

FIRMAS DIGITALES.

1. Introducción.
2. Conceptos.
3. Esquemas de Firmas Digitales.
4. Certificaciones.
5. Legislación.

Introducción.

Es España, al igual que en el resto del mundo, la seguridad informática sigue considerándose por parte de la dirección de las empresas como importante o muy importante.

Un reciente estudio de la consultora Ernst&Young apunta que para el 82% de los encuestados este aspecto es fundamental.

Las organizaciones necesitan proteger la confidencialidad de la información reservada. La seguridad en Internet consiste en implementar mecanismos para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor.

Las contraseñas y palabras clave ya no son un mecanismo suficientemente fiable y seguro, ya que éstas pueden ser interceptadas durante su transmisión.

Las personas que utilicen estas redes, tanto para envíos como para recepciones, van a requerir una serie de medidas de seguridad para validar y autenticar los mensajes electrónicos que intercambien.

La validación y la autenticación se van a referir a métodos que permitan certificar los contenidos de un mensaje y su origen respectivamente.

Ambas funciones pueden ser desarrolladas a través de las firmas digitales que se añaden a todo mensaje, o bien forman parte de él.

Conceptos.

La firma digital surge de las tecnologías utilizadas para conseguir la confidencialidad en las comunicaciones. La firma digital es únicamente una cadena de ceros y de unos que va asociada a un documento o fichero acreditando quién es su autor y que no ha existido ninguna manipulación posterior de los datos.

Las firmas digitales deben tener las mismas propiedades que las escritas:

- *Únicas.* Una firma digital debe de ser generada únicamente por su usuario.
- *No se podrán falsificar.* La generación por parte de otros usuarios de firmas de cara a falsificar una firma digital será imposible, es decir tendrán que resolver problemas intratables de una gran complejidad mientras intentan falsificar la firma.

- *Fácil de autentificar.* Cualquier persona que reciba la firma o un árbitro, encargado de solucionar las posibles disputas, debe ser capaz de conocer al autor, incluso después de un periodo de largo tiempo.
- *Imposible de negar.* Cualquier autor de una firma digital no podrá decir que su firma ha sido falsificada.
- *Barata y fácil de generar.*

Las diferencias entre las firmas digitales y las naturales:

1. Las firmas naturales de una persona son las mismas independientemente del documento que está autenticado. Por el contrario las firmas digitales, deben ser diferentes en función de cada mensaje firmado.
2. Las firmas naturales vienen acompañando un texto en un documento. Estas firmas al ser visibles pueden ser copiadas por un usurpador. Sin embargo en las firmas digitales, estas deben ser inimitables.

Para firmar un documento digital, su autor utiliza su propia clave secreta, a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

La firma se realizará de la siguiente forma:

1. El software del firmante aplica un algoritmo hash sobre el texto a firmar obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Este algoritmo matemático es unidireccional, es decir, lo encriptado no se puede descifrar. Un mínimo cambio en el mensaje produciría un extracto completamente diferente. Los algoritmos hash más utilizados para esta función son el MD5 ó SHA-1.
2. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits, en función del algoritmo hash empleado, se somete a continuación a cifrado mediante la clave secreta del autor. El algoritmo más utilizado en este procedimiento de encriptación pública es el RSA. Se obtiene un extracto final cifrado con la clave privada del autor el cual se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por la persona interesada que tenga la clave pública del autor.
3. El software del receptor, con la clave pública del remitente, descifraría el extracto cifrado del autor; a continuación calcula el extracto hash que le correspondería al texto del mensaje, y si el resultado coincide con el extracto anteriormente descifrado se consideraría válida.

Las condiciones que debe reunir una comunicación segura a través de una red son:

- *Confidencialidad:* evita que un tercero pueda acceder a la información enviada.
- *Integridad:* evita que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.
- *Autenticación:* permite a cada lado de la comunicación asegurarse que el otro lado es realmente quien dice ser
- *No repudio o irrefutabilidad:* Permite a cada lado de la comunicación probar fehacientemente que el otro lado ha participado en la comunicación.

Certificaciones.

Aparecen para garantizar tanto al emisor como al receptor la autenticación de las partes, es decir, que éstas son quienes dicen ser.

Una agencia o autoridad de certificación (*CA Certification authority*) podrá certificar e identificar a una persona con una determinada clave pública.

Estas autoridades emiten certificados de claves públicas de los usuarios firmando con su clave secreta un documento, válido por un periodo determinado de tiempo, que asocia el nombre distintivo de un usuario con su clave pública.

Actuaría como una especie de notario electrónico que extiende un certificado de claves, el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información.

Permiten verificar que una clave pública pertenece a una determinada persona, evitando que alguien utilice una clave falsa para suplantar la personalidad de otro.

Para la contratación on-line existen varias autoridades certificadoras de las que cabe destacar por su importancia y esfuerzo realizado:

- FESTE (Fundación para el estudio de la Seguridad de las Telecomunicaciones).
- ACE (Agencia de Certificación Electrónica).

Los certificados tendrán una vigencia de un año tras el cual ACE se encargará del proceso de renovación. Además de la Agencia de Certificación Electrónica se hará cargo de la gestión de renovaciones de certificados y de listas negras.

El sistema de certificación se estructura en base a dos clases de certificados:

- *Certificado de servidor*: autentifica al servidor frente al usuario que está accediendo al mismo, pero no autentifica al puesto cliente.
- *Certificado de navegador*: autentifica al cliente que está conectado al servidor, con las funciones de firma y cifrado de los mensajes que envíe. Asimismo, permite el correo electrónico seguro entre usuarios o suscriptores de certificados.

Los certificados digitales de la Agencia de Certificación Electrónica están basados en una tecnología denominada de Clave Pública (PKI).

Cada usuario posee un par de claves: una clave pública (que es de dominio público) y una clave privada (única y confidencial).

La autenticación de las personas intervinientes en el proceso se realiza mediante firmas digitales que van incorporadas en el mensaje y que son únicas para cada individuo.

Legislación.

Las causas que fuerzan la redacción de una legislación son:

- Falta de seguridad comercial(transacción insegura).
- Falta de seguridad jurídica (vacío jurídico).

Así, se consigue dotar a los documentos electrónicos de la misma validez jurídica que los escritos.

Antecedentes en EEUU:

- Estado de UTA en 1995. Detalla derechos y responsabilidades de las partes de una transacción.
- Estado de California: Permite el uso de la firma digital para transacción con entidad pública.
- Delaware: Permite su uso para fines financieros.
- Florida en 1996: concede los mismos efectos a las firmas digitales que a las manuscritas.

Antecedentes Europa:

- Ley Alemana en 1997: Ley técnica que da validez legal a las firmas. Similar a la española en cuanto a certificados.
- Ley Italiana de 1997: establece el concepto de firma digital y la validez del documento electrónico.
- Reino Unido, Bélgica y Francia tienen proyectos similares.
- Existe una directiva Europea de 1999 donde se crea un marco jurídico para:
 - La firma electrónica
 - La prestación de servicios de certificación
 - Pero no regula aspectos relacionados con la celebración y validez de los contratos.

España:

- Hay un real decreto de 1996 que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del estado.
- En 1997 una Ley de medidas administrativas habilita a la FNMT a actuar como autoridad de certificación.
- Se crea el proyecto CERES para la emisión de tarjetas inteligentes con fines de firma.
- Se realiza un Real-Decreto-Ley de 1999 basado en la Directiva del Parlamento Europeo.
- La principal diferencia es el empleo de la firma electrónica por las administraciones públicas:
 - Entre sus entes o con particularidades.
 - Posibilidad de incluir un servicio de consignación de fecha y hora.
- Orden de 28 de Junio de 2000 que establece condiciones generales y procedimiento para la presentación telemática de declaraciones del Impuesto de Sociedades.