Iago Pásaro Méndez

LA FIRMA DIGITAL

SEGURIDAD DEL EMPRESARIO EN LA RED

Las nuevas tecnologías y la sociedad de la información están creando nuevas vías de comunicación social y empresarial, siendo necesaria una adaptación continua a los avances y cambios que se producen. Sin embargo, el último estudio publicado en febrero de 2006 por la Asociación para la Investigación de los Medios de Comunicación (AIMC) refleja que la brecha digital todavía persiste en España, utilizándose un 50% menos que en países como Holanda o Alemania. Del estudio se desprende que los españoles somos reacios a comprar y contratar por Internet debido a la desconfianza que todavía genera el comercio por la red, factor determinante en el freno del desarrollo competitivo del mercado español.

Pese a ello, las compras, transacciones y contratación por vía telemática están aumentando a un ritmo elevado, convirtiéndose el ***e-commerce*** en uno de los principales sistemas de tráfico mercantil moderno, teniendo en cuenta que más del 70% de los usuarios de Internet han efectuado compras o han contratado algún servicio por la red en el último trimestre del 2005.

En este contexto, es esencial que el empresario desarrolle métodos de captación de nuevos clientes, afiance los existentes y, en definitiva, aumente la competitividad y expectativa de mercado de su empresa, siendo Internet, una de las herramientas idóneas para alcanzar esos objetivos.

El camino a seguir desde la empresa, de cara a un aumento en la utilización del comercio electrónico, pasa por ofrecer a los usuarios y potenciales clientes los mejores mecanismos de seguridad y las medidas de protección más fiables para las transmisiones e intercambios por la red, en la medida en que puedan generar la suficiente y necesaria confianza para su uso, siendo la firma digital una de las herramientas técnicas más seguras y fiables para ello, tanto para la propia empresa como para las relaciones con sus clientes y terceras empresas.

Iago Pásaro Méndez

¿Qué es la firma digital?

El artículo 3.1 de la Ley 59/2003 define firma electrónica como un conjunto de datos en forma electrónica, unidos a otros o asociados con ellos y que se utilizan para identificar al firmante, lo que permite comprobar la procedencia, autenticidad e integridad de los mensajes intercambiados a través de Internet.

Existen dos tipos de firma electrónica: ***la básica y la avanzada***. La básica no garantiza ni la identidad del firmante, ni la veracidad de la información recibida ya que no asegura que el envío lo haya realizado el emisor que conocemos, mientras que la firma avanzada permite identificar al firmante y detectar cualquier cambio posterior de datos que pudiese producirse.

Este tipo de firma es la que se conoce como ***firma digital***.

¿Cómo funciona?

La firma digital es una firma tecnológicamente específica y creada mediante los denominados ***sistemas de criptografía de clave asimétrica*** y cuyo funcionamiento se basa en que el titular posee dos claves: ***una clave pública y una clave privada***. La clave privada sólo la conoce el emisor y está asociada a la información que envía, mientras que los que la reciban, sólo conocerán su clave pública.

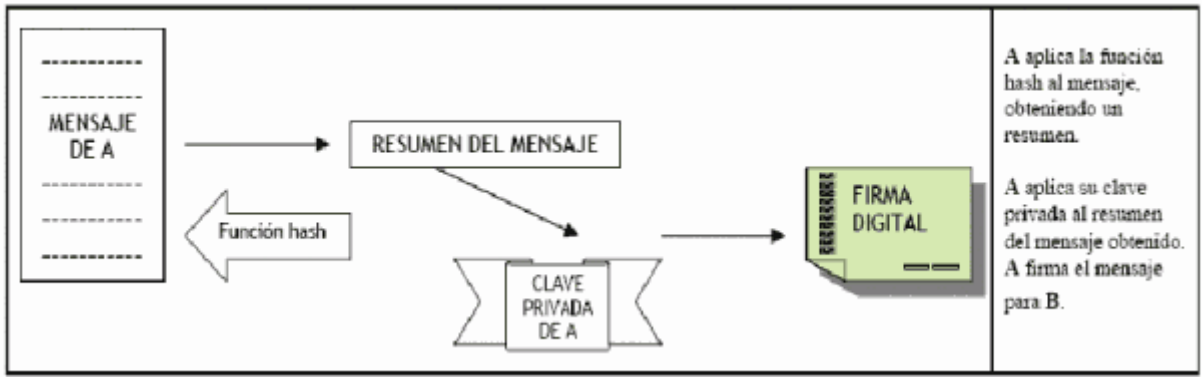
Las dos claves se necesitan y se complementan para conseguir que el mensaje cifrado aparezca como el original.

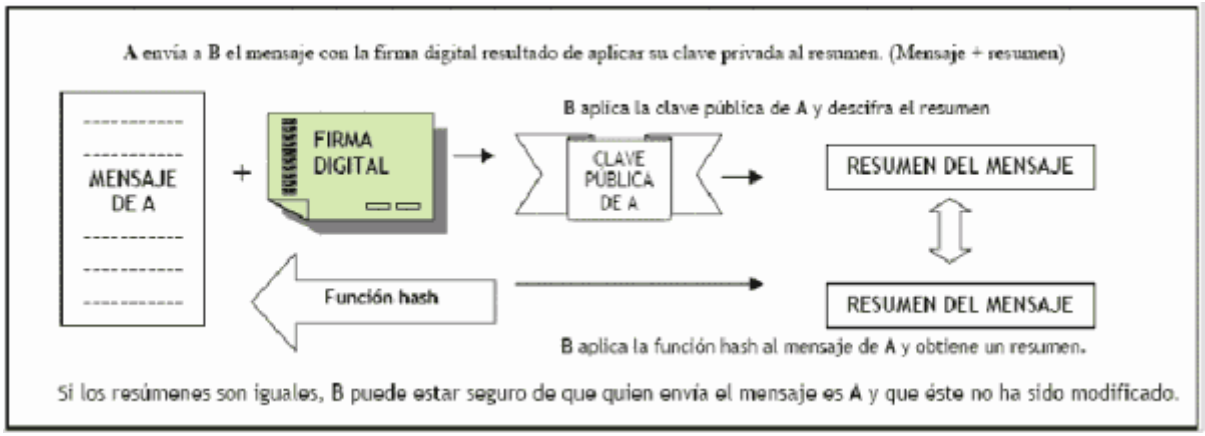
Mediante un sistema de operaciones matemáticas se protege la información que queremos enviar mediante el cifrado de datos, se oculta el texto al aplicarle unas instrucciones al mensaje y se convierte en un galimatías de números y letras (mensaje cifrado). El mensaje resultante sólo podrá ser descifrado por los que conozcan las instrucciones y la clave utilizada.

Para este proceso, la firma digital utiliza las denominadas ***funciones hash***, que aplicándola al mensaje genera un conjunto de datos asociados que se denomina ***resumen o huella digital***.

A la huella digital se le aplica la clave privada y el resultado es lo que se denomina ***firma digital*** que se enviará con el mensaje original.

De esta manera, el receptor recibe el mensaje y la firma digital. Aplicando la misma función al mensaje que el emisor y descifrando la firma digital con la clave pública del firmante, el receptor generará 2 resúmenes iguales lo que le permite comprobar y asegurar la autoría y que el mensaje recibido es el mensaje original.





De este modo, una firma digital nos asegura:

- la ***integridad*** del mensaje recibido, al no poder modificarse;
- su ***autenticación,*** al equivaler a la firma manuscrita y,
- el ***no repudio en origen,*** ya que el emisor no puede negar haber enviado el mensaje, al haber sido creado por medios que sólo él controla y conoce.

Iago Pásaro Méndez

Para que una firma electrónica equivalga y tenga el mismo valor jurídico que la firma manuscrita, debe estar basada en un ***certificado reconocido y generada mediante un dispositivo seguro de creación firma*** (firma avanzada reconocida).

¿Qué son los certificados?

Los certificados son documentos electrónicos que contienen la clave pública de un usuario y los que hacen posible el empleo de la firma electrónica por Internet, garantizando que cada firma se corresponde con ese usuario y no con otro.

El certificado es como una tarjeta de identificación (nombre, nif, dirección…) que permite identificarse e intercambiar información, pudiendo contener otros datos como el ámbito de su utilización, las competencias que tiene atribuidas el firmante, las fechas de inicio y término de la validez del certificado, etc.

Los certificados son emitidos y firmados por las ***Autoridades de Certificación***, entidades de confianza del emisor y del receptor del mensaje y a las que se denomina ***Terceras Partes de Confianza*** (TPC).

En cuanto a las claves privadas, éstas suelen mantenerse y guardarse en soportes físicos como las ***tarjetas inteligentes***, idénticas a una tarjeta de crédito y protegidas por un número personal (Nº PIN) que sólo conoce su propietario y que garantizan que nadie pueda usarla. En la tarjeta están las claves que no pueden ni salir de ésta, ni ser copiadas o usadas por un tercero lo que permite al propietario controlar el acceso y garantizar su seguridad.

¿Qué es una Autoridad de Certificación?

Las Autoridades de Certificación o Terceras Partes de Confianza (TPC) son como los almacenes de seguridad de los certificados, es decir, entidades que aseguran la realidad de los datos de sus poseedores.

Las TPC permiten que cualquier usuario pueda confiar en los certificados firmados por ésta, asegurando su validez y vigencia, es decir, que la clave pública es la correcta y que pertenecen a dicho emisor lo que nos asegura que la persona que dice ser la que envía el mensaje, realmente lo es.

En conclusión, se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si éste está avalado por la TPC, tercera parte en la que sí confiamos y que lo que avalará con su firma digital sobre el certificado.

¿Cómo se obtienen?

Para obtener los certificados deben seguirse 3 sencillos pasos:

1. **Solicitar el certificado por Internet a una entidad de certificación.**

La entidad certificadora por excelencia es la **Fábrica Nacional de Moneda y Timbre (FNMT)** (http://www.cert.fnmt.es).

La FNMT ofrece el soporte y los medios necesarios para la obtención, **de forma gratuita**, de certificados para particulares, organismos y empresas. Al introducir el NIF y solicitar el certificado, automáticamente se generan el par de claves. La clave privada se guarda en el navegador y la clave pública se envía a la FNMT para que la firme, lo que constituirá finalmente el correspondiente certificado, asignándole un código de solicitud para que lo presente en la posterior acreditación ante la entidad.

2. **Acreditar la identidad en la oficina de Registro.**

Una vez obtenido el código de solicitud debemos acreditar nuestra personalidad personándonos en la Oficina de Registro con el código de solicitud que se generó al introducir el NIF del paso 1.

3. **Descargar el certificado.**

Cuando nos hayamos acreditado ante la Oficina de Registro, introducimos el NIF y el código de solicitud al conectarnos en la dirección de Intenet de descarga de certificado de usuario.

Tras instalarlo está listo para su uso, siendo importante recordar que todos los pasos del proceso deben realizarse desde el mismo ordenador.

Iago Pásaro Méndez

En la actualidad, los certificados emitidos por la FNMT permiten a las empresas realizar trámites tributarios por Internet, al estar reconocidos por la Agencia Tributaria (AEAT). Sin embargo, para que estos certificados sean válidos para actuar fuera del ámbito tributario conforme la nueva ley de firma electrónica, la FNMT está esperando una respuesta del registro público, sin que a la fecha se haya dado una respuesta por el Ministerio de Industria, Turismo y Comercio. Tan pronto esté resuelta la disponibilidad de comprobación de los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación, procederá a emitir certificados reconocidos de persona jurídica.

Fecha: Marzo 2006