

# Capítulo 1

## Introducción y objetivos

### 1.1 La seguridad como cuestión transversal en el diseño de sistemas informáticos

A lo largo de los últimos años, la naturaleza de los sistemas informáticos ha ido evolucionando de forma vertiginosa como consecuencia de los grandes avances tecnológicos de la segunda mitad del siglo XX. La *sociedad de la información* no es un término vacío de contenido, un vaticinio acerca de la influencia de la tecnología en nuestra vida cotidiana; todo lo contrario, se trata de una nueva revolución sociológica que ha modificado algunos de nuestros hábitos más cotidianos, que ha conseguido transmitir a la humanidad la sensación de proximidad, de la posibilidad de acceder a un número ilimitado de servicios y datos en continua expansión.

La red Internet es hoy en día uno de los medios de comunicación de mayor difusión e impacto, quizá el más directo y dinámico, lo que ha permitido poner en contacto a personas de todo el mundo a un coste asequible. El correo electrónico, especial precursor de esta red, ha asumido y ampliado gran parte de los servicios ofrecidos no hace mucho por el correo tradicional. Las aplicaciones de videoconferencia o voz vía Internet han dejado de ser herramientas utópicas para convertirse en componentes cotidianos, y términos como comercio electrónico, tele-trabajo, administración electrónica, redes privadas virtuales, identidad digital o tele-enseñanza son hoy comunes y hacen referencia al gran número de posibilidades y de nuevos servicios que las tecnologías de la información pueden proporcionar.

Sin embargo, parece ser un hecho que los términos *conectividad* y *seguridad* frecuentemente resultan antagónicos. En la evolución de las tecnologías de la información, la carrera entre ambos términos siempre ha tenido al primero de ellos como gran vencedor. Es un cliché que se repite, y es que los diseños de la mayor parte de los componentes relacionados con las redes de comunicaciones han estado caracterizados por desconsiderar de forma drástica la mayor parte de las cuestiones relacionadas con la seguridad. Incluso hoy en día, sigue siendo una práctica habitual posponer el diseño de los mecanismos de seguridad relacionados con una aplicación concreta, esperar a ver si la propuesta tiene éxito y después empezar a enmendar todo aquello que ha sido vulnerado. La explicación a esta

falta de coordinación puede deberse normalmente a la necesidad de resultados, entiéndase éstos como resultados económicos en el caso del sector privado o experimentales en el caso de la comunidad académica. Independientemente de las razones que hayan propiciado esta filosofía de diseño, lo cierto es que el principal trabajo de los profesionales de la seguridad de la información ha sido dotar de mecanismos de seguridad a aplicaciones y componentes ya existentes cuya vulnerabilidad ha quedado claramente expuesta, en lugar de considerar la seguridad como un aspecto transversal a tener en mente desde los primeros pasos de diseño.

Dada la creciente presencia de las tecnologías de información en la vida cotidiana, las limitaciones y vulnerabilidades detectadas toman una mayor importancia si tenemos en cuenta las implicaciones que éstas pueden llegar a tener sobre comunidades de usuarios extensas. Conocidos son los casos en los que un atacante ha podido tener acceso a números de cuentas bancarias o perfiles de consumo almacenados en un servidor indebidamente protegido, situaciones en las que la propagación incontrolada de virus ha tenido consecuencias catastróficas sobre un porcentaje considerable de los ordenadores de una organización, ataques que han dejado fuera de servicio durante horas a algunos de los servidores más visitados de Internet, suplantaciones de la identidad de altos cargos, interceptación de contraseñas transmitidas en una red de área local y un largo etcétera de actos que han aprovechado las numerosas vulnerabilidades de seguridad de los elementos que componen la red, y por extensión los sistemas distribuidos.

Quizá para entender la evolución de los mecanismos de seguridad en estos entornos habría que analizar primero las tres etapas distintas por las que, hasta ahora, ha atravesado el campo de los sistemas distribuidos. Originariamente, la principal preocupación era poder gestionar la presencia de múltiples usuarios en un mismo supercomputador. Por un lado había que establecer los criterios mediante los cuales se pudiera comprobar que sólo aquellos usuarios que habían sido autorizados podían tener acceso al ordenador. Por otro lado, se debía proteger la información asociada a cada usuario de la interceptación o modificación realizada de forma intencionada, o incluso casual, por parte de otros usuarios.

Posteriormente, debido a la revolución que supuso la fabricación masiva de ordenadores personales y a la extensión de la red Internet, el número de posibles tipos de amenazas de seguridad se multiplicó por varios órdenes de magnitud. En primer lugar, debe tenerse en cuenta que los protocolos sobre los cuales se sustenta la actual Internet (TCP/IP) fueron diseñados en la década de los setenta para poner en contacto a un conjunto de centros militares y de investigación de los Estados Unidos. La red era un recurso controlado que formaba parte del perímetro de seguridad y, en consecuencia, sólo se consideró prioritario que los protocolos proporcionaran las mejores prestaciones posibles en lo que a conectividad se refiere. El escenario que encontramos actualmente es muy distinto, ya que los mismos protocolos han seguido empleándose para crear una red pública de escala mundial, lo que ha sacado a relucir las vulnerabilidades inherentes al diseño inicial de Internet. En segundo lugar, los ordenadores personales fueron concebidos como una herramienta de trabajo, monousuario y sin previsión de ser conectados entre sí a través de una red de comunicación. Hoy en día, el panorama es completamente distinto, las posibilidades de este tipo de equipos parecen ser cada vez más ilimitadas y no se concibe el uso de un ordenador como un

elemento aislado del resto del mundo. Ha sido durante esta etapa cuando más esfuerzos ha realizado la comunidad científica a la hora de proporcionar algoritmos, protocolos, servicios y aplicaciones de seguridad capaces de afrontar las amenazas presentes, algunas heredadas de los primeros diseños y otras surgidas tras la creación de nuevos servicios.

La tercera etapa, la cual forma parte del mañana más cercano, plantea un escenario de millones de procesadores que formarán parte de los objetos más cotidianos y que harán uso de la tecnología de transmisión inalámbrica. Es un hecho que durante los próximos años habrá más teléfonos móviles conectados a Internet que ordenadores personales, y que la tecnología empieza a hacer realidad el concepto de computación ubicua, es decir, la interacción espontánea entre dispositivos digitales cuya principal misión es proporcionarnos servicio (electrodomésticos, alarmas, coches, etc.). No es una precipitación aventurar que la computación ubicua puede llegar a tener un impacto sobre la sociedad de dimensiones similares a las causadas por el nacimiento del Web. Sin embargo, hemos de tener en cuenta también los innumerables riesgos que comporta la adopción de este tipo de tecnologías, así como las repercusiones derivadas de la explotación de sus vulnerabilidades. Esto conlleva una gran responsabilidad para los miembros de la comunidad científica, los cuales deben estudiar en profundidad todos los aspectos relacionados con la seguridad antes de que las aplicaciones y servicios sean desarrollados y puestos en marcha en entornos reales.

A pesar de esta evolución de los sistemas informáticos y de su heterogeneidad, todos ellos comparten la necesidad de disponer del mismo conjunto de servicios de seguridad que permitan proteger tanto a los usuarios como a los datos y equipos implicados. Dicho conjunto lo forman los servicios de *confidencialidad*, *integridad*, *disponibilidad* y *no repudio*:

- El término *confidencialidad* hace referencia a la imposibilidad de acceder a información protegida por parte de todas aquellas entidades que no han sido autorizadas para tal efecto [21]. Dicha definición se aplica tanto a la información que pueda encontrarse almacenada en algún componente del sistema como a aquellos datos que son transmitidos a través de una red de comunicaciones.
- El servicio de *integridad* proporciona los mecanismos necesarios para detectar cualquier posible modificación o eliminación de información llevada a cabo por parte de alguna entidad no autorizada [159]. Para ello, se habilitan tanto mecanismos de prevención como de comprobación y recuperación de los datos involucrados.
- El término *disponibilidad* hace referencia al grado en el que un sistema o componente está operativo y accesible cuando es necesario hacer uso del mismo [159].
- El término *no repudio* ha sido adoptado de la literatura científica, donde originalmente hacía referencia a la imposibilidad de falsificar una firma digital por parte de una tercera entidad [71]. Hoy en día, el concepto del término se ha extendido hasta ser definido como la garantía de que tanto el emisor como el receptor de un mensaje poseen las evidencias necesarias como para que ninguno de ellos pueda negar su participación en la comunicación.

Como se puede apreciar, la protección suele estar basada en el hecho de poder diferenciar entre las entidades que han sido autorizadas y las que no. Discriminar entre ambos conjuntos conlleva normalmente la realización de un proceso que puede dividirse en tres etapas distintas: *identificación* (proceso mediante el cual un sistema de información suele reconocer a una entidad), *autenticación* (medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o participante) y *autorización* (asignación de privilegios de acceso a usuarios, programas o procesos).

En otro orden de cosas, si analizamos los distintos niveles de abstracción de un sistema informático a los cuales se les ha dotado con alguno de los cuatro servicios básicos de seguridad comentados, apreciaremos que dicha protección abarca campos tan distintos como el diseño de coprocesadores o la computación distribuida basada en componentes software, lo cual indica que se trata también de una cuestión transversal no sólo en lo que a lo que a diseño de un componente específico se trata sino también respecto al conjunto de elementos que componen un sistema de información. En los últimos años hemos asistido a grandes avances en lo que respecta a cuestiones, pertenecientes a niveles de abstracción tan dispares, como el diseño de coprocesadores seguros que permiten detectar copias ilegales de código [63], técnicas de autenticación de memoria externa que permiten detectar las modificaciones que puedan haberse realizado sobre los datos durante su camino entre procesador y la memoria [83, 127], mecanismos que permiten administrar de forma remota y segura dispositivos autónomos [130, 183], protocolos seguros de comunicación asociados a los distintos niveles que forman parte de una arquitectura de red [9, 110, 111, 168], esquemas que permiten pagar de forma electrónica los bienes adquiridos a través de la red [142], y un larguísimo etcétera de propuestas que demuestran que la seguridad es un aspecto crucial independientemente del ámbito en el cual se encuentre ubicada.

Sin embargo, respecto a esa carrera anteriormente mencionada entre conectividad y seguridad, nos encontramos aún lejos de poder contemplar cómo ambos conceptos evolucionan a la par. La comunidad científica debe seguir realizando numerosas aportaciones que permitan que paulatinamente el grado de seguridad percibida en los sistemas informáticos alcance las cotas necesarias para trasladar a los usuarios la percepción de un concepto clave, la confianza.

## 1.2 Evolución de la certificación digital como herramienta de seguridad

Dos de las cuestiones a las que más respuestas se les ha intentado proporcionar durante la última década han sido las siguientes: por un lado, *¿quién es esta entidad?*, es decir, la necesidad de diseñar mecanismos de identificación y autenticación de entidades que permitan conocer quién se encuentra detrás de una determinada comunicación o información; por otro lado, una vez resuelta la primera cuestión, el siguiente paso consiste en responder a la pregunta *¿qué está autorizada a hacer esta entidad?*, esto es, determinar el conjunto de privilegios que tiene asociados una entidad con el fin de determinar si tiene derecho a

realizar la acción que está solicitando.

De entre el conjunto de técnicas que se han propuesto para resolver estas cuestiones, constituirá la piedra angular de este trabajo el uso de la certificación digital como herramienta de seguridad. Las aportaciones realizadas dentro del marco de esta tesis están íntimamente ligadas a las distintas tecnologías de certificación que han ido surgiendo durante los últimos años, las cuales se basan a su vez en la criptografía como herramienta fundamental. En consecuencia, a lo largo de esta sección se realizará una breve introducción de los conceptos fundamentales sobre criptografía y se comentará la evolución producida en el campo de la certificación digital, desde su concepción inicial como un mecanismo de definición de identidades hasta sus connotaciones más recientes relacionadas con la gestión de privilegios.

### 1.2.1 El papel de la criptografía

El término criptografía, procedente del griego *kriptos grafein* (escritura oculta), hace referencia al conjunto de técnicas y métodos que tienen como objetivo principal la transformación de información en una codificación que resulte ilegible para todas aquellas entidades que desconozcan alguno de los parámetros involucrados en dicha transformación. Se trata de una necesidad básica en el ámbito de la protección de las comunicaciones, al principio circunscrita al ámbito militar y diplomático, y que ha tomado gran importancia con el auge de las redes de comunicaciones.

Los elementos de un sistema criptográfico son los métodos utilizados para el cifrado y descifrado de información (los cuales pueden coincidir), la clave empleada como parámetro de dichos métodos, y el espacio en el cual se encuentran definidos tanto el mensaje a codificar (denominado también *texto en claro*) como su representación codificada (denominada también *criptograma*). En función de que la clave empleada para cifrar coincida o no con la clave utilizada para descifrar, los sistemas criptográficos se agrupan en dos grandes bloques: criptosistemas simétricos y criptosistemas asimétricos.

La *criptografía simétrica* se caracteriza por emplear la misma clave tanto para cifrar como para descifrar un mensaje. En la mayor parte de los casos, el parámetro que se supone secreto para que la información sea protegida de la interceptación de terceras personas es la clave empleada. Es un hecho contrastado que la seguridad de un criptosistema no puede recaer en el desconocimiento por parte de la comunidad del funcionamiento interno de los algoritmos de cifrado o descifrado. Un exponente de la robustez del sistema es que dichos algoritmos sean públicos, de forma que su fortaleza pueda ser sometida a escrutinio público y que la seguridad del sistema recaiga solamente en la no revelación de la clave empleada.

A este tipo de criptosistemas se les conoce también como sistemas de secreto compartido, y es que su correcto funcionamiento recae en la distribución confidencial de la clave a las entidades que formarán parte de la comunicación. Sin embargo, es la propia necesidad de compartir dicho secreto la que limita en muchas ocasiones el uso de este tipo de criptografía a la hora de poner en contacto entidades sin ningún tipo de relación previa. El uso aislado de la criptografía simétrica queda reducido a aquellos ámbitos en los cuales los participantes disponen de algún tipo de medio de comunicación externo mediante el cual

puedan realizar una transmisión confidencial previa del secreto a compartir. Otra posibilidad es emplear los denominados centros de distribución de claves (KDC, Key Distribution Center), los cuales actúan como terceras partes confiables a la hora de suministrar las claves que protegerán las futuras comunicaciones a realizar por parte de las entidades del sistema. No obstante, el uso de KDCs plantea también serios inconvenientes en lo que se respecta a privacidad, suplantación de identidad o disponibilidad [181].

El hecho de que coincida la clave empleada para cifrar y descifrar conlleva también otra serie de limitaciones en la aplicación de este tipo de criptografía. Por un lado, es necesario generar una clave distinta por cada par de entidades que deseen proteger su comunicación. En consecuencia, dado un sistema con  $n$  usuarios finales, el número total de claves necesarias para poner en conectar a todos los usuarios entre sí es del orden  $O(n^2)$ , lo cual puede llegar a limitar su escalabilidad. Por otra parte, el hecho de que dos usuarios compartan el mismo secreto hace imposible determinar con seguridad quién cifró o descifró una determinada información, lo cual impide que pueda ser utilizada como mecanismo de no repudio o de autenticación de la identidad.

La historia de la certificación digital comienza a germinarse a mediados de la década de los setenta, cuando Whitfield Diffie y Martin Hellman presentan un artículo titulado "*New Directions in Cryptography*" [60] que introduce el concepto de *criptografía asimétrica* o *criptografía de clave pública*. Su novedad fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares compuestos por una *clave privada* y una *clave pública*.

Cada usuario del sistema dispone de un par de claves único y, a diferencia de lo que sucedía con la criptografía simétrica, la clave privada no es un secreto compartido sino que debe ser protegida por cada usuario. Sin embargo, la clave pública debe difundirse con el fin de que otras entidades puedan emplearla para proteger las comunicaciones realizadas con el usuario en cuestión. Este tipo de criptosistema se basa en el hecho de que resulta computacionalmente intratable intentar descubrir una clave a partir del conocimiento de la otra, lo cual anula la necesidad de establecer secretos compartidos entre entidades ya que basta con tener acceso a las claves públicas.

Lo que resulta interesante del uso de muchos de los sistemas basados en este tipo de criptografía es que las operaciones realizadas con una de las claves pueden revertirse empleando la otra. Por ejemplo, en el caso de que cierta información se cifre utilizando la clave pública de un usuario ésta podrá ser descifrada empleando la clave privada. Dado que sólo el usuario tiene acceso a dicha clave, obtenemos de esta forma un medio para proteger la *confidencialidad* de la información. Por otra parte, el cifrado realizado mediante la clave privada también puede deshacerse empleando la clave pública. Aunque esta operación carece de interés desde el punto de vista de la confidencialidad dado que la clave de descifrado es pública, y por tanto conocida por todos, representa un mecanismo muy robusto de *autenticación*. La razón es que sólo hay un usuario capaz de cifrar información que podrá ser descifrada posteriormente empleando la clave pública: el poseedor de la clave privada. Esta técnica, combinada con el uso de funciones de resumen digital, es lo que se ha dado a conocer como mecanismo de *firma digital*, ya que además de autenticación es capaz de proporcionar también los servicios básicos de *integridad* y *no repudio*.

Sin embargo, el hecho de que una clave sea pública, y que por tanto no sea necesario acceder a ella haciendo uso de un canal adicional, no implica que ésta sea auténtica. Es decir, resulta vital tener la certeza de que la clave pública pertenece a la entidad con la cual se desea establecer contacto. Un error en la asociación entre la identidad del usuario y el valor de su clave pública puede conllevar la transmisión de información sensible a terceras partes o la asociación de cierta información a la entidad equivocada. El artículo de Diffie y Hellman [60] proponía la utilización de un Archivo Público (Public File) que sería consultado por los usuarios para averiguar las claves públicas del resto de entidades del sistema. Para evitar que un atacante pudiera hacerse pasar por el archivo, todas las comunicaciones llevadas a cabo por éste debían estar firmadas digitalmente. Sin embargo, esta propuesta inicial presenta numerosos inconvenientes tanto desde el punto de vista del rendimiento como de la seguridad: el servicio puede convertirse en un cuello de botella que degradaría el rendimiento global del sistema; constituye un objetivo claro para cualquier tipo de ataque de denegación de servicio; cualquier modificación no detectada de los datos contenidos puede tener graves consecuencias para el resto de los usuarios.

Esta necesidad de asociar de forma confiable las claves públicas de los usuarios a su identidad nos lleva a los orígenes de la certificación digital. Como se verá en los siguientes apartados, la certificación digital resuelve satisfactoriamente éste y otros problemas relacionados con la gestión de privilegios, lo cual la define como una herramienta esencial de seguridad.

### 1.2.2 Certificación de la identidad

Consciente de las limitaciones del Archivo Público de claves, Loren Kohnfelder propuso en 1978 el concepto de *certificado digital de clave pública* o *certificado de identidad* [115]. Kohnfelder argumentaba que sólo hay dos formas posibles de realizar de forma segura la adquisición de las claves públicas, bien directamente mediante los usuarios implicados o bien a través de una tercera entidad confiable. Dados los numerosos inconvenientes asociados al Archivo Público, introdujo el concepto de certificado como un documento firmado digitalmente que contiene tanto la clave pública como la identidad del poseedor de la clave privada correspondiente. La diferencia principal respecto a la propuesta de Diffie y Hellman era la no dependencia de una conexión con la base de datos centralizada de claves, sino la posibilidad de que los certificados fueran emitidos por cualquier otra entidad que disfrutara de la confianza de los usuarios implicados, a la cual se le denominó *Autoridad de Certificación* (CA, Certification Authority). Realmente, este esquema de generación de documentos de identidad por parte de una tercera entidad confiable es muy común en otros aspectos de la vida real. Un ejemplo de ello es el documento nacional de identidad (DNI) emitido por el Ministerio del Interior.

El hecho de que un certificado se encuentre firmado digitalmente por una autoridad de certificación proporciona al documento un mecanismo de verificación de su integridad, lo cual hace que no sea necesario protegerlo. Esto conlleva que pueda ser almacenado en repositorios de información no confiables que podrán ser replicados y que deberán preocuparse simplemente de asegurar su disponibilidad.

Una década después de que Kohnfelder definiera el término, el estándar X.500 [38] incorporó el uso de certificados digitales X.509 [99] en su propuesta de un directorio global de entidades. De dicha propuesta nació también el concepto de *infraestructura de clave pública* (PKI, Public Key Infrastructure), el cual hace referencia al conjunto de elementos y procedimientos relacionados con la gestión del ciclo de vida de un certificado digital. Las infraestructuras de clave pública son elementos clave a la hora de dotar al sistema de la capacidad de gestionar todos aquellos aspectos implicados en la creación, publicación, renovación, validación y revocación de certificados.

A pesar de su importancia y del apogeo del que fueron protagonistas a finales de la década de los noventa, actualmente la implantación de las PKIs parece encontrarse en un estado de estancamiento [90], quizá debido a la multitud de mitos y falsedades [71] procedentes principalmente del sector privado. Durante un tiempo se dijo que las PKIs eran una necesidad imperiosa para que el comercio electrónico pudiera florecer. Posteriormente, se ha comprobado que el comercio electrónico ha ido evolucionando, a una velocidad más lenta de la que en un principio se esperó, sin la existencia de dichas PKIs. Posiblemente habría sido más correcto enunciar que eran las PKIs comerciales las que necesitaban el comercio electrónico para florecer.

Entre las causas del estancamiento de las PKIs podríamos encontrar dos grandes bloques, las relacionadas con la adopción de mecanismos que resultan obsoletos hoy en día y las asociadas a la falta de desarrollos que sean capaces de ofrecer algunos servicios básicos de seguridad no contemplados por las PKIs tradicionales, como por ejemplo la autorización y el control de acceso.

En relación con la herencia de mecanismos obsoletos, se puede afirmar que la tendencia general del mercado ha sido intentar adaptar el mundo real al diseño de las PKIs basadas en X.509 en lugar de realizar el esfuerzo de adaptar dicha tecnología a las necesidades del mercado. Por ejemplo, la idea del directorio global X.500 es uno de los ejes sobre los cuales se ha basado siempre el estándar X.509. Sin embargo, a día de hoy, dicho directorio no es una realidad, y su filosofía de identificación de entidades ha demostrado no ser la más apropiada [67]. Otro ejemplo lo constituye el uso de las listas de certificados revocados (CRL, Certificate Revocation Lists), las cuales son una adaptación de las listas negras de tarjetas de crédito que empleaban los comerciantes en los años setenta para detectar fraudes. Este tipo de sentencias negativas no responden a la pregunta de si un certificado sigue siendo válido, sólo son capaces de indicar si ha sido revocado, lo cual no es exactamente lo contrario. Como consecuencia general, los nuevos diseños de PKIs deben innovar ciertos aspectos de su funcionamiento y aportar nuevos servicios que permitan realizar una gestión más versátil y eficiente de los certificados digitales.

Respecto a las limitaciones en el campo de la autorización, hemos de tener en cuenta que el principal objetivo de las PKIs ha sido proporcionar mecanismos que permitieran establecer una relación entre el nombre y las claves públicas de las entidades. Sin embargo, el nombre no es más que un índice, un valor al cual habrá que asociar posteriormente una serie de atributos con el fin de determinar de qué privilegios dispone el usuario correspondiente (por ejemplo, si puede acceder a un determinado fichero, si tiene saldo en su cuenta corriente, si puede acceder a un laboratorio tras validarse frente a un dispositivo de

control, si tiene derecho a obtener un descuento en la compra de un producto, etc.). Tradicionalmente, la asignación de privilegios ha sido tarea de las aplicaciones finales, las cuales debían especificar y validar dichos permisos utilizando sus propios criterios y mecanismos. Como se verá a continuación, los nuevos enfoques de certificación de privilegios aportan un nuevo abanico de posibilidades a la hora de llevar a cabo los procesos relacionados con la autorización.

### 1.2.3 Certificación de los privilegios

Aunque los términos “certificado” y “certificado de identidad” se han venido utilizando como sinónimos, lo cierto es que un certificado digital puede interpretarse como un documento que recoge cierta información acerca de la entidad para la cual fue emitido. Dicha información no tiene que restringirse sólo al ámbito de la identificación, sino que puede tratarse de cualquier tipo de atributo o cualidad que desee ligarse a la entidad, como por ejemplo el conjunto de roles a los que pertenece dentro de una organización o los privilegios de los cuales disfruta dentro de un sistema. Este tipo de certificados que asocian competencias o capacidades a claves públicas se conocen con el nombre de certificados de atributo o autorización, y más genéricamente como *certificados de credencial* o simplemente *credenciales*.

Los certificados de credencial son documentos que pueden estar ligados a los certificados de identidad, pero que tienen una gestión totalmente independiente. La razón de que los privilegios aparezcan reflejados en documentos independientes al certificado de identidad está justificada por dos motivos. En primer lugar, hemos de tener en cuenta que la asignación y revocación de privilegios suele ser más dinámica que la gestión de la identidad, lo cual hace poco apropiado insertarlos en un certificado de este tipo ya que conllevaría la continua actualización del mismo. En segundo lugar, hemos de considerar que la delimitación de responsabilidades dentro de una organización puede propiciar que no resulte apropiado que una única entidad sea la encargada de determinar tanto la identidad como los privilegios de los usuarios. Normalmente, los certificados de credencial tienen una validez local, restringida a un subconjunto de elementos del sistema, lo cual hace que resulte conveniente que puedan ser gestionados de forma distribuida por autoridades de autorización locales (quizá esto último se entienda mejor extrapolándolo al mundo real, donde el conjunto de cualidades de una persona no se incluye como parte de su pasaporte, sino que están representadas por documentos independientes emitidos por otras entidades, como es el caso de un permiso de conducir, el carné de un club deportivo, una tarjeta universitaria o una tarjeta de crédito).

Los certificados de credencial constituyen una herramienta crucial en el desarrollo de sistemas de control de acceso descentralizados. Si las autoridades que los emiten se consideran confiables, las credenciales son pruebas suficientes para determinar el conjunto de privilegios asociados a una entidad, y por tanto para decidir si una determinada solicitud debe ser aprobada o denegada.

A lo largo de los últimos años, varias han sido las especificaciones en materia de certificados de credencial que han sido propuestas por parte de la comunidad científica [27, 69, 106]. Todas ellas se caracterizan por proponer mecanismos concretos de gestión de pertenencia

a grupos y de especificación de privilegios. Además, algunas proporcionan métodos genéricos de toma de decisiones de autorización e introducen el mecanismo de delegación de privilegios como herramienta fundamental de gestión de la autorización.

Sin embargo, es un campo abierto de investigación el diseño e implementación de mecanismos de gestión del ciclo de vida de este tipo de certificados. Actualmente, no existe un modelo claro que especifique cómo debe realizarse tanto el proceso de especificación de políticas de autorización como el control de su cumplimiento. Del mismo modo, son líneas de investigación activas las relativas a la transmisión, almacenamiento y revocación de credenciales. Algunas de estas cuestiones, junto con otras enumeradas en el apartado anterior, forman parte del ámbito en el cual se encuentran ubicadas las aportaciones de este trabajo de tesis.

### 1.3 Objetivos y aportaciones propias

El trabajo aquí presentado tiene tres objetivos fundamentales. Por un lado, la propuesta de una infraestructura de clave pública versátil que sea capaz de proporcionar mecanismos avanzados de gestión, los cuales permitirán integrar dicha infraestructura en escenarios de aplicación con requisitos muy diversos. En segundo lugar, extender la PKI mediante un mecanismo de gestión distribuida de credenciales capaz de dotar al sistema de los servicios básicos de autorización y control de acceso. Por último, ilustrar cómo es posible integrar las propuestas anteriores en entornos de aplicación reales, siguiendo además un enfoque metodológico estructurado.

Para la consecución del primer objetivo, este trabajo de tesis realiza las siguientes aportaciones:

- *Diseño de un sistema de certificación avanzado.* El diseño de la infraestructura propuesta en la sección 3.2 presenta algunas diferencias respecto a otros esquemas tradicionales, sobre todo en lo que respecta a la versatilidad ofrecida a la hora de ofrecer sus servicios y en la visión unificada de su gestión.
- *Definición de un mecanismo de políticas de gestión de PKIs.* Se trata de una de las aportaciones más innovadoras en lo que respecta al bloque de certificación de identidad. Las políticas permiten reflejar las condiciones expresadas en las prácticas de certificación y asegurar su cumplimiento. Como se verá en la sección 3.4, la aportación concreta consiste en la definición de dichas políticas y la provisión de los mecanismos necesarios para su edición, distribución y aplicación.
- *Propuestas avanzadas de revocación y validación de certificados.* Este trabajo, en su sección 3.5, presta especial atención a dos de las operaciones que más han sido descuidadas tradicionalmente. Por un lado, ofrece diversas soluciones al problema de la revocación, especialmente desde el punto de vista de la disponibilidad y versatilidad del servicio. En segundo lugar, ofrece mecanismos alternativos de validación de certificados basados en sentencias positivas, es decir, en la construcción de documentos que demuestren por sí mismos la validez de un certificado.

Una vez definida la infraestructura que proporcionará los servicios de identificación digital, el siguiente paso será llevar a cabo su extensión para dotar al sistema de servicios de autorización. La consecución de este objetivo abarca la mayor parte de las aportaciones propias de este trabajo, las cuales pueden agruparse de la forma siguiente:

- *Análisis del control de acceso basado en delegación.* La sección 4.4 presenta un análisis cuya meta principal es identificar tanto los aspectos a incluir en una infraestructura de autorización como las principales carencias y oportunidades de este tipo de entornos de cara a proponer soluciones reales.
- *Propuesta de un marco de intercambio de información de autorización.* Se trata de definir una propuesta que permita realizar la transmisión segura de información relativa a autorización (credenciales, políticas, solicitudes, etc.). El marco presentado en la sección 5.2 puede adaptarse a entornos caracterizados por distintos parámetros, como por ejemplo el método de distribución de credenciales, la estrategia de revelación de políticas o la optimización del proceso de solicitud.
- *Propuesta de un sistema distribuido de gestión de credenciales.* Esta propuesta constituye una de las aportaciones cruciales de este trabajo de tesis. La sección 5.3 presenta una infraestructura de autorización que permite extender los servicios ofrecidos por la PKI, de tal forma que es posible gestionar el conjunto de credenciales de un sistema concreto haciendo uso de los conceptos de delegación y control de acceso basado en roles. La propuesta contempla tanto la arquitectura del sistema como la definición de todos los elementos de información involucrados en el proceso de generación de credenciales.

El último objetivo global es la definición de un marco metodológico que permita integrar las soluciones aportadas en escenarios reales. En relación con ello, las aportaciones realizadas son las siguientes:

- *Metodología de definición de estructuras de gestión.* La metodología propuesta en la sección 5.4 permite abordar la puesta en marcha de un escenario de autorización siguiendo un enfoque estructurado basado en la identificación de los distintos elementos que compondrán el sistema y la relación entre los mismos.
- *Integración en escenarios de aplicación concretos.* La viabilidad de todos los mecanismos de autorización ha sido verificada mediante su integración en escenarios de aplicación concretos. El capítulo 6 aporta un punto de vista práctico de las propuestas realizadas, el cual permite comprobar cómo tanto la infraestructura de clave pública como las aportaciones realizadas en materia de autorización son capaces de proporcionar soluciones reales a escenarios concretos.

Como consecuencia de dichas aportaciones, este trabajo de tesis ha permitido definir una infraestructura completa de servicios de identificación y autorización basada en el uso de la certificación digital como herramienta esencial.

## 1.4 Desarrollo de la Tesis

Este primer capítulo ha presentado el contexto en el cual se encuadra la tesis, haciendo especial énfasis en la certificación digital como línea argumental. Además, se han definido los objetivos principales del trabajo y se han enumerado las principales aportaciones realizadas.

El capítulo 2 muestra todos aquellos aspectos relacionados con la certificación de identidad desde el punto de vista de los modelos de confianza propuestos, el formato de los certificados y la gestión del ciclo de vida. Se recogen las principales especificaciones realizadas por la comunidad científica y se presentan algunas de las iniciativas de certificación más importantes que se han desarrollado a nivel tanto internacional como nacional, así como las propuestas que han surgido dentro del seno del grupo de investigación.

En el capítulo 3 se detalla el diseño de la PKI que forma parte del marco de esta tesis. Para ello, se introduce el diseño general de la PKI, es decir, sus elementos constituyentes y la relación entre los mismos. A continuación, se describen las operaciones básicas de gestión realizadas por dicha infraestructura. Por último, se detallan las propuestas innovadoras que incorpora este sistema, más concretamente el mecanismo de definición de políticas de certificación y los sistemas de validación y autorrevocación de certificados.

El capítulo 4 introduce la certificación de privilegios. En primer lugar se identifican las principales carencias de los sistemas tradicionales de certificación de identidad en materia de control de acceso. Posteriormente, se analizan los diferentes modelos de control de acceso que han surgido a lo largo del tiempo. A continuación, se exponen las diferentes especificaciones existentes en materia de certificados de credencial y se realiza un estudio acerca del estado del arte de la delegación en sistemas distribuidos como mecanismo de gestión de autorizaciones. El capítulo concluye con la identificación de las propuestas en materia de autorización que forman parte de esta tesis.

El capítulo 5 presenta los detalles relativos a los componentes de la infraestructura de autorización. En primer lugar introduce el marco de intercambio de información relativa a autorizaciones, tanto su diseño general como el protocolo que implementa las recomendaciones. A continuación, se describen tanto las entidades como las especificaciones relativas al sistema de gestión distribuida de credenciales basado en delegación y roles. Por último, el capítulo concluye con la presentación de la metodología que permitirá afrontar la puesta en marcha de un sistema de control de acceso de forma estructurada y haciendo uso de la infraestructura de autorización.

En el capítulo 6 se analiza la viabilidad de las propuestas formuladas en la tesis. Para ello, en primer lugar, se comentan los detalles relativos a la implementación tanto del marco de intercambio como del sistema de gestión de credenciales. A continuación, se describe cómo se integran parte de las aportaciones realizadas en dos escenarios de aplicación, concretamente en un entorno de control de acceso físico y en un sistema de suscripción electrónica basada en un protocolo seguro de pagos. Por último, se realiza un análisis del rendimiento de las propuestas con objeto de extraer conclusiones acerca de la sobrecarga que pueden llegar a introducir dentro de cualquier escenario de autorización.

El capítulo 7 presenta las conclusiones derivadas de este trabajo y las posibles vías de

investigación que quedan abiertas a partir de lo realizado.

El documento incluye además tres apéndices. El apéndice A contiene la especificación completa de los elementos de política empleados para gestionar la PKI descrita en el capítulo 3. El apéndice B proporciona todos los detalles relativos a los mensajes del protocolo de intercambio de autorizaciones. Finalmente, el apéndice C contiene la especificación de los elementos de información definidos por el sistema de gestión distribuida de credenciales.

