Expansión 23/01/2004

EL FUTURO DE LA SEGURIDAD EN LA RED

Las empresas se olvidan de la firma digital

Las administraciones públicas están haciendo un esfuerzo por implantar la firma electrónica, como un elemento seguro para desarrollar operaciones online. En cambio, las compañías se han quedado a la zaga y muy pocas ofrecen la posibilidad en sus páginas web de comerciar usando esta tecnología

Página II

Expansión 23/01/2004

Las administraciones públicas impulsan la firma digital en España

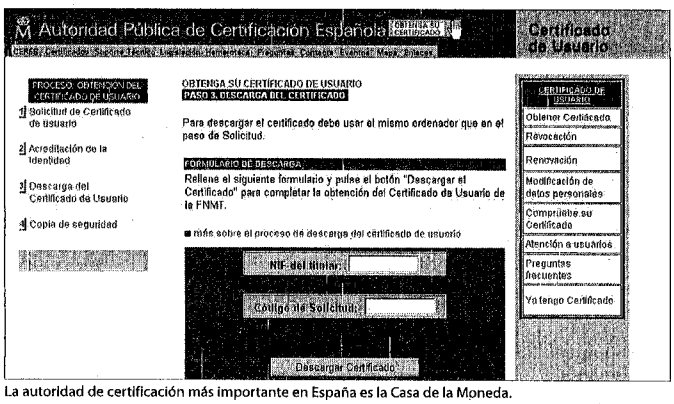
Realizar la declaración de la renta en Internet es una realidad gracias a la firma electrónica, que permite autentificar la identidad de las personas. Aun así, las empresas privadas todavía no se han aventurado a utilizarla debido a que no existe consenso sobre cuál es el estándar más adecuado.

URSULA GUERRA. Madrid

¿Se queda usted tranquilo tras introducir los 16 dígitos de su tarjeta de crédito en Internet? Esta sensación de inseguridad es el *talón de Aquiles* de los negocios online y el principal impedimento para su desarrollo. Una solución es el uso de la firma digital. Sus utilidades son infinitas, desde realizar una compra online, hasta hacer la declaración de la renta, pasando por transacciones bancarias, facturas electrónicas o rellenar documentos sanitarios.

La firma digital está compuesta por dos claves –una privada y otra pública–, que permiten identificar a la persona que ha firmado el documento y, por tanto, asegura que ha sido él y no otro el autor del texto. Como la firma ha sido creada por medio de un dato que sólo el firmante conoce (la clave privada), se evita así la posibilidad de suplantar su identidad. También impide que tanto el firmante como el receptor del texto nieguen haber realizado el mensaje y garantiza que, una vez firmado, nadie pueda modificar el documento durante su transmisión, ya que la clave privada lo encripta. La clave privada va ligada a una certificación electrónica que vincula los datos reales de una persona con su clave pública, lo que confirma su identidad. Estos certificados son emitidos por las autoridades de certificación reconocidas legalmente. (Ver apoyo).

A pesar de estas ventajas, existen pocas empresas privadas que ofrezcan la posibilidad de interactuar con ellas empleando la firma digital. La mayor parte requieren, como única medida de seguridad, una clave de usuario y una contraseña. En cambio, los entes públicos son pioneros en el uso de la firma digital. "La Administración Pública es líder en el uso de la firma digital porque a ella le corresponde velar por la seguridad en la red", comenta Jesús Rojas, socio de Accenture. "Además, el Gobierno ha sido quien ha impuesto el desarrollo de la Sociedad de la Información", dice Arjan Sundardas, profesor del Instituto de Empresa. Las empresas aún no han implantado esta tecnología porque no es vital para sus negocios y porque esperan que las distintas tecnologías que los certificadores usan sean compatibles.



La autoridad de certificación más importante en España es la Casa de la Moneda.

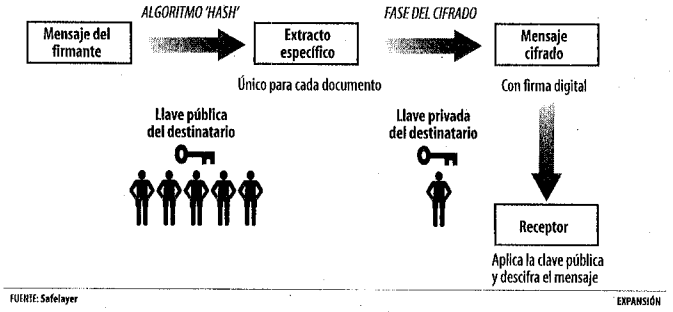
Autoridades de certificación

1. Fábrica Nacional de Moneda y Timbre. (www.cert.fnmt.es)
2. Camerfirma, autoridad de certificación de las Cámaras de Comercio. (www.camerfirma.com)
3. Firma Profesional, entidad creada por los colegios profesionales.
4. Fundación para el estudio de la Seguridad de las Telecomunicaciones (Feste), entidad formada por registradores, notarios, abogados, la Universidad de Zaragoza e Intercomputer. (www.feste.com)
5. Servicio de los registradores de la propiedad y mercantiles.
6. Algunas comunidades autónomas, como la de Asturias, Valencia, Cataluña o País Vasco.
7. La empresa de seguridad en Internet VeriSign.
8. Agencia de Certificación Electrónica (ACE), homologada por Visa y Mastercard, y participada por Telefónica, Ceca, Sermepa y Sistema 4B. (www.ace.es)
9. La empresa española Internet Publishing Services. (www.ips.es)

Un proceso complejo

La firma digital está formada por una serie de caracteres elaborados por un sistema informático, que se basa en algoritmos matemáticos. La firma digital emplea un método de encriptación que adjudica una clave pública y otra privada a cada sujeto. La clave pública es conocida por los usuarios de cada operación. Para firmar electrónicamente un documento, el software del firmante aplica un algoritmo llamado *hash* sobre el texto. Así, se obtiene un extracto específico para ese mensaje. El extracto conseguido se cifra por medio de la clave privada del autor. Y se obtiene el mensaje final cifrado con la firma digital. El receptor del mensaje sólo tiene que aplicar la clave pública para descifrar el mensaje.

Cómo funciona el cifrado de datos



FUENTE: Safelayer EXPANSIÓN

Organismos que permiten utilizarla

Administración central
- Agencia Estatal de Administración Tributaria
- Comisión del Mercado de las Telecomunicaciones
- Instituto de Crédito Oficial
- Instituto Nacional de Estadística
- Ministerio de Economía
- Presidencia de Gobierno
- Seguridad Social
- Dirección General del Catastro
- Dirección General de Costes de Personal y Pensiones Públicas

Administración autonómica
- Comunidad de Madrid
- Gobierno de Canarias
- Gobierno de Navarra
- Gobierno de La Rioja
- Junta de Andalucía
- Xunta de Galicia

Administración local
- Ayuntamiento de Alboraya (Valencia)
- Ayuntamiento de Laredo (Cantabria)
- Ayuntamiento de Catarroja (Valencia)
- Ayuntamiento de Madrid
- Ayuntamiento de Paterna (Valencia)
- Ayuntamiento de Totana (Murcia)
- Ayuntamiento de Valencia
- Ayuntamiento de Barcelona

Otros
- Asociación de Asesores de Empresas en Internet
- Consejo General del Notariado
- Gestor de Infraestructuras S. A.
- Paradores Nacionales de Turismo
- Saniline
- Seguros Broker
- Sociedad Digital de Auditores y Editores

Fuente: FNMT

Legislación

El 20 de marzo de este año entrará en vigor la nueva Ley de Firma Digital, que sustituye al Decreto de 1999. Las novedades radican en que la ley reconoce a la firma digital las mismas garantías legales que a la manuscrita y considera que las personas jurídicas puedan firmar electrónicamente. "Esto ha suscitado controversias porque no estamos acostumbrados a que detrás de un empresa no haya ninguna persona física", explica Carlos Galán, presidente de la Agencia de Tecnología Legal. Desde Camerfirma, la autoridad de certificación de las Cámaras de Comercio, se muestran muy esperanzados con la nueva ley. "Hasta ahora hemos emitido 2.000 certificados pero en 2004 esperamos llegar a 300.000", dice Julián Inza, director general de Camerfirma.

Novedad

La principal novedad que introduce la nueva ley es el documento nacional de identidad electrónico, que dotará a todos los españoles de firma digital. "La implantación del DNI será el impulso definitivo para el comercio electrónico, ya que la seguridad invadirá el sistema", opina Rojas. "El único problema es estandarizar las diferentes tecnologías de los proveedores. El Gobierno ha optado por la libre competencia en el sector, por lo que tendrá que favorecer que las distintas tecnologías de firma digital nacionales e internacionales interoperen", explica Sundardas.

Aún no hay ningún proyecto en marcha para implantar el DNI digital, aunque la ley lo contemple y ya se hayan desarrollado proyectos pilotos en algunas comunidades", explica Felix Calvo, director de Ventas de la empresa española de seguridad Safelayer para Iberia y Latinoamérica. De momento, cualquiera puede tener una firma digital. Sólo ha de acudir a una autoridad de certificación y pedirlo. El precio oscila desde los 10 euros hasta los 60, según el soporte que empleen (microchip, navegador, disquete).

El DNI electrónico supondrá el despegue definitivo del comercio a través de Internet