FIRMA ELECTRÓNICA 1/4

Introducción

La firma electrónica es un sistema para garantizar la autenticidad de su origen y la integridad de su contenido. La firma electrónica permite:

- Cifrar mensajes con las claves privada y pública del emisor y receptor del mensaje, de tal forma que es posible identificar a ambos en cuanto titulares de claves .
- Asegurar la integridad del mensaje recibido, al poderse comprobar a la recepción del mismo que nadie que no sea su emisor ha modificado su contenido a lo largo del recorrido realizado utilizando las redes de comunicaciones entre el emisor y el receptor del mensaje.

Por tanto, la utilización de la firma electrónica permite solventar los problemas de identificación en el envío de mensajes, garantizar la integridad del contenido y, eventualmente, en su caso, certificar la fecha y la hora del envío y la recepción de mensajes.

Un requisito imprescindible para el uso de la firma electrónica es la existencia de una tercera persona, distinta al emisor y receptor del mensaje, que pueda certificar la pertenencia de la clave pública con la que se ha cifrado el mensaje a la persona que efectivamente lo ha cifrado o firmado. De esto se encargará la entidad certificadora que es quien concede los certificados después de haber controlado la correcta configuración del proceso de encriptación (SSL) y haber comprobado los datos de la empresa solicitante. El certificado de servidor seguro se concede a entidades cuyas referencias han sido comprobadas, para asegurar que efectivamente quien recibe los datos encriptados es quien debe de recibirlos.

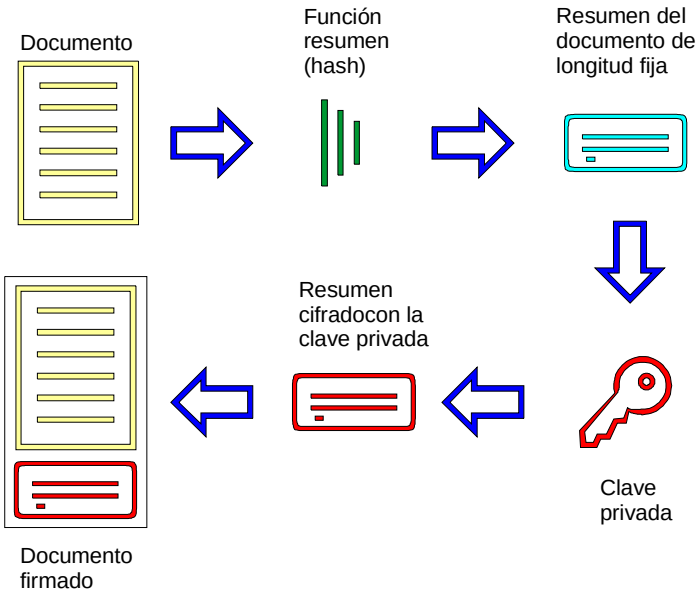
Para conseguir que los clientes tengan confianza en nuestra empresa, deberemos tener en cuenta estos aspectos relativos a la seguridad, pues esta demostrado que muchos usuarios ven la seguridad en la red como un obstáculo.

Funcionamiento

En la criptografía clásica el emisor del mensaje y su destinatario comparten una misma clave, que permite tanto cifrar como descifrar, es decir, actúa en ambos sentidos. La criptografía moderna aparece, en la década de los 70, con la invención de los denominados “sistemas de claves asimétricas”. En el nuevo método se utiliza una pareja de claves, tales que lo que se cifra con una de ellas solo puede descifrarse con la otra. En su uso práctico, hay una que se denomina “clave privada” ya que solo debe poseerla el emisor de mensajes y otra que denominamos “clave pública”, porque se distribuirá entre todos los interlocutores.

La utilización de claves privadas y públicas nos permite obtener, como la criptografía clásica, la confidencialidad de los mensajes. Para ello si alguien desea que distintas personas puedan enviarle mensajes confidenciales facilitará a éstos su clave pública. Cuando un emisor quiera enviar a un mensaje lo cifrará con la clave pública del destinatario, así sólo este, que es quien posee la clave privada, podrá descifrarlo. Este esquema mejora notablemente el anterior ya que no existe una clave compartida entre todo un grupo, sino que puede cifrarse el mensaje únicamente para un destinatario individual. En ningún momento es preciso revelar la clave privada y de ahí la virtualidad de esta técnica para garantizar la autenticidad de los mensajes.

Para garantizar la autenticidad de origen del documento basta con que el emisor añada al documento una firma cifrada con su clave privada y que el destinatario posea la clave pública del emisor para comprobarla. La firma debe encontrarse vinculada de forma unívoca con el documento, con lo que se garantiza además la integridad este. Para ello se calcula un resumen del documento mediante unas funciones denominadas *hash*. La función permite obtener de un conjunto de datos de cualquier longitud un resumen único que es un numero de longitud fija, cuyo valor varía ante cualquier modificación del conjunto de datos inicial. Para obtener la firma este resumen se cifra con la clave privada del firmante y se une al documento.



Firma de un documento

La comprobación de la firma se realiza del siguiente modo: por una parte se calcula de nuevo el resumen del documento con la misma función que se empleo al firmarlo, por otra se descifra la firma utilizando la clave pública del firmante con lo que obtenemos el resumen contenido en la firma. Esta última será correcta si el valor de ambos resúmenes coincide, ya que así sabremos con seguridad que el resumen de la firma fue cifrado con la clave privada del firmante, así como que el documento no ha sido modificado.

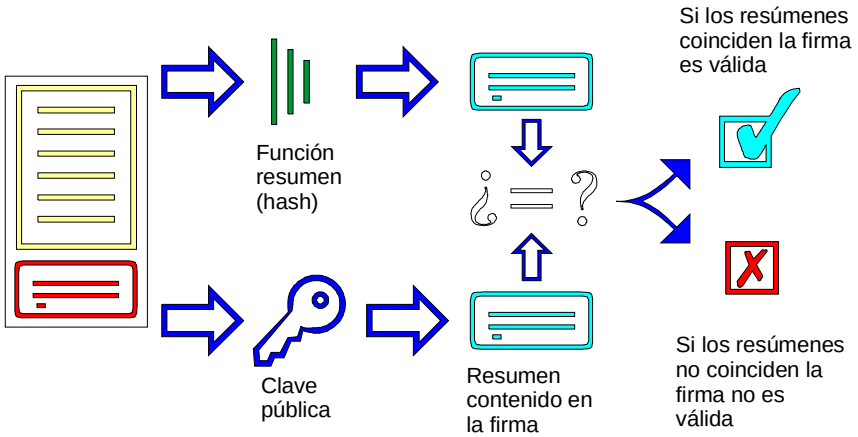


Figura 3.- Comprobación de la firma

Los certificados electrónicos

La clave pública es, por tanto, el mecanismo de comprobación de las firmas electrónicas. Pero, ¿cómo podemos saber que una clave pública pertenece a una persona dada?. En grupos pequeños puede ser suficiente con que las personas intercambien sus claves públicas de forma presencial. Cuando el ámbito es mayor se hace preciso el concurso de unas nuevas entidades que denominamos “Servicios de certificación”, aunque suelen ser conocidas por sus siglas inglesas CA *(Certification Authorities*).

Estos servicios emiten certificados electrónicos, que son el mecanismo de comprobación de las firmas. Se trata de documentos electrónicos firmados por la entidad de certificación en la que esta acredita que una determinada persona posee una clave criptográfica privada, vinculando su nombre y la clave gemela (pública). Por otra parte, los servicios de certificación deben difundir su clave pública de forma segura, ya que es el mecanismo para comprobar su firma y, con ella, la autenticidad de los certificados. El resultado es que podremos comunicarnos de forma segura con todos los poseedores de un certificado emitido por un Servicio de certificación conociendo únicamente la clave pública de éste.

Antes de emitir un certificado hay que realizar alguna comprobación sobre la identidad del poseedor de la clave y este debe manifestar de forma fehaciente ser el poseedor de la clave secreta, a fin de que posteriormente quede vinculado por los mensajes cifrados con dicha clave. La seguridad con que se realiza dicho trámite, que se denomina de inscripción o registro, es el principal factor a la hora de distinguir el nivel de confianza de los certificados. Habitualmente los Servicios de Certificación recurren a entidades que puedan realizar el trámite de firma presencial del compromiso con ciertas garantías y de forma cómoda para el usuario y que normalmente son grandes organizaciones como bancos, Universidades, etc. Finalmente, otro requisito importante que deben cumplir los Servicios de Certificación es mantener un directorio de certificados, activos y revocados, de forma que en caso de pérdida o compromiso de la clave privada los usuarios puedan invalidar el certificado y, con ello, las firmas posteriores al momento de la revocación.

Existen tradicionalmente documentos con una función similar a la de los certificados. Es así porque el reconocimiento de una persona exige siempre de una primera presentación o identificación, que nos permite asociarla con su nombre y otros rasgos. Para facilitar esta identificación las instituciones generan diversos documentos entre los que, en nuestro país, destaca el Documento Nacional de Identidad, expedido por la Dirección General de Policía. La simple posesión del documento constituye un factor muy importante en la identificación pero, además, se suelen asociar otras garantías como la fotografía, firma y otras características identificativas de la persona. Los certificados son el equivalente en las redes telemáticas. Normalmente se basan en la única garantía de la posesión de la clave privada correspondiente y del conocimiento de la de la palabra de paso que la protege, de forma similar a las tarjetas de crédito, aunque también pueden añadirse señas identificativas de carácter biométrico.

El conjunto de los elementos precisos para la utilización de la firma electrónica suele denominarse “infraestructura de clave pública” o PKI, según sus siglas inglesas. Aunque se encuentra todavía en fases muy iniciales de su desarrollo esta infraestructura tiende a tener, al igual que ocurrió con los nombres de dominio, alcance global. Hay que observar, sin embargo, que mientras el sistema de nombres de dominio se construyó de arriba hacia abajo, partiendo del un órgano único que fue

delegando en diferentes órganos nacionales, la PKI global, según parece, se construirá de abajo hacia arriba mediante acuerdos de confianza entre PKIs formadas en ámbitos locales.

Además de la autenticidad e integridad de los documentos, en muchos casos es precisa la denominada “no-repudiación”. Consiste en que debe quedar en poder de las partes prueba suficiente del contrato celebrado, de modo que ninguna de ellas pueda negarlo. Es importante determinar el momento en que cada una de las partes dispondrá de la prueba, de modo que no se generen intervalos de indefensión.

Aunque existen métodos criptográficos complejos que otorgan garantías suficientes, la solución más aceptada consiste en adoptar un sistema similar al empleado tradicionalmente, la interposición de un tercero dotado de fe pública. En esta solución, denominada “notarización electrónica”, el tercero conoce las claves de las partes y recibe sus consentimientos, facilitando prueba de ellos a quien tenga un interés legítimo. La intervención del fedatario facilita además, al igual que en la fe pública tradicional, la prueba del momento en que se realizo la acción.

(nota: tomado del libro J.F. Muñoz, Decisión jurídica y sistemas de información, Colegio de Resgistradores, Madrid, 2003)