# 56. Firma digital. Certificación digital. Entidades de Certificación

Antonio Villalón Huerta
Colegiado número 00033

***Resumen:*** *En este capítulo vamos a tratar los conceptos más básicos de la firma digital y su evolución lógica: la certificación digital. Tras conocer las bases teóricas y las aplicaciones elementales de estos esquemas, hablaremos de su gran aplicación práctica, las infraestructuras de clave pública, su arquitectura, los elementos que las conforman, sus funciones y aplicaciones y, por supuesto, sus grandes problemas (que los tienen).*

## 1 Introducción: firma digital

Dado que las nuevas tecnologías se introducen cada vez más en nuestra vida cotidiana, sustituyendo día a día incluso a tareas que hace tiempo era impensable realizar con un ordenador, parece obvia la necesidad de un proceso que emule nuestra firma manual, la rúbrica necesaria en multitud procesos cotidianos (en el banco, en la compra y venta, a la hora de presentar impresos oficiales...), con las mismas propiedades y garantías que ésta pero con la ventaja de que no necesite de nuestra presencia física en un determinado lugar para poderse llevar a cabo. Nace de esta necesidad la firma digital, un proceso potenciado especialmente desde hace unos años a todos los niveles (administrativo, empresarial, bancario), que no es más que el equivalente electrónico a la firma manual. Sus propiedades son, por tanto, muy similares a las de ésta:

- Sólo su propietario puede crearla.
- Debe depender del documento firmado (no puede exportarse una firma de un mensaje a otro).
- Debe ser fácilmente reconocible y verificable por emisor y receptor.
- No puede ser repudiada por su propietario.
- Debe ser imposible (al menos computacionalmente) alterarla.

- Debe ser barata y fácil de generar.

Actualmente se utiliza casi con exclusividad criptografía de clave pública para firmar digitalmente cualquier información, ya que presenta dos grandes ventajas con respecto a los modelos basados en cifrados simétricos: no requiere de ningún tipo de secreto inicial (clave) entre emisor y receptor, y además no es necesario renovar constantemente los pares clave pública / clave privada para proteger su confidencialidad.

Hoy en día existen dos grandes aproximaciones a la firma digital: la **firma directa** (*true signature*) y la firma arbitrada. En el primer caso, la idea que subyace al proceso es muy sencilla: la información a firmar se resume digitalmente con una función *hash* que genera un mensaje comprimido, mensaje que se cifra con la clave privada de quien está firmando la información (formando la firma en sí) y que sólo puede ser descifrado utilizando su clave pública. El receptor de la información original genera, con la misma función hash, un resumen que ha de ser idéntico al generado por el emisor, y por otro lado descifra la firma que a priori corresponde al mensaje y también ha recibido del emisor (para lo que usa la clave pública de este); si ambos resúmenes coinciden, la firma es válida. El proceso de firma digital directa se muestra gráficamente en la siguiente figura:

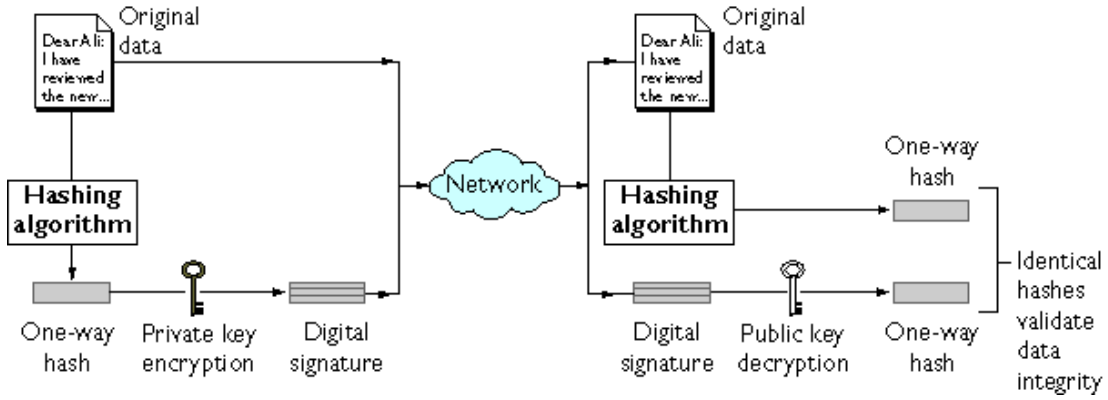


*Figura 1*. Proceso de firma digital (Netscape, 1998).

¿Qué significa *'la firma es válida*? Si el resumen de la información original y la firma descifrada coinciden, se puede asegurar por un lado que la información recibida es idéntica a la enviada en origen (valida su integridad), y por otro que fue firmada por la clave privada asociada a la pública que ha utilizado para descifrar: confirmar que la clave pública usada corresponde a una determinada persona u organización es algo más complejo, ya que se trata de un proceso en el que entran en juego los certificados y la autenticación, que trataremos en este capítulo. Si por el contrario ambos

resúmenes no coinciden, el mensaje original puede haber sido adulterado, o firmado con una clave privada diferente a la del emisor.

En el segundo gran esquema de firma digital al que hacíamos referencia, la **firma arbitrada**, cada mensaje firmado de emisor a receptor pasa por un árbitro, encargado de validar el origen y el contenido de tal mensaje; si tal validación es correcta, se envía al receptor junto a una marca de tiempo y una confirmación del árbitro de que el mensaje es válido. Evidentemente, ambas partes deben confiar en el correcto funcionamiento del árbitro, crucial para la seguridad de la firma, y que permite resolver el gran problema de la firma directa: dado que en esta la validez depende de la seguridad de la clave privada del emisor, es imposible resolver disputas, mientras que en la firma arbitrada es justamente la presencia del árbitro la que impide que el emisor pueda desconocer el mensaje.

# 2 Certificación digital

Parece obvio que la firma digital directa por sí misma puede ser extremadamente útil en ciertos casos, pero en muchos otros presenta graves carencias; la criptografía de clave pública ha resuelto el problema de la seguridad en la clave de cifra (recordemos que en el cifrado simétrico esta clave ha de transmitirse de forma segura), pero no los problemas de la adquisición de claves públicas, del reconocimiento, revocación, distribución, redistribución, validación y, más importante incluso, de la asociación entre una clave pública y una persona o entidad (Gerck, 1999). Y recordemos que una comunicación no es segura únicamente por ser privada: sin estar asociada a una persona o entidad con responsabilidad legal, una firma no es más que un conjunto de bits que pueden pertenecer a cualquier ente.

La asociación de una clave a una persona o entidad se denomina **certificado digital**, y no es más que un documento electrónico que contiene la clave pública del propietario del certificado junto a otra información necesaria para identificarlo, todo ello firmado digitalmente por una autoridad de certificación (CA, *Certification Authority*), que no es más que una tercera parte confiable (*Trusted Third Party*) para todos los actores del intercambio de información, tanto el receptor como el emisor; el hecho de que entre en juego esta autoridad de certificación es debido a un factor muy sencillo: dado que estamos hablando de información digital, cualquiera podría generar un certificado, por lo que es necesario validar su autenticidad mediante la firma de una autoridad de certificación en la que todas las partes deben confiar. La idea consiste en que dos usuarios pueden confiar directamente entre sí si ambos confían en una tercera parte que puede dar fe de la fiabilidad de los dos, y a la que denominamos Autoridad de Certificación.

De esta forma, los elementos básicos de un certificado serán:

- Clave pública de la persona o entidad certificada.
- Información identificativa: desde el nombre, nacionalidad o DNI, hasta una imagen de la persona o sus huellas dactilares.
- Firma de los dos elementos anteriores por parte de una CA confiable para emisor y receptor, que añade credibilidad al certificado.

Los anteriores pueden ser complementados con todo tipo de información relativa al propietario de la clave pública o a la autoridad de certificación; un certificado puede adoptar diferentes formatos, aunque el estándar se denomina X.509 y tiene unos campos determinados que comentaremos a continuación.

# 3 El estándar X.509

En 1988 aparece la propuesta más antigua para definir un formato normalizado en los certificados digitales a nivel mundial; tal propuesta tiene un origen ISO, y se trata del estándar X.509v1, el más utilizado a día de hoy. Unos años más tarde, en 1993, el estándar original fue ampliado por su versión 2 únicamente en dos campos, identificando de forma única el emisor y el usuario del certificado para manejar la posibilidad de reutilización de ambos en el tiempo; estos certificados X.509v2 no se usan habitualmente, debido en parte a que es recomendable que los nombres no se reutilicen y que los certificados no usen identificadores únicos.

El más reciente de los estándares X.509 es X.509v3, que data de 1996 y que soporta la noción de extensiones: cualquiera puede definir una extensión personalizada e incluirla en el certificado, además de marcarla como crítica (para indicar que debe ser validada de forma obligatoria y el certificado debe ser rechazado si no se cumplen las características indicadas).

El estándar X.509 define qué información puede ir en un certificado y cómo representarla (el formato del certificado). Todos los certificados X.509, sin importar su versión, contienen los campos mostrados en la figura 2:

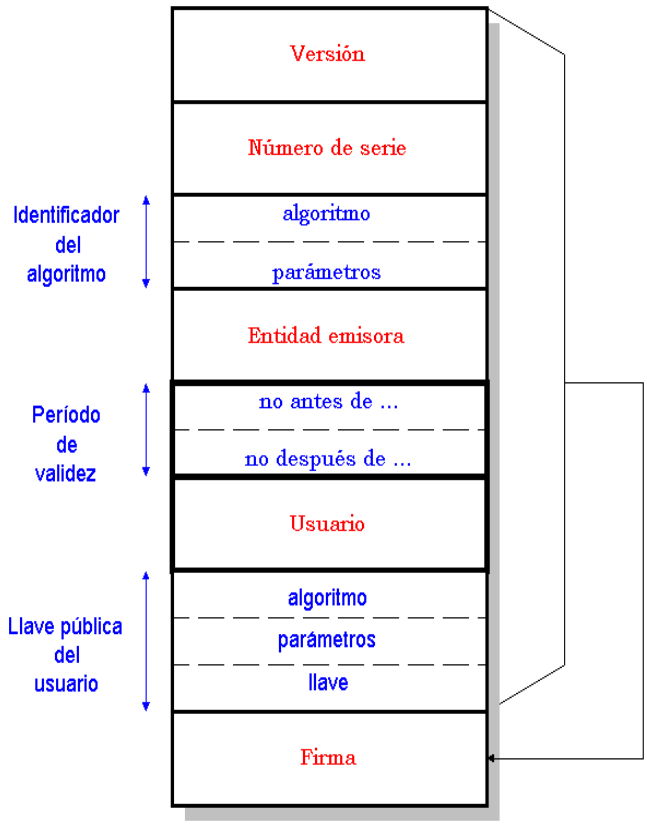


*Figura 2*. Formato de certificado X.509.

La descripción de cada uno de estos campos es la siguiente:

- VERSIÓN: Identificador de la versión del estándar X.509 a la que pertenece el certificado.
- NÚMERO DE SERIE: La organización que crea el certificado es la responsable de asignarle un número de serie para distinguirlo de otros certificados que puedan ser emitidos por la misma organización.
- IDENTIFICADOR DEL ALGORITMO: Identifica el algoritmo utilizado por la autoridad de certificación para firmar el certificado.
- ENTIDAD EMISORA: Nombre X.500 de la entidad que firma el certificado.
- PERIODO DE VALIDEZ: Define el periodo durante el que el certificado es válido, que puede oscilar entre unos pocos segundos y muchos años.

- USUARIO: Nombre de la persona o entidad a la que pertenece la clave pública identificada en el certificado. Se trata de un nombre en formato X.500, por lo que debe ser único en Internet.

- CLAVE PÚBLICA DEL USUARIO: Clave pública de la persona o entidad a la que pertenece el certificado, junto a un identificador del algoritmo que especifica a qué criptosistema de clave pública pertenece la clave, así como los posibles parámetros asociados a la misma.

- FIRMA: Firma de la autoridad de certificación para garantizar la autenticidad del certificado.

Los certificados X.509 se definen utilizando un lenguaje formal denominado ASN.1 (*Abstract Syntax Notation 1*); este lenguaje describe de forma abstracta los mensajes que van a ser intercambiados entre sistemas, lo que en el caso particular de los certificados digitales X.509 implica que mediante ASN.1 se especifican los tipos exactos de datos binarios que conforman el certificado. La notación ASN.1 puede ser codificada de diferentes formas, aunque el estándar es la codificación DER (*Distinguished Encoding Rules*), que representa el certificado digital en forma binaria (si queremos utilizarlo en formato ASCII, por ejemplo para utilizarlo en el correo electrónico, podemos codificar el resultado binario mediante base64).

# 4 Infraestructuras de clave pública

El modelo de confianza basado en terceras partes confiables es la base para la definición de las **Infraestructuras de Clave Pública** (PKI, *Public Key Infrastructure*). Aunque en su forma más simple podemos definir una infraestructura de clave pública sencillamente como un sistema para publicar las claves públicas (valga la redundancia) de sus usuarios, una PKI es algo más: se trata de un conjunto de protocolos, servicios y estándares que soportan diferentes tipos de aplicaciones basadas en criptografía de clave pública. En este punto vamos a hablar con cierto nivel de detalle de las infraestructuras de clave pública, un término muy de moda hoy en día pero todavía difícil de implantar en una organización real (hace apenas un par de años se bromeaba diciendo que las PKIs son '*only available for PowerPoint*').

A través del uso del cifrado y las firmas digitales, una infraestructura de clave pública puede proporcionar ciertos beneficios a cualquier organización y a las personas u organizaciones que de cierta forma se relacionan con ella; entre tales beneficios encontramos:

- **Autenticación**: Confirmación de la identidad de una persona o entidad.
- **Confidencialidad**: Protección de la privacidad de los datos de forma que sólo los elementos autorizados puedan acceder a ellos.
- **Integridad**: A través de las firmas digitales, en una infraestructura de clave pública se proporcionan los mecanismos para garantizar que cierta información no ha sido modificada.
- **No repudio**: Prueba de la participación en una acción o transacción.

## 4.1 Arquitectura

En una infraestructura de clave pública encontramos los siguientes elementos (Hunt, 2002):

### 4.1.1 Política de seguridad

La política de seguridad define las directrices generales de la organización en materias de seguridad informática (por ejemplo, los principios de utilización del cifrado). Una parte muy importante de la política es lo que se denomina la Declaración de Prácticas de Certificación (CPS, *Certificate Practice Statement*), un documento detallado que contiene los procedimientos operativos que indican como la política será implantada y apoyada en la práctica.

### 4.1.2 Autoridad de certificación

La autoridad de certificación (CA, *Certification Authority*) es la entidad que gestiona los certificados durante todo su ciclo de vida, desde su emisión hasta su revocación (cancelación), conformando por tanto la base para la infraestructura de clave pública. Entre sus funciones se encuentra:

- Emitir certificados asignando la identidad de una persona u organización a una clave pública.
- Planificar las fechas de expiración de los certificados.

- Garantizar que los certificados son revocados cuando es necesario publicando listas de revocación de certificados (CRLs, *Certificate Revocation Lists*).

### 4.1.3 Autoridad de registro

En una infraestructura de clave pública, la **autoridad de registro** (RA, *Registration Authority*) proporciona el interfaz entre el usuario y la autoridad de certificación, autenticando la identidad de los usuarios y enviando sus solicitudes de certificado a la CA; en función del proceso de autenticación implantado variará el nivel de confianza que puede ser depositado en los certificados (por ejemplo, si únicamente se solicita una dirección de correo electrónico y un nombre de usuario, tendremos una confianza menor en el certificado emitido que si se solicita previamente una huella dactilar y una fotocopia del DNI).

El registro puede ser llevado a cabo en una RA independiente o en la propia CA; la primera aproximación (RA y CA independientes) suele ser más aconsejable, ya que dificulta la violación de la seguridad global de la PKI (un potencial intruso debe violar varios sistemas y no uno sólo).

### 4.1.4 Repositorio y sistema de distribución de certificados

El repositorio de certificados proporciona un mecanismo para almacenar claves, certificados y listas de revocación de certificados; generalmente está basado en un servicio de directorio (por ejemplo, LDAP), y puede incorporar funcionalidades más avanzadas, como los servicios de recuperación automática de claves.

La distribución de los certificados depende por completo de la PKI con la que estemos trabajando, y puede llevarse a cabo de diferentes formas; una aproximación muy habitual puede ser la distribución a través de un servicio de directorio LDAP.

### 4.1.5 Aplicaciones con soporte PKI

Podemos ver la PKI como la base de una infraestructura de seguridad sobre la que diferentes aplicaciones son capaces de trabajar de forma segura (por ejemplo, sistemas de correo electrónico, de comercio electrónico, firma digital de código fuente, VPNs, etc.). Es la utilización de tales aplicaciones la que proporciona utilidad directa a los usuarios de la infraestructura, y no la PKI en sí.

## 4.2 Servicios

Entre los servicios ofrecidos por una infraestructura de clave pública encontramos:

- Emisión y renovación de certificados.

  Generación de nuevos certificados para las personas o entidades que los soliciten, y renovación de los certificados antiguos.

- Distribución de certificados.

  Capacidad para publicar el certificado digital de una persona o entidad, poniéndolo a disposición del resto de usuarios.

- Revocación de certificados.

  Cancelación de un certificado emitido previamente antes de la caducidad del mismo, por compromiso o corrupción del certificado. La revocación se suele llevar a cabo a través de listas de revocación de certificados.

- Suspensión de certificados.

  Invalidación temporal de un certificado digital cuando no deba ser utilizado durante un tiempo (por ejemplo, por ausencia del propietario).

- Recuperación de claves.

Recuperación de una clave de cifrado en caso de que haya sido corrompida, haya caducado, o simplemente se haya perdido.

- No repudio.

  Prueba técnica de la participación de un actor en una transacción.

- Marca de tiempo.

  Registro de tiempo oficial en todas las transacciones, que demuestra que cierto evento sucedió en una fecha y hora dadas.

En la tabla siguiente se muestran de forma clara los principales servicios de una infraestructura de clave pública, así como el componente de la misma encargado de llevarlos a cabo en cada caso.

*Tabla 1*. Servicios generales de una PKI.

| **Servicio** | **Descripción** | **Implementación** |
|---|---|---|
| Registro de usuarios | Recopilar la información necesaria para verificar la identidad de los usuarios | Autoridad de certificación o autoridad de registro |
| Emisión y renovación de certificados | Generación de los certificados | Autoridad de certificación |
| Revocación y suspensión de certificados | Generación y publicación de CRLs | Autoridad de certificación |
| Almacenamiento y recuperación de certificados y CRLs | Poner a disposición de los usuarios autorizados tanto los certificados como las listas de revocación | Servicio de directorio seguro |
| Validación de que el certificado se ajusta a la política definida | Asignar restricciones a la cadena de certificación y validar que todas ellas se cumplen | Autoridad de certificación |
| Marcas de tiempo | Asignar a cada certificado marcas | Autoridad de certificación o |

| | | |
|---|---|---|
| | de tiempo | servidor de tiempos dedicado |
| Gestión del ciclo de vida de las claves | Actualización, almacenamiento y restauración de las claves | Automatizado o manual |

Todas estas funciones se pueden resumir en tres: certificación (asociar una clave privada a una persona o entidad), validación (verificar que un cierto certificado es válido y revocarlo si no lo es) y gestión de claves (actualización, almacenamiento, etc.).

## 4.3 Problemas

Evidentemente, una infraestructura de clave pública no es la panacea ni la solución a todos los problemas de seguridad de una organización. Existen ciertos inconvenientes a la hora de implantar una PKI en un entorno real, entre los que se encuentran:

- Debilidades en el proceso de registro.

  El proceso de registro, incluyendo la identificación de la entidad, es quizás el elemento que por sí mismo más influye en la seguridad global de una infraestructura de clave pública. Si este proceso no presenta un alto grado de seguridad, es fácil romper la confianza en la PKI, lo que perjudica gravemente a la organización que la posee.

- Protección débil de la CA.

  La seguridad de la autoridad de certificación es vital para garantizar la seguridad total de la infraestructura de clave pública, ya que si dicha autoridad es violada, se pierde la confianza en todos los certificados que expide, con lo que la PKI al completo pierde su utilidad.

- Protección débil de las claves privadas.

  Las claves privadas de los usuarios son otro punto débil de la seguridad de una infraestructura de clave pública: si son comprometidas, se pierde la confianza en el usuario. Los medios de almacenamiento habituales son poco seguros, y utilizar medios que garanticen un mayor nivel de seguridad (tarjetas inteligentes, *tokens* criptográficos...) suele ser demasiado caro para muchísimas organizaciones. Estos problemas son especialmente críticos si los equipos informáticos en los que se almacenan las claves privadas son

compartidos entre varios usuarios y no ofrecen una protección robusta, que suele ser la mayor parte de las veces.

- Errores de concepto acerca de la PKI.

  Una infraestructura de clave pública no es ni mucho menos una solución a todos los posibles problemas de seguridad en una organización; una PKI sólo proporciona una serie de herramientas que proporcionan autenticación, confidencialidad, integridad y evidencia del no repudio, pero es tarea de la organización aprovechar correctamente dichas herramientas. Aún así, la seguridad global de un entorno es el resultado de diferentes procesos y tecnologías, y no puede ser garantizada totalmente por un único mecanismo, como una PKI.

# 5 Proyectos reales

## 5.1 E-FirmaGV

Desde noviembre de 2000 la Generalitat Valenciana ha comenzado a construir una infraestructura de clave pública para las administraciones públicas valencianas, en lo que se denomina el proyecto e-firmaGV; para ello se ha constituido en Prestador de Servicios de Certificación a través del Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano, por el que se regula la utilización de la firma electrónica avanzada en la Generalitat Valenciana.

El proyecto e-firmaGV pretende implantar una PKI en el seno de la administración pública valenciana con un clara finalidad: aprovechar las tecnologías de certificación digital en la relación con los ciudadanos y las empresas para lograr la realización de procedimientos sin presencia física ni papel, ahorrando tiempo y dinero tanto a los ciudadanos como a la administración pública. Para lograrlo, se definen diferentes objetivos dentro del proyecto e-firmaGV:

- Implantación de la plataforma de certificación.
- Formación.
- Soporte al desarrollo de aplicaciones y proyectos con uso de la PKI.
- Creación de un marco regulador autonómico.
- Definición y puesta en marcha de estructuras de soporte.

- Promoción de proyectos de infraestructuras de clave pública.

Como en toda infraestructura de clave pública, en e-firmaGV se ofrecen determinados servicios de certificación al ciudadano. En el caso particular de este proyecto los principales son:

- Servicio de registro, para verificar la identidad de los usuarios.
- Servicio de generación de certificados, que comprende la emisión de certificados digitales para el ciudadano (sujetos a la Política de Certificación de Correo y Aplicaciones seguras), para servidores web seguros (sujetos a la Política de Certificación para Servidores con soporte SSL), para firma de código informático (sujetos a la Política de Certificación de Certificados para firma de código) y para aplicación.
- Servicios de publicación de información (CPS, certificados emitidos, CRLs...).
- Servicio de revocación de certificados para poder invalidar un certificado digital de manera ágil y flexible (Call-Center, formularios web seguros, presencia física...).
- Servicio de validación o información de estado de certificados, incluyendo la generación de CRLs y el servicio OCSP para comprobación *on-line* del estado de un certificado digital.
- Servicio de sellado de tiempo (*timestamping*), sincronizado con el Real Instituto y Observatorio de la Armada para obtener la hora oficial española.
- Archivo de claves de cifrado, que permite el almacenamiento seguro de las claves necesarias para recuperar informaciones cifradas ante la pérdida de claves por parte del usuario, requerimiento judicial, etc.
- Soporte al desarrollo de aplicaciones, a usuarios y formación acerca del uso, bases teóricas, beneficios, etc. de la infraestructura de clave pública.

Con el proyecto e-firmaGV, la Generalitat Valenciana se sitúa a la cabeza de iniciativas telemáticas en el ámbito de las administraciones autonómicas españolas; podemos obtener más información sobre el proyecto en la URL http://www.pki.gva.es/.

## 5.2 CERES

El proyecto CERES (CERtificación ESpañola), liderado por la Fábrica Nacional de Moneda y Timbre, trata de poner en marcha una Entidad Pública de Certificación que

permita autenticar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación.

El objetivo de este proyecto es la securización (autenticidad, confidencialidad, disponibilidad e integridad) de las comunicaciones electrónicas con la Administración, siendo un intermediario transparente al usuario que garantizará a ciudadanos y administraciones la identidad de ambos partícipes en una comunicación, así como la confidencialidad e integridad del mensaje enviado. Para lograrlo, CERES ofrece una serie de servicios que se pueden clasificar en cuatro grandes grupos:

- Servicios primarios, que son servicios esenciales sobre los que se apoyan los demás servicios y que constituyen el núcleo del proyecto CERES
- Servicios interactivos, que permitirán la relación de CERES con los usuarios para garantizar la identidad de los interlocutores.
- Servicios de securización de mensajes y transacciones, que garantizarán la integridad de los contenidos y la fecha de la comunicación y proporcionarán constancia de haber enviado o recibido el mensaje al usuario destino u origen respectivamente.
- Servicios de confidencialidad, que facilitarán al usuario el intercambio confidencial de información y el acceso a su información cifrada en caso de pérdida de la clave.

Podemos obtener más información sobre el proyecto *CERES* en la URL http://www.cert.fnmt.es/.

# Referencias bibliográficas

Adams, C. (2002). *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley.

Brands, S. (2000). *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press.

Choudhury, S. (2002). *Public Key Infrastructure and Implementation and Design*. John Wiley & Sons.

Feghhi, J. y Williams, P. (1998). *Digital Certificates: Applied Internet Security*. Addison-Wesley.

Ford, W. (2000). *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*. Prentice Hall.

Gerck, E. (1999). *Overview of Certification Systems: X.509, PKIX, CA, PGP & SKIP*. Black Hat Conference, Las Vegas, 1999.

Hunt, R. (2002). PKI and Digital Certification Infrastructure. *Proceedings of the 9th IEEE International Conference on Networks (ICON'01)*, IEEE Press.

Netscape (1998). *Introduction to Public Key Cryptography.* Netscape Communications Corporation.

Schneier, B. (1994). *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley & Sons.