ANÁLISIS DE LAS FIGURAS ESENCIALES DEL RÉGIMEN JURÍDICO DE LA FIRMA ELECTRÓNICA: LA LEY 59/2003, DE 19 DE DICIEMBRE DE FIRMA ELECTRÓNICA

Teresa Parejo Navajas
Profesora Ayudante de Derecho Administrativo
Universidad Carlos III de Madrid

PALABRAS CLAVE

Firma electrónica, documento electrónico, certificado electrónico, prestador de servicios de certificación y DNI electrónico

RESUMEN

La firma electrónica pretende tener la misma función, para los documentos electrónicos, que la de la firma manuscrita en los documentos en soporte papel. Para ello, la Ley 59/2003, de 19 de diciembre de firma electrónica refuerza el marco jurídico existente otorgando seguridad jurídica al tráfico telemático y contribuyendo con ello al dinamismo del mercado de la prestación de servicios de certificación.

* * *

SUMARIO

I. Introducción: antecedentes y regulación actual

La sociedad de la información es un nuevo concepto relativo a la implementación de las nuevas tecnologías en las relaciones sociales. Su desarrollo, en lo que al tráfico jurídico se refiere, está condicionado, entre otras cuestiones, por la confianza de los ciudadanos en las comunicaciones telemáticas, esto es, en la aplicación de las técnicas de la telecomunicación y de la informática a la transmisión a larga distancia de información computarizada.

El primer paso en este sentido se dio con el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, norma que aportó un marco jurídico para la utilización de una herramienta que otorgaba confianza en la realización de las transacciones electrónicas en redes abiertas. Precisamente su tramitación a través de un Decreto-Ley evidencia la "extraordinaria y urgente necesidad" (art. 86.1 de la Constitución Española) de una regulación sobre esta materia. Este Real Decreto, además, supuso la incorporación al ordenamiento jurídico español, antes incluso, de su publicación en el Diario Oficial de las Comunidades Europeas, 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.

Como todo Decreto-Ley, éste debía ser sometido a debate y votación de totalidad en el Congreso de los Diputados en el plazo de los treinta días siguientes a su promulgación (art. 86.2 CE), con pronunciamiento sobre su convalidación o derogación. Posteriormente y, en el plazo establecido en el trámite anterior, las Cortes podían haberlo tramitado como proyecto de Ley por el procedimiento de urgencia (art. 86.3 CE), pero no se hizo por expiración del plazo establecido para ello. Resultado del cumplimiento del compromiso político adquirido sobre la materia es la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LFE) (BOE de 20 de diciembre de 2003), que deroga el Real Decreto-Ley 14/1999, además de modificar otras normas relacionadas, y que es la norma actualmente vigente. Junto a esta norma es

importante destacar el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, cuyo marco normativo básico queda fijado precisamente en la LFE, remitiéndose ésta a la normativa específica para concretar las peculiaridades del régimen jurídico, mandato que cumple este Real Decreto de 2005. Ambos textos normativos (principalmente, no obstante, en tanto que regulación básica de la firma electrónica, el primero) se analizarán en el presente trabajo.

II. La firma electrónica y su relación con el documento electrónico

La LFE regula la firma electrónica, su eficacia jurídica y las prestaciones de servicios de certificación. El Título I de la LFE señala, entre otras cuestiones, los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la Ley.

1. Ámbito objetivo

La Ley es de aplicación a los documentos electrónicos que, según el art. 3.5 de la LFE, son los redactados en soporte electrónico incorporando datos firmados electrónicamente. La relación, por tanto, entre firma y documento electrónicos es evidente: **el documento electrónico debe incluir, por definición, una firma electrónica**. El *soporte* de la información que se quiere acreditar es *el documento* y la *identificación de la persona* que lo realiza, *la firma*, ambos de realizados de manera electrónica. Varios, además, son los tipos de firmas:

A) La firma electrónica: concepto

Según el art. 3 se entiende por **firma electrónica** (FE) *"el conjunto de datos en forma electrónica, consignados junto a otros asociados con ellos, que pueden ser utilizados como medio de identificación del firmante"*. Se trata, por tanto, de una herramienta que proporciona seguridad jurídica en el tráfico de las comunicaciones telemáticas, mediante la identificación fidedigna del autor/a de dicha comunicación, en tanto que firmante de la misma.

Cuando la firma electrónica esté acreditada por una entidad de certificación (autoridad certificadora), función que, según la LFE, cumplen los prestadores de servicios de certificación (como se verá más adelante), estará vinculada a un certificado electrónico expedido por aquéllos, pues dicho certificado relaciona los datos de la firma electrónica de cada usuario con su identidad personal, garantizando así tanto la confidencialidad e integridad del mensaje como la autenticidad de la identidad de quien lo envía.

B) Tipos

La firma electrónica (FE) es una tecnología de seguridad empleada en la creación de documentos para identificar al autor del mismo. La FE así concebida, por las características singulares del tráfico en el que utiliza, no puede, sin más, equivaler a la firma manuscrita en soporte papel. Para que pueda ser así, es necesario dotar a la FE de unos mecanismos de seguridad que garanticen tanto la **integridad del mensaje**, para que se pueda determinar que el enviado es el mismo que el recibido, sin alteraciones, como la **identificación del firmante**, esto es, la garantía de su identidad. Esto es posible sin riesgos, en el tráfico telemático, a través de la incorporación de varios elementos a la FE: una **clave privada**, que sólo posee el firmante (clave secreta), una **clave pública**, conocida por todos, unos **programas informáticos** que son capaces de firmar y de comprobar dichas firmas, y un **certificado** que garantice que el poseedor de una clave secreta correspondiente a una clave pública es una persona concreta.

Funcionamiento del proceso de firma electrónica

1) Proceso de firma del emisor (A) del documento:

- (A) crea un documento electrónico con un mensaje. El mensaje se resume con una función informática (hash).
- (A) cifra el mensaje-resumido con una clave privada (clave privada de A).
- (A) envía a (B) el mensaje con los siguientes elementos:
    - cuerpo del mensaje (sin cifrar). Puede cifrarse utilizando la clave pública de (B);
    - firma del mensaje, compuesto por: i) hash (mensaje-resumen) cifrado con la clave privada de (A); y ii) certificado electrónico de (A) (datos personales y clave pública de (A))

2) Proceso de recepción y verificación de la firma por el receptor (B):

- Recepción del mensaje con todos los datos anteriores.
- (B) descifra el certificado electrónico de (A), incluido el mensaje, utilizando una clave pública otorgada por una Autoridad Certificante (la que ha emitido el certificado). Una vez descifrado el certificado, (B) tendrá acceso a la clave pública de (A) y a sus datos personales.
- Con la clave pública de (A) contenida en el certificado electrónico, (B) descifra el mensaje-resumen
- (B) aplica al mensaje (no resumido) la misma función hash para obtener el mensaje-resumen. (si el mensaje no resumido ha sido cifrado anteriormente, antes de la operación hash habrá de descifrarlo con su clave privada)
- (B) compara el mensaje-resumen descifrado con la clave con el mensaje-resumen obtenido a través del hash. Si coinciden es que no han sido alterado durante la transmisión.

Por eso, la LFE avanza un paso más en el cumplimiento de su objetivo de generación de confianza en el ámbito de las transacciones electrónicas en redes abiertas creando, a partir del concepto general de FE, otros dos tipos que otorgan mayor seguridad jurídica al sistema: por un lado, la **firma electrónica avanzada (FEA),** y por otro, la **firma electrónica reconocida (FER)**.

La FEA, que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, vinculada al firmante de manera única y a los datos a que se refiere en la comunicación y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control (art. 3.2 LFE).

La FER, que es la firma electrónica avanzada basada en un certificado reconocido, generada mediante un dispositivo seguro de creación de firma. Los datos consignados en forma electrónica en un documento con FER tienen el mismo valor que los consignados en papel en documento con firma manuscrita (FM) (art. 3 puntos 3 y 4). Dos son, por tanto, los requisitos complementarios que exige la LFE para que una FEA pase a ser FER: 1) estar basada en un certificado reconocido; y 2) estar generada mediante un dispositivo seguro de creación de firma.

En definitiva, **no basta con la FEA para la equiparación con la firma manuscrita; es preciso que la FEA esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación** (RODRÍGUEZ ADRADOS, p. 60), **esto es, que sea FER**.

C) El documento electrónico: concepto y clases

La firma electrónica, independientemente de sus características particulares, como ya se ha indicado, está necesariamente asociada al concepto de **documento electrónico** (DE) por incorporar, por definición, datos firmados electrónicamente.

Documento electrónico: FE	FEA	FER
Documento papel:		FM

Varias son las clasificaciones que pueden realizarse del documento electrónico, pero de la lectura del artículo 3.6 de la LFE se extrae la siguiente, en función de los sujetos firmantes del mismo, que en realidad viene a determinar su naturaleza jurídica:

Documento electrónico:
- Público
  - Civil
  - Administrativo
    - General
    - Judicial
- Privado
- Oficial
- Mixto

C.1.) Documento electrónico de naturaleza pública:

Según el art. 1.206 del Código Civil, los documentos públicos son los autorizados por un notario o empleado público competente, con las solemnidades exigidas por la Ley. El mismo sentido tiene la definición de documento público electrónico de la LFE, si bien dando mayor detalle de la competencia propia del funcionario firmante del documento, pues aclara que se trata de una "facultad de dar fe pública, judicial, notarial o administrativa", siempre actuando en el ámbito de sus competencias y con los requisitos exigidos por la Ley en cada caso (art. 3.6). Por tanto, de esta definición se extrae la diferenciación entre documentos públicos de naturaleza civil de los de naturaleza administrativa, en función de las características del firmante, que, para ser público, en todo caso deberá ser un funcionario competente para dar fe pública: el funcionario con competencia para otorgar fe pública notarial será el firmante de los documentos públicos notariales (de naturaleza civil), regidos por la normativa del art. 1.206 del Código Civil; el funcionario competente para otorgar fe pública administrativa (general), firmará los documentos públicos administrativos; y por último, el funcionario competente para otorgar fe pública judicial pondrá la rúbrica (electrónica) en los documentos electrónicos públicos judiciales, o de la Administración de Justicia.

Tal y como indica el art. 46 de la Ley 30/1992, de 26 de noviembre de régimen jurídico de las administraciones públicas y del procedimiento administrativo común (en adelante, LRJAP), tienen la consideración de documento público administrativo los documentos válidamente emitidos por los

órganos de las Administraciones públicas. La LRJAP no especifica que tales documentos deban constar necesariamente en soporte papel, por lo que se entenderán incluidos en esta regulación los emitidos electrónicamente con las características de la LFE.

De estas definiciones, por tanto, se pueden extraer las tres características fundamentales de todo documento público (electrónico, en este caso):

- El autor: tiene que haber sido emitido por una persona que tenga la condición de funcionario público.
- La competencia: el funcionario público ha de tener competencia para emitir ese documento y para dar fe pública sobre el mismo.
- La solemnidad: es necesario que ese documento haya sido emitido respetando las solemnidades establecidas en cada caso por la Ley.

C.2) Documentos "oficiales" electrónicos

El art. 3.6 de la LFE señala, sin darle nombre específico, otro tipo de documentos "expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica". La denominación de "oficiales" de este tipo de documentos está tomada del art. 109.1.c) de la Ley de Acompañamiento 24/2001, de medidas fiscales, administrativas y del orden social. Se trata de documentos semejantes a los públicos, en función del sujeto firmante, pero sin llegar a serlos (son documentos intermedios) por carecer dicho sujeto de facultad para *dar fe*, requisito, como se indicó, indispensable para su calificación como "públicos". Esto es así necesariamente porque, ni todos los funcionarios públicos tienen facultad para dar fe, ni todos los funcionarios públicos que tienen dicha facultad firman únicamente documentos de naturaleza pública.

C.3) Documentos electrónicos de naturaleza privada:

Nada dice sobre este tipo de documentos el art. 3.6 de la LFE más allá de la referencia a su soporte electrónico. Igual ocurre con el Código Civil. Es la Ley de Enjuiciamiento Civil, en su art. 317 y la doctrina civilista las que han aclarado, de una manera simplista pero eficaz, por exclusión, que se trata de aquellos que no son de naturaleza pública.

Al no señalar la LFE característica alguna propia de este tipo de documentos, no hace alusión tampoco, y a diferencia de los anteriores, a la necesidad de que éstos incluyan firma electrónica para tener plena eficacia jurídica. Esto es así porque los principios de libertad de forma y de ilimitabilidad de los medios de prueba imposibilitan la exigencia de unos requisitos generales comunes a todos los documentos de naturaleza privada (RODRIGUEZ ADRADOS; p. 33). Sin embargo, la LFE, en su art. 3.5, señala dicha firma como necesaria para la calificación de un documento como electrónico. Por lo tanto, de todos los documentos electrónicos privados existentes en el tráfico jurídico, únicamente estarán sujetos al articulado de la Ley aquellos que incorporen "datos que estén firmados electrónicamente", independientemente del tipo de firma (simple, avanzada o reconocida).

Para el caso de los documentos privados (en general, sin especificar en qué soporte están expedidos) dirigidos a las Administraciones Públicas, la LRJAP indica que las copias de estos documentos tendrán validez y eficacia en el ámbito de la actividad de las Administraciones Públicas cuando su autenticidad haya sido comprobada (art. 46.3). Además, los órganos competentes para la expedición de copias auténticas de documentos privados (y públicos) serán determinados por cada Administración Pública. Serán éstas, por tanto, las que establezcan los requisitos necesarios para que, en cada una de ellas, puedan surtir efectos las copias de tales documentos.

Cuando los documentos dirigidos a las Administraciones Públicas sean de **naturaleza electrónica** habrá que atender a lo establecido en el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el

régimen de las oficinas de registro, modificado por el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

Según el art. 3 del RD 772/1999, la presentación de solicitudes, escritos, comunicaciones y documentos (…) se podrá efectuar, además de en soporte papel, **por medios informáticos, electrónicos o telemáticos**, de acuerdo con lo previsto en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas en la Administración General del Estado.

Serán válidos a efectos jurídicos los documentos emitidos por los órganos y entidades del ámbito de la Administración General del Estado y por los particulares en sus relaciones con aquéllos que hayan sido producidos por medios electrónicos, informáticos y telemáticos en soportes de cualquier naturaleza, cuando se acredite la integridad y conservación del documento así como la identidad del autor y la autenticidad de su voluntad, mediante la constancia de códigos u otros sistemas de identificación (art. 6.1 RD 263/1996). En estos casos, tendrán éstos **idéntica validez jurídica** que los documentos de naturaleza electrónica expedidos en soporte papel. Además, las copias de los documentos originales (públicos o privados) almacenados por medios o en soportes electrónicos, informáticos o telemáticos, expedidas por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes, tendrán la **misma validez y eficacia del documento original** siempre que quede garantizada su autenticidad, integridad y conservación (art. 6.2 RD 263/1996).

Nada se dice en la normativa reguladora de qué se entiende por **"copia" de documento electrónico**, pero de la lectura del art. 7 del Real Decreto 772/1999 puede interpretarse que se trata de la **impresión del documento electrónico en soporte papel:**

1. *Cuando las normas reguladoras del correspondiente procedimiento o actuación administrativa requieran la aportación de documentos originales por los ciudadanos, éstos tendrán derecho a la expedición*

por las oficinas de registro de una copia sellada del documento original en el momento de su presentación. Las oficinas de registro no estarán obligadas a expedir copias selladas de documentos originales que no acompañen a las solicitudes, escritos o comunicaciones presentadas por el ciudadano.

2. *Para el ejercicio de este derecho el ciudadano aportará, junto con el documento original, una copia del mismo.*

   La oficina de registro cotejará la copia y el documento original, comprobando la identidad de sus contenidos, unirá el documento original a la solicitud, escrito o comunicación al que se acompañe para su remisión al órgano destinatario y entregará la copia al ciudadano, una vez diligenciada con un sello en el que consten los siguientes datos:

   a) *Fecha de entrega del documento original y lugar de presentación.*
   b) *Órgano destinatario del documento original y extracto del objeto del procedimiento o actuación para cuya tramitación se aporta.*

C.4) Otros documentos electrónicos:

Existen otros tipos de documentos no contemplados expresamente en la enumeración del art. 3.6 de la LFE. Se trata de los documentos probatorios y dispositivos y aquellos que tienen una naturaleza jurídica mixta.

En relación con la primera clasificación, se entiende por **documento electrónico de carácter probatorio**, el que constituye medio de prueba del hecho que está representado en el mismo. Dicha naturaleza probatoria está reconocida en el art. 3.8 de la LFE, y se le atribuye, en principio, a todos los documentos electrónicos por definición. Por el contrario, se entiende por **documento electrónico de carácter dispositivo**, los que incluyen un acto jurídico que supone una declaración o una manifestación de voluntad, y que constituyen, modifican o extinguen relaciones de derecho. Por tanto, frente a la naturaleza estática del documento probatorio, el dinamismo de los declaratorios hace necesario acompañarlos de mecanismos que garanticen la seguridad jurídica de estos documentos en el tráfico de las comunicaciones telemáticas.

Finalmente, los **documentos mixtos** responden a una categorización intermedia entre los públicos y los privados. Estos documentos son originariamente privados y adquieren la categoría de mixto cuando a éstos se les añade una intervención pública, sea ésta de carácter judicial, notarial o administrativo.

2. Ámbito subjetivo

Tal y como indica la propia LFE, los sujetos que hacen posible el empleo de la firma electrónica son los denominados **prestadores de servicios de certificación** (PSC).

A) Concepto de PSC

Son PSC las personas físicas o jurídicas que expiden certificados electrónicos o prestan otros servicios relacionados con la firma electrónica, que estén establecidos en España o domiciliados en otro Estado, pero que ofrezcan servicios de certificación a través de un establecimiento permanente en España (art. 2).

Para comprender el verdadero alcance de esta definición de la Ley, es necesario aclarar otros dos conceptos incluidos en la misma: el de certificado electrónico (sin perjuicio, en todo caso, del análisis más detallado que de éste se realiza más adelante) y el de servicio de certificación.

- Un certificado electrónico es un documento que sirve para identificar, sin dejar lugar a dudas, a una persona (física o jurídica). El certificado acompaña a la firma electrónica otorgándole credibilidad. Este concepto, no obstante, se verá con mayor detalle más adelante.

- Se entiende por servicio de certificación la función desempeñada por los PSC relacionada con la expedición de los certificados electrónicos,

como generación y emisión de claves; entrega de los datos de creación de firma como de dispositivos seguros de creación de firma; servicio de sellado temporal (consignación de fecha y hora); servicio de registro; de suministro de dispositivos de verificación de firma; servicio de validación y verificación de firmas electrónicas; o servicio de garantía de un certificado prestado por otro prestador no europeo (BERROCAL LANZAROT, p. 72).

B) Exigencias de la LFE que recaen sobre la noción de PSC

- Se entenderá que el PSC está establecido en España cuando su residencia o domicilio social se halle en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

- Se entenderá que el PSC opera mediante un establecimiento permanente situado en territorio español cuando disponga en él, de manera continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

- Se presumirá que un PSC está establecido en España cuando dicho PSC o una de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

- En todo caso, la mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por si sola, el establecimiento del PSC en España.

Los PSC son, en definitiva, los sujetos que, haciendo posible el empleo de la firma electrónica, expiden certificados electrónicos, que son los

documentos 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 (PLAZA PENADÉS, p. 168).

El concepto ha cambiado respecto de la anterior regulación: la nueva Ley otorga mayor grado de libertad a los PSC, aumentando la participación del sector privado en los sistema de certificación y eliminando las presunciones legales asociadas a dicha participación, favoreciendo así la autorregulación de la industria para que sea ésta la que diseñe y gestione, de acuerdo con sus propias necesidades, sistema voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación.

C) Régimen jurídico

C.1) Régimen general:

La PSC no está sujeta a autorización previa, si bien, según se indica en el Preámbulo de la LFE, se refuerzan las capacidades de inspección y control del Ministerio de Ciencia y Tecnología en las labores de supervisión y control sobre los PSC; y se realiza en régimen de libre competencia, lo que significa que no se podrán imponer restricciones a los servicios que provengan de otros Estados miembros del Espacio Económico Europeo. El mantenimiento de las condiciones de competencia efectiva está encomendado por la LFE a los órganos de defensa de la competencia (art. 5 puntos 1 y 2).

Cuando la PSC se realice por las Administraciones públicas, sus organismos o cualquiera de las entidades dependientes o vinculadas a las mismas, deberá someterse a los principios de objetividad, transparencia y no discriminación (art. 5.3), en orden a su sujeción al interés general (art. 3 LRJAP).

Además, las Administraciones públicas podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos, con el fin de salvaguardar las garantías de los mismos (art. 4.1). Dichas condiciones adicionales, en todo caso, sólo podrán hacer referencia a las características

específicas de la aplicación de que se trate, garantizando el cumplimiento del art. 45 LRJAP. Además, estas condiciones deberán ser objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la PSC al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo (art. 4.2). Estas condiciones quedan cumplimentadas en el ***Real Decreto 209/2003, de 21 de febrero****, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos (BOE de 28/02/2003), que modifica las regulaciones establecidas en el Real Decreto 263/1996, de 16 de febrero, de utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado; el Real Decreto 772/1999, de 7 de mayo, de presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro; y el Real Decreto 1465/1999, de 17 de septiembre, por el que se establecen criterios de imagen institucional y se regula la producción documental y el material impreso de la Administración General del Estado.*

El Real Decreto 209/2003 tiene como objeto la regulación de los registros telemáticos, las notificaciones telemáticas y los certificados y transmisiones telemáticas; en desarrollo de los artículos 38.9, 45, 59.3 y disposición adicional decimoctava de la LRJAP, así como de los apartados 3 y 8 del artículo 105 de la Ley 230/1963, de 28 de diciembre, General Tributaria.

Sea quien fuere el sujeto que realice las funciones de PSC, se someterá, en lo que al tratamiento de los datos se refiere, a lo dispuesto en la **Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y a sus normas de desarrollo** (art. 17.1) Por ello, cuando los PSC expidan certificados electrónicos al público, únicamente podrán recabar datos de carácter personal que sean necesarios para la expedición y mantenimiento del certificado electrónico o para la prestación de otros servicios relacionados con la firma electrónica, directamente de los firmantes o previo consentimiento expreso de éstos, que también será necesario en el caso de utilizar dichos datos para fines distintos a los especificados en la Ley (art. 17.2). La identidad del firmante sólo podrá ser revelada por orden judicial o por los

motivos establecidos en la Ley Orgánica de protección de datos antes señalada.

Quedan exceptuados de la previsión anterior los denominados datos especialmente protegidos, recogidos en el art. 7 de la Ley Orgánica de protección de datos.

C.2) Obligaciones de los PSC:

La LFE diferencia entre las obligaciones por expedición de certificados electrónicos y las obligaciones por expedición de certificados reconocidos. Como la expedición de certificados electrónicos es la principal función, como se verá, de los PSC, las obligaciones por expedición de los mismos es la referida al régimen general.

En este sentido, en lo que al **régimen general** de las obligaciones ser refiere, el art. 18 establece que los PSC deberán:

a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios
b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

    1. Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.
    2. Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.
    3. El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el

certificado en que el prestador garantiza su responsabilidad patrimonial.

4. Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.
5. Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.
6. Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

En definitiva, la LFE les obliga a los PSC a la tutela y gestión permanente de los certificados electrónicos que expiden, poniendo por escrito todos los detalles de dicha gestión en la denominada declaración de prácticas de certificación, así como a mantener un servicio de consulta sobre el estado de vigencia de tales certificados.

A las obligaciones generales de los PSC, la LFE añade otras, tal y como se indicó, **cuando éstos emitan certificados reconocidos**, en el art. 20. Así, en estos casos, el PSC deberá:

a) Demostrar la fiabilidad necesaria para prestar servicios de certificación;
b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia;
c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica;
d) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte;
e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante;
f) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo; y
g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

Por tanto, la LFE establece mayores exigencias para los PSC, que se añaden a las generales, cuando emitan certificados reconocidos, pues son los que acompañan a las firmas electrónicas avanzadas, que son las que tienen eficacia jurídica plena.

3. Régimen de responsabilidad

Los PSC responderán por los daños y perjuicios que causaren a cualquier persona en el ejercicio de su actividad por motivo del incumplimiento de las obligaciones que les impone la LFE, así como por el incumplimiento de las personas en quienes éstos hubieran delegado la ejecución de alguna de las funciones necesarias para la prestación de sus servicios (art. 22), y con los límites señalados en el art. 23. Tal y como señala RODRÍGUEZ ADRADOS (2004, p. 66), estas normas pretenden conseguir una seguridad preventiva para los documentos electrónicos que no le otorga la escasa visibilidad y las dificultades probatorias a posteriori del propio sistema.

Los PSC que expidan certificados reconocidos deberán constituir, además, y como novedad de la Ley, un seguro de responsabilidad civil de cuantía mínima única de 3 millones de euros y a la que se da una gran flexibilidad para su constitución mediante la combinación de instrumentos financieros establecidos en el art. 20.2 de la Ley, si bien el incumplimiento de esta previsión no será considerada como infracción muy grave, según se establece en el art. 31.2 a).

III. Los certificados electrónicos

Los PSC tienen como principal función, la expedición de los certificados electrónicos.

1. Concepto

Se denomina certificado electrónico (CE) al documento firmado electrónicamente por un PSC que vincula unos datos de verificación de firma a

un firmante (persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa) y confirma su identidad (art. 6). El PSC incorpora en el documento electrónico, a través del CE, una firma electrónica que garantiza que el contenido del mismo corresponde a ese firmante.

El CE acompaña a la FE, verificándola. Por tanto, **cuando la FE esté verificada por un CE reconocido (CER), producirá idénticos efectos jurídicos (misma validez jurídica) que la firma manuscrita en soporte papel**. Por el contrario, cuando la FE está verificada por un **CE simple (CES),** el valor de la firma será únicamente técnico. El certificado reconocido es, así, el elemento clave del sistema (ALAMILLO, 1999).

Además, el CE tendrá el valor y la eficacia jurídica que corresponda a su naturaleza de conformidad con la legislación que le sea aplicable (art. 3 apartados 6 y 7).

Cuando se esté certificando electrónicamente un **documento público administrativo** electrónico, habrá que atender al Real Decreto 209/2003, antes referenciado. De esta manera, según el art. 14, puntos 1 y 4 de dicha norma reglamentaria, el certificado telemático contendrá los datos objeto de certificación y la firma electrónica de la autoridad competente para expedirlos y producirá idénticos efectos a los expedidos en soporte papel. Por tanto, se trata en este caso, de un CER asociado a una FER. A tal efecto, su contenido deberá poder ser impreso en soporte papel, en el que la firma manuscrita será sustituida por un código de verificación generado electrónicamente que permita en su caso contrastar su autenticidad accediendo por medios telemáticos a los archivos del órgano u organismo emisor. El CE de **documento privado** tendrá la validez jurídica asociada al tipo de firma (simple o reconocida) verificada por dicho certificado.

2. Tipos

Auque la LFE no hace ninguna clasificación explícita de los certificados electrónicos, de su regulación puede extraerse la siguiente:

Certificados Electrónicos (CE)	En función del firmante representado por el PSC	De persona física
		De persona jurídica
	En función del grado de identificación del firmante	Simple (CES)
		Reconocido (CER)

1. CE de persona física: son aquellos certificados firmados por persona física (bien ella misma, bien a través de representante legal);

    1. CE de persona jurídica: son los certificados firmados por persona jurídica a través de su representante legal, aunque su solicitud podrá realizarla no sólo éste sino también sus administradores (art. 7);

    2. Certificados electrónicos reconocidos (CER): según el art. 11 de la Ley, estos certificados son los expedidos por un PSC que cumpla los requisitos establecidos en la Ley sobre comprobación de la identidad y demás circunstancias de los solicitantes del mismo, sobre su fiabilidad y sobre las garantías de los servicios de certificación que presten. La Ley aclara el concepto añadiendo los datos que necesariamente deberán incluir este tipo de certificados:

        1. Indicación de que se expide como reconocido;
        2. El código de identificación del certificado, que deberá ser único;
        3. La identificación y firma electrónica avanzada del PSC que lo expida, así como su domicilio;
        4. La identificación del firmante, bien por su nombre y apellidos y su número de DNI o por su seudónimo, si éste consta de manera inequívoca, si se tratase de certificado electrónico de persona física, bien a través de su

denominación o razón social y su CIF, en el caso de certificado de persona jurídica;

5. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante;
6. El comienzo y el fin del período de validez del certificado; y
7. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Certificados electrónicos no reconocidos o simples (CES): son todos aquellos documentos que no son reconocidos.

3. Régimen jurídico

La LFE dispone un régimen jurídico único para los CER y los CES, sobre los solicitantes y sobre las causas y efectos de la extinción de su vigencia.

En relación con los solicitantes, aunque en un primer momento la Ley regula separadamente las cuestiones relativas a la solicitud del CE, la custodia y límites al uso de datos, y la responsabilidad, de los CE de persona jurídica, el resto de cuestiones se mezclan con las correspondientes a los CE de persona física. Por eso, la distinción que aquí verdaderamente interesa es la de los CER y los CES y, por ello, es la que ahora se va a analizar.

La definición de certificado electrónico de la LFE indica claramente la **función principal** de todo CE, esta es, la de vincular un dato de verificación de firma a una persona concreta (MARTÍNEZ NADAL; 2004, p.88). La figura del PSC se crea, precisamente, para garantizar la identidad del emisor del mensaje, asumiendo, por tanto, la responsabilidad de dicha verificación dotando al sistema de mayor seguridad y, asimismo, confianza a los usuarios.

El sistema de verificación de firma es precisamente lo que lleva a la diferenciación entre los dos tipos principales de certificados; en efecto, el CER,

a diferencia del CES, **exige la personación física** del solicitante del certificado ante los encargados de la verificación de su identidad (art. 13.1). En el caso de CER de personas jurídicas, los PSC comprobarán, en su labor de verificación, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante (art. 13.2). A contrario *sensu*, en el caso del CES dicha personación no será requisito necesario para la expedición del mismo, por lo que es claro que los CER dan **mayor valor y seguridad** que los CES.

No obstante lo anterior, esta identificación en los CER **no será exigible** (art. 13.4): a) cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años; o b) cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años.

IV. Puesta en práctica: el DNI electrónico

Una novedad importante de la LFE es la regulación del documento nacional de identidad electrónico (DNIE), a través del cual se pretende generalizar el uso de los instrumentos de comunicación electrónica a través de mecanismos seguros. La regulación de la Ley es breve, en dos artículos (15 y 16), que establecen, respectivamente, la definición y los requisitos y características del DNIE. Esta regulación, tal y como ya se adelantó anteriormente, viene completada por el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica (RDDNIE).

1. Concepto

Se entiende por DNIE el documento nacional de identidad que acredita electrónicamente la identidad personal de su titula y permite la firma electrónica de documentos (art. 15.1). Esto es posible gracias al reconocimiento de la eficacia, por todas las personas físicas o jurídicas, públicas o privadas actuantes en el tráfico telemático, del mecanismo de acreditación asociado al mismo, tanto de la identidad y otros datos personales del titular del documento, como de la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónicas en el incluidos (art. 15.2).

2. Naturaleza jurídica

El DNIE es un **documento público (y oficial)** que tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo (art. 1.2 RDDNIE). Tiene, por tanto, verdadera **validez jurídica.** La LFE (y también el RD de desarrollo), en ese reconocimiento generalizado del DNIE, le dota, además, de **auténtica eficacia** (GARCÍA MÁS, p. 151) para el tráfico jurídico.

Además, el RDDNIE añade (art. 1.1) que se trata de un documento personal e intransferible emitido por el Ministerio del Interior (art. 3 RDDNIE), que goza de la misma protección que las leyes otorgan a los documentos públicos y oficiales.

A cada DNIE se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general (art. 1.3 RDDNIE). Las características de la tarjeta soporte del DNIE están reguladas en el art. 10 RDDNIE. El material, formato y diseño ha sido determinado por el Ministerio del Interior (art. 10.1) y se explican en la página web de la Dirección General de la Policía (www.policia.es): soporte de policarbonato, material

plástico muy resistente, de alta calidad y durabilidad, con los datos grabados con láser destructivo, impidiendo así su falsificación. Lleva estampados **en el anverso**; de forma destacada, los literales "Documento Nacional de Identidad", "España" y "Ministerio del Interior", además de los datos de filiación del titular, una fotografía en blanco y negro del titular con un holograma en la superficie y unos relieves, el número personal del DNI y unos caracteres de verificación, la firma manuscrita del titular, el número de serie del soporte, la fecha de validez del documento, una imagen cambiante grabada en láser y un kinegrama; y **en el reverso**, datos de filiación y caracteres OCR-B de lectura automática.

Fuente: http://www.dnielectronico.es/Asi_es_el_dni_electronico/

En definitiva, el DNIE:

- **Es un documento más seguro que el tradicional**, pues incorpora mayores y más sofisticadas medidas de seguridad que harán virtualmente imposible su falsificación.

- **Garantiza la identidad de los interlocutores** de una comunicación telemática, ya sea para intercambio de información, acceso a datos o acciones o compra por Internet y gestiona mejor e la información contenida en un ordenador, así como **la integridad del mensaje.**

- **Tiene verdadera validez y eficacia jurídicas.**

3. Evolución: del DNI al DNIE

El Documento Nacional de Identidad (DNI) es un documento emitido por la Dirección General de la Policía, dependiente del Ministerio del Interior (art.3 RDDNIE), que acredita, desde hace más de cincuenta años, la identidad, los datos personales que en él aparecen y la nacionalidad española, de su titular.

Desde su creación, el DNI ha ido evolucionado de manera paralela al mundo de las tecnologías incorporando nuevos mecanismos de acreditación de la personalidad, respondiendo a las necesidades demandadas por la sociedad de la información y a la generalización del uso de Internet, con el fin de aumentar, tanto la seguridad jurídica del documento, como su ámbito de aplicación. De esta manera, el DNIE logra fundamentalmente: a) acreditar electrónicamente y de forma indubitada la identidad de la persona; y b) firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la de la firma manuscrita.

El DNIE, por tanto, es un documento equivalente al DNI tradicional pero en un soporte material plástico, que incorpora un pequeño circuito integrado (mediante un chip que contiene los mismos datos que aparecen impresos en la tarjeta (datos personales, fotografía, firma digitalizada, huella dactilar digitalizada) junto con los certificados de Autenticación y de Firma Electrónica. El nuevo DNI no contiene ningún otro dato del titular relativo a datos personales diferentes a los actuales ni de cualquier otro tipo. Este DNIE permitirá acceder, además de aquellos usos asociados al DNI ya conocidos, a los nuevos servicios, en constante avance, de la sociedad de la información, ampliando las capacidades de los ciudadanos para actuar a distancia con las Administraciones públicas, con las empresas privadas y con los demás ciudadanos del Estado (se trata, eso sí, de un documento *nacional*).

4. Características legales

El art. 16 de la LFE establece una serie de criterios generales del DNIE: por un lado, que los órganos competentes para la expedición del DNIE (dependientes del Ministerio del Interior) deberán cumplir las obligaciones que la Ley impone a los PSC que expidan CER, salvo en lo relativo a la garantía del art. 20.2.; y por otro, la garantía de la compatibilidad del DNIE con los instrumentos generalmente aceptados (garantía de la operabilidad del DNIE).

El ejercicio de las competencias sobre gestión, dirección, organización, desarrollo y administración de todos los aspectos relativos a la expedición y confección del DNI, incluida la emisión de certificados de firma electrónica reconocidos y la custodia y responsabilidad de los archivos y ficheros, automatizados o no, relacionados con el DNI, corresponde a la Dirección General de la Policía (art. 3 RDDNIE).

Una de las cuestiones quizá más interesantes del DNIE es la posibilidad de incorporar al mismo dispositivos varios de firma electrónica (art. 15.2). Se trata, el DNIE, en realidad, tal y como señala el Preámbulo de la LFE, de un **certificado electrónico reconocido** en sí mismo, llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. Por eso, el art. 1.5 RDDNIE indica que **la firma electrónica realizada a través del DNIE tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel**.

El DNIE, incluye, en su chip, dos certificados electrónicos: el **certificado de autenticación**, que permite la identificación del titular en una comunicación telemática; y el **certificado de firma**, que permite la firma electrónica de los documentos garantizando su integridad, procedencia y la autenticidad de origen.

El único organismo autorizado a emitir los certificados digitales para el DNIE es la Dirección General de la Policía **(Autoridad de Certificación, AC).**

Los procedimientos de solicitud, revocación, renovación y período de vigencia de los certificados están regulados en la Política de Certificación.

Además de la AC, el sistema de validación del DNIE dispone de dos prestadores de servicios de validación (Autoridades de Validación, AV): por un lado, la **Fábrica Nacional de Moneda y Timbre–Real Casa de la Moneda**, que presta sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas; y por otro, el **Ministerio de Administraciones Públicas**, para el conjunto de las Administraciones Públicas. Adicionalmente, la **Entidad Pública Empresarial Red.es** podría completar los servicios de validación en un futuro próximo.

La Autoridad de Validación (AV) tiene como función suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro (AR) y certificados por la Autoridad de Certificación (AC).

La información sobre los certificados electrónicos revocados (no vigentes) se almacena en las denominadas listas de revocación de certificados (CRL).

En la infraestructura de *clave pública* del DNIE, las funciones de AV están asignadas a una entidad diferente a la AC con el fin de separar la comprobación de la vigencia de un certificado electrónico de los datos de identidad de su titular. De esta manera, ni la AC tiene acceso a los datos de las transacciones que se realicen con los certificados que ella emite, ni la AV tiene acceso a la identidad de los titulares de los certificados electrónicos que maneja, reforzando aún más, si cabe, la transparencia del sistema.

En todo caso, la prestación de estos servicios de validación se realiza sobre la base del **Online Certificate Status Protocol** (OCSP). A través de este protocolo, un cliente OCSP envía una petición sobre el estado de un certificado a la AV y ésta, tras consultar su base de datos, le responde dándole información sobre el estado del mismo vía Internet.

En definitiva, el nuevo DNIE es el mejor ejemplo de aceptación por el tráfico jurídico de un **documento electrónico con firma reconocida verificada por el certificado reconocido emitido por la Dirección General de la Policía** que es, además, ya una realidad: está funcionando, desde el pasado 16 de marzo de 2006, en la ciudad de Burgos, dinamizando la sociedad de la información, permitiendo al ciudadano operar con total seguridad, rapidez, comodidad en los medios telemáticos, para la inmediata realización de trámites administrativos y comerciales.

V. Bibliografía

- ALAMILLO DOMINGO, I. *Confianza digital basada en certificados*. Revista de Derecho informático. Alfa-Redi, nº 13, agosto de 1999. http://www.alfa-redi.org/rdi-articulo.shtml?x=315
- ALAMILLO DOMINGO, I. *Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica*. Revista de contratación electrónica, nº 46, 2004. p.3-64.
- BERROCAL LANZAROT, A. *Régimen jurídico de los prestadores de servicios de certificación en la nueva Ley 59/2003, de 19 de diciembre, de firma electrónica*. Revista Aranzadi de derecho y nuevas tecnologías, n. 6 (2004), p. 69-100.
- GARCÍA MÁS, F.J. *La firma electrónica: clases de firma electrónica. Los documentos electrónicos. Análisis del art. 3 de la Ley 59/2003, de 19 de diciembre*. Actualidad civil, nº 17 (2005), p.2064-2075.
- GARCÍA MÁS, F.J. Algunos comentarios a la Ley 59/2003, de 19 de diciembre, de firma electrónica. Revista jurídica del notariado, nº 51, 2004, p.117-154.
- ILLESCAS ORTÍZ, R. *La firma electrónica y el Real Decreto Ley 14/1999, de 17 de septiembre.* Derecho de los Negocios, octubre 1999.

- MÁRQUEZ LOBILLO, P. *La prestación de servicios de certificación en la Ley 59/2003, de 19 de diciembre, de firma electrónica*. Revista de la contratación electrónica, nº 47 (2004), p. 3-37.
- MARTÍNEZ NADAL, A. La *nueva Ley 59/2003, de firma electrónica*. Revista de la contratación electrónica, nº 47 (2004), p. 73-103.
- PLAZA PENADÉS, J. *La Ley 59/2003, de Firma Electrónica*. Revista Aranzadi de Derecho y Nuevas Tecnologías, nº 6 (2004), p.157-175.
- RODRÍGUEZ ADRADOS, A. "Firma Electrónica y documento electrónico". Escritura Pública. Ensayos de actualidad. Colegios Notariales de España. Madrid 2004.