



CON LA RECIENTE ENTRADA EN VIGOR DE LA LEY 59/2003, DE 19 DE DICIEMBRE, DE FIRMA ELECTRÓNICA SE PRETENDE GENERALIZAR LA CONFIANZA DE LOS CIUDADANOS EN LAS COMUNICACIONES TELEMÁTICAS, SOBRE TODO INTERNET Y EL CORREO ELECTRÓNICO, DOTÁNDOLAS DE SEGURIDAD. EL MEDIO PARA ALCANZAR ESTA META ES, ENTRE OTROS, LA FIRMA ELECTRÓNICA, LA CUAL ES CONSIDERADA EL EJE FUNDAMENTAL PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN Y DEL COMERCIO ELECTRÓNICO.



Firma electrónica: seguridad a través de la Red

Javier Álvarez Hernando

Pocos podían pensar cuando nació Internet en 1969 en Estados Unidos que apenas 30 años después la Red de redes conseguiría en poco tiempo interconectar a millones de personas, instituciones y empresas en todo el mundo, mayoritariamente en los países más desarrollados, y que su evolución y espectacular difusión tendría importantes efectos económicos, culturales y sociales.

Así, en el marco de un mundo cada vez más globalizado, Internet se erige como un medio idóneo para que las empresas se den a conocer y realicen transacciones comerciales, para que los ciudadanos se comuniquen y accedan a un torrente de información (para Manuel Castells, en su trilogía *La era de la información*, Internet ha constituido un paradigma de un modelo social de comunicación libre) y para que las instituciones públicas se interrelacionen con ambos agentes

para facilitar la realización de trámites burocráticos.

No obstante, el desarrollo definitivo del comercio electrónico encuentra en la seguridad su principal problema. Pero **la necesidad de seguridad técnica también exige la existencia de una cierta seguridad jurídica**. Para ello, en los últimos tiempos, con más o menos fortuna, tanto el legislador comunitario como el español han creado todo un elenco normativo que pretende generar esa confianza y dotar a los



ciudadanos y empresas de mecanismos de protección jurídica.

Qué es la firma electrónica

Desde un punto de vista general, la Ley nos dice que la firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

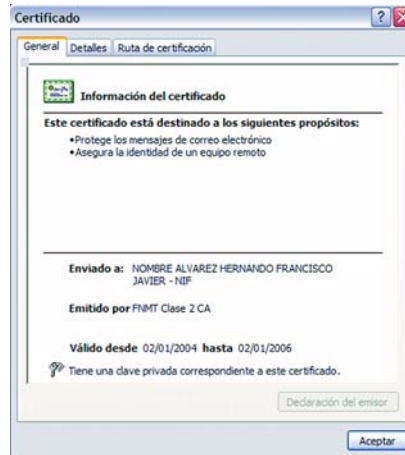
Si sólo nos quedáramos con este concepto, estaríamos hablando simplemente de una firma manuscrita digitalizada, por lo que el legislador nos describe dos tipos más de firma electrónica: La **avanzada**, que es la firma que va a permitir identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a los que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control, y la **firma electrónica reconocida**, que es como la anterior pero basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La importancia de esta última reside en que **tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita** en relación con los consignados en papel.

Siguiendo la pauta marcada por la Ley 34/2002 de comercio electrónico (conocida como LSSICE), se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

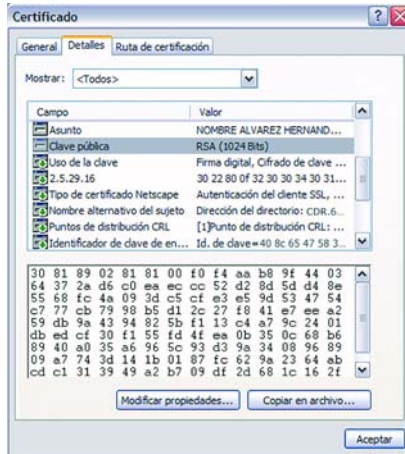
Características esenciales de la firma electrónica

Cuatro son las características esenciales que envuelven a la firma electrónica: **Autenticidad, integridad, confidencialidad y no repudio**.

La firma electrónica trata de garantizar por este medio, que una persona determinada sea quien real-



Información sobre un certificado de la FNMT Clase 2CA



Ejemplo de clave pública

mente interviene en una transacción o negocio jurídico telemático, y que el documento está íntegro y responde a su contenido. Para ello, existe un método seguro que asocie una clave electrónica a una persona, es decir, firma electrónica de un documento, y correlativamente existe otro método para que el receptor pueda comprobar que realmente esa persona lo firmó.

Igualmente, la firma electrónica permite que el documento viaje en un entorno seguro, impidiéndose su interceptación por parte de terceros, aunque esta característica de confidencialidad de la información transmitida no se configura como un elemento básico en la Ley de firma electrónica, sino más bien como un valor añadido.

El último aspecto fundamental de la firma electrónica es el denominado «no repudio», es decir, una vez aceptado un negocio jurídico concreto éste no puede ser rechazado por las partes que intervinieron en él, debido a que la intervención de una tercera parte de confianza –un prestador de servicios de certificación– impide que una parte pueda «repudiar» posteriormente una relación jurídica aceptada inicialmente.

Por tanto, la firma electrónica se constituye como un instrumento capaz de permitir una comprobación de la procedencia (autenticidad) y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio (es decir, el «yo no he sido»), si se adoptan las medidas oportunas basándose en fechas electrónicas.

La firma electrónica y el cifrado de clave pública

El cifrado de datos consiste en someter el mensaje concreto a un tratamiento basado en técnicas de encriptación o cifrado con el objeto de hacer a éste legible únicamente para el destinatario de los datos, el cual conoce la clave.

Existen en la actualidad dos tipos de cifrado: el de **clave simétrica y asimétrica**. Mientras que en el primero la clave para cifrar y descifrar los datos es la misma, en el segundo, en el cifrado de clave asimétrica, el utilizado generalmente, existen un par de claves: una pública y una privada. Una sirve para cifrar (clave pública) y la otra para descifrar (clave privada), pero el conocimiento de una no permite conocer la otra, es decir, para descifrar un mensaje encriptado con una clave pública determinada es necesario aplicar su correspondiente clave privada. La clave privada debe permanecer secreta a diferencia de la pública que se da a conocer, ya que es condición necesaria para completar el proceso.



Prestadores de servicios de certificación

Una figura importante que regula la Ley son los llamados **prestadores de servicios de certificación (PSC)**. Éstos son personas físicas o jurídicas que expiden certificados electrónicos o prestan servicios relacionados con la firma electrónica.

La **Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda** (www.cert.fnmt.es) se constituye legalmente como el certificador público de firma electrónica. No obstante, el legislador pretende que los PSC privados tengan un mayor protagonismo en los sistemas de certificación. Así, por ejemplo, la obligación de constitución de garantía económica por parte de los PSC que emitan certificados reconocidos, pasa de 6 millones de euros, según se establecía en la normativa anterior, a 3 millones. Se flexibiliza, además, la combinación de los diferentes instrumentos para constituir dicha garantía.

En otro orden de cosas, mencionar que la Ley obliga a los PSC a efectuar una tutela permanente de los certificados que expiden. Los detalles de esta gestión deben recogerse en la llamada **Declaración de prácticas de certificación**, donde se deben de especificar las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados



Proceso de autenticación del certificado



Proceso (automático) de firma con clave privada

electrónicos. Puede consultarse la Declaración de prácticas de certificación de la FNMT-RCM en la dirección: www.cert.fnmt.es/convenio/dpc.pdf

La Ley equipara esta declaración con el **documento de seguridad** a los efectos previstos en la legislación en materia de protección de datos de carácter personal, por lo que deberá contener todos los requisitos que se exigen en dicha normativa específica

(es decir, en el Real Decreto 994/1999 y en la Ley Orgánica 15/1999).

Qué son los certificados electrónicos

Son documentos electrónicos expedidos por los PSC que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

Físicamente es un archivo de aproximadamente 2 Kb de tamaño que contiene, principalmente, los datos de una persona física o jurídica, su clave pública, y la firma de un prestador de servicios de certificación que cuenta con la capacidad de poder comprobar la identidad de la persona y valida la clave pública asociada al firmante.

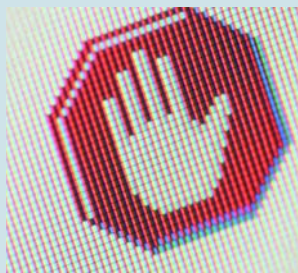
Clases de certificados electrónicos de PSC públicos y cómo obtenerlos

El más extendido es el **Certificado de Usuario** (llamado «Clase 2 CA de la FNMT»). Para obtenerlo hay que acceder al sitio web de la FNMT (www.cert.fnmt.es/clase2/main.htm) y cumplimentar un formulario de datos personales, tras lo cual se mostrará un código alfanumérico. Posteriormente, es necesario personarse con el DNI y con el código anterior en una de las oficinas de registro

Sabía que...

► España fue el cuarto país de la UE (por detrás de Alemania, Italia y Portugal) en aprobar una norma (RD-L 14/1999) que otorga validez jurídica a la firma electrónica.

► El sistema criptográfico más antiguo conocido es el llamado «Método de Julio César» y se empleaba en la época del Imperio Romano en los correos para comunicarse sin que sus enemigos consiguieran adivinar el contenido de los mensajes. El sistema consistía en reemplazar cada letra por la situada tres posiciones por delante en el alfabeto.



► En enero de 2004 la autoridad de certificación de la Generalitat Valenciana fue la primera, además de la FNMT, cuyos certificados de firma electrónica fueron aceptados

en las relaciones entre la Agencia Tributaria y los contribuyentes.

► Finlandia fue el primer país europeo en adoptar el DNI electrónico (1999), siendo Bélgica el segundo en expedirlo de manera oficial.

► El voto electrónico se probó por primera vez en España en marzo de 2003 en Hoyo de Pinares (Ávila) donde se simuló una votación. El Gobierno ha anunciado que para el referéndum sobre la Constitución Europea para el 2005 pretende que el voto electrónico sea una realidad.

► El uso de la firma electrónica en las facturas electrónicas ha supuesto un ahorro de millones de euros al año al eliminarse las facturas en papel y permitir el uso de la firma electrónica en ellas.

► El Centro Penitenciario de Tarragona ha sido el primero en España donde se aplica una experiencia piloto que consiste en el uso de la firma electrónica para que los abogados del Colegio de Reus puedan solicitar pases de acceso a dicha prisión para realizar su cometido profesional.



LEGISLACIÓN MÁS DESTACADA SOBRE FIRMA ELECTRÓNICA

- ▶ **Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000**, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.
- ▶ **Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999**, por la que se establece un marco comunitario para la firma electrónica.
- ▶ **Ley 59/2003, de 19 de diciembre**, de firma electrónica.
- ▶ **Ley 34/2002, de 11 de julio**, de servicios de la sociedad de la información y de comercio electrónico.
- ▶ **Real Decreto-ley 14/1999, de 17 de septiembre**, regula el uso de la firma electrónica. (Derogado).



Proceso de instalación de un certificado electrónico

señaladas en la página web de la FNMT. Una vez acreditados en la oficina de registro se deberá firmar el contrato y el funcionario procederá a activar ese código personal. Finalmente hay que descargar en el ordenador el Certificado de Usuario desde la web de la FNMT. Tanto la obtención como el uso del certificado son gratuitos.

Completado el proceso de forma correcta podremos acceder a todos los servicios que la Administración Electrónica ofrece a los ciudadanos de una forma sencilla y segura.

Existe, además, un certificado propio de la Seguridad Social llamado **SILCON** que es necesario para acceder a los servicios del Sistema RED, Mutuas de



Accidentes de Trabajo, Centros Públicos de Salud o Instituto Cervantes.

El proceso para obtener este certificado es similar al anterior con la diferencia que en la oficina de acreditación se hace entrega de un disquete que contiene el certificado y un sobre con una contraseña.

El certificado de usuario puede, además, estar en una **tarjeta criptográfica**, siendo uno de los elementos clave en el sistema de seguridad ofrecido por la FNMT, ya que se incrementa la seguridad del sistema de certificación debido a que las claves se generan en la propia tarjeta inteligente. Para su uso es necesario un lector de tarjeta.

El precio del kit básico (tarjeta, lector y

software) viene a costar unos 43 euros, aproximadamente, y se comercializa por la empresa C3PO (www.c3po.es/cryptokit.html), la cual de forma conjunta con la FNMT, ha creado el sistema de cifrado e identificación electrónica llamado **Cryptokit**.

Firma electrónica de las personas jurídicas

Otra de las novedades que se incluyen en la Ley es la posibilidad de que se emitan certificados de personas jurídicas, cuestión que no era posible en el Real Decreto-Ley de 1999 el cual sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión tributaria.

La firma electrónica de las personas



LA FIRMA ELECTRÓNICA EN LA JURISPRUDENCIA

► Sentencia de la Audiencia Nacional de 15 de noviembre de 2002.

Respecto a las formas que acreditan la celebración de un contrato, la AN menciona en esta sentencia la existencia de formas de formalización que ofrecen garantías similares a la forma escrita, refiriéndose a la firma electrónica avanzada (según el concepto del Real Decreto-Ley 14/1999).

► Sentencia del Tribunal Superior de Justicia de Canarias de Las Palmas de Gran Canaria, de 23 de julio de 2002.

El Tribunal reitera la validez de los documentos electrónicos, al poner de manifiesto –respecto al Sistema RED– que la firma electrónica permite comprobar por parte de la Administración gestora si el documento ha sido generado de manera remota en el ordenador a partir de los datos que obran en la base de datos pública. Por tanto, el documento así generado, surte efectos ante terceros, ya que es una certificación emitida por la

TGSS.

► Sentencias del Tribunal Supremo de 2 de julio de 2001.

El TS viene a confirmar que la FNMT se configura como un prestador de servicios de certificación en régimen de competencia que expide certificados de firma electrónica pudiendo desempeñar funciones relacionadas, no pudiendo extenderse a lo que es propio de la seguridad jurídica contractual, es decir, no sustituye ni modifica las funciones que corresponde realizar a las personas facultadas para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

► Sentencia del Tribunal Supremo, de 3 de noviembre de 1997.

Se cuestiona la validez de los documentos electrónicos en un asunto relativo a su consideración como mercantiles, a efectos de la aplicación del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados. Si se dan todas las circunstancias necesarias para acreditar la autenti-

cidad de los ficheros electrónicos y se garantiza, con las pruebas periciales en su caso necesarias, la veracidad de lo documentado y la autoría de la firma electrónica utilizada, el documento mercantil en soporte informático, con función de giro, debe gozar de plena virtualidad jurídica operativa.

Otras sentencias relacionadas con la firma o el documento electrónico:

► Sentencia de la Audiencia Provincial de Asturias, de 3 de marzo de 2003.

► Sentencia del Tribunal Supremo de 12 de febrero de 2002.

► Auto del Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 3.ª), de 11 de abril de 2000.

► Sentencia de la Audiencia Provincial de Las Palmas núm. 121/1998, de 19 de octubre de 1998.

► Sentencia del Tribunal Supremo, de 30 de noviembre de 1992.

► Sentencia del Tribunal

jurídicas establece una figura, distinta a la de la firma electrónica de los representantes de las personas jurídicas, que persigue dar firma a las entidades, no a sus representantes, si bien con el objeto de que así se puedan distribuir entre personas físicas vinculadas a la organización y que no tienen capacidad formal de representación. Es decir, se pretende, por ejemplo, que un empresario pueda repartir firmas electrónicas entre sus empleados para el desempeño de las actividades ordinarias de la empresa, y dentro de unos límites impuestos por la persona jurídica por razón de la cuantía o de la materia. Estas condiciones deberán figurar en el certificado electrónico.

Pero, ¿quién puede solicitar los cer-

tificados electrónicos de personas jurídicas? La Ley exige una legitimación especial para que las personas físicas puedan solicitar la expedición de certificados. Se limita esta facultad a los **administradores y los representantes legales y voluntarios con poder bastante**. Además, a los solicitantes se les considera responsables de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad.

En cuanto a la **responsabilidad** que se deriva frente a terceros por el uso de una firma por parte de una persona jurídica, se van a entender realizadas por ella los actos o contratos en

los que su firma se hubiera empleado dentro de los límites y condiciones estipuladas, las cuales figuran en el propio certificado. En el supuesto de que la firma sobrepasara esos límites la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su propio interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable custodiar esa firma electrónica, quien podrá dirigirse, en su caso, contra quien la hubiera utilizado.

DNI electrónico

La ley establece el marco normativo básico del nuevo DNI electrónico apuntando que éste sirve para acredi-



tar la identidad de su titular en cualquier procedimiento administrativo y, además, permite la firma electrónica de documentos. Las bases para su implantación se establecieron en Consejo de Ministros el 13 de febrero de 2004 dentro del 'Plan de Actuaciones para el desarrollo de la Sociedad de Información'.

Servicio de notificaciones telemáticas

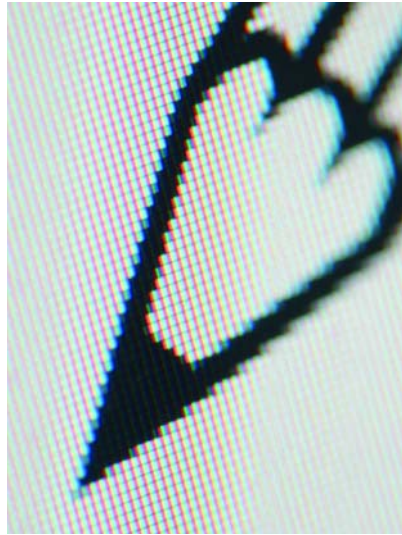
El correo electrónico se ha convertido en una herramienta fundamental en las comunicaciones. Sin embargo, no existen garantías de seguridad cuando enviamos un *e-mail* que nos aseguren que el destinatario recibió el mensaje, que tanto el emisor como el receptor son quienes dicen ser, que el mensaje no ha sufrido cambios en el tránsito o que el mensaje se envió en un día y hora determinada.

El **Ministerio de Administraciones Públicas y Correos** han desarrollado un **servicio de notificaciones telemáticas seguras** que proporciona, de forma gratuita, a cada ciudadano o empresa una dirección electrónica personal y única en la que puede recibir todas las notificaciones de la Administración con pleno valor jurídico, y con las **mismas garantías y valor probatorio que le correo certificado o el burofax**. Tan sólo es necesario un certificado digital, emitido por la FNMT u otros prestadores autorizados.

Administración electrónica

Con un certificado electrónico se puede acceder a numerosos servicios telemáticos de la E-Administración. Así, a través del portal de la **Seguridad Social (www.seg-social.es)** se puede, desde acceder al informe de vida laboral y bases de cotización, hasta solicitar un duplicado del documento de afiliación a la Seguridad Social. Otros servicios destacados son el acceso al Sistema RED o el servicio de Mutuas de Accidentes de Trabajo y Centros Públicos de Salud, entre otros.

La Agencia Tributaria (www.aeat.es)



tampoco se queda atrás en sus servicios *on line* y permite la presentación electrónica de declaraciones y su con-

sulta, la obtención de certificaciones tributarias electrónicas, la tramitación de recursos y reclamaciones, la facturación telemática, etc.

En definitiva, poco a poco la Administración electrónica está evolucionando progresivamente, permitiéndose la realización de trámites *on line*, mediante certificado digital, en prácticamente todos los ministerios y órganos administrativos, así, por ejemplo, citar, los sitios web del Ministerio de Industria, Turismo y Comercio (<http://www.min.es>), Ministerio de Economía: <http://www.mineco.es>, Comisión Nacional del Mercado de Valores (<http://www.cnmv.es>), Ministerio del Interior (<http://www.mir.es>), o Ministerio de las Administraciones Públicas: (<http://www.map.es>), por mencionar los más destacados. ⁿ

PARA SABER MÁS SOBRE LA FIRMA ELECTRÓNICA

- ▶ Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. www.setsi.mcyt.es
- ▶ Instituto Notarial para las Tecnologías de la Información. www.inti.ancert.com/
- ▶ Agencia de Certificación Electrónica (ACE). www.ace.es/
- ▶ Camerfirma. www.camerfirma.es/
- ▶ Firmaprofesional (PSC dirigido exclusivamente a colegios profesionales). www.firmaprofesional.com
- ▶ Autoritat de Certificació de la Comunitat Valenciana. www.pki.gva.es
- ▶ Autoridad de Certificación de la Abogacía (ACA) del Consejo General de la Abogacía Española. www.acabogacia.org
- ▶ Colegio de Ingenieros de Caminos, Canales y Puertos. www.pki.ciccp.es/
- ▶ Agencia Notarial de Certificación. www.ancert.com/
- ▶ Banesto. www.ca.banesto.es/
- ▶ IZANPE (Sociedad creada por instituciones públicas vascas). www.izenpe.com
- ▶ Internet Publishing Services, S.L. www.ips.es/
- ▶ Fundación para el Estudio de la Seguridad de las Telecomunicaciones. www.feste.com
- ▶ Portal que describe los procesos de estandarización correspondientes al Plan eEurope de la Comisión Europea. www.europe-standards.org
- ▶ Iniciativa de estandarización de la firma electrónica europea (EESSI) www.ictsb.org



Para saber más sobre la firma electrónica en particular y el comercio electrónico en general, consulte la segunda edición de la obra: *Comercio y firma electrónicos. Análisis jurídico de los servicios de la sociedad de la información*, de Francisco Javier García Más (Editorial Lex Nova).