

INTERNET

Firma electrónica: seguridad en la red todavía lejana para el usuario

Se proponen cambios en la regulación de la firma electrónica, para impulsar el comercio electrónico. La confianza y la seguridad de los usuarios es clave para conseguirlo. Pero, ¿sabe usted qué es exactamente y cómo funciona? Se lo explicamos paso a paso.

La firma electrónica o digital es un conjunto de datos electrónicos que, identifican a una determinada persona en los documentos realizados en soporte electrónico. Suelen unirse al documento que se envía por medio telemático, como si de la firma tradicional y manuscrita se tratara: de esta forma el receptor del mensaje está seguro de quién ha sido el emisor, así como que el mensaje no ha sido alterado o modificado. Se trata de nuestra marca personal e intransferible para los documentos electrónicos, como lo es para los escritos en papel nuestra firma manuscrita.

La firma electrónica puede utilizarse en el sector privado, para contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo, la compra de un libro o un compacto por Internet) y entre empresas (por ejemplo, realizar un pedido a un distribuidor) o incluso entre los mismos consumidores finales (por ejemplo, venta de una raqueta de 2º mano, una colección de monedas etc).

También nos sirve para realizar actuaciones con y entre la Administración, es decir, sirve tanto para las relaciones entre los propios entes públicos que la forman como para las relaciones del ciudadano con la Administración (por ejemplo, algo tan simple como la renovación del D.N.I, la solicitud de prestaciones a la Seguridad Social o incluso la presentación de la declaración de la renta por Internet con el conocido programa "Padre").

¿Cómo funciona la firma electrónica?

La firma electrónica funciona mediante la encriptación o cifrado de los datos que la componen, de forma que si no se tiene la clave, el documento se convierte en ilegible.

Para ello es necesario contar con un par de claves: clave privada y clave pública, que se corresponden de forma matemática. Pongamos un ejemplo, escribimos un documento y lo firmamos con nuestra clave privada y lo enviamos a nuestro receptor al cual previamente le habremos otorgado nuestra clave pública, esta clave pública es la que permite verificar la procedencia del mensaje y que verdaderamente ha sido firmado por nosotros (que somos los únicos poseedores de la clave privada).

Con esta encriptación se consigue:

- Que la información enviada bajo la firma electrónica sólo pueda leerse por la persona autorizada que posea la clave.
- Acreditar la identidad de quien firma el documento electrónicamente.

¿Cuántos tipos de firma electrónica existen?

En nuestra actual normativa existen dos tipos: la básica y la avanzada.

La firma electrónica básica contiene un conjunto de datos recogidos de forma electrónica que formalmente identifican al autor y se incorporan al propio documento. Pero este sistema tiene un gran problema: ¿cómo sabemos que los datos enviados hayan sido creados por la persona que lo firma o que verdaderamente lo ha firmado él y no una tercera persona haciéndose pasar por él?.

Para resolver este problema se crea la firma electrónica avanzada, a la que nuestro ordenamiento atribuye plena eficacia jurídica y valor probatorio en juicio. Permite la identificación del emisor del mensaje ya que está vinculada de manera única al que firma el documento y a los datos que incorpora, pues es el signatario quien únicamente posee el control exclusivo de estas claves, además de que permite saber si estos datos han sido modificados posteriormente o en su transcurso.

Sin duda son figuras todavía desconocidas y complicadas para la mayoría de la población, no sólo porque son tratadas desde un punto de vista excesivamente técnico, sino por la propia ambigüedad que produce la lectura de las definiciones que ofrece la regulación actual.

¿Quién autentifica las firmas electrónicas?

Las autoridades de certificación, que son personas o entidades que cumplen una serie de requisitos legales (y que deben ser autorizados por el Ministerio de Justicia) para otorgar certificados que acrediten que la persona o entidad que usa dicha firma es ciertamente quien dice ser.

Las principales autoridades de certificación que operan en España son:

1.- Agencia de Certificación Electrónica (ACE): está homologada por Visa y Mastercard y ofrece certificados para Entidades y Corporaciones dentro de Comercio electrónico y de comunicaciones a través de Internet. (www.ace.es)

2.- Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE): se trata de entidad formada por registradores, notarios, abogados, la Universidad de Zaragoza e Intercomputer S.A y su principal actuación se dirige a la contratación privada. (www.feste.es)

3.- Certificación Española (CERES): es una entidad de certificación pública que lleva a cabo la Fábrica Nacional de Moneda y Timbre. Su campo de actuación es la garantía de seguridad, validez y eficacia de comunicaciones entre los órganos de la Administración Pública y entre las personas físicas y jurídicas que se relacionen con ella, sin olvidar servicios de Comunidades autónomas, Entidades Locales y de derecho público siendo necesario únicamente un convenio previo. (www.fnmt.es/faq.htm)

En España la prestación de estos servicios es libre, si bien existe un procedimiento voluntario, que es la acreditación, mediante el cual la Administración, realizando las evaluaciones técnicas de rigor, emite una resolución o documento oficial donde certifica que ese prestador cumple con las normas de calidad y seguridad establecidas en cuanto a sus procedimientos y a los productos y tecnología que utiliza.

Viene el DNI electrónico

La firma electrónica pasará en unos meses a regularse por Ley, recogiendo en lo fundamental lo establecido en el Decreto actual y añadiendo dos novedades importantes:

1º Creación del DNI electrónico, de este modo todos los ciudadanos podrán emitir firmas electrónicas certificadas por la Administración del Estado. Se espera que facilite el acceso y uso de las firmas electrónicas por los ciudadanos, especialmente para trámites administrativos, transacciones electrónicas y banca online.

2º Regulación de los certificados de personas jurídicas.

Las empresas y asociaciones también podrán "firmar" electrónicamente, pero a través de sus administradores, representantes legales y apoderados; es decir: se requiere que haya una persona física con vinculación a la persona jurídica.

ADICAE demanda transparencia y seguridad

España fue uno de los primeros países en regular la firma electrónica mediante el Real Decreto Ley 14/1999, de 17 de septiembre, aprobado con carácter de urgencia, y que fue publicado antes que la Directiva europea de 13 de diciembre de 1999 de armonización de la firma electrónica. Tal premura en establecer la regulación, sin embargo, ha dado lugar a un texto con importantes problemas cuya resolución demandamos desde ADICAE:

1. Careció del consenso y debate previo que una norma tan novedosa hubiera requerido y, por no haber esperado a la aprobación de la Directiva, una vez aprobada ésta, hay que modificar el Decreto.
2. Su contenido es demasiado técnico y de difícil comprensión por personas no especializadas en la materia (incluidos jueces y abogados)
3. Se centra demasiado en aspectos administrativos, dejando un vacío respecto al verdadero y cotidiano uso de la firma por particulares.
4. No hay distinción clara entre firma básica o simple y firma avanzada, en qué consisten, cuales son sus efectos y qué utilidades ofrecen para el usuario en función del destino que le vaya a dar.
5. Existe una falta de concreción con respecto a los requisitos necesarios para la prestación de servicios de certificación y en qué medida la estar o no acreditado influye en la prestación del servicio y las responsabilidades que conlleva.
6. No se establecen requisitos de transparencia e información hacia los ciudadanos sobre la operativa de las entidades de certificación, sus servicios, quién puede y cómo acceder a los mismos y su correcta utilización. En la práctica nos encontramos con servicios dirigidos a un público demasiado especializado, que producen impotencia en el usuario ante la amalgama de términos empleados, siendo frecuentes los enlaces a otras paginas, lo que lleva al usuario al desconcierto y la confusión.
7. Tampoco se aclara la posición de preeminencia que se otorga a las Administraciones Públicas, que parece dificultar el acceso al mercado de otros operadores privados, limitando la libertad de competencia.
8. A pesar de tal preeminencia administrativa, no se designa una autoridad claramente definida competente para la tramitación y supervisión de la actividad de los operadores de los "servicios de la sociedad de la información", como en el caso que nos ocupa la firma electrónica, ya que da la sensación de no saberse adónde acudir.