documento. Así, la Sección 5.1 comprende la lista completa de publicaciones referenciadas, mientras que la Sección 5.2 ofrece la lista de las diferentes publicaciones que han sido elaboradas durante el desarrollo de esta tesis doctoral.

Chapter 2

Abstract

2.1. Motivation and Goals

In recent years, the *Internet of Things* (IoT) [4] has become a widely used term to describe a global network of interconnected smart objects, whose envisioned scenarios promise to transform our everyday lives. The concept of IoT was mentioned for the first time by Kevin Ashton (co-founder of the *Massachusetts Institute of Technology* (MIT)'s Auto-ID Center in 1999. However, its realization has been possible in recent years due the confluence of different advances in pervasive computing and wireless communications. These developments are enabling physical devices with capabilities to sense, process and communicate information, becoming *Smart Objects* [45] that start to compose our surrounding environment. While there are different projections on the IoT impact, this has been identified as one of the major emerging paradigms in the area of *Information and Communications Technology* (ICT), as indicated by the renowned company Gartner in its last *Hype Cycle for Emerging Technologies*, which is shown in Figure 2.1. In this sense, different predictions suggest that this trend will continue in the coming years, reaching the interconnection among 50 and 100 billion devices in 2020 [60].

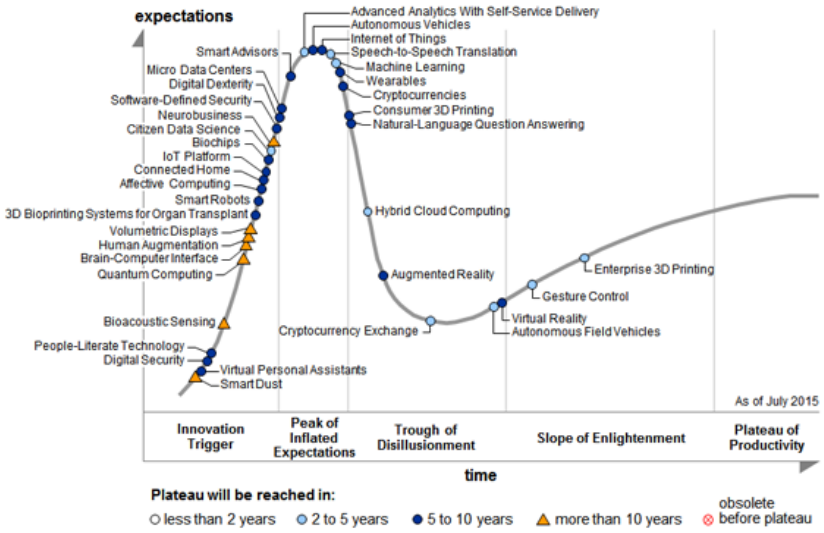

Figure 2.1: Gartner's 2015 Hype Cycle for Emerging Technologies[1]

The IoT foundations provide the ability to develop innovative services based on its ubiquitous nature, as a result of the integrated view of smart objects composing our personal sphere. However, while there is a convergence between academia and industry on the need for initiatives towards the realization of the IoT paradigm, there are different divergent aspects about how this accomplishment should be driven. This has led to the creation of several worldwide initiatives, with the main goal to provide a common framework to encourage the design and development of these services, as well as their deployment in the context of Smart Cities [84]. In Europe, the *Alliance for Internet of Things Innovation* (AIOTI) has been recently launched by the European Commission as an ambitious initiative to support the dialogue and interaction among institutions in different sectors and industries. The AIOTI, mainly driven by the previous work of the *IoT Research Cluster* (IERC), distributes its efforts in various working groups addressing different IoT areas, in order to build a dynamic ecosystem at European level.

The deployment of IoT scenarios promises a cross revolution to all areas of our everyday lives. However, the inherent nature of the IoT requires multidisciplinary approaches in order to agree on a common understanding of its implications. Particularly, in order to unlock its huge potential and maximize its benefits, it is necessary to minimize the risks associated to its implications. In this sense, security and privacy are currently considered as the main barriers for the IoT deployment on a broad scale [82] [29]. On the one hand, this is due to the need to reconcile the security and privacy requirements coming from the different IoT stakeholders, such as citizens, governments, companies, device manufacturers and regulatory bodies. These requirements, often conflicting, are generally addressed by partial approaches that are accommodated to the needs of a particular scenario or use case. On the other hand, many of the obstacles for the adoption of IoT arises from the need to adapt existing security and privacy technologies to be integrated into emerging scenarios. These solutions, mainly designed for Web or Cloud environments in recent years, need to be tailored to environments where a large number of heterogeneous smart objects will be enabled to exchange information.

These needs require that security and privacy concerns in IoT are to be addressed by cross and multidisciplinary approaches, which demand for tough efforts from different areas. From a social and legal point of view, the IoT requires approaches covering security and privacy needs from different perspectives under the integration of a legal framework to support them. This process is essential in order to introduce citizens in the IoT ecosystem, while their security and privacy are not compromised. Indeed, this has led to the conception of the *"Opinion 8/2014 on the Recent Developments on the Internet of Things"*[2], based on the current *"Data Protection Directive 95/46/EC"*[3], which regulates the processing of personal data within the EU. This document highlights the need for the application of the *Privacy by Design* (PbD) [47] foundations on IoT scenarios, by applying *data minimization* and *purpose limitation* principles. In addition, the EU has recently agreed on a new legal framework for data protection under the *General Data Protection Regulation* (GDPR)[4], in order to strengthen citizens' privacy rights, and whose implementation, scheduled for 2018 (although already applicable), will repeal the previous directive on data protection. From a technical point of view, the IoT requires holistic security and privacy approaches with a high degree of flexibility to support scenarios with heterogeneous devices (sensors, actuators, gateways or backend servers) interacting among each other, facing the inherent requirements regarding scalability, interoperability and usability throughout the life cycle of the smart object. In this sense, the AIOT "IoT Standardisation" Working Group (WG03) provides an exhaustive list of IoT *"Standards Developing Organizations"* (SDOs), and Alliances, as a first step towards the definition of a high level IoT Architecture. Furthermore, the *Internet Engineering Task Force* (IETF) has established specific working groups (WGs) intended to accommodate widely deployed security and privacy technologies and protocols to the requirements of IoT scenarios.

The set of requirements and challenges described above has doubly stimulated the development of this thesis. Firstly, in spite of the already mentioned initiatives, the lack of a unified vision on security and privacy considerations in the IoT paradigm has motivated the **Design of an Architectural**

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[3] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[4] http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Framework encompassing the main Security and Privacy needs during the Lifecycle of Smart Objects. Secondly, the need to accommodate security and privacy mechanisms to the inherent requirements of IoT deployments has motivated the **Design and Development of Security and Privacy Mechanisms and their Deployment in different IoT scenarios**, as a result of the proposed architectural framework instantiation.

Furthermore, to cope with the needs previously described, the main objectives that have determined the course of this thesis are described below:

- O1. Analysis and identification of security and privacy requirements associated to the different stages of the lifecycle of a smart object.
- O2. Proposal of an architectural framework to capture the main security and privacy needs of smart objects throughout their lifecycle.
- O3. Analysis of existing proposals in the literature addressing access control issues in IoT scenarios to identify their limitations and restrictions.
- O4. Proposal of a flexible and distributed access control model by considering dynamic authorization aspects, to be instantiated and deployed in IoT environments.
- O5. Proposal of privacy-preserving mechanisms and their integration into the proposed access control approach.
- O6. Instantiation, deployment and validation of the access control model and its extensions in different IoT environments to demonstrate its feasibility.

This list of objectives has guided the work line to be followed during this thesis. Specifically, through the analysis of security and privacy requirements in IoT, the need for the design of an architectural framework to provide a unified view of this problem was identified. In this sense, the proposed framework is based on the *Architectural Reference Model* (ARM), derived from the European project IoT-A [5], representing a functional instantiation focused on security and privacy aspects to be addressed by smart objects during their lifecycle. Furthermore, the definition of the different stages composing this lifecycle is based on the work proposed by [35], in which *bootstrapping*, *operation* and *management* (or maintenance) stages are already identified. Additionally, an intermediate phase, known as *registration/discovery* has been added in order to emphasize the need for name resolution infrastructures to enable smart objects to be addressable and discovered by other devices to interoperate. In addition, this analysis laid bare the limitations of the current access control models to be deployed in IoT environments, as well as the lack of holistic approaches allowing the integration of mechanisms to support the management of security credentials, by considering privacy concerns. Based on that, the design, development and deployment of these mechanisms represent, in turn, the result of the proposed framework instantiation, as part of the outcomes achieved during this thesis, which are described in the next section.

2.2. Results

The achievement of the objectives that were set out at the beginning of this thesis has led to different contributions that have been presented in several publications contained in journals, conferences and book chapters. These contributions reflect most of the results achieved during the development of this thesis, which are summarized in Table 2.1.

The realization of these results has been driven by different analysis, design and development stages during the course of this work. As a preliminary step, the identification of the key security and privacy requirements in IoT environments was carried out [99], in terms of scalability, interoperability, flexibility and lightness. This description was then enriched in [96], where some of these needs are addressed in the case of bootstrapping and operation stages of the lifecycle. In addition, the work

Nr.	Result	Objective	Publication
1	Analysis and proposal for extending the smart objects' lifecycle stages, and identification of the main security and privacy needs to be addressed during each phase.	O.1	[99], [96], [92]
2	Design of an instantiation from an architecture reference model in order to capture the main security and privacy requirements of each lifecycle's stage.	O.2, O.3	[96], [88], [98]
3	Design and implementation of credentials management mechanisms to support the security and privacy needs during the operation of smart objects.	O.3, O.4	[96], [92], [91]
4	Design and implementation of a flexible and distributed authorization model to be deployed in IoT environments.	O.4	[93], [94]
5	Design and implementation of extensions to the proposed authorization model to consider dynamic aspects for an enriched access control mechanism.	O.4	[90], [89]
6	Design and implementation of privacy-preserving mechanisms during the access to IoT services, and their integration with the authorization model initially proposed.	O.5	[91]
7	Instantiation and validation of the authorization model and its extensions on different IoT use cases and scenarios	O.6	[95], [93], [87], [91]

Table 2.1: Summary of the achieved results associated to the objectives and publications in which they are presentd

presented in [98] provides an integrated approach for these requirements, by considering an extension of the lifecycle proposed by [35], through the inclusion of the aforementioned registration/discovery stage. The initial design of the proposed framework is described in [88], where the main components are identified, covering a subset of the required functionality to address the different security and privacy concerns of smart objects. In addition, the interactions among these components for bootstrapping and operation are described and instantiated in [96]. Furthermore, the work proposed in [98] shows the main relationships and interactions among the identified components and their intervention during the different stages of the lifecycle.

Moreover, the initial requirements identification process revealed the lack of access control models considering the inherent requirements of IoT environments, in terms of flexibility, scalability and lightness. This motivated the proposal on an access control mechanism based on authorization credentials, whose description is contained in [94] [93]. The work proposed in [96] extends this initial mechanism through the integration with a policy-based authorization approach, as a first step to automate the process of obtaining such credentials. The proposal presented in [95] emphasizes the need for credentials managing and provisioning procedures, by defining an instantiation in the context of *smart buildings*. The work presented in [92] also provides of a proposal to extend bootstrapping protocols to enable smart objects to obtain such credentials.

The need to consider dynamic aspects during access control procedures between smart objects is addressed in [97], in which an overview about how contextual data can be used by other functional components of the proposed framework is provided, in order to adapt security and privacy decisions accordingly. This approach is instantiated in [90] by considering location information as an additional aspect for the access control process. In addition, the work presented in [89] integrates the proposed authorization approach with a multidimensional trust and reputation model based on fuzzy logic. This integration represents, in turn, an instantiation of the authorization credential initially designed,

by considering trust values associated to smart objects that are dynamically checked when the token is evaluated by the target device. In addition, the work presented in [91] provides the design and development of different mechanisms to prove the possession of the authorization credential in a privacy-preserving way. The design of these mechanisms is proposed as an instantiation of the proposed framework where different techniques are compared and analyzed qualitatively.

Finally, the validation of the proposed access control model, as well as its extensions, is described within the different referenced publications. However, it should be pointed out that the work developed during this thesis has been further instantiated and deployed in the field of two European projects, whose focus is the design and development of security and privacy solutions on IoT scenarios. In particular, the proposed authorization model, along with the credential management mechanisms previously mentioned have been integrated under the umbrella of the SMARTIE[5] project. In addition, an instantiation of this model has been developed during the SocIoTal[6] project [87], in order to accommodate the proposed mechanisms to be integrated with different components of the European FI-WARE platform[7].

The previous description provides an overview of the main work spaces that have been covered during this thesis. This summary is extended in Chapter 3, which provides a thorough description of the main processes involved during the realization of the described results.

2.3. Conclusions and Future Work

The IoT paradigm represents the next step of the digital age, in which the design and development of new applications and services need to tackle the requirements arising from the inclusion of physical devices into the Internet infrastructure. Indeed, the enormous potential of the resulting ecosystem may be threatened, if security and privacy concerns are not undertaken by holistic approaches that address such needs throughout the lifecycle of smart objects making up these scenarios.

The set of requirements previously described has been addressed in this thesis through the Definition of an Architectural Framework for managing Security and Privacy aspects during the Lifecycle of Smart Objects. The design of this framework is the result of the theoretical analysis and literature review regarding the main security and privacy concerns to be addressed in the IoT paradigm. The resulting framework is based on the *Architectural Reference Model* (ARM) from the IoT-A[8] project, representing an instantiation of it with a strong emphasis on those aspects. In this sense, this framework can be, in turn, instantiated by other initiatives tailored to specific IoT scenarios or use cases, where security and privacy must be preserved.

Indeed, based on this theoretical analysis, the instantiation of the proposed framework has resulted in the definition of different security and privacy mechanisms, as part of the results obtained in this thesis. In particular, the need for a suitable access control model addressing scalability, lightness and interoperability requirements of IoT environments, has led to the development of an authorization mechanism considering aspects and specific technologies for its adaptation to such scenarios. This mechanism is based on the definition of lightweight authorization credentials and has been integrated with a policy-based access control approach. The results from the validation of this mechanism are not only included in different publications, but come from its development and deployment in the field of two European initiatives focused on security and privacy issues in IoT: SocIoTal and SMARTIE, in which the Intelligent Systems and Telematics of the University of Murcia has participated.

From the access control model initially proposed, different extensions have been set out in order to address cross-cutting issues to this problem. In particular, the authorization credentials management process has been undertaken through the extension of network access protocols to enable smart objects to be provisioned with such credentials. Indeed, the proposed extensions are being currently deployed

[5] http://www.smartie-project.eu/
[6] http://www.sociotal.eu/
[7] http://www.fiware.org/
[8] http://www.iot-a.eu/public

under the SMARTIE project, which aims to provide an approach for managing security and privacy aspects during bootstrapping and operation stages of smart objects. In addition, the initial approach has been extended by considering two complementary work lines. On the one hand, the inclusion of dynamic aspects that can be used during the access control process, has motivated the need for considering contextual information as an additional factor to be considered during the access control evaluation. Thus, the initial authorization model has been integrated with an indoor location system based on magnetic field measurements to be used on IoT-enabled buildings. On the other hand, privacy concerns have been addressed by integrating this model with different mechanisms for proving the possession of the authorization credential, while the requesting smart object's privacy is preserved. In particular, these mechanisms are based on the use of identity-based cryptography, attribute-based cryptography and anonymous credential systems, which have been designed as alternative options and compared in terms of design and performance.

The achievement of the objectives set out at the beginning of this thesis, and the instantiation of the designed mechanisms under the umbrella of two European projects, demonstrates the feasibility, applicability and practicality of the proposed approaches. Furthermore, the instantiation of the proposed architectural framework constitutes an excellent starting point for the design and development of additional mechanisms that delve into different issues, which are derived from the need to consider a holistic approach for managing security and privacy issues through the whole lifecycle of smart objects.

In particular, one of the main future work areas stems from the integration of the proposed access control model with a global name resolution infrastructure, in order to allow a selective discovery of services provided by smart objects. This mechanism can be considered as an additional authorization level previous to the access control itself. While other initiatives, such as the IoT6 project[9], already proposed the application of name resolution approaches for IoT environments, currently there is a lack of solutions considering security and privacy aspects during registration and discovery processes of smart objects, which are jointly considered as a required stage previous to the operation phase within the lifecycle.

Moreover, given the scale and dynamism of IoT scenarios, the application of security and privacy mechanisms involving groups of smart objects remains as a challenging aspect. These groups may be further opportunistically created, for example, based on physical proximity and using short range communication technologies. Indeed, this issue is already reflected in the proposed framework, through the definition of a functional component that is specifically to manage security and privacy aspects within coalitions of smart objects. This component has been already instantiated in the scope of the SocIoTal project by applying attribute-based cryptography, in the case of smartphones, whose development has been integrated with different components of the European platform FI-WARE. In this sense, the main underlying challenge comes from the extension of these security mechanisms for groups of devices with tight resource constraints, which has attracted the interest from several IETF working groups, such as the *Constrained RESTful Environments* (CoRE) or the *Authentication and Authorization for Constrained Environments* (ACE).

Finally, another promising research line arises from the need to consider contextual information as a fundamental aspect of the security and privacy concerns in IoT. In such scenarios, smart objects are physically deployed in environments where conditions are dynamic and changeable. Therefore, the information that is sensed by smart objects from their surrounding environment may allow to adapt their security and privacy preferences according to such conditions. While the proposed access control model has been enriched with location data, as one of the main factors of such contextual information, it still arises the need to consider a more comprehensive set of contextual features to help smart objects to make security and privacy decisions in a more effective and automated way.

[9] http://iot6.eu/

2.4. Thesis structure

The presentation of this thesis is framed under the publications compendium model. In order to satisfy the requirements of the current regulation that is established for this type of thesis with International mention, the current chapter provides the English version of the abstract already provided in the Chapter 2. Therefore, as in the previous chapter, this includes the main motivating aspects of this thesis, as well as an overview about the realization of the goals initially set out through the description of different results. Furthermore, Chapter 3 is intended to provide a more detailed view of the proposed architectural framework, and the set of mechanisms that has been designed and developed as a result of the instantiation of this framework. In addition, a detailed description of these mechanisms is provided in Chapter 4, where the set of publications composing this thesis is included, and they are summarized below:

The paper entitled *DCapBAC: embedding authorization logic into smart things through ECC optimizations* describes the need to provide authentication and authorization mechanisms on devices with resource constraints due to the integration of physical objects in the Internet. After a description of the main limitations and restrictions of the related work in this area, the proposed authorization model intended to be deployed on IoT scenarios is detailed. In addition, this model is integrated with an optimized version of elliptic curve cryptography, providing feasible results on constrained devices.

The paper with the title *A soft computing based location-aware access control for smart buildings* introduces the need to consider dynamic aspects when making access control decisions, given the ubiquitous nature of IoT use cases. Towards this end, this paper presents an extension of the previous work, in order to design an access control mechanism whose authorization decisions are based on a combination of access credentials and location data. Specifically, this mechanism makes use of a location system based on magnetic field measurements, which is combined with authorization credentials to be deployed in the context of smart buildings. Additionally, this system is evaluated within a building at the University of Murcia, validating the accuracy of the location system and processing time during the access.

The paper with title *SAFIR: Secure access framework for IoT-enabled services on smart buildings* presents some of the main security requirements that must be taken into account in the scope of smart buildings. In addition, it provides a description about the need to consider abstract architectures that are able to capture the security and privacy requirements in these scenarios. In this sense, the paper provides the design of a security and privacy framework that is abstracted from the underlying technologies, and is instantiated in the context of IoT-enabled smart buildings. In particular, this instantiation is based on the use of discovery mechanisms of smart objects within a building, as well as their integration with processes for obtaining and using authorization credentials when accessing to such devices.

The paper with title *Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for M2M-Enabled Internet of Things* presents the need to integrate privacy-preserving mechanisms for the access control process in IoT scenarios, as well as the requirements that are derived from such integration. To do this, the initially proposed authorization model is extended with different mechanisms, which are compared in design and performance. Additionally, these mechanisms are framed within the architectural framework presented in previous works, and designed as an instantiation of such framework.

In addition, Chapter 5 includes the references that are used in this document. Thus, Section 5.1 includes the complete list of referenced publications, while Section 5.2 provides the list of the different publications that have been elaborated during the development of this thesis.

Chapter 3

Introduction

Since the birth of the Internet, security and privacy have represented recurring concerns in the design and development of new services and applications. With the advent of the so-called *Internet of Things* (IoT) era [4], these issues take a broader dimension due to the inclusion of physical devices or *things* in the Internet infrastructure. Significant efforts from academia and industry are promoting the emergence of innovative and valuable services to be leveraged by society in future smart cities, enabling new business opportunities for organizations. However, unlike the current Internet, IoT environments are expected to be formed by heterogeneous devices and potentially managing particularly sensitive data. As a consequence, security and privacy are becoming key factors for the deployment of new applications, since IoT stakeholders will only accept these deployments if these are based on secure, trustworthy and privacy-preserving infrastructures.

The IoT promotes global interconnectivity through the application of recent wireless communication technologies and pervasive computing, turning things into real *smart objects*. Therefore, traditional security and privacy enterprise-centric approaches and user-centric solutions need to be moved to a *user-managed smart object-centric* view, while interests from different IoT stakeholders (such as citizens, governments, companies or regulatory bodies) are still reconciled. IoT security and privacy concerns demand for cross and multidisciplinary approaches, which require efforts from different areas in order to bring citizens into the loop. From the security point of view, smart objects will be often deployed in uncontrolled environments where basic security properties must be still ensured. This circumstance requires the adaptation of current security protocols and technologies to operate on devices and networks with resource constraints that can operate in critical scenarios, such as e-health or smart grid [28]. From the privacy point of view, the IoT is becoming an active enabler of the *Big Data* era [17], fostering the development of a data-driven economy. While the integration of these initiatives will bring new opportunities in scenarios, such as Industry 4.0 or Mobile Crowd Sensing [49], it will also come with new challenges. In particular, the vision of the *Privacy by Design* (PbD) and minimal disclosure principles [47] is opposed to the data maximization notion promulgated by Big Data. With the advent of IoT, the scale and sensitivity degree of information will be higher, and the application of aggregation and correlation techniques will exacerbate this concern, facilitating profiling and tracking tasks. Some of these challenges are derived from a recent document published by the *European Union Agency for Network and Information Security* (ENISA)[1], where the use of different anonymization techniques and cryptographic schemes are proposed to ensure the control of how information can be disseminated within the resulting sharing ecosystem. Such requirements need to be tackled by holistic and all-encompassing approaches with high degree of flexibility to support scenarios with a huge number of heterogeneous devices (e.g. sensors, actuators, gateways or backend servers), while facing inherent challenges related to flexibility, scalability, interoperability and lightness throughout the lifecycle of a smart object [35].

In recent years, a huge number of world-wide initiatives have been launched in order to provide a

[1] https://www.enisa.europa.eu/publications/big-data-protection

common understanding in order to promote the design and development of IoT services. In Europe, the *Alliance for Internet of Things Innovation* (AIOTI) was initiated by the European Commission in 2015 as an ambitious effort to support the dialogue and interaction among different IoT players in Europe. Specifically, the "IoT standardization" working group (WG03) provides a comprehensive list of IoT *Standards Developing Organizations* (SDO) and Alliances, with the main purpose to promote a common understanding of the global landscape of initiatives, as well as the development of future proposals under the IoT umbrella. Additionally, the AIOTI WG03 has initiated the development of a *High Level Architecture* (HLA)[2] for IoT in order to foster architectural convergence among others WGs. Furthermore, it provides a functional model mapping to other architecture proposals, such as the oneM2M Functional Architecture[3], the ITU-T IoT Reference Model (recommendation ITU-T Y.2060[4]) and the Three-Tier IIS Architecture from the *Industrial Internet Reference Architecture* (IIRA)[5].

Under the *Internet Engineering Task Force* (IETF), the IoT vision has been partially realized through the specification of suitable communications protocols for these environments due to the effort of noteworthy initiatives, such as the *IPv6 over Low power WPAN* (6LoWPAN) [46] and the *Constrained RESTful Environments* (CoRE) [75] WGs. Additionally, security and privacy concerns have led to the creation of specific WGs addressing such needs. In particular, the *DTLS In Constrained Environments* (DICE) WG [6] was focused on supporting the use of the *Datagram Transport Layer Security* (DTLS) [61] in environments with constrained devices and networks. Furthermore, the *Authentication and Authorization for Constrained Environments* (ACE) WG [72] aims to develop authentication and authorization mechanisms to be integrated on IoT devices. While these initiatives represent a step forward in order to achieve a secure and privacy-aware IoT, it still arises the need to consider comprehensive approaches addressing security and privacy requirements of smart objects throughout its whole lifecycle [35].

In addition to the aforementioned initiatives, other proposals derived from several European research projects have provided different approaches through the definition of architectural frameworks that are tailored to specific IoT use cases or scenarios. However, in spite of these emerging efforts, nowadays there is a lack of a unified architectural vision on the security and privacy implications in the IoT paradigm covering the whole lifecycle of smart objects that are composing the future digital landscape. Furthermore, while IETF initiatives represent a step forward in order to achieve a secure and privacy-aware IoT, research community and industry still have to address divergent aspects about the application of suitable mechanisms that can support a seamless integration among each other, in order to achieve holistic security and privacy approaches for the IoT. Under this perspective, this thesis provides an architectural framework that aims to provide a comprehensive view of security and privacy needs during the lifecycle of smart objects. The analysis, design and instantiation of this framework have been carried out under the umbrella of two European initiatives in the IoT area, by considering security and privacy as first-class components in the development of new services and applications.

The structure of this chapter is as follows: Section 3.1 describes the main security and privacy requirements for each stage of the lifecycle, as well as some of the major IETF initiatives to address such needs. Section 3.2 provides a description of related proposals in literature coping with security and privacy concerns, which are tackled in this work. The specification of the proposed security and privacy architectural framework is given in Section 3.3, along with an explanation of the required interactions among functional components. Section 3.4 provides a detailed explanation of the security and privacy mechanisms that were designed and developed as a result of the instantiation of the proposed framework. Finally, Section 3.5 provides an overview of the main conclusions derived from this thesis.

[2] http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11812
[3] http://www.etsi.org/deliver/etsi_ts/118100_118199/118101/01.01.00_60/ts_118101v010100p.pdf
[4] http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060
[5] http://www.iiconsortium.org/IIRA-1-7-ajs.pdf
[6] https://datatracker.ietf.org/wg/dice/charter/

3.1. Addressing Security and Privacy challenges in the Lifecycle of Smart Objects

Nowadays, the application of security and privacy mechanisms and protocols to manage the lifecycle of smart objects is one of the most critical challenges in the IoT paradigm [65]. The interpretation of the lifecycle is based on the definition of different stages that are gone through by a smart object, since it is manufactured until it is discarded. The main purpose of this section is to motivate the need for a holistic IoT security and privacy architectural framework through an overview of the main requirements that must be addressed during the different stages of the smart objects' lifecycle. The proposed lifecycle is based on the work presented in [35], where some of these challenges are additionally identified. Following its description, the smart object's lifecycle begins when it is manufactured to be later installed and commissioned within a network. During this phase, the smart object is provisioned with security credentials through the application of bootstrapping mechanisms. In this sense, we propose the addition of an explicit registration/discovery stage, after a successful bootstrapping process, in order to allow smart objects to be named, addressable and discovered by other devices or services before they can operate among each other. Then, the smart object is in the operational phase providing the functionality for which it was manufactured. In this stage, the application of security and privacy mechanisms is essential so that the object can interact with other devices in a secure and, optionally, privacy-preserving way when it is required. Furthermore, a smart object can be in a maintenance (or management) stage, in which it can be updated or configured by the manufacturer or owner. Finally, it can be recommissioned, decommissioned or discarded, which requires appropriate mechanisms for the revocation of credentials that were obtained during the previous stages. In addition to the identification and description of the lifecycle's stages, we discuss some of the major emerging approaches being undertaken by the IETF [44] [37] to address such needs for each stage of smart objects' lifecycle.

3.1.1. Bootstrapping

Following the identified stages that are proposed by [35], the lifecycle of a smart object begins when it is installed and commissioned in a network during the *bootstrapping* process. This process usually consists of a set of procedures in which a smart object joins a network. During the bootstrapping, the cryptographic material statically configured in the *manufacturer domain* is used to derive dynamic credentials and keys to be used in the *deployment domain*. Therefore, the bootstrapping process represents the root of trust of the lifecycle. Indeed, this stage is crucial; security and privacy operational concerns do not matter if this process is not carried out securely by suitable and well-known mechanisms. However, in the IoT ecosystem, the application of traditional bootstrapping mechanisms is a challenging aspect, which must take into account the requirements and needs of constrained environments.

In this direction, [34] provides some design considerations that must be taken into account in the design of an appropriate IoT bootstrapping protocol. In addition to provide basic security properties, they state that it should consider practical aspects of IoT devices, such as lack of user interface, as well as scalability and flexibility for the envisioned scenarios. In this sense, it is necessary to move toward minimal human interaction approaches, in order to realize a *Plug-and-Play* solution for smart objects, while security and privacy are considered. Moreover, [55] presented three main alternatives for the security bootstrapping of IoT devices: *Host Identity Protocol Diet EXchange* (HIP-DEX) [54], the *Protocol for Carrying Authentication for Network Access* (PANA) [26] and 802.1X [1]. From these alternatives, PANA is widely accepted as the main candidate for security bootstrapping, and it is being employed by ZigBee Alliance and ETSI M2M in conjunction with the *Extensible Authentication Protocol* (EAP) [2] and *Transport Layer Security* (TLS) [22] as authentication protocols.

In this thesis, we have relied on bootstrapping technologies in order to provide support for authorization credentials management, as part of the proposed access control model. In particular, we have made use of an optimized version of EAPOL [1], called *Slim* EAPOL (SEAPOL) to trans-

port EAP messages, which has been integrated with the *Extensible Access Control Markup Language* (XACML) [64] for authorization purposes. Furthermore, we have proposed the extension of the notification messages semantics that are sent during the PANA *Access* phase to support this functionality. These proposals represent an excellent starting point for the integration of these mechanisms in recent IoT bootstrapping approaches, such as the work proposed in [27], which employs the *Constrained Application Protocol* (CoAP) [75] as EAP *lower-layer*, and it is described in [66] as part of the IETF ACE WG. In this thesis, we have relied on bootstrapping technologies in order to provide support for authorization credentials management, as part of the proposed access control model. In particular, we have made use of an optimized version of EAPOL [1], called *Slim* EAPOL (SEAPOL) to transport EAP messages, which has been integrated with the *Extensible Access Control Markup Language* (XACML) [64] for authorization purposes. Furthermore, we have proposed the extension of the notification messages semantics that are sent during the PANA *Access* phase to support this functionality. These proposals represent an excellent starting point for the integration of these mechanisms in recent IoT bootstrapping approaches, such as the work proposed in [27], which employs the *Constrained Application Protocol* (CoAP) [75] as EAP lower-layer, and it is described in [66] as part of the IETF ACE WG.

3.1.2. Registration and Discovery

An essential feature for achieving the realization of the IoT is to provide an infrastructure that allows smart objects to be addressable, named and discovered by others. Firstly, a smart object must be identifiable through the assignation and management of addresses/identifiers. Indeed, the identification of smart objects requires scalable and flexible identity management approaches for a potentially huge amount of heterogeneous devices. In this sense, identity management foundations must be extended to smart objects in order to deal with identification issues coping with the high degree of dynamism in IoT environments. While smart objects can be identified by network identifiers or IPv6 addresses, it is necessary to provide an additional abstraction level by considering additional location-independent attributes, such as manufacturer, owner or hardware version, as part of the smart object's identity. Secondly, such infrastructure must provide a name resolution mechanism that allows smart objects to be organized according to taxonomies or hierarchical classifications. Furthermore, it should provide a registration/discovery process that allows the specification of security and privacy preferences to determine how an object wants to be discovered (for example, showing only a subset of its services) and by whom. This is an additional and necessary level of access control that should be considered for a protected and privacy-aware discovery process.

Currently, the IETF presents different proposed Internet identifier services addressing some of these aspects. X.500 [83] is the OSI Directory Standard defined by the ISO and the ITU. It defines a hierarchical data model with a set of protocols to allow global name lookup and search. In the same direction, the *Lightweight Directory Access Protocol* (LDAP) [74] was developed as a more lightweight alternative, while bringing different problems related to the hierarchical data model, as well as to the complex search/query process. Addressing some of these main concerns, the *Handle System* (HS) [77] is a general purpose distributed information system that provides efficient, extensible, and secure identifier and resolution services for the Internet [78] [79]. In HS, a Digital Object (DO) has a machine and platform independent structure that allows it to be identified, accessed and protected. The syntax of the DO is a set of pairs (type, value) that can be hierarchic, providing descriptions and identifiers of other DOs in its parameters. The HS represents an alternative to well-known resolution approaches, such as the *Domain Name System* (DNS) [18], by providing a higher degree of flexibility to enrich the resolution infrastructure with security aspects.

In this thesis, the identification of smart objects has been linked to the definition of *partial identities* [76], as a flexible identity management scheme providing additional privacy-preserving features. In addition to identifiers or network addresses, a partial identity may be composed of additional attributes, such as the owner or the services being provided by the smart object. The concept of partial identity has been mainly realized by using Idemix [14], as the most representative example

of anonymous credentials systems. As already mentioned in Section 2.3, the integration of the proposed security and privacy mechanisms, such as the use of partial identities, with name resolution infrastructures, represents part of the future work derived from this thesis. The deployment of the HS on IoT scenarios has already been analysed under the EU IoT6 project [85] due to its flexibility and security-by-design approach. Indeed, the integration with HS represents and ongoing work to provide security and privacy features to the registration and discovery processes of smart objects.

3.1.3. Operation

At operational level, security and privacy guarantee that only trusted and legitimate instances of an application can communicate (optionally, in a privacy-preserving way). As for the previous stages, security and privacy aspects can be considered at different levels depending on the layer of the IoT protocol stack [28]. However, given the high level of flexibility that is required, the application of security and privacy mechanisms at higher layers is preferable, abstracting from the details of underlying lower layer technologies. In the IoT landscape, CoAP [75] is considered as the standard application layer protocol, which defines a security binding through the use of the DTLS [61] with three alternatives: *PreSharedKey*, *RawPublicKey* and *Certificate*. However, it does not cover the use of authorization and access control mechanisms at the application level.

Under the umbrella of the IETF, the application of DTLS in IoT devices with tight resource constraints has been considered by the DICE WG, while the *Object Security of CoAP* (OSCOAP) [73] approach is being currently analyzed within the ACE WG, as an alternative in scenarios where the application of DTLS is not feasible, or as a complementary approach in case transport layer security is not enough. Furthermore, the ACE WG is mainly focused on the definition of a suitable authorization framework for IoT scenarios based on the OAuth 2.0 [32]. While OAuth 2.0 is widely deployed in Web environments, its applicability in IoT environments has not been demonstrated. This has led to the application of additional building blocks [70] by considering the use of CoAP as application layer protocol, the *Concise Binary Object Representation* (CBOR) [13], and application layer security through the use of *CBOR Object Signing and Encryption* (COSE) [67]. Although privacy concerns are not considered by this approach, the integration of these building blocks represents an ongoing effort to accommodate access control solutions in IoT scenarios.

In this sense, the proposed access control approach in this thesis is built on top of the *Distributed Capability-based Access Control* (DCapBAC) model [93]. DCapBAC is based on *SPKI Certificate Theory* [23] by linking access privileges to the public key of the smart object through the use of *Elliptic Curve Cryptography* [53]. This approach has been integrated with a policy-based mechanism based on the XACML standard, and represented as access tokens using *JavaScript Object Notation* (JSON) [20] by following a similar approach to the *JSON Web Token* (JWT) format [39]. In addition, privacy concerns are addressed through the integration of DCapBAC with privacy-preserving techniques to prove the possession of the token. In particular, approaches such as *Identity-Based Encryption* (IBE) [11] and anonymous credential systems [15], has been explored in order to foster the realization of a privacy-preserving access control approach for the IoT.

Furthermore, given the global scale of the IoT, it is likely that smart objects often operate as groups of entities (e.g. interacting or collaborating for a common purpose). In IoT scenarios with a huge number of devices, it is necessary to provide flexible mechanisms that allows communication among groups of smart objects that can be opportunistically created, as well as a scalable mechanism to share or outsource data, while end-to-end security and privacy are still preserved. Some of these challenges are derived from the already mentioned document from ENISA, where the use of different anonymization techniques and cryptographic schemes are proposed to ensure the control of how information can be disseminated within such ecosystem. In particular, the use of *Sticky Policies* [56] or functional and homomorphic encryption techniques are intended to mitigate the set of threats that are derived from these scenarios. In this sense, the *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) [8], as an example of the sticky policies foundations application, has been recently proposed as a highly flexible cryptographic scheme, which provides the ability to define groups and subgroups of

smart objects according to different combinations of identity attributes. The application of CP-ABE for IoT scenarios has already been analysed and implemented during this thesis in the case of non-heavily constrained devices (e.g. smartphones), and integrated with OMA NGSI-9/10 [6] under the EU SocIoTal project to outsource encrypted data for groups of devices. As already mentioned, the integration of this proposal with schemes that allow group management and communications in constrained environments is part of our future work. In this sense, recent initiatives under the umbrella of CoRE WG [59] represent promising initiatives in this area.

3.1.4. Management

After a smart object is successfully bootstrapped, it can be managed at any time. This stage may involve procedures related to software updates by the manufacturer, as well as configuration tasks by the owner. Consequently, the management process should be supported by mechanisms that allow the ownership transfer to be done correctly to ensure that only legitimate and authorized users are able to manage their smart objects. In this sense, the set of security and privacy considerations during the operation stage are also applicable for this phase. However, in addition to the previous considerations, the management of smart objects implies the need for considering lightweight and efficient data models to be used in IoT environments. Indeed, the application of well-known protocols, such as the *Simple Network Management Protocol* (SNMP) [58] or the *Network Configuration Protocol* (NETCONF) [24], has not been demonstrated in the case of such scenarios. These mechanisms and their associated data models need to be adapted to provide a suitable degree of flexibility, scalability and lightness to be employed by the whole range of IoT smart objects.

Different IETF initiatives are emerging in order to cope with the aforementioned requirements during management procedures. In particular, the *CoAP Management Interface* (CoMI) [81] is an adaptation of the RESTCONF protocol [9], specifically intended to be employed on IoT devices and networks. It uses CoAP to access the management data resources, which are specified in YANG [10] and binary encoding. CoMI is based on a lightweight design to reduce message complexity. It allows access to data resources similarly as any traditional RESTCONF server, but optimizing the messages and encoding. CoMI security is based on the set of mechanisms that are already available for CoAP, through the use of DTLS. Similarly, OMA *Lightweight M2M* (LWM2M) [80], like CoMI, provides a RESTful device management service over CoAP. However, CoMI provides a higher degree of flexibility since it reuses existing YANG data models, whereas LWM2M defines a new object resource model. However, the latter is considered as a more mature technology with different available open source implementations. The set of security considerations for this stage are similar to the issues previously discussed for the operation phase. In this sense, security and privacy mechanisms for management protocols have not been specifically designed during the development of this thesis. However, the different approaches that have been designed and implemented for the operation may be applicable to the management stage in order to ensure that only legitimate and authorized entities are able to manage a smart object.

Indeed, the security and privacy mechanisms designed and developed during this thesis are mainly framed within the *operation* stage of smart objects. However, we have further complemented these techniques in order to provide a more comprehensive view about the security and privacy needs to be addressed within the different lifecycle's stages. In particular, we have proposed the extension of *bootstrapping* technologies to enable smart objects to be provisioned with authorization credentials, in order to interact with other devices and services during their operation. Furthermore, we have proposed the use of partial identities, as a first step to enhance the *registration/discovery* process of smart objects with security and privacy aspects. A more detailed description of these proposals is provided in Section 3.4.

3.2. Related Work

The constant evolution of IoT is producing a wide range of technologies and protocols, resulting in a still disharmonized and fragmented landscape of solutions. Therefore, it is necessary to provide high-level architectures able to disengage from the technical details, in order to provide a common understanding of the security and privacy needs in IoT scenarios. Towards this end, the AIOTI WG03 has initiated the development of a *High Level Architecture* (HLA) for IoT. The proposed architecture is based on a layered functional model (Network, IoT, Application), and a domain model that is mainly derived from the functional model proposed under the umbrella of the European project IoT-A. Furthermore, this working group is in close cooperation with AIOTI WG04, which is addressing policies issues related to security and privacy. In addition to AIOTI, currently there are other initiatives mainly focused on the definition of a high-level architecture for IoT. In particular, the purpose of the IEEE "*Standard for an Architectural Framework for the Internet of Things (IoT)*" (IEEE P2413)[7] is to define an architectural framework, addressing descriptions, definitions and common aspects in different domains IoT, in order to increase compatibility, interoperability and transparency of IoT systems. The proposed architecture is based on a three-tier approach (Sensing, Networking and Data Communications, and Applications). Moreover, the oneM2M initiative represents a joint effort with 14 partners (the *European Telecommunications Standards Institute* (ETSI) among others) in order to ensure efficient M2M deployments through the use of IoT. oneM2M provides a layered model (Network Services, Common Services and Application) that is mapped to a functional architecture composed of three entities with the same name. Furthermore, the *ITU Telecommunication Standardization Sector* (ITU-T) under the recommendation Y.2060 "*Overview of the Internet of Things*" has designed a reference model based on four levels (Device, Network, Service Support and Application Support, and Application) and two cross-layer levels (Security capabilities and Management capabilities), in order to group different functional aspects in each layer. In addition, the ITU-T Study Group 20 (SG20) "*Internet of Things (IoT) and its applications including smart cities and communities (SC&C)*"[8] is intended to develop standards to enable coordinated development of IoT technologies, and mechanisms for the interoperability of IoT applications and datasets employed by various vertically oriented industry sectors.

Moreover, in the scope of European research projects, the huge range of IoT application scenarios of IoT has led to the specification of different architectures that are usually tailored to be deployed on specific domains or addressing particular requirements. This was already identified as a significant barrier for IoT adoption on a broad scale and the main incentive for the development of coordinated efforts driven by the *Internet of Things European Research Cluster* (IERC). One of the first proposals to address this need of a common and harmonized IoT architecture was IoT-i [9], a European research project that dealt with the analysis of different architectures in order to create a joint and aligned vision of the IoT in Europe. This effort meant a step forward for the creation of a holistic environment that encourages a broader adoption of IoT. IoT-A[10] was a large-scale project focused on the design of an *Architecture Reference Model* (ARM) to be additionally instantiated by other IoT architectures through a set of specific tools and guidelines. Moreover, the focus of the architecture proposed by IoT6 [85] was to use the results of previous projects to design an IPv6-based service-oriented architecture, in order to achieve a high degree of interoperability among different applications and communication technologies. Additional architectures were proposed by other remarkable efforts at European level, such as BUTLER[11], SENSEI[12] or FI-WARE[13] based on the specific set of requirements from particular application domains. On the one hand, SENSEI focused on designing the service layer in wireless sensor and actuators networks. On the other hand, FI-WARE, under the FI-PPP program,

[7] https://standards.ieee.org/develop/project/2413.html
[8] http://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx
[9] http://postscapes.com/iot-i-iot-initiative
[10] http://www.iot-a.eu/public
[11] http://www.iot-butler.eu/
[12] http://www.sensei-project.eu/
[13] https://www.fiware.org/

designed an open platform based on an architecture composed by components, which are referred as *Generic Enablers* (GEs).

This set of EU projects addresses the definition of an IoT architecture considering different levels of abstraction to fit in specific scenarios. Furthermore, these initiatives do not address security and privacy concerns from a holistic point of view. On the contrary, one of the main results of this thesis is the definition of an architectural framework considering the security and privacy needs during the lifecycle of smart objects, as a result of the instantiation of the architecture proposed by IoT-A. The main motivation for choosing the ARM as a starting point is due to the fact that it provides a comprehensive definition of the IoT ecosystem, by proposing different models and architectures. In addition, IoT-A results are strongly supported by emerging initiatives, such as the IEEE P2413 or the initial definition of HLA provided by AIOTI WG03, for the specification of a reference architecture for IoT.

As previously discussed, the instantiation of the proposed architectural framework has led to the definition of different security and privacy mechanisms, which have been integrated in order to achieve a suitable access control model to be used in IoT environments. In the IETF, OAuth 2.0 [32] represents an authorization approach based on the use of access tokens to access protected resources. OAuth 2.0 architecture is based on the definition of four roles: *Resource Owner* (RO), *Resource Server* (RS), *Client* (C) and *Authorization Server* (AS). Currently, OAuth is widely accepted and deployed especially in the case of Web scenarios. Specifically, OAuth 2.0 is based on the use of access tokens as "*a string representing an authorization issued to the client*", which are usually referred as a *bearer token*. In this sense, [41] defines a bearer token as "*a security token with the property that any party in possession of the token (a "bearer") can use the token in any way that any other party in possession of it can*". Therefore, the use of a bearer token does not require a bearer to prove that it is actually the entity associated with the token presented, which can lead to misuse or abuse of access tokens.

This issue has motivated the creation of a recent initiative based on the use of the *Proof-of-Possession* (PoP) architecture [36], in order to complement the OAuth 2.0 standard with mechanisms to prove the possession of access tokens. Such proposal also provides a list of use cases with additional security requirements to encourage the use of the PoP mechanism. The architecture proposed by PoP is based on two approaches through the use symmetric and asymmetric cryptography. Both solutions assume the AS binds access tokens to cryptographic keys, which are then used by a client to access the RS, in order to prove that it is the holder of the provided token. An instantiation of this mechanism in the case of *JSON Web Token* (JWT) [39] is proposed in [40], which describes how to specify a PoP key within JWT by adding a claim confirmation "*cnf*". Additionally, it provides the semantics required to specify this key as asymmetric (using *JSON Web Key* (JWK) [38]) or symmetric (through the use of *JSON Web Encryption* (JWE) [42]).

These proposals are mainly focused on the format for defining authorization credentials and how they can be used for the access to other services. However, these efforts do not address other issues of security and privacy concerns that are transverse to the access control problem in IoT scenarios. Firstly, they do not consider the specification of access conditions to be locally verified by the target service during the access to it. This feature is required in IoT scenarios with a high degree of dynamism, where changing aspects (e.g., related to context) can affect the access control evaluation. Secondly, these proposals are based on the use of symmetric or asymmetric cryptography for the proof of possession process of the authorization token. Therefore, they do not consider the use of privacy-preserving techniques for obtaining or proving the possession of such credentials. Thirdly, they do not explicitly deal with the process of authorization credentials generation process, in order to automate the consent of the resource owner to grant access to their resources. Finally, they do not consider the integration of bootstrapping protocols to allow smart objects to obtain these credentials, in order to achieve a more comprehensive view of the access control process that is required in IoT scenarios.

In this sense, the access control model proposed in this thesis makes use of access tokens, in which a set of *access rights* (as <action, resource> pairs) are bound to the client's public key. This model has been called *Distributed Capability-Based Access Control* (DCapBAC) and uses JSON for encoding access tokens, with a similar JWT semantics. The set of access privileges are represented, in turn,

with a simple semantics in which an action is mapped to a CoAP method, and the resource is specified as a service within a smart object (indicated by a *Uniform Resource Identifier* (URI) [7]). It should be pointed out that under the umbrella of ACE WG, the approach presented in [71] proposes the use of *Authorization Information Format* (AIF) [12] (as an "*aif*" claim) similar to this specification. Additionally, the token provides a simple semantics to specify access conditions to be verified locally by the smart object being accessed. These conditions have been used for the specification of a threshold trust value, as part of the IoT trust and reputation model proposed in [89]. Moreover, unlike Oauth that has defined a profile with *User-Managed Access* (UMA) [31] to specify how ROs can control the access to their resources, DCapBAC has been integrated with the well-known and established XACML standard (OASIS) for defining access control policies, in order to automate the token generation process. While this is analogous to the use of authorization decision statements from the *Security Assertion Markup Languaje* (SAML) [69] to carry authorization decisions, DCapBAC is based on the use of technologies that are specifically designed to be used in IoT environments.

In addition, as already mentioned, the set of proposed PoP mechanisms do not explicitly make use of privacy-preserving techniques. Towards this end, DCapBAC has been extended [91] to consider different alternatives to prove the possession of the token in a privacy-preserving way, by using IBE and CP-ABE cryptographic schemes, as well as the *Identity Mixer* (Idemix) [14], as the main example of anonymous credential systems. Specifically, the approach is based on binding access privileges to a pseudonym (or a partial identity [76], instead of the public key) specified in the access token, which is proved in a privacy-preserving way through the use of the already mentioned techniques. Moreover, DCapBAC has been instantiated and deployed in the field of two European IoT initiatives: SMARTIE and SocIoTal. In the first case, it has been integrated with FI-WARE components to allow protected access by considering the set of methods provided by OMA NGSI-9/10. In the second case, it has been deployed in the case of non-heavily constrained devices using CoAP and DTLS, as well as on mobile devices (such as smartphones) to enable a protected access to smart objects. Moreover, it has been deployed in the case of devices with tight resource constraints through the integration with an optimized ECC library based on the use of Shifting Primes [51].

3.3. Framework for a Secure and Privacy-aware Lifecycle of Smart Objects

The constant evolution of the IoT is resulting in a disharmonized and fragmented landscape of technologies and protocols. Indeed, as already described in the previous section, there are different emerging initiatives in the field of IoT security and privacy that still lack of mature approaches and implementations to be deployed in real environments. Consequently, it is required to define high-level architectures able to disengage from the technical details to provide a common understanding of security and privacy needs. Towards this end, IoT-A was a large-scale European project focused on the design of an *Arquitectural Reference Model* (ARM) [5], in order to enhance the interoperability among isolated IoT domains. While it represented a key step to move from an *Intra*net of Things to a real *Inter*net of Things [86], the current great challenge lies in the design of secure and privacy-preserving IoT-enabled services to be deployed in everyday scenarios.

The set of results derived from IoT-A embrace: a *Reference Model* (RM) to promote common understanding at high abstraction level; a *Reference Architecture* (RA) to describe essential building blocks and build compliant IoT architectures; and a set of Best Practices/Guidelines to help in developing an architecture based on the RA. In particular, the RA provides several views and perspectives focused on different architectural aspects. Among these views, the Functional View (shown in Figure 3.1) describes a set of *Functional Components* (FC), which are organized into nine *Functional Groups* (FG), as well as their responsibilities and interfaces. In particular, the Security FG is composed of five functional components: *Authentication*, *Authorization*, *Identity Management* (IdM), *Key Exchange and Management* (KEM) and *Trust and Reputation* (T&R). Nevertheless, while it provides a set of basic security and privacy functionality of an IoT system, it does not define the interactions

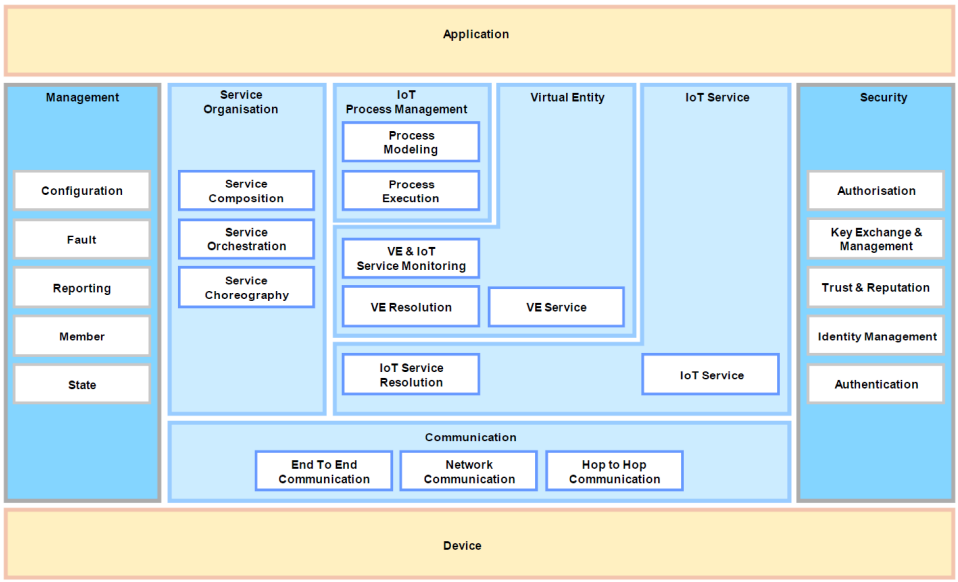

Figure 3.1: IoT-A Functional View

among these components or the use of specific technologies to instantiate such functionality. On the one hand, the proposed framework is based on the different stages of the smart objects' lifecycle derived from [35]. On the other hand, it represents an extension of the Security FG, as well as an instantiation of it by defining the main interactions among the identified FCs to address different security and privacy needs during the smart objects' lifecycle.

In particular, this extension is based on the inclusion of two additional FCs: Context Manager and Group Manager, to complement the functionality of the other FCs that are already proposed by the Security FG. The *Context Manager* aims to realize the vision of an adaptive security and privacy to the current context conditions in which the smart object operates [57]. Its main functionality is to reason about contextual information being perceived by a smart object from its surrounding environment, so other Security FCs are able to adapt their behavior based on it. It is meant to be instantiated by data analysis techniques or simple rule-based mechanisms in case of more constrained smart objects. The *Group Manager* is designed to deal with security and privacy concerns when information needs to be shared or outsourced with a group of smart objects. It is intended to be implemented through the application of attribute-based cryptographic techniques (or symmetric key cryptography in case of resource-constrained devices), and deployed on smart objects participating in scenarios where publish/subscribe or multicast communications are employed.

In order to describe the functionality of the framework components, and for the sake of clarity, we adopt a *producer/consumer* approach, which is derived from the abstract role that can be played by smart objects as information producers and consumers. The description of the relationship among components will be based on the existence of an infrastructure level, abstracting the set of elements (e.g. gateways or backend servers) that are required in a real IoT deployment for supporting secure and privacy-aware interactions among smart objects. It should be noted that the proposed framework is intended to describe the functionality and interactions only among Security FCs to address security and privacy requirements during smart object's lifecycle. This is complementary to other interactions required among FGs to realize a particular use case or scenario. Furthermore, it is abstracted from underlying technologies, which means that the same FC can be instantiated by a different technology (or implementing different aspects of the same technology), depending whether that FC is instantiated at infrastructure or smart object level.

Figure 3.2 shows the required interactions during the bootstrapping and registration/discovery

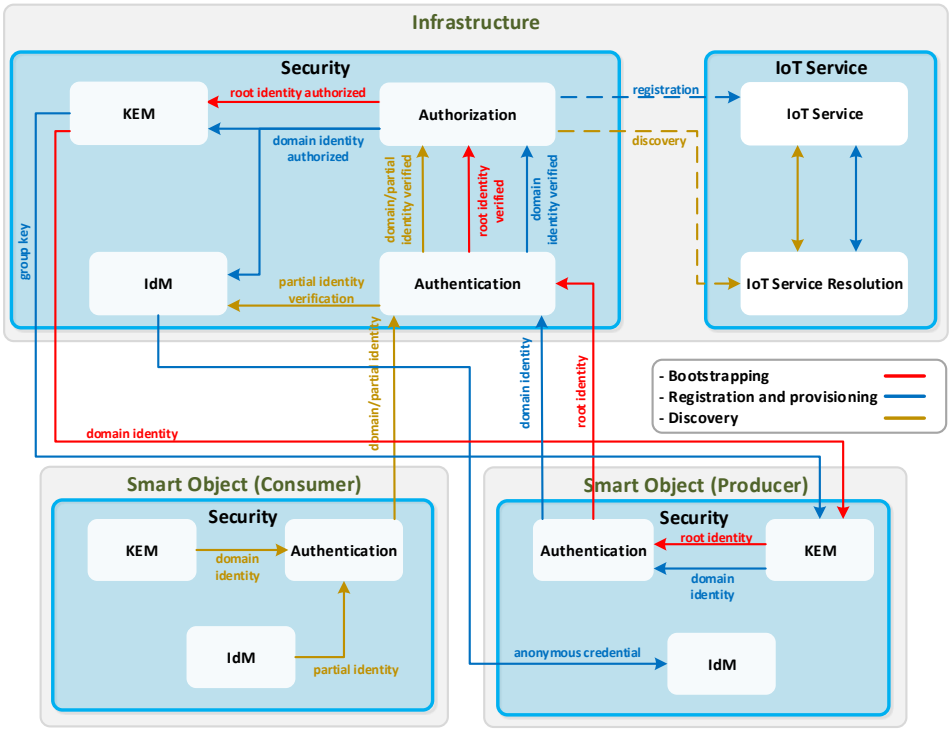

Figure 3.2: Framework Bootstrapping and Registration/Discovery interactions

stages. Indeed, the smart objects' lifecycle begins when it is installed and commissioned during the *Bootstrapping* process. For this phase, it is assumed smart objects are endowed with statically configured cryptographic material to enable subsequent operation in the deployment domain. Such credentials could be embedded by the manufacturer, and it can be considered as the *root identity* that is employed for bootstrapping procedures. By using its root identity, the smart object is commissioned and connected to the network, which implies an authentication and authorization process. As a result, it obtains some cryptographic material (*domain identity*) that is shared with the infrastructure to be identified in subsequent processes. The root identity and the domain identity make up the *complete identity* of the smart object. Then, it is also registered to be discovered by other smart objects. This functionality is already considered by IoT-A through the IoT Service Resolution FC, within the IoT Service FG, by providing lookup, resolution and discovery functionalities. Moreover, a successful authentication and authorization process could derive other cryptographic material to be employed by the smart object during its operation (*provisioning*), such as *anonymous credentials* and *group keys* associated to identity attributes that are previously demonstrated. Therefore, these credentials would be linked to the root identity, preserving the accountability of the anonymity condition. During the *Discovery* process, a smart object (consumer) tries to discover the services being provided by another device (producer). Before this process, it is assumed that both smart objects have already completed the previous stages. It also requires authentication and authorization procedures to determine whether a legitimate smart object is authorized to find that service or not. This authentication can be performed through the use of the *domain identity*, or by considering privacy concerns of the consumer through the use of *partial identities* (as a subset of its identity attributes), derived from the anonymous credential.

Then, a smart object can get into the *Operation* phase providing the services for which it was manufactured, or into the *Management* stage. The required interactions among functional components are shown in Figure 3.3. For the Operation stage, two different cases are considered, in which

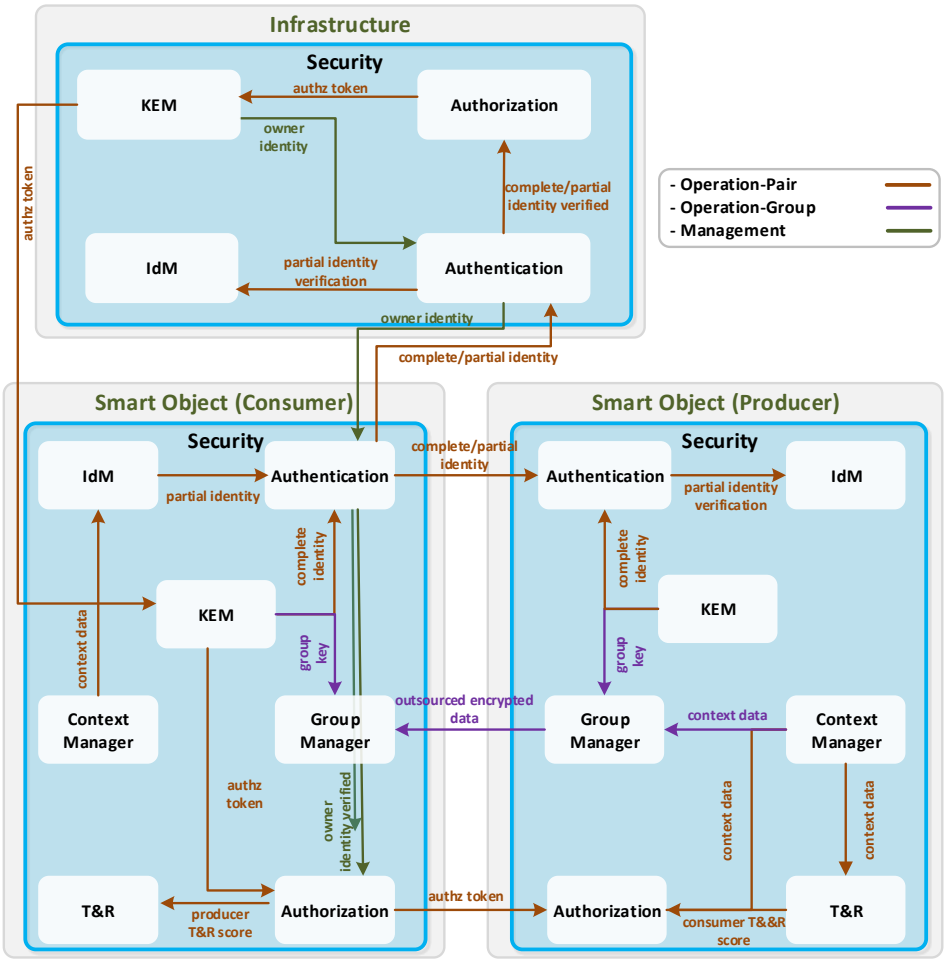

Figure 3.3: Framework Operation and Management interactions

communication is performed either directly between two smart objects, or involving a group of them. Nevertheless, it should be noted that the interactions between FCs involving both smart objects are direct (i.e. Authentication, Authorization and Group Manager) to emphasize that end-to-end security and privacy are to be preserved, even if communication is established through infrastructure components (e.g. a gateway). For the *Operation-Pair* case, a smart object (consumer) tries to get some kind of credential to perform a specific action over the discovered smart object. Therefore, it is authenticated and authorized by the infrastructure level and, if successful, he gets an authorization token, which is bound to the discovered service. This procedure can be performe by using the complete identity or taking into account privacy concerns through the selection of a different partial identity (according to contextual information being sensed) to get the token. Then, it uses this credential, along with the identity (e.g. a pseudonym) required to prove the possession of the token. Then, the producer evaluates this token by considering additional information, such as context data or trust and reputation scores associated to the requesting smart object for a more fine-grained access control. For the *Operation-Group* case, a smart object (producer) makes a piece of data available to a group of (consumers) smart objects. The notion of group in the proposed framework is realized by the association of identity attributes to cryptographic *group keys*, which are previously obtained. This functionality is carried out by the Group Manager FC, which is responsible for encrypting (and decrypting) certain

information by selecting (depending on the context being detected) the set of identity attributes that must be satisfied by the consumer smart objects in order to access the outsourced information.

Besides operation, a smart object can be managed, either directly by another smart object, or more commonly, by the infrastructure layer (as shown in Figure 3.3). The *Management* stage implies an authentication and authorization process, so that only legitimate and authorized infrastructure components are able to perform the main management tasks of an IoT system, which are already are provided by the Management FG from IoT-A. Finally, the smart object can be *decommissioned* (or *recommissioned*), which implies management and revocation procedures related to the credentials previously obtained. This process will require scalable mechanisms that take into account the dynamism and scale of IoT scenarios.

3.4. Framework Instantiation for advanced Access Control in IoT deployments

The instantiation of the functionality described in the previous section has resulted in the definition of several mechanisms, in order to address different security and privacy issues during the lifecycle of smart objects. Such instantiation and deployment has been primarily driven by two European projects: SocIoTal and SMARTIE, whose overall goal is the application of secure and privacy-preserving mechanisms to different IoT use cases and scenarios. The proposed deployment is based on the definition of several deployment components that have been designed and implemented under the umbrella of such initiatives, to implement some of the main functionality provided by the different FCs of the proposed framework.

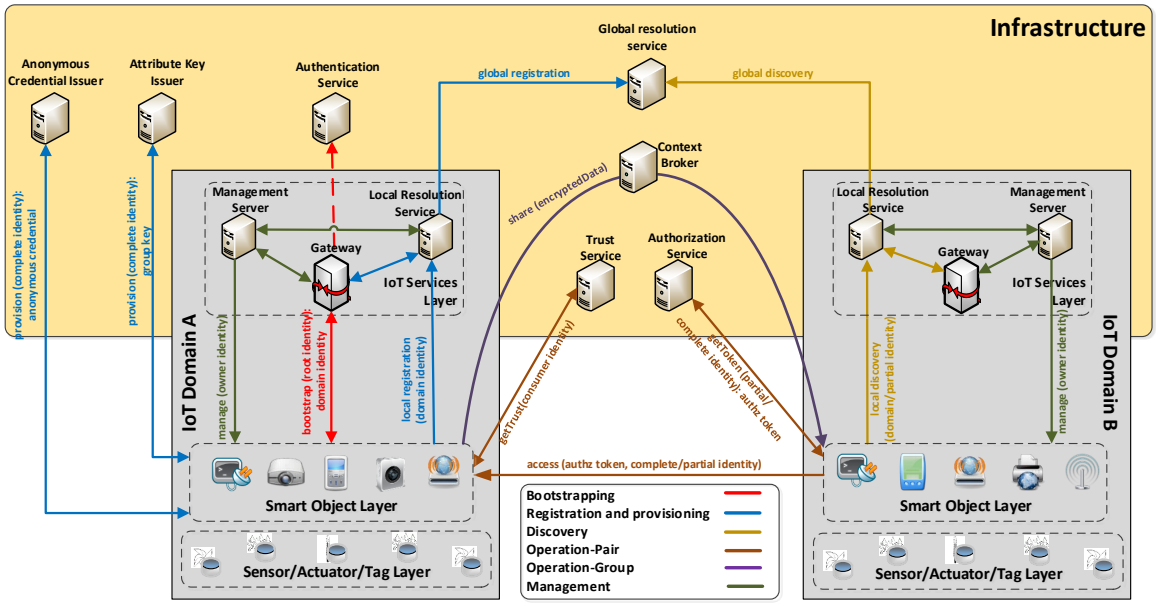

Figure 3.4: Proposal for Framework Instantiation and Deployment

Figure 3.4 provides an overview of the main interactions that are required among deployment components to accomplish the framework's functionality. The main purpose of the figure is to point out the need for different hardware components to support the security and privacy functionality within different stages of the smart objects' lifecycle. It should be noted that a subset of these deployment components has been implemented in the scope of the mentioned initiatives. To abstract from the details of the scenarios in which it has been instantiated and deployed, a layered approach

is adopted, considering an *IoT Domain* as a concept encompassing a local IoT-enabled environment (e.g. a smart building) as part of a more global ecosystem. The *Smart Object Layer* embraces the set of heterogeneous devices (or things) composing an IoT environment. Furthermore, a smart object may be composed of sensors, actuators or tags, as well as other smart objects. *IoT Services Layer*, while being part of the IoT domain, is considered as part of the Infrastructure layer and consists of deployment components that support devices in managing security and privacy aspects within the domain.

Following the notation from previous sections, for the sake of clarity, we consider two domains where a producer (in the *IoT Domain A*) and a consumer (within the *IoT domain B*) smart objects are intended to interact each other. Thus, bootstrapping interaction represents the process in which the device contacts the *Gateway* to access the security domain, and a security association is established, which is derived from a successful EAP authentication. As a result of a successful bootstrapping, the producer obtains a domain identity, which could be *registered* in the *Local Resolution Service*, and then, in the *Global Resolution Service* to make this smart object globally available by using a name resolution infrastructure. Furthermore, during provisioning, the producer tries to get an anonymous credential (through an Anonymous Credential Issuer based on Idemix) and a group key (using the Attribute Key Issuer based on CP-ABE) associated to its complete identity.

In the same way, the discovery process would be performed through the Local Resolution Service, and the Global Resolution Service by the consumer smart object. It should be pointed out that these services are intended to instantiate global resolution names procedures and it represents part of the future work derived from this thesis, as mentioned in Section 2.3. Once the producer is discovered, in the *Operation-Pair* case, the consumer tries to get an authorization credential by contacting the *Authorization Service*. In particular, this service has been implemented by using a XACML *Policy Decision Point* (PDP) for evaluating authorization policies, as well as a *Capability Manager* that is responsible for generating DCapBAC tokens in case of a successful authorization. Furthermore, the authentication required to get such credential has been implemented by considering traditional approaches based on certificates, as well as through the use of anonymous credential systems. In this case, the consumer obtains a DCapBAC token that is bound to the pseudonym and proved in a privacy-preserving way to the consumer. Furthermore, this device can query the *Trust Service* to get the trust value associated to the consumer for a more fine-grained and enriched access control process. Specifically, such service has been instantiated by using the trust and reputation model proposed in [89]. Furthermore, in the case of the *Operation-Group* case, we have made use of CP-ABE in non-heavily constrained devices (smartphones), to communicate context information to groups of devices for supporting end-to-end confidentiality. Specifically, this has been developed in the scope of the SocIoTal project through the use OMA NGSI-9/10 to outsource information to the *Context Broker*, as part of the European initiative FI-WARE.

Following, a more detailed view of these mechanisms is provided. The resulting approaches are intended to complement each other as an initial step towards a holistic security and privacy approach for the IoT.

3.4.1. Supporting Lightweight and Flexible Authorization in the IoT

The realization of IoT scenarios imposes significant restrictions on privacy and access control, since everyday physical objects are being seamlessly integrated into the Internet infrastructure. Different requirements related to heterogeneity, scalability, flexibility and interoperability make the application of existing and access control solutions to these emerging ecosystems a challenging task. As already mentioned in previous sections, one of the results derived from this thesis is the definition of a flexible and lightweight access control model to be deployed in IoT environments, which has been called *Distributed Capability-based Access Control* (DCapBAC) [93]. From a conceptual perspective, DCapBAC is based on binding access rights or capabilities to smart objects that are identified by their public key, following a similar approach to *SPKI Certificate Theory* [23], or *AuthoriZation-based Access Control* (ZBAC) [43]. The application of the capability model to IoT environments was firstly

proposed by [30], as a result derived from the IoT@Work project[14]. Recently, other approaches have been proposed [50], by using this approach as a basis due to their ability to support the *least privilege* principle [68] or to avoid the *Confused Deputy* problem [33]. In this model, the concept of capability refers to a "*token, ticket, or key that gives the possessor permission to access an entity or object in a computer system*" [21]. This concept is used by the Policy Machine project [25] from the *National Institute of Standards and Technology* (NIST), and has been used as the basis for the definition of an authorization credential to be used in IoT scenarios. From a technical perspective, DCapBAC is based on the use of authorization credentials (or capability tokens), represented with JSON, and following a similar semantics to JWT. However, unlike JWTs, capability tokens contain the access rights that are bound to a smart object's public key, as well as a set of access conditions to be locally verified at the end device when then token is presented. On the one hand, access rights are represented by <action, resource> pairs, where the resource refers to a URI that identifies a service being hosted by a smart object. On the other hand, the specification of these conditions follows a simple semantics based on [48], and they are intended to enhance the flexibility of DCapBAC since certain parameters, which are read o sensed by the smart object, could be used during the capability token evaluation. Furthermore, it makes use of CoAP as an application layer protocol to carry the capability tokens and ECC for cryptographic operations.

The proposed initial model has been complemented with other mechanisms and technologies in the scope of this thesis, in order to provide a more complete and consistent access control approach. In particular, the capability token generation process has been instantiated by defining infrastructure components that implement different functionality for this stage. On the one hand, DCapBAC has been integrated with a policy-based approach through the use of XACML, by defining a *Policy Decision Point* (PDP) and a *Policy Administration Point* (PAP) based on it. XACML is the de facto standard from OASIS to express access control policies, by specifying the set of subjects who can perform certain actions on a specific set of resources, based on information (attributes) of them. Furthermore, XACML is also a representation format to encode access control requests and responses, which are generated according to the standard specification. In this way, users are enabled to define access control policies through the PAP, in order to control the access to their resources. Furthermore, it has been integrated with an infrastructure component, called *Capability Manager* (CapM), which is responsible for generating capability tokens depending on the authorization response obtained from the PDP. Thus, an entity that wishes to obtain a capability token, makes a query to the CapM which, in turn, asks the PDP in order to generate (in case of a *PERMIT* response) the requested credential. This integration has been developed and instantiated in the scope of SocIoTal and Smartie. For the former, DCapBAC functionality has been deployed on non-heavily constrained devices (such as gateways, or smartphones), by using DTLS. In this case, the actions contained in the access rights of the capability token are mapped to a CoAP method. For the latter, DCapBAC has been integrated with different components from the European FI-WARE platform. On the one hand, it has been combined with the KeyRock Identity Management component, so authorization decisions are based on the identity attributes that are stored in a Keyrock IdM instance. On the other hand, the token evaluation process has been integrated within the SocIoTal Context Manager, as an extended instance of the FI-WARE Context Broker.The functionality of this component is based on the OMA NGSI-9/10 specification, so the capability token format has been adapted to consider the set of NGSI methods as actions to be included in the set of access rights within the credential. The different instantiations that have been developed in the scope of this thesis demonstrate the flexibility and applicability of the approach to be deployed in different real IoT scenarios and use cases.

In addition to the capability token generation process, in order to achieve a more holistic approach for the access control issue in IoT, DCapBAC has been integrated with bootstrapping protocols to enable smart objects to apply for authorization credentials that can be used during their operation. In particular, DCapBAC has been integrated with a lightweight version of EAPOL [1], called *Slim EAPOL* (SEAPOL) for transporting EAP messages. Thus, SEAPOL is used to initiate a security

[14] http://www.iot-at-work.eu/

bootstrapping process by integrating standard technologies, such as EAP [2] and the *Remote Authentication Dial In User Service* (RADIUS) [62]. Furthermore, this initial stage is extended with the *Multiple Decision Profile* (MDP) [63] from XACML for authorization procedures. However, in this case, all the authorization tokens for a smart object should be obtained during the initial bootstrapping stage, since EAPOL does not provide semantics to enable an on-demand credentials provisioning [96]. In order to address this problem, within the scope of this thesis, we have proposed the extension of the PANA protocol by defining a simple semantics to provide a mechanism for supporting authorization credential management procedures [92]. PANA is a protocol widely accepted as a bootstrapping mechanism that is currently used by initiatives, such as ETSI M2M and ZigBee Alliance. The protocol considers four main entities [52]. The *PANA Client* (PaC) is the client entity trying to get access to the network service provided by the *Enforcement Point* (EP). Furthermore, the EP is under the control of the *PANA Authentication Agent* (PAA), which is responsible for authenticating and authorizing the network access. Moreover, the core PANA operation comprises four main phases [26]: *Authentication and Authorization*, *Access*, *Re-Authentication* and *Termination*. In particular, during the *Access* stage, PaC and PAA can send notification messages to check if the PANA session is active. Additionally, this stage can enter into the *Re-Authentication* phase, in which PaC or PAA may initiate a re-authentication process to update the lifetime of the session. Both phases are based on the use of notification messages *PANA-Notification-Request/Answer* (PNR/PNA). In addition, each message that is exchanged during these phases can carry zero or more *Attribute-Value Pairs* (AVPs). Currently, PANA defines a standard set of AVPs to satisfy the functionality of the protocol. Our proposal is based on the extension of the set of PANA AVPs that are used in these stages within PNR/PNA messages, in order to allow the application and delivery of capability tokens. For this purpose, we consider the addition of two new *Action* and *Resource* AVPs to be optionally used by the PaC in order to obtain a DCapBAC token within a PNR message. The Resource AVP makes reference to a URI where the resource is hosted (for example, coap://weatherstation1.umu.es/temperature). Moreover, the Action AVP refers to a possible CoAP method to be performed on that resource (for example, GET). This process has been further enriched with the authorization components previously described for the token generation process. Therefore, the PAA queries the Capability Manager to obtain a capability token for a PaC that is sent within a PNA message as a new AVP called *DCapBAC-Token*.

It should be pointed out that this PANA extension proposal for the application and delivery of capability tokens is currently being developed and deployed in the scope of the Smartie project. Indeed, the definition of mechanisms for the provisioning of security credentials to be employed by smart objects is currently a prominent research topic, especially in the case of devices and networks with tight resource constraints. In this sense, the proposed mechanism is an excellent starting point to be integrated with novel bootstrapping approaches, such as the proposal presented by [27]. Furthermore, its integration with other complementary approaches, such as the use of *Object Security of CoAP* (OSCOAP) [73] or representation tokens by more compact representation formats, as CBOR [13], is part of our ongoing work in this area.

3.4.2. Privacy-preserving Access Control: a M2M approach

The IoT represents a global ecosystem in which where privacy of individuals is seriously threatened since their personal data (coming from their devices) can be disclosed without their awareness or consent. *Privacy-Enhancing Technologies* (PETs) help to deal with this problem providing means to achieve pseudonymity, data minimization, unlinkability as well as other techniques to provide confidentiality and integrity of sensitive data. Furthermore, given the M2M nature of these emerging scenarios, the application of current privacy-preserving technologies needs to be reconsidered and adapted to be deployed in such global ecosystem, addressing aspects such as *Privacy by Design* (PbD) [47], in order to give people maximum control over their personal data. In this sense, as already mentioned in Section 3.1.2, in the scope of this thesis, we have proposed the use of partial identities to identify smart objects, by using different subsets of attributes from their whole identity.

The concept of partial identity has been driven through the application of anonymous credential

systems [15] and different encryption schemes, which have been integrated into the proposed access control model. Specifically, this integration is based on binding the set of access rights to different cryptography material to prove the possession of the token in a privacy-preserving way. Towards this end, three alternative approaches have been considered. On the one hand, *Identity-based Encryption* (IBE) [11], allows to encrypt a message under a characters string that is considered as the identity of the message's recipient. Consequently, an entity does not need access to the recipient's public key to encrypt a message, simplifying key management tasks and providing higher flexibility. In this case, the capability token is bound to a pseudonym, whose possession is proved to an IBE key associated to that pseudonym. On the other hand, in the *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) scheme [8], a piece of data is encrypted under a policy of attributes, while keys of participants are associated with sets of attributes. By considering this alternative, access tokens are bound to a certain partial identity represented as a policy of attributes, which must be satisfied by the requesting smart object through the use of its CP-ABE key.

In addition, DCapBAC has been conceptually integrated with Idemix [14], as the most representative approach of anonymous credential systems. Idemix is based on the *Camenisch-Lysyanskaya* (CL) signature scheme [16], which allows to prove the possession of a signature avoiding the disclosure of underlying messages, or even the signature itself, by using zero-knowledge proofs. Through the use of Idemix, a smart object can use its Idemix credential to get a capability token in a privacy preserving way. Specifically, the Idemix proof generated by the device is associated with a particular partial identity (i.e. a subset of identity attributes from its complete identity), which are used by the authorization components described in previous section, for authorization purposes. Such proof also contains a pseudonym generated by the smart object to be specified in the token. Then, the smart object makes use of the capability token to get access to a service being hosted by another smart object through the Idemix proving protocol. This process allows the requesting device to prove it is the entity associated with the token while concealing any other identity attributes.

It should be pointed out that the use of privacy-preserving techniques during the use of capability tokens, could be seen as alternative approaches to the different proof-of-possession proposals, which have been currently considered in [36] through the use of traditional symmetric and asymmetric cryptography. In this sense, while these approaches haven been deployed on non-heavily constrained devices, the need to accommodate mechanisms (e.g. Idemix) on smart objects with tight resources constraints currently represents an important research topic to be further explored.

3.4.3. Integrating Dynamic Information towards Adaptive IoT Security and Privacy

The increasing development of IoT is dramatically changing the way people share information and communicate with their surrounding environment, enabling a constant, invisible and sometimes unintended data exchange. These communications are often carried out among smart objects that are deployed within uncontrolled environments, with changing and dynamic contextual conditions. Given the pervasive, distributed and dynamic nature of the IoT, context should be a first-class security component in order to drive the behavior of devices. This would allow smart objects to be enabled with context-aware solutions, in order to make security and privacy decisions adaptive to the context in which transactions are performed. At the same time, context information should be managed by taking into account security and privacy considerations. In particular, current IoT devices can obtain context information from other entities of their surrounding environment, as well as to provide contextual data to other smart objects. In this sense, the application of trust and reputation mechanisms is essential to assess the trustworthiness of data being provided by other entities in the environment. Furthermore, high-level context information can be reasoned and inferred by considering privacy concerns. Thus, a smartphone could be configured to provide information about a person's location with less granularity (e.g. giving the name of the city where he is, but not the GPS coordinates), or every long periods of time in order to avoid the disclosure of daily habits of that person [97]. While the notion of context awareness has been well researched in recent years [57], currently there is a lack of security

and privacy-preserving mechanisms that take into account dynamic context conditions [19] for the IoT, which can be used by them to modify their operation or behavior accordingly.

The processing of contextual information has been carried out from different points of view within the scope of this thesis. In this sense, the need to consider dynamic contextual aspects has led to the inclusion of the Context Manager functional component, as part of the proposed framework, which is specifically designed to provide inferred high-level contextual data to other security components, for example, to use a different partial identity, or to make an authorization decision based on the information being provided. As an essential component of the context, the use of location information is crucial to protect the access to devices that are physically deployed in everyday environments [90]. For example, in a smart buildings scenario, a smart door lock located at a certain room may require that the requesting user is in front of such door. Otherwise, the access could be denied. Indeed, location restrictions have been considered as a relevant factor for the corresponding access control mechanism. In this direction, many efforts based on the *Location-based Access Control* (LBAC) model [3] have been proposed in recent years, in which the user's physical location is considered when determining her access privileges. In this direction, the proposed access control model has been integrated with an indoor location system, so authorization decisions are based on the combination of user location data and capability tokens. At this point, it should be noted that the token evaluation process could consider dynamic aspects during its evaluation, which cannot be evaluated when the token is generated, since the same credential can be used several times to access the same service. The proposed indoor localization system is based on the use of different sensors that are integrated in common current smartphones. Therefore, it does not require the deployment of additional hardware or devices, providing a flexible and easy-manageable indoor localization system for users. To compensate this lack of infrastructure, which is usually employed to ensure good performance of localization systems, this systems is based on a combination of soft computing techniques, which are employed to estimate the user's location. Under this approach, smart objects are configured with a security zone where the requesting user could be authorized to access it. In this way, if the requesting user provide a valid capability token and she is in this area, access is granted; otherwise, access is denied.

In addition to location data as a component of contextual information, it is necessary to consider other dynamic aspects that can be used for the access control process. In this sense, the application of trust and reputation models is crucial to ensure that data are generated from trustworthy and legitimate sources. As an extension of the proposed access control model, this approach has been integrated with a multidimensional trust model to calculate the overall trustworthiness about an IoT device [89]. It considers different properties that could be taken into account in the Internet of Things paradigm. These properties are considered to come up with an overall value about four main trust dimensions. Thus, in addition to traditional considerations such as service feedback and reputation, our trust model takes into account security aspects and social relationships within the peer device. In the end, this approach leads to a more accurate and reliable value of trustworthiness about a given IoT device. The integration of this trust model with the proposed control system access has been realized as an access condition that is specified in the capability token. This condition is represented as a threshold trust value and generated as a XACML obligation to be locally verified at the target smart object, by following the proposed multidimensional trust model.

3.5. Lessons Learned

The Internet of Things paradigm represents the next natural step in the digital age through an integrated vision of smart objects composing our surrounding environment. In recent years, the confluence of efforts from academia, industry and administrative institutions is constantly promoting its development. In a hyper-connected world, we claim that security and privacy are a must, which requires stringent efforts from different disciplines and stakeholders to get a unified view about their requirements, including incentives to make the society aware of the associated risks.

Given the constant evolution of technologies and protocols that are emerging for the IoT, in the

scope of this thesis, we have proposed the definition of an architectural framework that abstracts from the underlying technologies for managing security and privacy concerns during the lifecycle of a smart object. The proposed design is based on an instantiation of the Architectural Reference Model, derived from the IoT-A project, in order to provide a comprehensive overview of the security and privacy functional needs that must be addressed in the IoT paradigm. The resulting framework is intended to be instantiated, in turn, by specific mechanisms and technologies to be deployed in IoT scenarios where security and privacy requirements need to be addressed. We consider a unified view of IoT security and privacy concerns to be key for the success of the next generation of IoT-enabled Smart Cities.

The all-encompassing approach of the proposed framework has been instantiated, developed and deployed under the umbrella of two European research projects in the field of security and privacy on IoT. In this sense, the high flexibility of the designed mechanisms has allowed their deployment in different IoT scenarios derived from these initiatives, demonstrating their feasibility and applicability to be accommodated in different environments. Therefore, the results from this thesis have not only been provided in different journals or conference publications, but they are derivated from the deployment of such mechanisms in real IoT use cases and scenarios.

In particular, different security and privacy solutions are being proposed under the umbrella of several standardization bodies, such as the IETF. While many of these efforts are currently considered as alternatives to be deployed in IoT environments, given the high degree of heterogeneity of these scenarios, a large part of these solutions are intended to coexist in the future. In this sense, the extension of technology to all aspects of our daily lives entails the need for usable security and privacy approaches that enable citizens to control how their information is shared with other IoT stakeholders. Furthermore, the application of security and privacy mechanisms in environments with resource-constrained devices and networks represents a current hot research topic, in which scalability, lightness and interoperability aspects must be balanced. In this direction, the set of proposed mechanisms in this thesis represent an excellent basis for the definition of novel security and privacy approaches under a common framework to support them, as well as their integration with complementary solutions in order to achieve a real secure and privacy-aware IoT ecosystem.

Chapter 4

Publications composing the PhD Thesis

4.1. DCapBAC: embedding authorization logic into smart things through ECC optimizations

Title	DCapBAC: embedding authorization logic into smart things through ECC optimizations
Authors	Hernández-Ramos, José L. and Jara, Antonio J. and Marín, Leandro and Skarmeta Gómez, Antonio F.
Type	Journal
Journal	International Journal of Computer Mathematics
Impact factor (2013)	0.721
Publisher	Taylor & Francis
Pages	345-366
Volume	93
Issue	2
Year	2014
ISSN	0020-7160
DOI	http://dx.doi.org/10.1080/00207160.2014.915316
URL	http://www.tandfonline.com/doi/abs/10.1080/00207160.2014.915316
State	Published

Journal details: Special Issue: Innovative Security Technologies against Insider Threats and Data Leakage
ISSN: 1424-8220
Publisher: Taylor & Francis
Impact factor (2013): 0.721
Website: www.tandfonline.com/loi/gcom20

Authors – Personal details	
Name	**José Luis Hernández Ramos**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. Antonio J. Jara**
Position	Postdoctoral Researcher and Lecturer
University	University of Applied Sciences Western Switzerland (HES-SO)
Name	**Dr. Leandro Marín**
Position	Lecturer of the Department of Applied Mathematics
University	University of Murcia
Name	**Dr. Antonio F. Skarmeta**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia

Abstract

In recent years, the increasing development of wireless communication technologies and IPv6 is enabling a seamless integration of smart objects into the Internet infrastructure. This extension of technology to common environments demands greater security restrictions, since any unexpected information leakage or illegitimate access to data could present a high impact in our lives. Additionally, the application of standard security and access control mechanisms to these emerging ecosystems has to face new challenges due to the inherent nature and constraints of devices and networks which make up this novel landscape. While these challenges have been usually addressed by centralized approaches, in this work we present a set of Elliptic Curve Cryptography optimizations for point and field arithmetic which are used in the design and implementation of a security and capability-based access control mechanism (DCapBAC) on smart objects. Our integral solution is based on a lightweight and flexible design that allows this functionality is embedded on resource-constrained devices, providing the advantages of a distributed security approach for Internet of Things (IoT) in terms of scalability, interoperability and end-to-end security. Additionally, our scheme has been successfully validated by using AVISPA tool and implemented on a real scenario over the Jennic/NXP JN5148 chipset based on a 32-bit RISC CPU. The results demonstrate the feasibility of our work and show DCapBAC as a promising approach to be considered as security solution for IoT scenarios.

4.2. A soft computing based location-aware access control for smart buildings

Title	A soft computing based location-aware access control for smart buildings
Authors	Hernández-Ramos, José L. and Moreno, María Victoria. and Jara, Antonio J. and Skarmeta Gómez, Antonio F.
Type	Journal
Journal	Soft Computing
Impact factor (2013)	1.304
Publisher	Springer
Pages	1659-1674
Volume	18
Issue	9
Year	2014
Month	April
ISSN	1432-7643
DOI	http://dx.doi.org/10.1007/s00500-014-1278-9
URL	http://link.springer.com/article/10.1007%2Fs00500-014-1278-9
State	Published

Journal details: Soft Computing for Security Services in Smart and Ubiquitous Environments
ISSN: 1432-7643
Publisher: Springer
Impact factor (2013): 1.304
Website: `http://link.springer.com/journal/500`

Authors – Personal details	
Name	**José Luis Hernández Ramos**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. María Victoria Moreno**
Position	Postdoctoral Researcher
University	Research Institute of Energy and Environment of Heidelberg (ifeu)
Name	**Dr. Antonio J. Jara**
Position	Postdoctoral Researcher and Lecturer
University	University of Applied Sciences Western Switzerland (HES-SO)
Name	**Dr. Antonio F. Skarmeta**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia

Abstract

The evolution of wireless communications and pervasive computing is transforming current physical spaces into real smart environments. These emerging scenarios are expected to be composed by a potentially huge amount of heterogeneous smart objects which can be remotely accessed by users via their mobile devices anytime, anywhere. In this paper,we propose a distributed location-aware access control mechanism and its application in the smart building context. Our approach is based on an access control engine embedded into smart objects, which are responsible to make authorization decisions by considering both user location data and access credentials. User location data are estimated using a novel indoor localization system based on magnetic field data sent by user through her personal phone. This localization system implements a combination of soft computing techniques over the data collected by smartphones. Therefore, our location-aware access control mechanism does not require any intermediate entity, providing the benefits of a decentralized approach for smart environments. From the results obtained, we can consider our proposal as a promising approach to tackle the challenging security requirements of typical pervasive environments.

4.3. SAFIR: Secure access framework for IoT-enabled services on smart buildings

Title	SAFIR: Secure access framework for IoT-enabled services on smart buildings
Authors	Hernández-Ramos, José L. and Moreno, M. Victoria and Bernal Bernabe, Jorge and García Carrillo, Dan and Skarmeta, Antonio F.
Type	Journal
Journal	Journal of Computer and System Sciences
Impact factor (2013)	1.091
Publisher	Elsevier
Pages	1452–1463
Volume	81
Issue	8
Year	2014
Month	December
ISSN	0022-0000
DOI	http://dx.doi.org/10.1016/j.jcss.2014.12.021
URL	http://www.sciencedirect.com/science/article/pii/S0022000014001858
State	Published

Special section on AINA 2014
ISSN: 0022-0000
Publisher: Elsevier
Impact factor (2013): 1.091
Website: http://www.sciencedirect.com/science/journal/00220000

Authors – Personal details	
Name	**José Luis Hernández Ramos**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. María Victoria Moreno**
Position	Postdoctoral Researcher
University	Research Institute of Energy and Environment of Heidelberg (ifeu)
Name	**Dr. Jorge Bernal Bernabe**
Position	Researcher of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dan García Carrillo**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. Antonio F. Skarmeta**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia

Abstract

Recent advances on ubiquitous computing and communication technologies are enabling a seamless integration of smart devices in the Internet infrastructure, promoting a new generation of innovative and valuable services for people. Nevertheless, the potential of this resulting ecosystem may be threatened if security and privacy concerns are not properly addressed. In this work, we propose an ARM-compliant IoT security framework and its application on smart buildings scenarios, integrating contextual data as fundamental component in order to drive the building management and security behavior of indoor services accordingly. This framework is instantiated on a holistic platform called City explorer, which is extended with discovery and security mechanisms. Such platform has been validated in a reference smart building, where reasonable results of energy savings, services discovery and authorization are achieved.

4.4. Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things

Title	Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things
Authors	Hernández Ramos, José L. and Bernal Bernabé, Jorge and Moreno Cano, Victoria and Skarmeta, Antonio F.
Type	Journal
Journal	Sensors
Impact factor (2014)	2.245
Publisher	MDPI AG
Volume	33
Issue	4
Year	2015
ISSN	15611-15639
DOI	http://dx.doi.org/10.3390/s150715611
URL	http://www.mdpi.com/1424-8220/15/7/15611/htm
State	Published

Journal details: Special Issue "Select Papers from UCAmI & IWAAL 2014 – The 8th International Conference on Ubiquitous Computing and Ambient Intelligence & the 6th International Workshop on Ambient Assisted Living (UCAmI & IWAAL 2014: Pervasive Sensing Solutions)
ISSN: 1424-8220
Publisher: MDPI AG
Impact factor (2014): 2.245
Website: `http://www.mdpi.com/journal/sensors`

Authors – Personal details	
Name	**José Luis Hernández Ramos**
Position	PhD student of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. Jorge Bernal Bernabé**
Position	Researcher of the Department of Information and Communications Engineering
University	University of Murcia
Name	**Dr. María Victoria Moreno**
Position	Postdoctoral Researcher
University	Research Institute of Energy and Environment of Heidelberg (ifeu)
Name	**Dr. Antonio F. Skarmeta**
Position	Professor of the Department of Information and Communications Engineering
University	University of Murcia

Abstract

As we get into the Internet of Things era, security and privacy concerns remain as the main obstacles in the development of innovative and valuable services to be exploited by society. Given the Machine-to-Machine (M2M) nature of these emerging scenarios, the application of current privacy-friendly technologies needs to be reconsidered and adapted to be deployed in such global ecosystem. This work proposes different privacy-preserving mechanisms through the application of anonymous credential systems and certificateless public key cryptography. The resulting alternatives are intended to enable an anonymous and accountable access control approach to be deployed on large-scale scenarios, such as Smart Cities. Furthermore, the proposed mechanisms have been deployed on constrained devices, in order to assess their suitability for a secure and privacy-preserving M2M-enabled Internet of Things.

Chapter 5

Bibliography

5.1. References

[1] IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control, 2010.

[2] B. Aboba, D. Simon, and P. Eronen. RFC 5247 - Extensible Authentication Protocol (EAP) Key Management Framework. 2008.

[3] C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Supporting Location-Based Conditions in Access Control Policies. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security - ASIACCS'06*. Association for Computing Machinery (ACM), 2006.

[4] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.

[5] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, and S. Meissner. *Enabling Things to Talk*. Springer Science Business Media, 2013.

[6] M. Bauer, E. Kovacs, A. Schulke, N. Ito, C. Criminisi, L. Goix, and M. Valla. The Context API in the OMA Next Generation Service Interface. In *2010 14th International Conference on Intelligence in Next Generation Networks*. Institute of Electrical & Electronics Engineers (IEEE), 2010.

[7] T. Berners-Lee, R. Fielding, and L. Masinter. RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax. 2005.

[8] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In *2007 IEEE Symposium on Security and Privacy'07)*. Institute of Electrical & Electronics Engineers (IEEE), 2007.

[9] A. Bierman, M. Bjorklund, and K. Watsen. RESTCONF Protocol. *IETF Internet Draft, draft-ietf-netconf-restconf-13 (work in progress)*, 2016.

[10] M. Bjorklund. RFC 6020 - YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF). 2010.

[11] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology — CRYPTO 2001*, pages 213–229. Springer Science Business Media, 2001.

[12] C. Bormann. An Authorization Information Format (AIF) for ACE. *IETF Internet Draft, draft-ietf-ace-oauth-authz-01 (work in progress)*, 2016.

[13] C. Bormann and P. Hoffman. Concise Binary Object Representation (CBOR). 2013.

[14] J. Camenisch and E. Van Herreweghen. Design and Implementation of the idemix Anonymous Credential System. In *Proceedings of the 9th ACM conference on Computer and communications security - CCS'02*. Association for Computing Machinery (ACM), 2002.

[15] J. Camenisch and A. Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Lecture Notes in Computer Science*, pages 93–118. Springer Science Business Media, 2001.

[16] J. Camenisch and A. Lysyanskaya. A Signature Scheme with Efficient Protocols. In *Security in Communication Networks*, pages 268–289. Springer Science Business Media, 2003.

[17] M. Chen, S. Mao, and Y. Liu. Big Data: A Survey. *Mobile Networks and Applications*, 19(2):171–209, 2014.

[18] S. Cheshire and M. Krochmal. RFC 6763 - DNS-Based Service Discovery. 2013.

[19] M.J. Covington, P. Fogla, Zhiyuan Zhan, and M. Ahamad. A Context-Aware Security Architecture for Emerging Applications. In *18th Annual Computer Security Applications Conference, 2002. Proceedings.* Institute of Electrical & Electronics Engineers (IEEE).

[20] D. Crockford. The application/json Media Type for JavaScript Object Notation (JSON). 2006.

[21] J. B. Dennis and E. C. Van Horn. Programming semantics for multiprogrammed computations. *Communications of the ACM*, 26(1):29–35, 1983.

[22] T. Dierks and E. Rescorla. RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2. 2008.

[23] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. SPKI Certificate Theory. 1999.

[24] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman. RFC 6241 - Network Configuration Protocol (NETCONF). 2011.

[25] D. F. Ferraiolo, S. Gavrila, V. Hu, and D. Richard Kuhn. Composing and Combining Policies Under the Policy Machine. In *Proceedings of the tenth ACM symposium on Access control models and technologies - SACMAT'05*. Association for Computing Machinery (ACM), 2005.

[26] D. Forsberg, B. Patil, H. Tschofenig, and A. Yegin. RFC 5191 - Protocol for Carrying Authentication for Network Access (PANA). 2008.

[27] D. Garcia-Carrillo and R. Marin-Lopez. Lightweight CoAP-Based Bootstrapping Service for the Internet of Things. *Sensors*, 16(3):358, 2016.

[28] J. Granjal, E. Monteiro, and J. Sa Silva. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, 17(3):1294–1312, 2015.

[29] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7):1645–1660, 2013.

[30] S. Gusmeroli, S. Piccione, and D. Rotondi. A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling*, 58(5-6):1189–1205, 2013.

[31] T. Hardjono, E. Maler, M. Machulak, and D. Catalano. User-Managed Access (UMA) Profile of OAuth 2.0. *IETF Internet Draft, draft-hardjono-oauth-umacore-14 (work in progress)*, 2016.

[32] D. Hardt. RFC 6749 - The OAuth 2.0 Authorization Framework. 2012.

[33] N. Hardy. The Confused Deputy. *ACM SIGOPS Operating Systems Review*, 22(4):36–38, 1988.

[34] A. He and B. Sarikaya. IoT Security Bootstrapping: Survey and Design Considerations. *IETF Internet Draft, draft-he-6lo-analysis-iot-sbootstrapping-00 (work in progress)*, 2015.

[35] T. Heer, O. Garcia-Morchon, R. Hummen, S. Loong Keoh, S. S. Kumar, and K. Wehrle. Security Challenges in the IP-based Internet of Things. *Wireless Pers Commun*, 61(3):527–542, 2011.

[36] P. Hunt, J. Richer, W. Mills, P. Mishra, and H. Tschofenig. OAuth 2.0 Proof-of-Possession (PoP) Security Architecture. *IETF Internet Draft, draft-ietf-oauth-pop-architecture-07 (work in progress)*, 2016.

[37] I. Ishaq, D. Carels, G. Teklemariam, J. Hoebeke, F. Abeele, E. Poorter, I. Moerman, and P. Demeester. IETF Standardization in the Field of the Internet of Things (IoT): A Survey. *JSAN*, 2(2):235–287, 2013.

[38] M. Jones. RFC 7517 - JSON Web Key (JWK). 2015.

[39] M. Jones, J. Bradley, and N. Sakimura. RFC 7519 - JSON Web Token (JWT). 2015.

[40] M. Jones, J. Bradley, and H. Tschofenig. RFC 7800 - Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs). 2016.

[41] M. Jones and D. Hardt. RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage. 2012.

[42] M. Jones and J. Hildebrand. RFC 7516 - JSON Web Encryption (JWE). 2015.

[43] A. Karp, H. Haury, and M. Davis. From ABAC to ZBAC: The Evolution of Access Control Models. In *International Conference on Information Warfare and Security*, page 202. Academic Conferences International Limited, 2010.

[44] S. Loong Keoh, S. S. Kumar, and H. Tschofenig. Securing the Internet of Things: A Standardization Perspective. *IEEE Internet of Things Journal*, 1(3):265–275, 2014.

[45] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy. Smart Objects as Building Blocks for the Internet of Things. *IEEE Internet Computing*, 14(1):44–51, 2010.

[46] N. Kushalnagar, G. Montenegro, and C. Schumacher. RFC 4919 - IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. 2007.

[47] M. Langheinrich. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing*, pages 273–291. Springer Science Business Media, 2001.

[48] S Li, J Hoebeke, F Van den Abeele, and A Jara. Conditional observe in coap. *Constrained Resources (CoRE) Working Group, Internet Engineering Task Force (IETF), draft-li-core-conditional-observe-03 (work in progress)*, 2012.

[49] H. Ma, D. Zhao, and P. Yuan. Opportunities in mobile crowd sensing. *IEEE Commun. Mag.*, 52(8):29–35, 2014.

[50] P. N. Mahalle, B. Anggorojati, N. Rashmi Prasad, and R. Prasad. Identity driven capability based access control (ICAC) scheme for the Internet of Things. In *2012 IEEE International Conference on Advanced Networks and Telecommunciations Systems (ANTS)*. Institute of Electrical & Electronics Engineers (IEEE), 2012.

[51] L. Marin, A. J. Jara, and A. F. G. Skarmeta. Shifting Primes: Extension of Pseudo-Mersenne Primes to Optimize ECC for MSP430-Based Future Internet of Things Devices. In *Lecture Notes in Computer Science*, pages 205–219. Springer Science Business Media, 2011.

[52] R. Marin-Lopez, F. Pereniguez-Garcia, A. Gomez-skarmeta, and Y. Ohba. Network Access Security for the Internet: Protocol for Carrying Authentication for Network Access. *IEEE Commun. Mag.*, 50(3):84–92, 2012.

[53] A. Menezes. *Elliptic Curve Public Key Cryptosystems*. Springer Science Business Media, 1993.

[54] R. Moskowitz and R. Hummen. HIP Diet EXchange (DEX). *IETF Internet Draft, draft-moskowitz-hip-dex-05 (work in progress)*, 2016.

[55] C. O'Flynn, B. Sarikaya, Y. Ohba, Z. Cao, and R. Cragie. Security Bootstrapping of Resource-Constrained Devices. *IETF Internet Draft, draft-oflynn-core-bootstrapping-03 (work in progress)*, 2012.

[56] S. Pearson and M. Casassa-Mont. Sticky Policies: An Approach for Managing Privacy across Multiple Parties. *Computer*, 44(9):60–68, 2011.

[57] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos. Context Aware Computing for The Internet of Things: A Survey. *IEEE Communications Surveys & Tutorials*, 16(1):414–454, 2014.

[58] R. Presuhn. RFC 3416 - Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP). 2002.

[59] A. Rahman and E. Dijk. RFC 7390 - Group Communication for the Constrained Application Protocol (CoAP). 2014.

[60] D. A. Reed, Dennis B. Gannon, and James R. Larus. Imagining the Future: Thoughts on Computing. *Computer*, 45(1):25–30, 2012.

[61] E. Rescorla and N. Modadugu. RFC 6347 - Datagram Transport Layer Security Version 1.2. 2012.

[62] C. Rigney, S. Willens, A. Rubens, and W. Simpson. RFC 2865 - Remote Authentication Dial In User Service (RADIUS). 2000.

[63] E Rissanen. XACML v3.0 Multiple Decision Profile version 1.0. *OASIS committee specification, Organization for the Advancement of Structured Information Standards (OASIS)*, 2010.

[64] E Rissanen. eXtensible Access Control Markup Language (XACML) version 3.0 OASIS Standard, 2012.

[65] R. Roman, J. Zhou, and J. Lopez. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. *Computer Networks*, 57(10):2266–2279, 2013.

[66] R. Sanchez, R. Marin, and D. Garcia. EAP-based Authentication Service for CoAP. *IETF Internet Draft, draft-marin-ace-wg-coap-eap-03 (work in progress)*, 2016.

[67] J. Schaad. CBOR Encoded Message Syntax. *IETF Internet Draft, draft-ietf-cose-msg-11 (work in progress)*, 2016.

[68] F. B. Schneider. Least Privilege and More. In *Monographs in Computer Science*, pages 253–258. Springer Science Business Media.

[69] OASIS Security Services Technical Committee et al. Security Assertion Markup Language (SAML) 2.0, 2012.

[70] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig. Authorization for the Internet of Things using OAuth 2.0. *IETF Internet Draft, draft-ietf-ace-oauth-authz-01 (work in progress)*, 2016.

[71] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig. Authorization for the Internet of Things using OAuth 2.0. *IETF Internet Draft, draft-ietf-ace-oauth-authz-01 (work in progress)*, 2016.

[72] G. Selander, M. Mani, and S. Kumar. RFC 7744 - Use Cases for Authentication and Authorization in Constrained Environments. 2016.

[73] G. Selander, J. Mattsson, F. Palombini, and L. Seitz. Object Security of CoAP (OSCOAP). *IETF Internet Draft, draft-selander-ace-object-security-04 (work in progress)*, 2016.

[74] J. Sermersheim. RFC 4511 - Lightweight Directory Access Protocol (LDAP): The Protocol. 2006.

[75] Z. Shelby, K. Hartke, and C. Bormann. RFC 7252 - The Constrained Application Protocol (CoAP). 2014.

[76] J. M. Such, A. Espinosa, A. Garcia-Fornes, and V. Botti. Partial identities as a foundation for trust and reputation. *Engineering Applications of Artificial Intelligence*, 24(7):1128–1136, 2011.

[77] S. Sun, L. Lannom, and B. Boesch. RFC 3650 - Handle System Overview. 2003.

[78] S. Sun, S. Reilly, and L. Lannom. RFC 3651 - Handle System Namespace and Service Definition. 2003.

[79] S. Sun, S. Reilly, L. Lannom, and J. Petrone. RFC 3651 - Handle System Protocol (ver 2.1) Specification. 2003.

[80] L. Tian. Lightweight m2m (oma lwm2m). *OMA Device Management Working Group (OMA DM WG), Open Mobile Alliance (OMA)*, 2012.

[81] P. van der Stok and A. Bierman. CoAP Management Interface. *IETF Internet Draft, draft-vanderstok-core-comi-09 (work in progress)*, 2016.

[82] R. H. Weber. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30, 2010.

[83] C. Weider, J. Reynolds, and S. Heker. RFC 1309 - Technical Overview of Directory Services Using the X.500 Protocol. 1992.

[84] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 1(1):22–32, 2014.

[85] S. Ziegler, C. Crettaz, L. Ladid, S. Krco, B. Pokric, A. F. Skarmeta, A. Jara, W. Kastner, and M. Jung. IoT6 – Moving to an IPv6-Based Future IoT. In *The Future Internet*, pages 161–172. Springer Science Business Media, 2013.

[86] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi. From today's INTRAnet of things to a future INTERnet of things: a wireless-and mobility-related view. *Wireless Communications, IEEE*, 17(6):44–51, 2010.

5.2. Publications

[87] J. Bernabe, J. Hernandez, M. Moreno, A. Skarmeta, N. Palaghias, M. Nati, and K. Moessner. A User-Centric Decentralised Governance Framework for Privacy and Trust in IoT. In *Models, Algorithms, and Implementations*, pages 477–519. Informa UK Limited, 2016.

[88] J. Bernal Bernabe, J. L. Hernández, M. V. Moreno, and A. F. Skarmeta Gomez. Privacy-Preserving Security Framework for a Social-Aware Internet of Things. In *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services*, pages 408–415. Springer Science Business Media, 2014.

[89] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez. TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Comput*, 20(5):1763–1779, 2015.

[90] J. L. Hernández, M. V. Moreno, A. J. Jara, and A. F. Skarmeta. A soft computing based location-aware access control for smart buildings. *Soft Comput*, 18(9):1659–1674, 2014.

[91] J. Hernández-Ramos, J. Bernabe, M. Moreno, and A. Skarmeta. Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things. *Sensors*, 15(7):15611–15639, 2015.

[92] J. L. Hernandez-Ramos, D. Garcia Carrillo, R. Marin-Lopez, and A. F. Skarmeta. Dynamic security credentials PANA-based provisioning for IoT smart objects. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. Institute of Electrical & Electronics Engineers (IEEE), 2015.

[93] J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta Gómez. DCapBAC: embedding authorization logic into smart things through ECC optimizations. *International Journal of Computer Mathematics*, 93(2):345–366, 2014.

[94] J. L Hernández-Ramos, A. J. Jara, L. Marın, and A. F. Skarmeta. Distributed capability-based access control for the Internet of Things. *Journal of Internet Services and Information Security (JISIS)*, 3(3/4):1–16, 2013.

[95] J. L. Hernández-Ramos, M. V. Moreno, J. Bernal Bernabé, D. García Carrillo, and A. F. Skarmeta. SAFIR: Secure access framework for IoT-enabled services on smart buildings. *Journal of Computer and System Sciences*, 81(8):1452–1463, 2015.

[96] J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid. Toward a Lightweight Authentication and Authorization Framework for Smart Objects. *IEEE J. Select. Areas Commun.*, 33(4):690–702, 2015.

[97] J. L. Hernandez Ramos, J. Bernal Bernabe, and A. F. Skarmeta. Managing Context Information for Adaptive Security in IoT Environments. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*. Institute of Electrical & Electronics Engineers (IEEE), 2015.

[98] A. Skarmeta, J. L. Hernandez-Ramos, and J. Bernal Bernabe. A required security and privacy framework for smart objects. In *2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*. Institute of Electrical & Electronics Engineers (IEEE), 2015.

[99] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno. A decentralized approach for security and privacy challenges in the Internet of Things. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*. Institute of Electrical & Electronics Engineers (IEEE), 2014.