LA FIRMA ELECTRÓNICA EN LA UE Y ESPAÑA:

PANORAMA DEL MARCO REGULATORIO GENERAL

SALVADOR SORIANO MALDONADO
Subdirector General de Servicios de la Sociedad de la Información. *Ministerio de Ciencia y Tecnología*

ESTE ARTÍCULO INTRODUCE LOS CONCEPTOS DE FIRMA ELECTRÓNICA Y FIRMA ELECTRÓNICA AVANZADA Y OFRECE UNA PANORÁMICA GENERAL DEL MARCO REGULATORIO AL QUE ESTÁ SOMETIDA LA FIRMA ELECTRÓNICA, TANTO EN EL ámbito comunitario como en el ámbito nacional.

De manera previa al inicio de la descripción del marco regulatorio general sobre firma electrónica, resulta conveniente fijar las definiciones y conceptos técnicos básicos asociados a la misma.

Empecemos por considerar las características propias de Internet, que está configurada como una red abierta, de fácil accesibilidad, que ofrece la posibilidad de establecer comunicaciones interactivas, a bajo coste, con gran capilaridad, entre puntos situados en lugares cualesquiera a nivel mundial, situándola, en principio, como candidata idónea para la prestación de multitud de servicios, tanto en el sector privado como en el sector público.

El carácter abierto y fácilmente accesible de Internet constituye uno de sus puntos fuertes, pero también hace necesario disponer de herramientas que añadan una mayor seguridad en las comunicaciones que se efectúen con soporte en la misma. Como respuesta a esta necesidad de mejora de la seguridad de las comunicaciones por Internet, surge, entre otros, el concepto de firma electrónica.

LA FIRMA ELECTRÓNICA Y LA FIRMA ELECTRÓNICA AVANZADA

En lo que se refiere a los conceptos de «firma electrónica» y de «firma electrónica avanzada», también denominada esta últi-

ma «firma digital», vamos a ceñirnos en este artículo a las definiciones recogidas en la Directiva 1999/93/CE, de 13 de diciembre de 1999 y en el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

Entenderemos por firma electrónica al conjunto de datos, en forma electrónica, asociados a un mensaje, que se utilizan como medio de autenticación. El concepto de firma electrónica así definido es muy amplio, e incluye desde los métodos de autenticación más simples, como insertar una imagen digital de una firma manuscrita o simplemente teclear un nombre al pie de un mensaje, a los más complejos, que reúnen un mayor número de requisitos de seguridad desde el punto de vista técnico, como es el caso de la firma electrónica avanzada.

Entenderemos por firma electrónica avanzada o firma digital, la que cumple los cuatro requisitos siguientes:

✓ Estar vinculada al firmante de manera única.

✓ Permitir la identificación del firmante.

✓ Haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control.

✓ Estar enlazada con a los datos a que se refiere, de modo que cualquier cambio de los mismos de manera posterior a la firma sea detectable.

La firma electrónica avanzada, tal y como se ha definido, aporta un claro valor añadido desde el punto de vista de la seguridad de las comunicaciones, basándose en herramientas técnicas específicas, cuyos aspectos básicos resulta conveniente conocer, por lo que, a continuación, se expondrán algunos conceptos técnicos relevantes en relación con la firma electrónica avanzada.

Fases de la firma electrónica

La firma electrónica avanzada o firma digital está basada en la aplicación de una transformación matemática (en inglés,

hash) sobre un documento o mensaje, de manera que, se extrae del mismo un resumen o huella digital (en inglés, digest), de mucho menor tamaño que el documento original. A partir de esta huella digital extraída no resulta posible reconstruir el documento original y, además, presenta la característica de que dos documentos diferentes dan lugar a huellas digitales también diferentes, por lo que, si se modifica un documento, la huella digital que se obtenga del documento modificado será distinta a la huella digital inicial. Las dos funciones más conocidas para la obtención de huellas digitales son SHA-1 y MD5.

Una vez obtenida, mediante la aplicación de la función hash, la huella digital de un documento, ésta se encripta con un sistema criptográfico asimétrico, también conocido como sistema criptográfico de clave pública.

En este punto, resulta oportuno hacer una breve referencia a las funcionalidades relevantes de un sistema criptográfico asimétrico.

Un sistema criptográfico asimétrico se basa en la generación de un par de claves relacionadas entre sí complementariamente, de manera que un mensaje encriptado con una de ellas sólo puede ser desencriptado usando la otra clave. El funcionamiento habitual requiere que una clave del par se mantenga en secreto (clave privada), mientras que la otra se haga pública (clave pública).

De esta forma, cuando un usuario encripta un mensaje con su clave privada, este puede ser desencriptado por todos aquellos otros usuarios que conocen la clave pública correspondiente a la clave privada del primero. Igualmente, si se remite electrónicamente un mensaje encriptado con la clave pública del destinatario, sólo éste podrá desencriptarlo, utilizando su clave privada correspondiente, que sólo él conoce.

Como se exponía anteriormente, al aplicar la firma electrónica avanzada sobre un documento se obtiene su huella digital y ésta se encripta usando un sistema criptográfico asimétrico, para lo que se utilizará la clave privada en poder del firmante.

Una vez efectuada la firma y remitido un mensaje firmado, el destinatario dispondrá de un documento y de su huella digital encriptada con la clave privada del remitente.

El destinatario del mensaje puede proceder a desencriptar la huella digital, usando la clave pública correspondiente al firmante y obtener así la huella digital del documento en claro (no encriptada), de manera segura. Ahora, el destinatario puede comprobar que el documento no ha sido modificado, de manera posterior a su firma, si aplica la función «hash» sobre el documento y la huella digital obtenida como resultado coincide con la huella digital desencriptada. Este procedimiento proporciona al destinatario seguridad en la integridad del documento recibido.

Adicionalmente a esta comprobación de la integridad de un documento, dadas las características de complementariedad del par de claves de los sistemas criptográficos asimétricos, si una determinada clave pública ha podido desencriptar la huella digital de una firma, esto asegura que la firma fue efectuada por el poseedor de la clave privada complementaria correspondiente.

Si a lo anterior se añade la intervención de una tercera parte de confianza que relaciona una clave pública con una iden-

tidad personal concreta, podremos identificar al firmante del mensaje. Para ello se utilizan los denominados certificados electrónicos, emitidos por los prestadores de servicios de certificación. Estos prestadores, en base a una serie de políticas de certificación, comprueban la identidad del titular del certificado y la relacionan con un par de claves criptográficas asimétricas, emitiendo el certificado que corresponda.

Por tanto, un certificado vincula unos datos de verificación de firma con una persona firmante y confirma la identidad de ésta. Los certificados contienen típicamente un código identificativo, la identificación del firmante, la clave pública de verificación de firma, su período de validez y sus límites de uso y de valor de transacciones que pueden efectuarse con el mismo. El prestador de servicios que emite el certificado aplica su firma electrónica avanzada sobre el mismo (usando su clave privada), por lo que se añade al certificado la característica de integridad de la información contenida en el mismo y pueden ser verificados usando la clave pública del prestador.

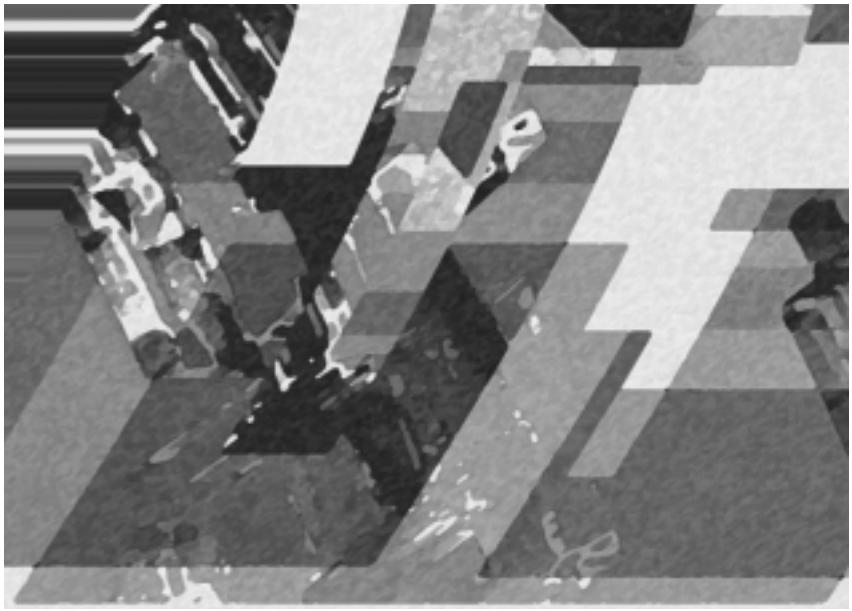
La firma electrónica descrita, que aplica un sistema criptógrafico asimétrico a la huella digital de un documento y basada en un certificado emitido por un prestador de servicios, cumple las características de:

Integridad: garantía de que los datos originales no han sido modificados, si la firma se verifica correctamente por el destinatario.

Autenticación: garantía de que el firmante de un documento electrónico está identificado a través del certificado emitido por el prestador de servicios de certificación.

No repudio: la firma electrónica está asociada unívocamente a la clave privada del firmante, por lo que mediante el uso de la clave pública correspondiente, la firma puede serle atribuida directamente a éste.

El procedimiento y los elementos técnicos expuestos anteriormente, constituyen la base para cumplir con los requisitos legales necesarios para que una firma electrónica pueda ser considerada como firma electrónica avanzada o firma digital.



Por otra parte, en lo que se refiere a la salvaguarda de la confidencialidad de los mensajes, ya no a su autenticación e integridad, pueden utilizarse también los sistemas criptográficos asimétricos para aplicarlos directamente al documento que se desea proteger, en lugar de a su huella digital, como ocurre en el caso de la firma electrónica. Para este uso de confidencialidad de las comunicaciones, las políticas de seguridad aconsejan la utilización de un par de claves diferentes de las que puedan ser utilizadas para efectuar la firma digital.

MARCO REGULATORIO COMUNITARIO SOBRE LA FIRMA ELECTRÓNICA

La 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, publicada en el Diario Oficial de las Comunidades Europeas de 19 de enero de 2000 (en adelante, la Directiva), tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico, garantizando además el correcto funcionamiento del mercado interior.

LA DIRECTIVA QUE ESTABLECE EL MARCO: CONTENIDO

La Directiva establece que para la prestación de servicios de certificación no será necesario la obtención de autorización previa. Esta premisa se declara compatible con el posible establecimiento de sistemas voluntarios de acreditación que promuevan una mejora en los niveles de la calidad de prestación de servicios de certificación.

Asimismo, la Directiva, en cuanto al correcto funcionamiento del mercado interior, establece que los Estados Miembros no podrán restringir la prestación de servicios de certificación que procedan de otro Estado Miembro.

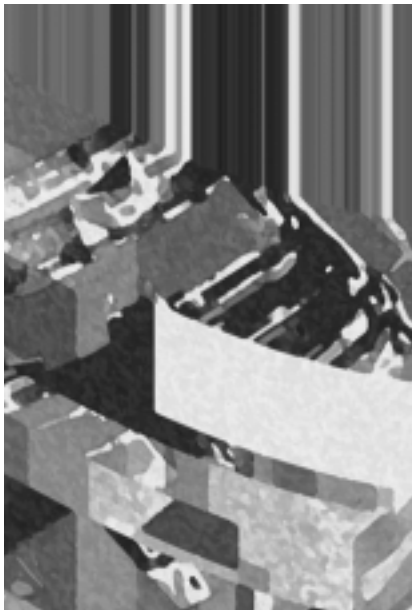
En lo que se refiere a los efectos jurídicos de la firma electrónica, resulta relevante destacar que la Directiva establece una equivalencia entre una firma manuscrita y una firma electrónica avanzada, que esté basada en los siguientes requisitos:

1| Esté soportada por un certificado reconocido, que es aquél que:

Cumple con el anexo I de la Directiva, es decir, que contiene: la indicación de que el certificado se expide como reconocido; la identificación del prestador y del Estado en que está establecido; el nombre y apellidos del firmante o seudónimo; un atributo específico del firmante (en caso de que fuera significativo en función de la finalidad del certificado); los datos de verificación de firma que correspondan a los de creación de firma bajo control del firmante; el período de validez del certificado; un código identificativo del certificado; la firma electrónica avanzada del prestador que emite el certificado; los límites de uso (si procede) y los límites del valor de transacciones en las que puede utilizarse el certificado (si procede).

Es suministrado por un prestador de servicios de certificación que sea capaz de: demostrar la fiabilidad necesaria para prestar servicios de certificación; garantizar un servicio rápido y seguro de guía de usuarios y un servicio de revocación seguro e inmediato; garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado; comprobar debidamente la identidad y atributos específicos de la persona a la que se expide un certificado; emplear personal con los conocimientos, experiencia y cualificaciones necesarias; utilizar sistemas y productos fiables; tomar medidas contra la falsificación de certificados y, en caso de que el prestador genere datos de creación de firma, garantizar la confidencialidad del proceso de generación; disponer de recursos suficientes, en particular, para afrontar el riesgo de responsabilidad por daños y perjuicios; registrar la información relativa a un certificado durante un tiempo adecuado, en particular, para aportar pruebas de certificación en procedimientos judiciales; no almacenar ni copiar datos de creación de firma de terceros; informar de las condiciones de utilización del certificado y de los procedimientos de reclamación y solución de litigios y utilizar sistemas fiables para almacenar certificados, de forma verificable.

2] Haber sido creada mediante un dispositivo seguro de creación de firma, que cumple con los requisitos del Anexo



III de la Directiva, es decir, que los dispositivos citados garanticen que: los datos utilizados para la generación de la firma sólo puedan producirse una vez en la práctica y se garantice razonablemente su secreto; que exista seguridad razonable de que los datos utilizados para la generación de la firma no puedan ser hallados por deducción y la firma está protegida contra falsificación; que los datos de generación de firma puedan ser protegidos de forma fiable y que, además, estos dispositivos no alteren los datos que deben firmarse, ni impidan que éstos se muestren antes del proceso de firma.

Por otra parte, este reconocimiento de equivalencia con la firma manuscrita no excluye la eficacia jurídica de una firma electrónica que no cumpla con los requisitos anteriores, debiendo determinarse, en cada caso, su validez y eficacia jurídica.

En cuanto al régimen de responsabilidades, la Directiva se centra en los prestadores de servicios que expiden certificados reconocidos, siendo responsables: de la veracidad de los datos contenidos en los mismos; de la complementariedad de los datos de creación (clave privada) y verificación de firma (clave pública) expedidos por el prestador; de que el titular del certificado dispone de los datos de creación de firma correspondientes a los datos de verificación que figuran en el certificado y de registrar la revocación de los certificados. No obstante, se contempla la posibilidad de eximir al prestador de estas responsabilidades cuando demuestre que no ha actuado con negligencia.

Asimismo, la Directiva prevé una limitación de la responsabilidad de los prestadores de servicios de certificación por la utilización de certificados reconocidos emitidos por ellos, en caso de que no se respeten los límites de utilización o los valores límite de transacciones establecidas en los certificados, siempre y cuando estos límites sean reconocibles para terceros.

Finalmente, es de destacar que la Directiva crea una comité de firma electrónica, cuyos trabajos se centrarán en la clarificación de los requisitos establecidos en los anexos de la Directiva y en determinar las normas técnicas que gocen de reconocimiento general para productos de firma electrónica.

DECISIÓN SOBRE ORGANISMOS EVALUADORES

La Comisión Europea adoptó una Decisión, con fecha 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados Miembros para designar organismos responsables de evaluar la conformidad de los dispositivos seguros de creación de firma, de conformidad con el apartado 4 del artículo 3, de la 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.

En esta Decisión se recogen una serie de requisitos que deben ser cumplidos por el organismo responsable de evaluar la conformidad de los dispositivos seguros de creación de firmas, destacando los siguientes: ser independiente de las partes interesadas (fabricantes, proveedores, o prestadores de servicios) y gozar de independencia financiera; disponer de suficiente competencia técnica e integridad profesional y recursos humanos y

materiales suficientes; ser transparente en las prácticas de determinación de la conformidad y aplicar procedimientos no discriminatorios; proporcionar una cobertura de las responsabilidades resultantes de sus actividades y garantizar la confidencialidad de la información obtenida.

Estos organismos podrán delegar en terceros, cuya competencia sea demostrable, parte de la determinación de conformidad.

MARCO REGULATORIO NACIONAL SOBRE FIRMA ELECTRÓNICA

El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, publicado en el Boletín Oficial del Estado de 18 de septiembre de 1999, se anticipó, a la publicación de la ya referida Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

El Real Decreto-Ley se elaboró sobre la base del texto de la posición común del proyecto de Directiva citado, informado favorablemente en la sesión del Consejo de Ministros de Telecomunicaciones de la Unión Europea de 22 de abril de 1999 y ratificado mediante Resolución de 21 de octubre de 1999 del Congreso de los Diputados.

El Real Decreto-Ley recoge la regulación establecida en la Directiva 1999/93/CE, de 13 de diciembre de 1999, citada anteriormente, y además, concreta y desarrolla aspectos que corresponden, en base al principio de subsidiariedad, a cada uno de los Estados Miembros. Por tanto, lo expuesto para la Directiva 1999/93/CE, de 13 de diciembre, resulta trasladable a este Real Decreto-Ley y nos centraremos en este artículo en repasar algunos aspectos relevantes adicionales a los ya establecidos en la citada Directiva.

El Real Decreto-Ley crea, en el Ministerio de Justicia, un registro de prestadores de servicios de certificación, que será de acceso público por vía telemática o a través de certificación registral, y en el que los prestadores deberán solicitar su inscripción, con carácter previo al inicio de su actividad (artículo 7).

Asimismo, el Real Decreto-Ley detalla, en mayor medida de lo que lo hace la Directiva, las condiciones aplicables para el uso de la firma electrónica en las Administraciones Públicas. En particular, se prevé que las normas estatales que regulen las condiciones adicionales sobre el uso de la firma electrónica se dictarán a propuesta del Ministerio de Administraciones Públicas, previo informe del Consejo Superior de Informática (artículo 5).

El Real Decreto-Ley desarrolla también las obligaciones exigibles a los prestadores de servicios de certificación, en particular, concreta la garantía que debe constituirse en el caso de expedición de certificados reconocidos. La cuantía de la garantía se establece en función de si los certificados limitan o no el importe de las transacciones que pueden efectuarse con los mismos (artículo 12).

Por otra parte, hay que destacar que el Real Decreto-Ley prevé el establecimiento de un sistema de acreditación de prestadores de servicios de certificación y de certificación de productos de firma electrónica (artículos 6 y 21), que en la Directiva se apunta como una posibilidad y se deja su aplicación práctica a criterio de los Estados Miembros. Este sistema de acreditación se ha desarrollado mediante la Orden de 21 de febrero de 2000, que se comenta en el siguiente apartado de este artículo. Asimismo, el Real Decreto-Ley establece una tasa por el reconocimiento de acreditaciones y certificaciones (Título IV).

Asimismo, el Real Decreto-Ley establece un régimen de supervisión y control de los prestadores de servicios de certificación, que corresponde a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, imponiendo el deber de colaboración de los prestadores de servicios de certificación con la citada Secretaría de Estado, en el ejercicio de sus funciones (Título II, Capítulo IV).

Adicionalmente, la citada norma recoge un régimen de infracciones y sanciones, clasificando las infracciones en leves, graves y muy graves, detallando las sanciones correspondientes a cada uno de los tipos de infracciones y estableciendo la posibilidad de adoptar medidas cautelares en procedimientos sancionadores por infracciones graves o muy graves, respetando el principio de proporcionalidad, para asegurar la eficacia de la resolución que definitivamente se dicte (Título V).

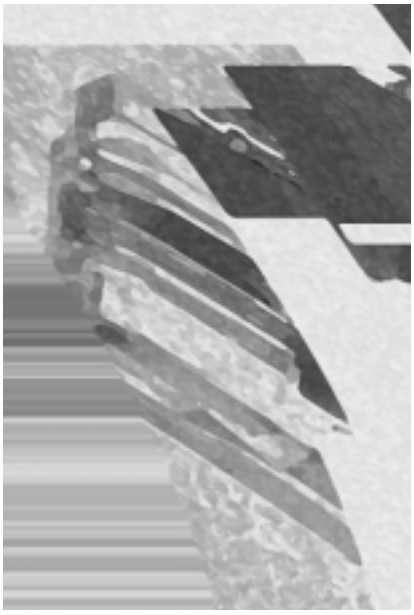
Reglamento de acreditación de prestadores de servicios

El Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, aprobado mediante Orden de 21 de febrero de 2000 (en adelante, Reglamento de acreditación), desarrolla el sistema de acreditación previsto en el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, y pretende que este sistema se constituya como un sello de calidad de los prestadores de servicios y de los productos de firma electrónica, permitiendo incrementar la confianza de los usuarios en estas herramientas de seguridad.

El Reglamento de acreditación establece que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información es el órgano competente para acreditar a los prestadores de servicios de certificación y para certificar productos de firma electrónica que estén destinados a conectarse a puntos de terminación de una red pública de telecomunicaciones, o que estén destinados a garantizar la seguridad de la información que se transmita por vía electrónica mediante redes de telecomunicación (artículo 2).

El Reglamento de acreditación establece la figura de las entidades de evaluación (Capítulo II), que son organismos públicos o privados acreditados por la Entidad Nacional de Acreditación (en adelante, ENAC). A estos efectos, se prevé que se celebre un Convenio de colaboración entre la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y la ENAC, (Capítulo III). Este convenio ha sido firmado el pasado 27 de noviembre de 2001.

Las entidades de evaluación informarán sobre el cumplimiento de las condiciones técnicas que se hayan previsto para la acreditación de prestadores de servicios o la certificación de dispositivos de firma electrónica, emitiendo un informe de evaluación previo a la solicitud de acreditación o certificación de conformidad (artículo 3 y capítulos IV y V).



Real decreto sobre prestación de servicios por la ENMT

El Real Decreto 1317/2001 de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, en materia de prestación de servicios de seguridad, por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas, desarrolla las condiciones de prestación por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (en adelante, FNMT) de los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de las comunicaciones de la Administración General del Estado y sus organismos públicos. Esta prestación se efectúa en régimen de libre concurrencia con otros prestadores de servicios presentes en el sector.

De este Real Decreto sólo destacaremos algunos de sus aspectos más relevantes a efectos de prestación de los servicios por parte de la FNMT.

El citado Real Decreto prevé que la FNMT proporcione a cada usuario un certificado electrónico, que deberá reunir las condiciones necesarias para ser considerado como certificado reconocido, según lo dispuesto en el citado Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

El Real Decreto 1317/2001, de 30 de noviembre, establece en su Capítulo II que la prestación de servicios por la FNMT a las Administraciones, organismos públicos o entidades de derecho público se regirá mediante un convenio tipo que debe ser aprobado por el Ministerio de Economía, previo informe favorable de los Ministerios de Administraciones Públicas y de Ciencia y Tecnología. Asimismo, se prevé la celebración de convenios entre la FNMT y las Administraciones Públicas para la constitución de oficinas de acreditación, a fin de facilitar a los ciudadanos los trámites necesarios para la obtención de certificados.

El citado Real Decreto prevé también, en su Capítulo IV, la fijación de precios públicos por parte del Ministerio de Economía, a propuesta de la FNMT, en contraprestación de los servicios prestados por ésta.

La regulación de la firma electrónica: para registradores y notarios

La Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, publicada en el Boletín Oficial del Estado de 31 de diciembre de 2001, contiene una sección octava «Incorporación de técnicas electrónicas, informáticas y telemáticas a la seguridad jurídica preventiva», donde se regula la atribución y uso de la firma electrónica por parte de notarios y registradores de la propiedad, mercantiles y de bienes muebles, en el ejercicio de sus funciones públicas (artículos 106 a 115).

La citada sección octava de la Ley 24/2001, de 27 de diciembre, obliga a notarios y registradores de la propiedad, mercantiles y de bienes inmuebles (en adelante, registradores) a disponer de sistemas telemáticos para la emisión, comunicación y recepción de información, cuyas características serán determinadas

por la Dirección General de los Registros y del Notariado.

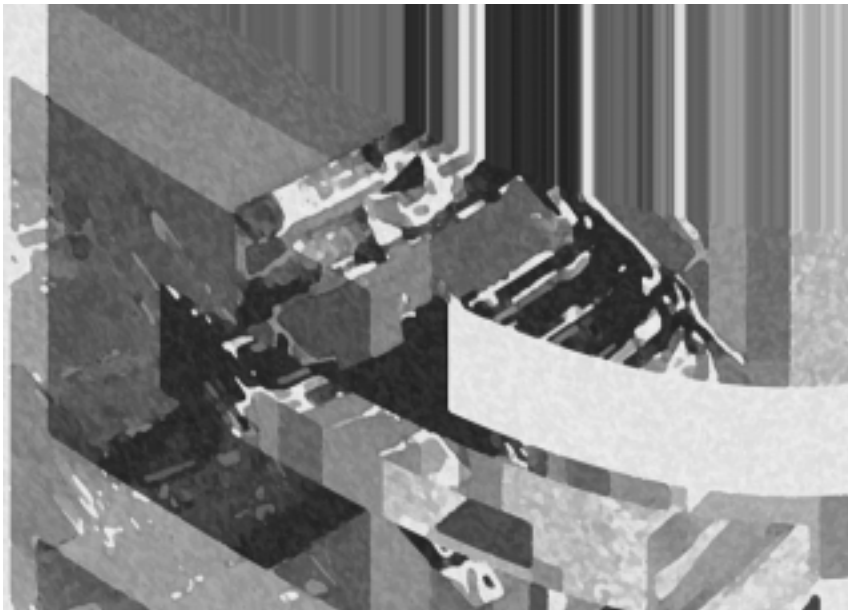
En particular, los notarios y registradores deberán disponer de una firma electrónica avanzada, amparada por un certificado reconocido emitido por un prestador de servicios de certificación acreditado, que vincule los datos de verificación de firma a la identidad del titular, su condición de notario o registrador en servicio activo y la plaza de destino, y cuyo uso estará limitado a la suscripción de documentos públicos u oficiales propios del oficio del firmante. Asimismo, notarios y registradores, deberán disponer de un dispositivo seguro de creación de firma.

Mediante el uso de esta firma electrónica, los notarios y registradores podrán remitir, por vía electrónica, documentos públicos notariales, comunicaciones, partes, declaraciones y autoliquidaciones tributarias, solicitudes o certificaciones, a las administraciones públicas o a cualquier órgano jurisdiccional. Asimismo, mediante este medio seguro podrán ser transmitidas a las entidades y personas interesadas copias simples electrónicas o notas simples informativas, por parte de notarios y registradores, respectivamente.

Adicionalmente, la sección octava de la Ley 24/2001, de 27 de diciembre, prevé la posibilidad de formalización de negocios jurídicos a distancia, mediante el intercambio de documentos públicos autorizados por dos o más notarios, así como la presentación, por vía telemática, en los Registros de la Propiedad, Mercantiles o de Bienes Muebles, de documentos susceptibles de calificación e inscripción, mediante la utilización de firmas electrónicas avanzadas de notarios.

EVOLUCIÓN DEL MARCO NACIONAL: NUEVO PROYECTO DE LEY

El Ministerio de Ciencia y Tecnología, en estrecha colaboración con los Ministerios de Administraciones Públicas, Economía,



Interior y Justicia ha elaborado un nuevo borrador de anteproyecto de Ley de firma electrónica, que reemplazará al Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. Este anteproyecto se ha sometido a consulta pública durante el mes de enero de 2002, por lo que el texto actual, que está disponible en www.setsi.mcyt.es, está aún sujeto a modificaciones.

El anteproyecto de Ley en tramitación persigue promover un uso más generalizado de la firma electrónica, recogiendo la experiencia acumulada y los avances constatados en el terreno normativo y tecnológico desde la entrada en vigor del Real Decreto-Ley 14/1999, de 17 de septiembre.

De esta forma, introduce modificaciones en la normativa actual, ofreciendo una regulación más clara, completa y desarrollada en aspectos tales como: la ampliación de la definición de «prestador de servicios de certificación», que incluye ahora a las entidades que efectúan una prestación de cualquier servicio relacionado con la firma electrónica, aunque no emitan certificados propiamente dichos; el reconocimiento de la eficacia jurídica de la firma utilizada sujeta a acuerdos privados de uso; el fortalecimiento de los mecanismos destinados a salvaguardar la libre competencia; se clarifica la obligación de constitución de una garantía económica por parte de los prestadores que emitan certificados reconocidos, estableciendo una cuantía mínima única; se modera la responsabilidad de los prestadores, al considerar también los necesarios deberes de diligencia y custodia que corresponden a los titulares de los certificados y se desarrolla, con mayor detalle, los medios que deben ser utilizados por los prestadores de servicios para la identificación de los solicitantes de certificados reconocidos.

Asimismo, el Anteproyecto de Ley incorpora principalmente dos aspectos novedosos que contribuirán a incrementar la disponibilidad, utilidad y accesibilidad de la firma electrónica.

Por una parte, se incluye la regulación del Documento Nacional de Identidad Electrónico (DNI Electrónico), cuya implantación representará un avance sustancial en el desarrollo de la Administración y comercio electrónicos. El DNI Electrónico regulado en el anteproyecto está impulsado, en su ejecución, por el Ministerio del Interior, integrándose en el conjunto de iniciativas del Plan de Acción INFO XXI, y pondrá a disposición de los ciudadanos certificados reconocidos, que garantizan digitalmente su identidad y proporcionan la posibilidad de firmar documentos electrónicos.

El DNI Electrónico tendrá el mismo valor que el DNI a efectos de identificación de los ciudadanos, debiendo ser admitido por todas las administraciones públicas para la identificación y de documentos electrónicos firmados haciendo uso de los instrumentos incluidos en el mismo.

Por otra parte, el anteproyecto de Ley contempla la emisión de certificados a nombre de personas jurídicas y el régimen aplicable a la actuación de personas jurídicas como firmantes. En este caso, se restringe a una sola persona natural la responsabilidad por la utilización del certificado y la solicitud de certificados sólo podrá efectuarse por los representantes legales o voluntarios de la entidad titular del certificado.

Durante las diferentes fases de tramitación, el anteproyecto irá recogiendo las sugerencias de prestadores, fabricantes y usuarios y de los diferentes Ministerios, de manera que el texto final que se remita a las Cortes Generales contará ya con amplio consenso en el sector.