Capítulo 2

Ciclo de vida de la identidad digital: infraestructuras de clave pública

El objetivo principal de este capítulo es mostrar todos aquellos aspectos relacionados con la certificación de identidad, tanto desde el punto de vista del formato de sus certificados como de la gestión de su ciclo de vida. Para ello, inicialmente se expondrán los principales estándares relacionados con este tipo de certificación y se analizarán sus modelos de confianza correspondientes. A continuación, se detallará el formato de los certificados X.509, estándar de certificación que más reconocimiento ha alcanzado entre la comunidad científica y empresarial. Posteriormente, se analizarán cuáles son las operaciones implicadas en el ciclo de vida de un certificado de identidad y se recogerán las principales recomendaciones realizadas por la comunidad científica en dicha materia. Por último, se presentarán 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.

2.1 Estándares de certificación digital de identidad

Tal y como se ha comentado en el capítulo anterior, a lo largo de los últimos años son muchos los esquemas de certificación de identidad que han ido surgiendo. De entre todos ellos, sólo dos han obtenido una gran aceptación por parte de la comunidad de Internet y de los organismos gubernamentales: el estándar X.509 [99] y el sistema PGP (Pretty Good Privacy) [37]. Otros esquemas que también ofrecen servicios de certificación de identidad, como SPKI [69] (Simple Public Key Infrastructure) o SDSI [170] (Simple Distributed Security Infrastructure), serán analizados en capítulos posteriores como parte de infraestructuras más complejas que abarcan además servicios de autorización, definición de grupos, asignación de permisos a roles, etc. En esta sección, no se entrará en los detalles acerca de la estructura de los certificados X.509 o PGP, sino que se analizará su propuesta desde el punto de vista de las relaciones de confianza existentes entre los participantes, su adecuación a los principales entornos de aplicación de Internet y su grado de implantación.

2.1.1 Modelos de confianza

Antes de analizar los modelos de confianza de ambos sistemas, quizá sería necesario empezar definiendo qué entendemos por dichos modelos. En torno al concepto de confianza se han realizado numerosas definiciones, clasificaciones, recomendaciones y formalizaciones por parte de la comunidad científica en los últimos años [3, 108, 135].

Según Gambetta [82], *"la confianza es un nivel subjetivo de probabilidad con la cual un agente realizará una acción concreta"*. Es decir, en cierto sentido, es la cantidad de riesgo que estamos dispuestos a asumir de que una determinada acción en un determinado instante pueda realizarse de forma incorrecta. Hay tres puntos importantes derivados de este tipo de definiciones: el primero es que la confianza es subjetiva; el segundo es que afecta a aquellas acciones que no podemos controlar; el último es que el nivel de confianza depende de cómo nuestros actos se vean afectados por el comportamiento del agente en el cual confiamos.

Entendemos por tanto que por modelos de confianza de los sistemas de certificación se hace referencia al tipo de relación que se establece entre las entidades emisoras de certificados, los poseedores de dichos certificados y las entidades encargadas de verificar los documentos relacionados con los mismos. X.509 y PGP tienen modelos de confianza muy distintos, tanto en lo que a relación entre entidades certificadoras y entidades certificadas se refiere, como entre las propias entidades certificadoras.

Modelo basado en autoridades de certificación específicas

El estándar X.509 considera que los certificados deben ser emitidos por entidades especiales, a las cuales denomina autoridades de certificación, que tienen la potestad especial de poder emitir certificados que serán considerados como válidos por parte de una comunidad de usuarios más o menos extensa. Se tiene así una relación asimétrica de confianza entre las entidades del sistema, donde sólo algunas de ellas tienen la capacidad de crear nuevas identidades digitales. Es un modelo donde la confianza le viene impuesta tanto a los poseedores de certificados como a las entidades encargadas de verificarlos. Cada certificado está firmado por una, y sólo una, autoridad de certificación. El modelo es muy similar al empleado en el ámbito gubernamental, donde una entidad, el Estado, es la encargada de emitir documentos que son considerados como válidos por el resto de las entidades. Por supuesto, X.509 no restringe el modelo a la existencia de una única autoridad de certificación mundial, sino que contempla la posibilidad de que muchas autoridades de certificación independientes puedan operar de forma simultánea. La existencia de relaciones de confianza entre las distintas autoridades de certificación es lo que da lugar a las distintas configuraciones posibles de confianza entre entidades emisoras: modelo jerárquico, certificación cruzada y modelo basado en autoridad de certificación puente [79].

En el modelo jerárquico mostrado en la figura 2.1 se puede observar la existencia de una autoridad de certificación raíz cuya clave pública está contenida en un certificado autofirmado, el cual debe ser distribuido de forma confiable a todas las entidades del sistema ya que no proporciona de por sí autenticación, sino sólo integridad sobre la información

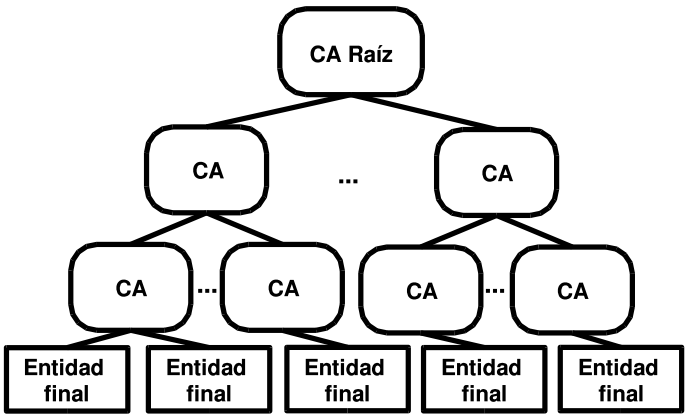

Figura 2.1: Modelo de confianza jerárquico

contenida. El resto de autoridades de certificación están subordinadas, lo que requiere que establezcan algún tipo de relación de dependencia con respecto a una autoridad de mayor nivel. Este esquema plantea algunas desventajas importantes: en primer lugar, la clave privada de la autoridad raíz representa un punto de ataque potencial que puede tener consecuencias sobre todos los certificados del sistema, puesto que en caso de compromiso de dicha clave, todos los certificados del sistema deberían ser revocados y refirmados; en segundo lugar, el enfoque jerárquico implica una cierta relación de dominancia o subordinación entre las organizaciones a las cuales están ligadas las autoridades de certificación, lo cual no es siempre cierto.

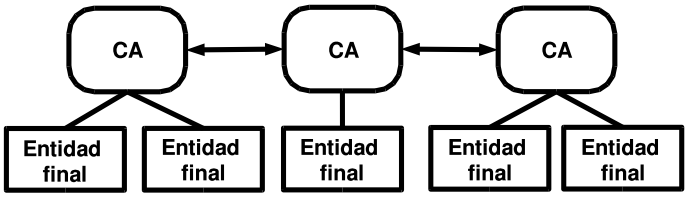

Figura 2.2: Modelo de certificación cruzada

Cuando las autoridades de certificación operan bajo la premisa de una relación de igualdad, el modelo jerárquico puede ser sustituido por la certificación cruzada o certificación punto a punto. Según este modelo, cada par de autoridades de certificación que desean establecer una relación de confianza, intercambian sus claves públicas y se certifican la una a la otra. La figura 2.2 muestra tres autoridades donde la primera y la segunda tienen una certificación cruzada, al igual que la segunda y la tercera. Con este modelo, cada autoridad de certificación es como una autoridad raíz.

Sin embargo, el modelo de la certificación cruzada puede llegar a generar del orden de $O(n^2)$ certificados en el caso de querer establecer relaciones de confianza entre un conjunto de N autoridades. La figura 2.3 muestra un esquema de certificación donde las autoridades no se certifican entre sí, sino respecto a una entidad central llamada autoridad de certificación puente [10], lo cual en el caso de disponer de N autoridades de certificación requiere

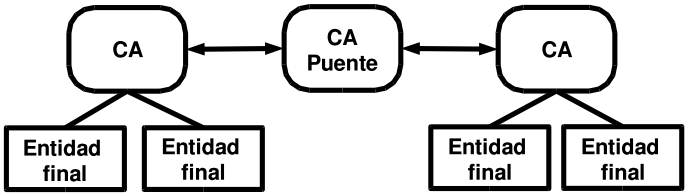

Figura 2.3: Modelo de autoridad de certificación puente

sólo N certificados punto a punto, un número sustancialmente menor que el necesario para el caso de la certificación cruzada.

Telaraña de confianza (web of trust)

En PGP no hay concepto de autoridad de certificación como tal; cualquier usuario puede certificar la clave pública de cualquier otro usuario PGP. Sin embargo, dicho certificado tendrá sólo validez para aquellas entidades que hayan decidido reconocer al signatario como certificador de confianza (*trusted introducer*, en terminología PGP). De esta forma, los usuarios PGP pueden construir caminos de certificación arbitrarios a través de toda la comunidad PGP, de ahí que este modelo de confianza se suela denominar *telaraña de confianza*.

El proceso de gestión de certificados es totalmente manual. Cada usuario dispone de una colección de claves públicas a las cuales se les asocia dos indicadores: uno que ilustra si la clave se considera válida, o no; el otro indica el nivel de confianza que se deposita en dicha clave con el propósito de que sirva como certificador de otras claves adquiridas en el futuro. El hecho de que una clave sea válida, o no, es independiente de que sea confiable como autoridad de certificación.

De hecho, mediante PGP sería posible simular el modelo de confianza de X.509 basado en autoridades de certificación específicas. Para ello, los usuarios tendrían que aceptar como certificadores válidos a aquellas entidades que asumirían el mismo rol que tiene una autoridad de certificación X.509, y considerar como no confiables al resto de claves.

2.1.2 Adecuación a entornos de aplicación e implantación

El modelo de confianza de PGP permite que cualquier entidad actúe como una autoridad de certificación capaz de emitir certificados para cualquier otra entidad. Este modelo funciona muy bien con comunidades relativamente pequeñas en las que no hay demasiada interacción entre los individuos. Debe tenerse en cuenta que PGP nació como el propósito personal de Phil Zimmerman [189] de ofrecer un servicio de confidencialidad, integridad y autenticación para el correo electrónico, entorno al cual está completamente ligado PGP. El hecho de que muchos individuos deban realizar decisiones importantes acerca de la gestión de la confianza conlleva un alto riesgo, puesto que determinaciones incorrectas pueden afectar a la comunidad en general. Se puede afirmar que, en comunidades reducidas de usuarios PGP, donde los usuarios de las claves públicas tienen una relación muy directa con

los certificadores de dichas claves, el sistema puede resultar muy apropiado. Sin embargo, esta característica no se extiende a entornos más conflictivos, automatizados, o distribuidos, como es el caso del comercio electrónico o las comunicaciones móviles. Además, el sistema PGP está muy ligado a las direcciones de correo electrónico como mecanismo de identificación de usuarios y certificadores, lo cual hace excesivamente complejo adaptarlo a otros escenarios que hagan uso de otros esquemas de nombramiento o que necesiten asociar otro tipo de atributos a las claves públicas de las entidades participantes.

Por otro lado, el esquema centralizado en el cual se basa el estándar X.509 ha sido adoptado con mayor facilidad por gran parte de organismos gubernamentales y empresas privadas. Hemos de considerar que el uso de autoridades de certificación centralizadas se asemeja bastante a la mayoría de los esquemas de funcionamiento interno de las grandes organizaciones, ya que en estos casos la emisión de documentos oficiales, la toma de decisiones, o la certificación en general suele realizarse por un número reducido de entidades, claramente identificado, y de gran confianza dentro del sistema. Además, los modelos de interrelación entre autoridades de certificación derivados a partir del estándar X.509 logran reflejar de forma bastante fiel la naturaleza de las relaciones que se establecen entre distintas organizaciones, ya sea ésta de tipo jerárquica, punto a punto, o a través de entidades mediadoras. Por último, tal y como se verá en la sección 2.2, el formato del certificado X.509 ha permitido implantar este sistema de certificación en múltiples entornos además del correo electrónico seguro, como pueden ser la navegación web segura, la protección de comunicaciones en el nivel de red o la certificación de código ejecutable. Debido a este alto grado de implantación y de aceptación, este capítulo detallará las características de este sistema de certificación y expondrá las distintas propuestas realizadas en lo que a gestión del ciclo de vida de este tipo de certificados se refiere.

2.2 El estándar X.509

X.509 [106] es el marco de trabajo de autenticación que fue inicialmente diseñado para dar soporte a los servicios de directorio X.500 [38]. Tanto X.509 como X.500 son parte de las series X de los estándares internacionales propuestos por la ISO (International Organization for Standardization) y la ITU (International Telecommunication Union). Los estándares X.500 se diseñaron para proporcionar servicios de directorio a las grandes redes de ordenadores, mientras que X.509 proporcionó el marco para autenticar dichos servicios.

El formato de los certificados X.509 ha evolucionado a través de tres versiones en diferentes ediciones del estándar. X.509v1 fue diseñado en 1988 para certificar las claves públicas de aquellas entidades que tenían asociado, de forma única, un nombre X.500 (para más información acerca de los nombres X.500 ver sección 2.2.1). La segunda versión del estándar, propuesta en 1993, proporcionaba un rango mucho más flexible de identificadores que asociar a las entidades. X.509v3, publicado en 1997, mejoró enormemente la flexibilidad de los certificados mediante la provisión de un mecanismo genérico para añadir extensiones. Esta última versión permite el uso de nombres locales en los certificados, puesto que se ha reconocido que un esquema de nombramiento único mundial es inabordable.

Son muy numerosos los estándares y los productos de certificación que se han desarrollado a partir del marco X.509. X9.55 [11], por ejemplo, es un estándar ANSI (American National Standard Institute) desarrollado por la Asociación Americana de Bancos, el cual es muy similar a X.509 pero más enfocado al sector de los servicios financieros. Algunas de las implementaciones de los certificados X.509 incluyen los sistemas de correo electrónico seguro PEM (Privacy Enhanced Mail) [109] y S/MIME (Secure/Multipurpose Internet Mail Extensions) [168], el sistema Fortezza (el estándar para correo electrónico seguro y cifrado de ficheros adoptado por el Departamento de Defensa de los Estados Unidos), los protocolos de seguridad SSL versión 3 (Secure Socket Layer) [9] y TLS (Transport Level Security) [59], y el protocolo de pago electrónico SET (Secure Electronic Transaction) [137]. Mención especial merece el grupo de trabajo PKIX [99] del IETF, el cual en los últimos años ha ido proponiendo una larga serie de borradores y especificaciones con el fin de generalizar el uso de este tipo de certificados en Internet.

En esta sección, se describirá la última versión del estándar X.509. Para una mejor comprensión del mismo, se introducirá primero el concepto de directorio y nombramiento basado en la propuesta X.500.

2.2.1 Directorio X.500

El estándar X.500 define tanto el protocolo utilizado para acceder a la información contenida en el directorio (DAP, Directory Access Protocol), como el modelo que define cómo se almacenan y gestionan los datos. El directorio X.500 es muy similar a un listín telefónico donde, dado el nombre de una persona, se puede encontrar información adicional acerca de la misma. De hecho, la idea original del proyecto X.500 era definir una única infraestructura pública formada por múltiples directorios gestionados de forma independiente, pero estructurados según un único espacio de nombres.

Una entrada en un directorio X.500 puede contener un conjunto de atributos, como el nombre de la organización para la cual trabaja la persona, su puesto de trabajo, su dirección de correo electrónico o sus certificados digitales, por nombrar sólo algunos de ellos. Estas entradas pueden representar a cualquier entidad del mundo real, no sólo personas sino también ordenadores, periféricos, compañías o naciones.

La indexación del directorio se realiza mediante la utilización de nombres globalmente únicos llamados nombres distinguidos *(DN, Distinguished Names)*. Con el fin de intentar asegurar su unicidad, los nombres se asignan de forma jerárquica siguiendo una estructura denominada *árbol de información del directorio (DIT, Directory Information Tree)* (ver figura 2.4).

Cada nodo, o vértice, del árbol tiene un nodo padre (excepto la raíz) y cualquier número de nodos hijo. Cada nodo, excepto la raíz, tiene asignado un nombre distinguido relativo *(RDN, Relative Distinguished Name)*, el cual es único entre todos los descendientes del nodo. Los RDNs de cada uno de los antecesores de un nodo se concatenan con el RDN del propio nodo para formar su nombre distinguido (DN). En la figura 2.4 se ilustra este proceso. Tras el nodo raíz, hay una entrada para cada uno de los países del mundo. Esas entradas tienen un RDN representado por un código único de dos letras asignado por la

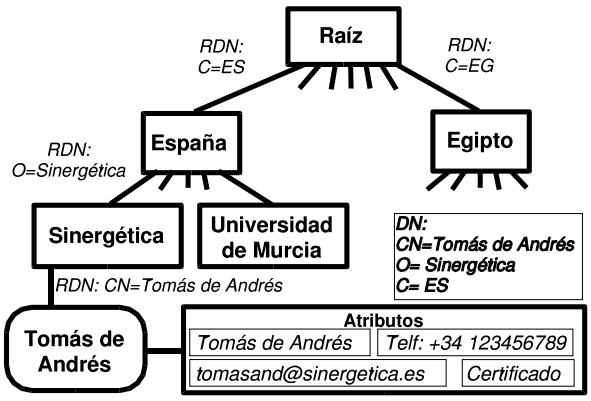

Figura 2.4: Árbol de directorio X.500

ISO. De los nodos de cada país, descienden cada una de las entradas correspondientes a las organizaciones de dicho país, como las empresas privadas, administraciones públicas, etc. Finalmente, cada organización crea entradas para cada una de sus unidades organizativas *(OU, Organizational Units)* y para sus empleados, máquinas, y cualquier otra entidad que quieran registrar. En el ejemplo de la figura, Tomás de Andrés trabaja para Sinergética, una compañía española. Sinergética ha asignado un RDN a Tomás que especifica su nombre *(CN, Common Name)*. Su entrada de directorio, accesible mundialmente haciendo uso de su DN, contiene algunos atributos, tales como su teléfono, correo electrónico, certificado, etc.

Por otro lado, con el fin de atender la necesidad de proporcionar un método de acceso y consulta a los directorios, se creó el Protocolo de Acceso Ligero a Directorios *(LDAP, Lightweight Directory Access Protocol)*. En 1997, el IETF propuso como estándar LDAPv3, publicado como RFC (Request For Comments) 2251 [188]. LDAP hace uso de una pila estándar TCP/IP y es mucho menos exigente, en lo que a recursos se refiere, que el protocolo de acceso propuesto por el estándar X.500. De hecho, LDAP se convirtió rápidamente en el estándar *de facto* a la hora de acceder a información contenida en directorios públicos.

2.2.2 Formato de los certificados X.509v3

En el periodo comprendido entre 1993 y 1994, cuando se intentó por primera vez implantar a gran escala los certificados X.509, se constató el hecho de que las versiones 1 y 2 de dichos certificados resultaban bastante deficientes en varios aspectos. Las principales razones que llevaron a considerar la posibilidad de que los certificados incluyeran otro tipo de información, que además pudiera ser extensible, fueron:

- Dado que una misma entidad puede disponer de varios certificados distintos, con claves públicas diferentes, empleados para propósitos muy diversos, es necesario poder identificar cada uno de ellos de forma independiente.

- Algunas aplicaciones necesitan identificar a los usuarios por nombres específicos, no

haciendo uso de los nombres X.500. Por ejemplo, en el ámbito del correo electrónico seguro, es más importante ligar una clave pública a una dirección de correo electrónico que a un nombre X.500.

- Los diferentes certificados pueden ser emitidos siguiendo distintas políticas y prácticas de certificación (para más información al respecto, ver sección 2.3.6), lo cual implica la necesidad de constatar las garantías aplicables a cada certificado.

Con el fin de satisfacer estos y otros requisitos, era necesario incorporar nuevos campos al formato de los certificados. De hecho, lo que se constató fue que progresivamente irían surgiendo nuevas necesidades que conllevarían la inclusión de nuevos campos, por lo que la tercera versión del estándar introdujo un mecanismo genérico de extensión de los certificados X.509. La figura 2.5 ilustra el contenido de un certificado X.509v3.

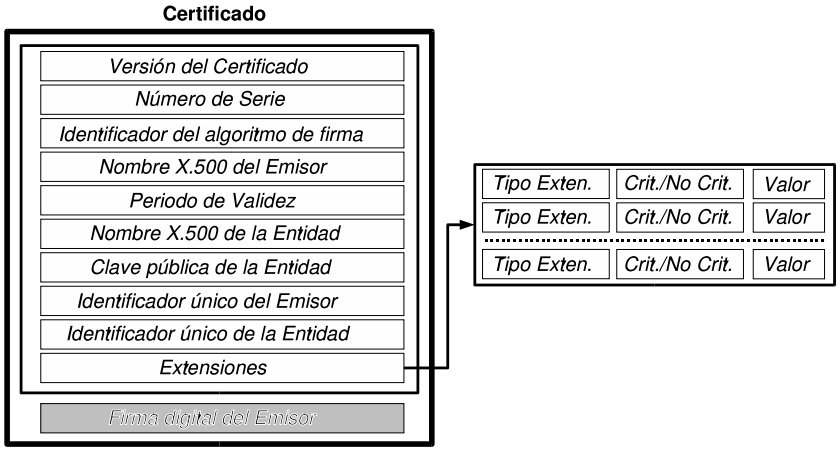

Figura 2.5: Certificado X.509v3

Los campos del certificado se interpretan de la siguiente forma:

- *Versión.* Indicador de la versión del certificado (en este caso, versión 3).
- *Número de serie.* Identificador único del certificado, asignado por la autoridad emisora del mismo.
- *Algoritmo de firma.* Identificador del algoritmo empleado por la entidad emisora para firmar el certificado.
- *Emisor.* Nombre X.500 de la entidad emisora
- *Validez.* Periodo durante el cual el certificado se considera válido, salvo revocación.
- *Entidad certificada.* Nombre X.500 de la entidad poseedora de la clave privada que está asociada con la clave pública contenida en el certificado.

- *Clave pública de la entidad.* El valor de la clave pública de la entidad, junto con un identificador del algoritmo con el cual debe usarse dicha clave.

- *Identificador único de emisor.* Secuencia de bits utilizada para identificar unívocamente a la entidad emisora, incluso en el supuesto de que el nombre de la entidad hubiera sido asignado a otras entidades a lo largo del tiempo.

- *Identificador único de entidad.* Secuencia de bits utilizada para identificar unívocamente a la entidad receptora del certificado, incluso en el supuesto de que el nombre de la entidad hubiera sido asignado a otras entidades a lo largo del tiempo.

- *Extensiones.* Las extensiones tienen un tipo asociado, que debe ser registrado mediante la asignación de un identificador único de objeto *(OID, Object Identifier)*, un indicador acerca de la criticidad y un valor. El indicador de criticidad refleja si la extensión puede ser ignorada por aquellos sistemas que no la reconozcan. Por último, el campo denominado *Valor* contiene los datos asociados a la extensión, siendo su estructura interna dependiente del tipo de extensión.

- *Firma digital.* La firma digital es un valor criptográfico obtenido a partir del resumen digital del certificado y la clave privada de la entidad emisora. Se trata del elemento que le confiere al certificado integridad y autenticidad.

Una de las diferencias más importantes entre la versión 3 y las anteriores hace referencia al mecanismo de nombramiento. La versión 3 no siguió imponiendo el sistema X.500 como único esquema de nombramiento para identificar a los emisores y los receptores de los certificados. Cualquier entidad puede ser identificada por uno o más nombres expresados mediante esquemas distintos. Es perfectamente razonable emitir un certificado que contenga varios nombres para una misma entidad, los cuales pueden ser usados por cualquier aplicación que reconozca su formato. Entre los formatos de nombramiento reconocidos explícitamente en el estándar X.509 encontramos: direcciones de correo electrónico, nombres de dominios de Internet, direcciones de correo electrónico X.400, nombres X.500, identificadores uniformes de recursos *(URI, Uniform Resource Identifier)* y direcciones del protocolo de Internet *(IP, Internet Protocol)*.

2.3 Ciclo de vida de un certificado digital

El ciclo de vida de un certificado digital de identidad, y más concretamente un certificado X.509, abarca todas aquellas operaciones de gestión de la información contenida en el mismo (par de claves, extensiones, identificadores, periodos de validez, datos sobre la entidad emisora, etc.) realizadas por las distintas entidades que componen el sistema de certificación. En esta sección, además de detallar las operaciones relacionadas con los certificados, se analizarán algunas cuestiones asociadas con la gestión de los pares de claves pública-privada, en especial las operaciones de generación y protección de claves.

2.3.1 Gestión de claves

El proceso de creación de claves criptográficas requiere aleatoriedad, de forma que el par de claves generado no sea fácilmente predecible. En el supuesto de que el valor de las claves se pudiera averiguar, o que el espacio de búsqueda se redujera de forma tan drástica que pudiera ser recorrido en un tiempo razonablemente corto, la seguridad de todo el sistema de gestión del ciclo de vida de los certificados digitales se vería seriamente afectada. Además, las circunstancias en las cuales se generen los pares de claves dependerán del uso que se les vaya a dar. Hay dos alternativas básicas a la hora de generar pares de claves:

- *Generación por parte del propietario.* El par de claves se genera en el mismo sistema (posiblemente en el mismo token hardware o módulo software) en el cual la clave privada va a almacenarse y a usarse posteriormente. Para el caso de las claves privadas de firma digital, esta alternativa resulta la más conveniente, ya que la información privada nunca abandona su lugar de generación, lo cual puede llegar a ser incluso un requisito en ciertos entornos como el descrito en el estándar X9.57 [12].

- *Generación en un elemento central.* El par de claves se genera en algún sistema central, y la clave privada se transporta de forma segura al equipo del usuario correspondiente. Este enfoque es necesario cuando los sistemas de almacenamiento de los usuarios, como ciertas tarjetas inteligentes, tienen unos recursos de memoria y de procesamiento muy limitados, o cuando la generación por parte de dichos dispositivos no es posible. La generación basada en un elemento centralizado es también aconsejable por otras razones, como por ejemplo la posibilidad de generar claves de mayor calidad o de realizar copias de seguridad de las mismas, si bien este último punto ha sido tradicionalmente foco de controversia entre la comunidad científica [4].

El uso de una u otra alternativa implicará una serie de variaciones en los procedimientos de gestión de los certificados digitales ofrecidos por un determinado sistema, aunque lo más común es que ambas alternativas sean una opción válida dentro del mismo entorno de gestión de certificados.

Una vez generado el par de claves, es necesario proteger convenientemente la clave privada, ya que la aplicabilidad de los certificados digitales recae en el hecho de que éstas sólo sean utilizadas por la persona o el dispositivo al cual pertenecen. Normalmente, las claves privadas son protegidas utilizando alguno de estos métodos:

- Almacenamiento en un módulo hardware, como una tarjeta inteligente o tarjeta PCMCIA.

- Almacenamiento en un fichero cifrado contenido en un disco duro u otro medio de almacenamiento de datos.

- Almacenamiento en un servidor de credenciales, el cual distribuye la clave privada al usuario después de haberlo autenticado.

En todos los casos, el acceso a la clave necesita estar protegido mediante el uso de uno o más mecanismos de autenticación personal. Los más comunes son los basados en PIN (Personal Identification Number) o password (palabra de paso). Otros métodos de autenticación están basados en análisis de datos biométricos [107].

2.3.2 Emisión de certificados

Como ya se comentó en la sección 2.1.1, la emisión de certificados digitales necesita de la actuación de una autoridad de certificación. Ahora bien, las interacciones entre dicha autoridad y los subscriptores o usuarios del servicio se realizan a través de entidades intermediarias conocidas como *autoridades de registro (RA, Registration Authorities)*. Estas entidades están encargadas de verificar la identidad del solicitante mediante la comprobación de los documentos acreditativos presentados de forma personal. La autoridad de registro no emite los certificados, sino que simplemente valida o rechaza las solicitudes que se le presentan. Es la autoridad de certificación la que posteriormente se encarga de emitir y publicar todas aquellas solicitudes que fueron previamente validadas. Entre las funciones ligadas a una autoridad de registro encontramos:

- Validar solicitudes de certificación.
- Aprobar o rechazar modificaciones sobre los atributos contenidos en los certificados de los usuarios.
- Generar, hacer copia de seguridad y recuperar pares de claves.
- Aceptar y autorizar solicitudes para la revocación o suspensión de certificados existentes.
- Distribuir físicamente tokens personales que contengan información criptográfica.

Una vez que las solicitudes han sido validadas y autorizadas por parte de alguna de las autoridades de registro presentes en el sistema, la siguiente etapa correspondiente al ciclo de vida del certificado es la generación del mismo. Este proceso implica los siguientes pasos:

1. La autoridad de certificación recibe la solicitud de certificación previamente validada.
2. La autoridad de certificación confirma que el certificado cumple la política de certificación y que está en consonancia con lo especificado en las prácticas de certificación (para más información al respecto, ver sección 2.3.6).
3. El certificado es firmado por un dispositivo de firma que contiene la clave privada de la autoridad de certificación. Este dispositivo puede ser un tarjeta criptográfica, un módulo software o incluso una tarjeta inteligente.

4. Se envía una copia del certificado al usuario y/o a un repositorio público de certificados.

5. Como servicio opcional, la autoridad de certificación puede archivar una copia del certificado con el fin de proporcionar una base de evidencias que podría ser utilizada en un futuro para servicios de no repudio.

6. La autoridad de certificación puede registrar ciertos detalles del proceso de generación de certificados, e incluso almacenar una copia de la clave privada asociada a la clave pública que acaba de certificar.

2.3.3 Distribución de certificados

Para poder cifrar datos o verificar firmas digitales, un usuario necesita el certificado asociado a la clave pública correspondiente, además de todos aquellos certificados asociados a las autoridades de certificación necesarias para completar el camino de certificación. Se trata de una cuestión de distribución de información, y no de un problema de seguridad, ya que los certificados no tienen que ser protegidos por tratarse de documentos firmados digitalmente. En esta sección se analizan las dos formas fundamentales de distribución de certificados.

En relación con las operaciones de firma digital, hay una forma muy apropiada para distribuir los certificados. Dado que el signatario dispone normalmente de una copia de su propio certificado, puede adjuntarlo al documento firmado digitalmente para que cualquiera que desee verificar la firma disponga de la información necesaria. De igual modo, el signatario puede añadir todos aquellos certificados que puedan ser necesarios para validar su propio certificado. Sin embargo, hay varias razones por las cuales esta técnica podría no resultar siempre apropiada. Por un lado, se puede realizar un gasto excesivo de los recursos de comunicación o de almacenamiento, ya que el usuario encargado de la verificación de la firma podría disponer previamente de una copia de los certificados. Por otro lado, no es siempre fácil averiguar qué certificados necesita el receptor para validar el mensaje, ya que las cadenas de certificación pueden ser muy complejas.

El otro método de distribución más ampliamente utilizado es el basado en servidores de directorio. Para las operaciones de cifrado de información, el acceso a certificados mediante consultas a servidores de directorio es uno de los métodos más habituales. Además, dichos servidores pueden proporcionar otro tipo de información acerca del destinatario, como la dirección de correo electrónico, información laboral, etc. Como ya se comentó en la sección 2.2.1, el estándar X.500 y el protocolo LDAP constituyen los ejes fundamentales sobre los cuales gira este servicio.

2.3.4 Renovación de certificados

Los certificados tienen un tiempo de vida limitado y, en general, deben ser renovados tras su expiración. Dicha renovación puede conllevar también un cambio de pares de claves,

aunque no es siempre obligatorio ya que es posible emitir nuevos certificados que incluyan las claves contenidas previamente en certificados ya caducados. Esta renovación puede realizarse de forma totalmente transparente de cara al usuario, con el fin de ocultarle los detalles relativos a periodos de validez, cambios de claves, y otros procesos de gestión, o por contra puede implicar la actuación del mismo, sobre todo en aquellos casos en los que se requiera la notificación del cambio de algunos datos contenidos en el certificado.

2.3.5 Revocación de certificados

Cuando se emite un certificado, se espera que el intervalo de uso del mismo coincida con el que se encuentra reflejado en el periodo de validez. Sin embargo, bajo ciertas circunstancias, los usuarios deben dejar de confiar en ciertas claves antes de que éstas caduquen. Tales circunstancias incluyen el conocimiento o la sospecha del compromiso de una clave privada, el cambio de nombre, o el cambio de relación entre la entidad certificada y la autoridad de certificación (por ejemplo, causado por una baja laboral). En estos casos, se debe revocar el certificado, logrando de esa forma que el periodo operativo del mismo sea inferior al proyectado inicialmente.

La decisión de revocar un certificado, generalmente, es responsabilidad de la autoridad de certificación, la cual actúa en respuesta a una solicitud formulada por parte de alguna entidad autorizada. El conjunto exacto de personas que está autorizado a revocar un certificado depende de las prácticas de certificación. Generalmente, el usuario afectado está autorizado a solicitar su propia revocación, además de los operarios de las autoridades de certificación o de las autoridades de registro.

Después de decidir que un certificado debe ser revocado, una autoridad de certificación debe propagar la noticia con el fin de evitar que el certificado en cuestión siga empleándose. El método más común para proporcionar información acerca de las últimas revocaciones es la emisión periódica de las llamadas listas de certificados revocados *(CRL, Certificate Revocation List)*. De hecho, el concepto de CRL forma parte del propio estándar X.509 [99]. Una CRL puede ser descrita como un documento firmado digitalmente por la autoridad de certificación que contiene una entrada para cada uno de aquellos certificados que han tenido que ser revocados antes de su expiración. Cada entrada puede contener información suplementaria, como el motivo de la revocación, o la fecha a partir de la cual el certificado debe considerarse como no válido. Estos documentos se emiten de forma periódica, con un intervalo que depende completamente de las prácticas de certificación de la autoridad, y con independencia de si han producido, o no, nuevas revocaciones. Sin embargo, como veremos en la sección 2.4, existen nuevos métodos de validación delegada y validación en línea que tratan de solventar algunas de las deficiencias asociadas a las listas de certificados revocados [113, 172].

2.3.6 Políticas y prácticas de certificación

El grado mediante el cual una entidad puede confiar en la información contenida en un certificado depende de muchos factores. Estos factores incluyen las prácticas seguidas

por la autoridad de certificación a la hora de autenticar a la entidad, las obligaciones del usuario (por ejemplo, a la hora de proteger su clave privada), y las obligaciones legales de la autoridad de certificación, es decir, garantías y limitaciones en la responsabilidad. De acuerdo con el estándar X.509, una política de certificación es un conjunto identificado de reglas que indica la aplicabilidad de un certificado a un entorno concreto de aplicación. La política de certificación, normalmente reflejada mediante una extensión contenida en cada certificado emitido, puede ser utilizada por parte de un usuario para decidir si el enlace entre identidad y clave, establecido por un determinado certificado, se puede considerar lo suficientemente confiable para el entorno de aplicación en cuestión. Se podría decir que se trata de un identificador digital que resume el conjunto de acciones llevadas a cabo por cierto sistema a la hora de gestionar el ciclo de vida de los certificados que emite.

Por otro lado, las prácticas de certificación son una declaración de los detalles del sistema y de los procedimientos seguidos a la hora de realizar las operaciones relacionadas con los certificados. Al tratarse de un documento que será consultado por los usuarios del servicio, debe ser bastante explícito, y debe proporcionar una descripción muy en profundidad de los servicios ofrecidos, responsabilidades y garantías. Ahora bien, desde el punto de vista de la interoperabilidad entre distintos sistemas de certificación, las políticas de certificación constituyen un vehículo más apropiado. Una autoridad de certificación con unas únicas prácticas de certificación puede tener asociadas distintas políticas de certificación, cada una quizá para un entorno de aplicación distinto. Para una información más en profundidad a cerca de aspectos legales relacionados con prácticas y políticas de certificación, consultar [18, 79].

2.4 Recomendaciones PKIX para el desarrollo de PKIs

Una infraestructura de clave pública *(PKI, Public Key Infrastructure)* puede ser definida como un conjunto de recursos software, hardware y humanos que posibilitan el uso de de la criptografía de clave pública para proporcionar los servicios básicos de seguridad de confidencialidad, autenticación, integridad y no repudio. En esta tesis, el concepto de infraestructura de clave pública está principalmente centrado en los componentes que forman parte de la gestión del ciclo de vida de los certificados de identidad. A lo largo de esta sección, se detallarán algunos aspectos fundamentales a considerar a la hora de construir PKIs que puedan dar soporte a grandes comunidades de usuarios. Para ello analizaremos las propuestas que ha ido desarrollando el grupo de trabajo PKIX [103] del IETF (Internet Engineering Task Force) en materia de servicios de certificación.

El grupo de trabajo PKIX se formó en Octubre de 1995 con el fin de desarrollar los estándares de Internet relacionados con el diseño de PKIs. El primer documento de trabajo fue la especificación del formato de certificación X.509 en base a la recomendación del ITU-T. A lo largo de su existencia, este grupo de trabajo ha publicado varias recomendaciones en materia de especificación de certificados de identidad y de atributo, listas de certificados revocados, mecanismos de validación de certificados, servicios de sellado de tiempo, prácticas de certificación, protocolos de gestión, o protocolos operacionales, por

citar sólo algunas de ellas.

2.4.1 Arquitectura de una PKI

Una PKI, según el modelo propuesto por el grupo PKIX, contiene cinco tipos de elementos:

- Una autoridad de certificación que emita y revoque los certificados de clave pública.
- Autoridades de registro que atestigüen la relación entre las claves públicas y la identidad de los usuarios.
- Poseedores de los certificados, los cuales pueden firmar documentos digitalmente y descifrarlos usando sus claves privadas.
- Usuarios de los certificados, los cuales pueden validar las firmas digitales y las cadenas de certificación originadas a partir de una autoridad de certificación raíz confiable, y cifrar documentos utilizando las claves contenidas en los certificados.
- Repositorios que almacenen y publiquen los certificados y las listas de certificados revocados.

La figura 2.6 ilustra la relación existente entre estos elementos. En ella se muestran las operaciones que pueden ser solicitadas por partes de los usuarios finales, las distintas funciones asociadas a cada uno de los elementos de gestión, y la relación que puede existir con otras autoridades de certificación pertenecientes a PKIs distintas. Cómo se produce la relación entre estos elementos, cuál es el formato de los mensajes intercambiados, y cuáles son los nuevos servicios de valor añadido que complementan la gestión básica del ciclo de vida de un certificado es la materia de los próximos apartados.

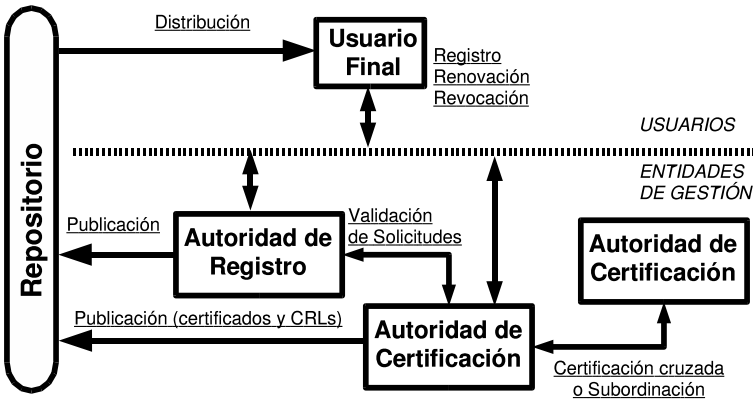

Figura 2.6: Entidades de una PKI

2.4.2 Protocolos de gestión

Los protocolos de gestión son el mecanismo mediante el cual se producen las interacciones entre los usuarios de la PKI y las entidades de gestión de la misma. Por ejemplo, un protocolo de gestión puede emplearse para transmitir la información de registro de un usuario, una solicitud de revocación, etc. Estos protocolos tienen dos componentes fundamentales: por un lado, el formato de los mensajes a enviar; por otro, el conjunto de reglas que gobierna la transmisión de esos mensajes.

Respecto al formato de los mensajes, algunas de las especificaciones PKIX se han basado en parte de la serie de estándares PKCS (Public Key Cryptography Standard) desarrollados por RSA Security, en concreto en dos ellos. El estándar PKCS#10 [120] define el formato de un mensaje de solicitud de certificación mediante el cual un solicitante puede codificar sus valores de clave pública, así como otros datos adicionales a incluir en el certificado. Por otro lado, el estándar PKCS#7 [118] especifica un formato de envoltura digital que, entre otros usos, resulta muy apropiado para encapsular los certificados emitidos como respuesta a las solicitudes en formato PKCS#10. La combinación de estos dos estándares ha sido muy popular entre la mayor parte de las implementaciones de PKI, sobre todo debido al hecho de que el software necesario para construir y decodificar estas estructuras de datos está ampliamente extendido en la mayoría de las librerías criptográficas.

Sin embargo, a mediados de la década de los 90, el grupo de trabajo PKIX inició un proyecto que tenía como fin desarrollar un protocolo de gestión capaz de tratar todas las operaciones relacionadas con el ciclo de vida de los certificados. Como consecuencia, se realizaron dos propuestas totalmente distintas. La primera de ellas se basaba en el diseño de un nuevo protocolo llamado Protocolo de Gestión de Certificados *(CMP, Certificate Management Protocol)* [7], mientras que la segunda era una propuesta que optaba por incrementar las especificaciones PKCS mediante la inclusión de nuevas características. El decepcionante resultado fue que ambas líneas de trabajo avanzaron de forma paralela, provocando que implementaciones de distintas compañías ofrecieran los mismos servicios mediante protocolos de gestión que, aunque conceptualmente iguales, eran incompatibles técnicamente. La propuesta basada en los estándares PKCS evolucionó hacia lo que hoy se conoce como CMC *(Certificate Management over CMS)* [151].

Certificate Management Protocol (CMP)

CMP especifica los mensajes a enviar en las comunicaciones entre elementos de la PKI, o entre elementos de la PKI y aplicaciones o servicios que hacen uso de la misma. Estos mensajes se definieron con el fin de dar soporte a las siguientes funciones:

- *Certificación.* Se especifica el formato de los mensajes de solicitud y de respuesta para la operación de solicitud de certificación. El formato generalmente utilizado es CRMF (Certificate Request Message Format) [149], aunque también se permite el uso de PKCS#10.

- *Prueba de posesión.* Cuando se emite un certificado, la autoridad de certificación

debe estar segura de que el solicitante está en posesión de la correspondiente clave privada. CMP especifica los intercambios de mensajes a realizar para este propósito.

- *Renovación de certificado.* Tanto para el caso de que las claves se mantengan como para el caso en el que sean reemplazadas.

- *Revocación de certificado.* Se proporciona soporte para que la solicitud pueda realizarla tanto el usuario afectado como cualquier otra entidad autorizada.

- *Notificaciones.* Se han definido mensajes para informar acerca de hechos puntuales, como la actualización del par de claves de la autoridad de autorización, emisión de CRLs, etc.

- *Envoltura digital.* CMP utiliza su propio formato de envoltura digital en caso de que sea necesario proteger un mensaje para propósitos de autenticación, integridad o confidencialidad.

Como puede comprobarse, los objetivos de CMP eran bastante ambiciosos. CMP define 25 tipos de mensajes, incluyendo solicitudes y confirmaciones. Su complejidad frente a los enfoque basados en PKCS#10 y PKCS#7 ha sido uno de sus principales puntos débiles a la hora de extenderse entre la comunidad científica y los productos comerciales.

Certificate Management over CMS (CMC)

La especificación CMC define un conjunto de mensajes destinados principalmente al proceso de registro y emisión de certificados. CMC también proporciona soporte para las solicitudes de revocación y renovación, no presentes en los sistemas PKCS. El sistema de envoltura digital está basado en la sintaxis CMS (Cryptographic Message Syntax) [98] de S/MIME [168], dado que la idea principal de CMC es emplear S/MIME como protocolo de de gestión de la PKI. El enfoque seguido por esta especificación se basa en la combinación de técnicas existentes, más que en el diseño de una propuesta completamente nueva (como CMP).

2.4.3 Protocolos operacionales

Los protocolos operacionales tienen la función de distribuir información acerca de los certificados, las listas de certificados revocados o la relación existente entre un documento y un determinado instante de tiempo. La distribución se puede realizar utilizando distintos medios, como DNS (Domain Name System) [64], LDAP [188], HTTP (Hypertext Transfer Protocol) [77] o X.500 [38]. Especial atención merecen aquellos protocolos relacionados con la distribución de información acerca del estado de los certificados, también conocidos como protocolos de verificación en línea, y los mecanismos de sellado digital de tiempo.

Validación de certificados

Por protocolos operacionales de validación de certificados entendemos aquellos mecanismos que proporcionan información acerca del estado actual del certificado (revocado, válido o estado desconocido), o relativa a la cadena de certificación necesaria para validar la autenticidad del certificado. Para ello, hay definida una serie de protocolos de entre los cuales analizaremos OCSP (Online Certificate Status Protocol), DPD (Delegated Path Discovery), DPV (Delegated Path Validation) y SCVP (Simple Certificate Validation Protocol).

Una de las principales deficiencias de las CRLs es que la periodicidad con la cual se publican las últimas revocaciones no está bajo el control de las aplicaciones que deben validar los certificados. De forma ideal, el conocimiento acerca de si un certificado se encuentra revocado, o no, debería ser adquirido en el mismo momento en el cual necesita utilizarse el certificado. Mediante un mecanismo de verificación en línea, una aplicación o usuario puede obtener respuestas instantáneas acerca del estado de los certificados implicados. Conscientes de este hecho, el grupo de trabajo PKIX desarrolló OCSP (Online Certificate Status Protocol) [150], un protocolo que define el formato estándar de las solicitudes y respuestas intercambiadas para averiguar el estado de un certificado. Este protocolo se basa en la existencia de un servidor OCSP, encargado de procesar las solicitudes de validación que recibe, verificar el estado de los certificados implicados utilizando algún mecanismo confiable y responder con una sentencia firmada digitalmente que incluya dicho estado.

Los protocolos DPV (Delegated Path Validation) y DPD (Delegated Path Discovery) [165] están relacionados con el procesamiento de cadenas de certificación. Ambos están basados en la posibilidad de delegar, en una tercera entidad confiable, la realización de ciertas comprobaciones que involucran a varios certificados relacionados por formar parte de la misma cadena de confianza. DPV establece los formatos de solicitud y respuesta necesarios para consultar si los certificados implicados siguen siendo válidos (es decir, si no están revocados y siguen unidos por una relación de confianza). Por otro lado, los servidores DPD tienen la función de descubrir, en nombre de sus usuarios, toda la información de estado para validar localmente un certificado (certificados de autoridades de certificación, listas de certificados revocados, respuestas OCSP, etc).

SCVP (Simple Certificate Validation Protocol) [134] es una línea actual de trabajo que intenta ocultar a los clientes los detalles concretos del método de validación de certificados que se está empleando en un sistema para averiguar el estado de los mismos. Independientemente de que la consulta sea a una CRL, mediante OCSP o cualquier otro mecanismo, SCVP proporciona una única visión de la operación de validación con el fin de evitar que las distintas aplicaciones deban conocer los detalles concretos de los métodos de validación empleados. De esta forma, el cliente delega en un servidor SCVP la responsabilidad de obtener (mediante consultas OCSP, CRLs, DPV, DPD, etc.) toda la información necesaria para determinar si un conjunto de certificados es confiable.

Sellado de tiempo

El sellado de tiempo (del inglés, *time-stamp*) se emplea para atestiguar que un determinado evento se produjo en un determinado instante de tiempo. Por ejemplo, en una transacción económica, el sellado de tiempo puede emplearse para establecer una relación entre la factura y el instante de compra, o entre la distribución del producto comprado y el momento en el cual se efectuó dicha distribución. Sin embargo, su uso no está sólo restringido a escenarios de pago, sino que puede ser empleado igualmente en entornos de validación de documentos, notaría electrónica, bases de datos, etc. En un sentido amplio del término, un sellado de tiempo es el establecimiento de una relación confiable entre un determinado elemento digital y un instante de tiempo en el cual se quiere dejar constancia de que el elemento digital existió. No es necesario que dicho sellado contenga completamente el elemento digital a sellar, sino que bastará en la mayoría de los casos con la presencia de su resumen digital.

Para que el sellado de tiempo pueda ser considerado como confiable, la estructura de datos que lo contiene debe estar protegida criptográficamente, y además la marca de tiempo debe haber sido obtenida de una fuente confiable. Esto último puede asegurarse mediante la utilización de proveedores de valores temporales basados en UTC (Universal Time Coordinated). Dichos proveedores son entidades nacionales o internacionales que funcionan de forma totalmente independiente a los servicios que hacen uso de ellos y que aseguran una alta precisión en los datos temporales que suministran.

Respecto a la protección criptográfica del documento que contiene la asociación entre el evento y el instante de tiempo en el cual fue sellado, debe ser suficiente como para hacer imposible que de forma retroactiva pueda modificarse la información contenida. Uno de los mejores métodos para lograr este objetivo es que el documento se encuentre firmado digitalmente por una entidad confiable.

En concreto, el grupo de trabajo PKIX define el sellado de tiempo como un servicio en el cual una tercera parte confiable (a la cual denominan autoridad de sellado de tiempo -*TSA, Time Stamp Authority*-) firma un mensaje con el fin de probar que existía antes de un determinado instante de tiempo. En el documento de definición del servicio [6], se especifica el protocolo basado en mensajes de solicitud y respuesta que debe emplearse para asociar marcas temporales confiables a documentos digitales.

Frente a este modo de operación básico, se han propuesto también esquemas encadenados que tratan de minimizar las consecuencias derivadas del compromiso de la clave de la TSA [32, 62]. Dichos esquemas se basan en el uso de secuencias lógicas de resumenes digitales distribuidas entre los distintos sellos de tiempo, las cuales establecen un orden cronológico que dificulta la falsificación posterior de alguno de los elementos de información contenidos en el sello.

2.5 Entornos de PKI

Durante los últimos años, muchos han sido los desarrollos en materia de PKI que han sido llevados a cabo en distintos países e instituciones con el fin de dotar de servicios de certificación a comunidades de usuarios extensas. En esta sección, vamos a describir las iniciativas internacionales y nacionales más importantes que tienen como base el estándar X.509 y las recomendaciones PKIX. Por último, se analizarán los desarrollos realizados previamente por el grupo de investigación ANTS en materia de certificación, con el fin de ubicar la línea de partida para el diseño y la implantación de la infraestructura de clave pública del Proyecto PISCIS, proyecto dentro del cual se encuadran los desarrollos de gestión de identidad digital que forman parte de esta tesis.

2.5.1 Desarrollos nacionales e internacionales

La gran mayoría de las PKI desarrolladas con éxito están bajo el control de una única empresa, y su ámbito de aplicación no va más allá del uso interno o de sus filiales. Sin embargo, en este apartado nos vamos a centrar en aquellas infraestructuras de clave pública que implican a múltiples organizaciones, ya sean nacionales o internacionales. No se trata de describir los detalles concretos de las implementaciones asociadas a estas infraestructuras, sino de conocer los propósitos de dichos sistemas, las comunidades de usuarios implicadas y los servicios ofrecidos.

PEM (Privacy Enhaced Mail)

En el año 1993, la comunidad científica de Internet completó el desarrollo de un conjunto de estándares para el sistema PEM [109], los cuales incluían protocolos de correo electrónico seguro y especificaciones relacionadas con la PKI de soporte. La infraestructura PEM, ilustrada en la figura 2.7, seguía el modelo de confianza jerárquico. A pesar de que el sistema PEM no tuvo gran aceptación por parte de las empresas privadas y de la comunidad Internet en general, el diseño de su PKI has sido lo suficientemente significativo como para que muchas PKIs posteriores hayan basado sus desarrollos en este modelo.

El modelo PEM está basado en tres tipos de autoridades de certificación:

- *Internet Policy Registration Authority (IPRA).* Se trata de la autoridad raíz de la infraestructura. Está controlada por la *Internet Society*, una organización internacional sin ánimo de lucro.

- *Policy Certification Authorities (PCAs).* Las PCAs son las únicas autoridades certificadas por la IPRA. Una PCA debe registrarse frente a la IPRA y publicar su política de certificación de usuarios y autoridades de certificación subordinadas. Dado que cada camino de certificación PEM contiene exactamente una única PCA, los usuarios pueden identificar fácilmente las políticas de certificación seguidas.

- *Certification Authorities (CAs).* Estas entidades representan, por ejemplo, organizaciones privadas, unidades organizativas o áreas geográficas concretas.

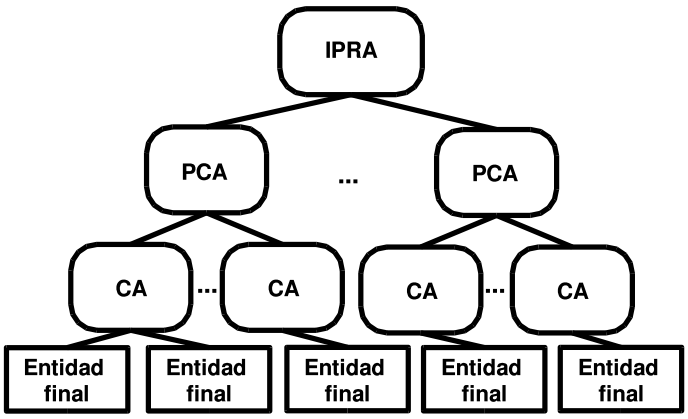

Figura 2.7: Infraestructura PEM

El desarrollo de PEM presentó algunas soluciones a problemas muy importantes. Por ejemplo, fue pionero en el concepto de política de certificación. Sin embargo, la implantación del sistema PEM a gran escala fracasó por varios motivos, entre ellos la aparición de nuevas tecnologías de correo electrónico seguro como S/MIME [168].

Secure Electronic Transaction (SET)

Las principales compañías de tarjetas de crédito, lideradas por Visa y MasterCard, desarrollaron el sistema SET [137], el cual está compuesto por un complejo protocolo de intercambio seguro de datos y una infraestructura de clave pública. El sistema SET está destinado a dar soporte a los pagos basados en tarjetas de crédito a través de Internet, y está compuesto por varios tipos distintos de entidades, como los emisores de tarjetas, los usuarios de las tarjetas, bancos de clientes, comerciantes, bancos de los comerciantes, autoridades de certificación y pasarelas de pago (las cuales conectan el sistema con la red interbancaria, medio en el cual se realizan realmente las transacciones).

La criptografía de clave pública se emplea para proporcionar servicios de autenticación y confidencialidad a todas las partes implicadas en una transacción electrónica. La estructura jerárquica de la PKI de SET, mostrada en la figura 2.8, incluye los siguientes tipos de autoridades de certificación:

- *Autoridad de Certificación Raíz.* Esta autoridad se mantiene desconectada (off-line) y se utiliza sólo para emitir certificados a las distintas autoridades de certificación de las compañías de tarjetas de crédito.

- *Autoridad de Certificación de las Compañías.* Cada compañía, como Visa o MasterCard, dispone de una autoridad de certificación a este nivel. Desde el punto de vista de las políticas de certificación, cada compañía puede establecer sus propios criterios.

- *Autoridad de Certificación Geopolítica.* Este nivel opcional de la jerarquía permite a las compañías distribuir la responsabilidad de la gestión de los certificados entre distintas regiones geográficas o políticas.

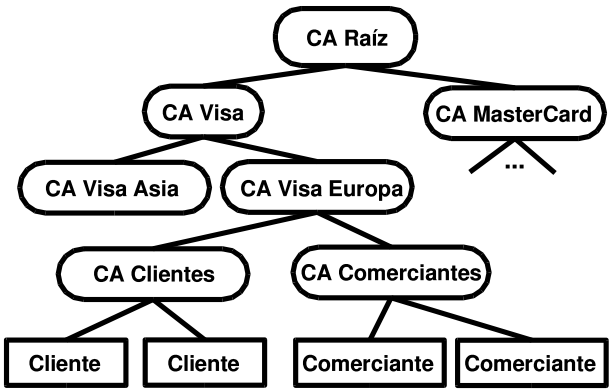

Figura 2.8: Infraestructura SET

- *Autoridad de Certificación de los Clientes.* Son las encargadas de emitir los certificados digitales a todos aquellos subscriptores de la compañía correspondiente. Estas autoridades suelen ser gestionadas por entidades financieras con las cuales el cliente tiene una relación contractual.

- *Autoridad de Certificación de los Comerciantes.* Emiten certificados digitales a los comerciantes que forman parte del sistema SET.

A pesar de todos los esfuerzos de estandarización, las detalladas especificaciones del sistema y el gran interés que despertó en su momento esta iniciativa entre las principales entidades financieras, el sistema SET ha ido decayendo en los últimos años, hasta ser hoy en día una propuesta que apenas ha llegado a implantarse a nivel mundial. Las claves de su anunciado fracaso pueden encontrarse en la complejidad intrínseca del sistema (protocolos con gran carga criptográfica, gran número de mensajes, complicados procedimientos de registro, necesidad de entidades mediadoras como las pasarelas de pagos), la necesidad de la colaboración de muchas entidades con intereses muy distintos, la reticencia de las entidades financieras a usar la red Internet como mecanismo de transporte y la influencia muy negativa que ha tenido la escasa implantación de la tecnología de PKI durante los últimos años.

Identrus

Identrus [102] se formó en 1999 como un consorcio de las principales entidades financieras del mundo, entre las cuales también se encuentran las principales entidades bancarias españolas. Su principal objetivo es potenciar el comercio electrónico B2B (*Business to Business* o comercio entre empresas). Las entidades financieras proporcionan los servicios de gestión de confianza, intentando crear un proceso comercial donde los participantes posean una única identidad digital que habilite los mecanismos de no repudio.

El núcleo de Identrus es una PKI de escala internacional donde las empresas son certificadas a través de sus instituciones financieras. Toda la infraestructura está dotada de un

sistema de validación en línea del estado de los certificados que opera mediante el protocolo OCSP. La PKI está estructurada jerárquicamente en los siguientes niveles:

- *Autoridad Raíz Identrus.* La raíz establece los procedimientos y las políticas de gestión de riesgos del resto del sistema. A este nivel se encuentra definido un repositorio público que proporciona información en tiempo real del estado de las entidades de nivel 1.

- *Autoridad de nivel 1.* Este nivel está formado por las principales instituciones financieras, las cuales certifican a las entidades de nivel 2 y a sus propios clientes.

- *Autoridad de nivel 2.* En este nivel se encuentran las instituciones financieras de menor entidad, las cuales deben ser certificadas por las instituciones de nivel 1.

- *Empresas.* Se trata de los clientes comerciales de las instituciones tanto de nivel 1 como de nivel 2, las cuales establecen transacciones entre sí haciendo uso de los servicios proporcionados por Identrus.

Este sistema se encuentra actualmente en marcha, y supone una simplificación sustancial frente a SET, ya que el sistema se ha reducido a un mecanismo de certificación digital para empresas, con las cuales es más fácil mantener relaciones comerciales confiables y de largo plazo.

EuroPKI

En lo que respecta a infraestructuras de certificación de ámbito europeo, varias han sido las iniciativas llevadas a cabo durante los últimos siete años destinadas a desarrollar un sistema de tales características. Tomando en consideración los resultados de proyectos como ICE-TEL [101] y ICE-CAR [100], varias organizaciones europeas definieron en Diciembre de 1999 la infraestructura denominada EuroPKI [72].

EuroPKI proporciona una autoridad de certificación raíz y un marco sobre el cual desarrollar pruebas de certificación jerárquica y cruzada entre las organizaciones participantes. La estructura actual de dicha infraestructura está formada por los siguientes elementos:

- Una autoridad raíz (denominada *Top Level CA*) getionada por el Instituto Politécnico de Turín.

- Varias autoridades de certificación subordinadas de nivel nacional, entre las cuales se encuentran la *CA Italiana*, *CA Eslovena*, *CA Polaca*, *CA Noruega (UNINETT)*, *CA Británica (University College of London)*, *CA Irlandesa (Trinity College of Dublin*, *CA Austriaca (IAIK)* y la *CA Española (IRIS-PCA).*

- Autoridades de certificación de tercer nivel asociadas a distintas instituciones y empresas de cada país.

Actualmente, este iniciativa se encuentra en una fase de indefinición, ya que tras haberse realizado las pruebas pertinentes en lo que respecta a interoperabilidad de los certificados emitidos por las distintas autoridades, la propuesta no ha establecido ningún objetivo concreto desde mediados del año 2001, y el número de países y organizaciones participantes sigue siendo muy bajo.

Proyecto CERES

La iniciativa española de certificación puesta en marcha por la Administración es el denominado Proyecto CERES (CERtificación ESpañola) [58], el cual se encuentra liderado por la Fábrica Nacional de Moneda y Timbre (FNMT). Su objetivo principal es el establecimiento de una autoridad de certificación pública que permita dotar de servicios básicos de autenticación y confidencialidad a las comunicaciones, realizadas vía Internet, entre las administraciones públicas y las empresas o ciudadanos.

El proyecto, además del uso de ficheros criptográficos, incluye la posibilidad del uso de dispositivos de almacenamiento seguro de información, como tarjetas inteligentes que contengan las claves privadas asignadas a las empresas y ciudadanos.

Su infraestructura de clave pública no es jerárquica, ya que está constituida por una única autoridad de certificación raíz gestionada por la FNMT. El proyecto especifica que las candidatas a constituirse como autoridades de registro son las oficinas de correos, presentes en la mayoría de localidades españolas.

En la actualidad, el principal entorno en el cual se ha hecho uso de este proyecto es en la presentación telemática del Impuesto sobre la Renta de las Personas Físicas (IRPF). Mediante dicho servicio, los ciudadanos tienen la posibilidad de presentar su declaración a la agencia tributaria a través de Internet previa obtención de un certificado digital X.509, el cual puede solicitarse actualmente sólo en las oficinas de la Agencia Tributaria, ya que las oficinas de correos no actúan en este momento como autoridades de registro.

2.5.2 Desarrollos previos realizados en la Universidad de Murcia

En el año 1997, la Universidad de Murcia inició un proyecto bajo el nombre de Proyecto SSL [35], cuyo objetivo principal era dotar a sus miembros de mecanismos que hicieran posible el establecimiento de comunicaciones seguras a través de la red corporativa. Se trataba de un problema bastante complejo debido a la gran cantidad de usuarios implicados (cerca de 40.000) y la heterogeneidad de los mismos (profesores, investigadores, personal de administración y servicios, alumnos). Uno de los objetivos fundamentales era que los desarrollos pudieran ser utilizados desde los puestos de trabajo, desde el hogar, o desde las ALAs (Aulas de Libre Acceso), lo que conllevaba tener que considerar varios sistemas operativos, dispositivos, navegadores, lectores de correo electrónico, etc.

El sistema diseñado finalmente tenía tres piedras angulares. En primer lugar, se basaba en el uso de las tarjetas inteligentes que la Universidad de Murcia proporciona a todos sus miembros, las cuales tienen capacidad para almacenar información confidencial. El segundo concepto clave era hacer uso de los estándares de seguridad existentes en dicho momento

para proteger las comunicaciones entre los miembros de la comunidad, más concretamente el protocolo SSL [9] para las comunicaciones HTTP seguras, y el protocolo S/MIME [168] para el envío de correo electrónico. La última piedra angular era hacer uso del estándar de certificación X.509 [99] para dotar de identidad digital a todos los usuarios y procesos.

Respecto a este último punto, es importante recalcar que en aquellos momentos los desarrollos en materia de certificación X.509 eran escasos y que, ya desde el principio, se tomó conciencia de que el ciclo de vida de los certificados y su integración con las tarjetas inteligentes sería la cuestión más compleja a resolver. La infraestructura de clave pública desarrollada finalmente [36] tomaba como base la herramienta Netscape Certificate Server (ahora conocida como Certificate Management System [155]), sobre la cual se construían el resto de los elementos del sistema, tales como las autoridades de registro o los servidores de directorio. El otro punto importante del proyecto respecto a la integración de los certificados X.509 y las tarjetas inteligentes fue el desarrollo de un módulo que seguía las especificaciones del estándar PKCS#11 [121]. Mediante dicho software era posible hacer uso de la información contenida en las tarjetas inteligentes (claves privadas y certificados de identidad) a la hora de establecer conexiones seguras mediante SSL o de intercambiar correos confidenciales y autenticados mediante S/MIME.

Centrándonos en los detalles de la infraestructura de clave pública, se desarrolló un sistema distribuido formado por varias autoridades de registro, una autoridad de certificación, y un servidor de directorio. Sólo las autoridades de registro se diseñaron e implementaron como parte del proyecto, siendo el resto de elementos productos comerciales. La PKI resultante proporcionaba servicios de certificación a través de las autoridades de registro, almacenamiento de información en las tarjetas inteligentes, publicación de datos en el servidor de directorio y gestión de solicitudes de revocación. Se trataba de un sistema piloto, muy limitado en ciertos aspectos, pero que era capaz de proporcionar la mayor parte de los servicios demandados en dicho momento.

La concesión posterior en el año 1999 del proyecto de investigación PISCIS (Piloto de definición de una Infraestructura de Seguridad para el Comercio Inteligente de Servicios), conllevaba la necesidad de diseñar y desarrollar una infraestructura mucho más versátil, capaz de proporcionar más servicios que los desarrollados en el marco del Proyecto SSL, así como de adaptarse a las nuevas tecnologías surgidas durante los últimos años tanto en materia de PKI como de tarjetas inteligentes e interfaces criptográficas. En el siguiente capítulo se abordarán los detalles de dicha PKI, diseñada e implementada en el marco de esta tesis.