

La Firma Digital

Tabla de Contenidos

7. La Firma Digital.....	2
Infraestructura de clave pública.....	2
Situación en la administración pública	3
7.1 Firma Digital con Outlook (Windows, MacOS).....	4
7.2 Firma Digital con Mozilla (Unix, Windows, MacOS X).....	5



7. La Firma Digital.

El concepto de firma digital fue introducido por Diffie y Hellman en 1.976. Básicamente una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. Aparentemente estos se consiguen con los criterios de autenticidad e integridad anteriormente citados, pero estos no son suficientes si se pretende equiparar a la firma manuscrita que además tiene las propiedades de:

- ser barata y fácil de producir.
- ser fácil de reconocer tanto por el propietario como por otros.
- ser imposible de rechazar por el propietario.

Para ello existen 2 métodos de firma digital:

- Firma digital con árbitro donde dos usuarios con desconfianza mutua confían en un tercero. Se utilizan criptosistemas de clave única (una sólo clave para cifrar y descifrar). El emisor y el receptor tienen sus propias claves por lo que es el árbitro el encargado de recibir el mensaje del emisor, descriptarlo con la clave del emisor. De esta forma el emisor y el receptor no necesitan compartir claves.
- Firma digital ordinaria en la cual el usuario firmante envía directamente la firma al destinatario, y este debe poder comprobar la validez de la firma sin necesidad de un árbitro. A este método pertenecen los sistemas de firmas actuales que se basan en criptosistemas de clave pública.

El modo de funcionamiento de la firma digital basado en clave pública es el siguiente:

- cada participante tiene un par de claves, una se usa para encriptar y la otra para desencriptar.
- cada participante mantiene en secreto una de las claves (clave privada) y pone a disposición del público la otra (clave pública).
- el emisor calcula un resumen del mensaje a firmar con una función hash. El resumen es un conjunto de datos de pequeño tamaño que tiene la propiedad de cambiar si se modifica el mensaje.
- el emisor encripta el resumen del mensaje con una clave privada y ésta es la firma digital que se añade al mensaje original.
- el receptor, al recibir el mensaje, calcula de nuevo su resumen mediante la función hash. Además desencripta la firma utilizando la clave pública del emisor obteniendo el resumen que el emisor calculó. Si ambos resúmenes coinciden entonces la firma es válida por lo que cumple los criterios ya vistos de autenticidad e integridad además del de no repudio ya que el emisor no puede negar haber enviado el mensaje que lleva su firma.

Infraestructura de clave pública

El sistema de firma digital basado en clave pública resuelve la mayoría de los criterios de seguridad que cumple la firma manual. Tan sólo queda la asociación de la firma con un propietario evitando así la existencia de firmas anónimas. Se trata, pues, de asociar a una firma la identidad de la persona que la utiliza. Para ello se usan los certificados digitales. Un certificado digital es un documento que identifica cada clave pública con su propietario correspondiente. Para que un certificado tenga validez es necesario que vaya firmado por una Autoridad de Certificación que es una entidad en la que confían el emisor y el receptor y que certifica la identidad de los participantes. Los certificados, por tanto, son emitidos y firmados por la Autoridad Certificadora y están identificados por un número de serie y un período de validez. Por último, existe la firma de Autoridad de Registro que es una entidad que identifica de forma inequívoca al solicitante de un certificado para después suministrar a la Autoridad Certificadora los datos verificados del solicitante a fin de que ésta emita el correspondiente certificado. Actualmente se usa el estándar x.509 que materializa estos conceptos formando lo que se denomina una Infraestructura de Clave Pública (PKI; Public Key Infrastructure) Un certificado contiene:

- información de identidad
- la clave pública
- el modo de utilización de las claves (encriptación, firmado?)
- un período de validez
- un número de serie
- la identidad de la Autoridad Certificadora
- la firma digital de la Autoridad Certificadora

Una infraestructura de clave pública consiste en la aplicación de los certificados digitales basados en el estándar X509 para establecer la seguridad en las comunicaciones, mensajería y/o transacciones en redes de comunicaciones.

Situación en la administración pública

En España, las distintas administraciones están apostando decididamente por Internet como vía de comunicación. El primer paso ha sido la creación de webs para ofrecer información de interés público. Estas iniciativas están provocando un gran interés en el público que comienza a demandar nuevos servicios en la red. La más ambiciosa de estas iniciativas puesta en marcha por la Administración es el denominado proyecto CERES (Certificación Española) que lidera la Fábrica Nacional de la Moneda y Timbre (FNMT) y que, en líneas generales, consiste en una Infraestructura de Clave Pública dotada de una Entidad Pública de Certificación que permite autenticar y garantizar la confidencialidad e integridad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación. CERES utiliza términos y sistemas criptográficos basados en criptosistemas de clave pública con dos características básicas:

- la identidad del usuario, al igual que su capacidad de firma, se encuentra almacenada en una tarjeta inteligente (el documento de identificación electrónica, informática y telemática) que no puede ser accesible salvo por un propietario cuando introduzca el número de identificación personal, similar a la clave de una tarjeta de crédito.

- el sistema es completamente transparente al usuario, es decir, no es necesario conocer ninguna técnica criptográfica para realizar o verificar una firma electrónica o cifrar o descifrar un mensaje.

Los servicios que presta la Entidad Pública de Certificación se agrupan en servicios básicos y servicios avanzados:

A. servicios básicos: incluyen servicios de certificación de claves, registros de usuarios, publicación, etc. Sobre estos servicios se apoyan otros servicios.

1. servicios de certificación de claves. Se opera como una entidad certificadora siguiendo el estándar X509. Incluye los siguientes servicios:
 - emisión y renovación de certificados
 - archivo de certificados
 - generación de claves
 - archivo de claves
2. servicios de registro de usuarios. Se opera como una Autoridad de Registro realizando la emisión y renovación de Registros. Entrega al usuario una tarjeta inteligente.
3. servicios de publicación mediante los cuales se da a los usuarios acceso a los certificados, listas de revocación, directorios, etc.

B. servicios avanzados:

1. certificación temporal (time stamping)
2. certificación de contenido
3. confirmación de envío, entrega y recepción de documentos en sistemas de mensajerías.
4. servicios de recuperación de claves, únicamente para las claves orientadas a la confidencialidad.

7.1 Firma Digital Con Outlook (Windows, MacOS)

Acceda al menú [**Herramientas**] / [**Cuentas...**].

Seleccione en la solapa [**Correo**] el nombre de su cuenta de correo (probablemente sólo exista una) y luego presione [**Propiedades**]. Accediendo a la solapa [**Seguridad**] seleccione [**Usar identificador digital ...**] y luego presione en [**Identificador digital...**].

Seleccione el Certificado de Clave Pública que acaba de obtener y luego presione [**Aceptar**].

Cierre las pantallas presionando [**Aceptar**] y [**Cerrar**].



Para firmar digitalmente un correo electrónico redactar un mensaje y antes de enviarlo hacer un click en el menú de [**Herramientas**] y luego hacer click en el ítem [**Firmar Digitalmente**] de esta forma le estaremos indicando al cliente de correo que antes de enviar el mensaje lo firme digitalmente. Si desea que por defecto todos los correos que Usted envía salgan firmados, acceda al menú [**Herramientas**] / [**Opciones...**] y luego en la solapa de [**Seguridad**] seleccione [**Firmar digitalmente todos los mensajes salientes**].

Para finalizar presione [**Aceptar**].

7.2 Firma Digital Con Mozilla (Unix, Windows, MacOS X)

Acceda al menú [**Edit**] / [**Mail & Newsgroups Accounts Settings...**].

Seleccione el directorio [**Security**].

A continuación deberá indicar cual será el certificado a utilizar para firmar y cifrar un e-mail. Para seleccionar el certificado que se va a utilizar se debe presionar el botón [**Select...**] correspondiente a la seccion "Digital signing" y "Encryption" .

Para finalizar cierre las pantallas presionando [**OK**].

