capítulo segundo

Seguridad en las transacciones electrónicas

1. FIRMA ELECTRÓNICA

El desarrollo de la Sociedad de la Información necesita de un ámbito generalizado de confianza en las comunicaciones telemáticas o electrónicas que poco a poco se va fraguando pero que requiere de impulsos como la aprobación de la Ley 59/2003, de 19 de diciembre, de firma electrónica[38] (en adelante, LFE).

1.1. Introducción

La firma electrónica es un instrumento que permite garantizar la autenticación del mensaje y de las partes, la integridad del mismo, esto es, que no ha sufrido variaciones desde que fue enviado por el remitente hasta que llega al destinatario. Del mismo modo por medio de la firma electrónica se evitan supuestos de repudio porque el remitente no puede alegar no haber enviado el mensaje. Además, también puede proporcionar confidencialidad.

Por estos caracteres la firma electrónica trata de llevar al entorno electrónico las mismas posibilidades que las firmas manuscritas ofrecen en el mundo *off line.* No toda firma electrónica tiene el mismo valor jurídico que las firmas manuscritas, deben reunir unos requisitos especiales para poder otorgar esta equivalencia funcional.

Conforme a la Ley de firma electrónica podemos distinguir tres tipos de firma electrónica, así, la firma electrónica que 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*. En segundo lugar, la firma electrónica avanzada, que permite igualmente identificar al firmante y además detectar cualquier cambio ulterior de los datos firmados. Está vinculada al firmante de manera única y a los datos a que se refiere y ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. En tercer y último lugar la firma electrónica reconocida que es la *firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*.

Visto esto decir que en el cuadro que representamos a continuación reflejamos como los tres tipos de firma tienen requisitos acumulativos que partiendo de la función de identificar al firmante van aportando al usuario nuevas funciones para que éste pueda optar por utilizar uno u otro tipo de firma según sus necesidades concretas en cada caso. Es importante interpretar el cuadro en el sentido de que las funciones de los tipos de firma se suman a las del tipo de firma anterior:

[38] *Publicada en el Boletín Oficial del Estado núm. 304, de 20 de diciembre.*

CLASES DE FIRMA ELECTRÓNICA	FUNCIONES
Firma electrónica	• Identificación del firmante.
Firma electrónica avanzada	• Detectar cualquier cambio ulterior de los datos firmados. • Vinculación al firmante y a los datos a que se refiere de manera única. • Creada por medios que el firmante puede mantener bajo su exclusivo control.
Firma electrónica reconocida	• Basada en un certificado reconocido. • Generada mediante un dispositivo seguro de creación de firma.

Con el fin de conocer mejor el funcionamiento de la firma electrónica es necesario atender a los conceptos de datos de creación de firma, dispositivo de creación de firma, dispositivo seguro de creación de firma y datos de verificación de firma. Así, la Ley entiende por datos de creación de firma *los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica*, por su parte un dispositivo de creación de firma se entiende como *un programa o sistema informático que sirve para aplicar los datos de creación de firma* y cuando este dispositivo tenga la consideración de seguro, que es el que se exige para que la firma electrónica tenga el carácter de reconocida, será porque además de reunir las características expuestas ofrezca al menos las siguientes garantías:

a) *Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.*

b) *Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.*

c) *Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.*

d) *Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.*

Otros elementos que se deben conocer en el uso de la firma electrónica son los datos de verificación de firma electrónica que son *los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica* y por otro lado los dispositivos de verificación de firma electrónica que son los programas o sistemas informáticos que sirven para aplicar los datos de verificación de firma.

Por último, es necesario conocer que existen diferentes figuras que pueden intervenir en el funcionamiento de la firma electrónica, integrándose éstas en una Infraestructura de Clave Pública (PKI, *Public Key Infraestructure)* cuyo objeto es proporcionar servicios de certificación, entre los que se incluye la firma electrónica, a los usuarios. Así, y en orden jerárquico, encontramos en primer lugar la Autoridad Raíz, que es quien emite el certificado raíz en el que se basará la confianza del resto de certificados electrónicos que se emitan para las diferentes finalidades con las que se vayan a utilizar. Por debajo de esta Autoridad Raíz se encuentran las Autoridades de Certificación o Prestadores de Servicios de Certificación[39] (PSC), y las Autoridades de Registro, que se encargan de identificar a los solicitantes de certificados electrónicos, comprobando en su caso su identidad y remitiendo las correspondientes solicitudes a los PSC. Por último, encontramos a los usuarios de los servicios de certificación, que pueden ser titulares de un certificado electrónico y firmantes[40].

[39] *El artículo 2.2 de la LFE define al prestador de servicios de certificación como "la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica".*

[40] *El firmante es definido en el artículo 6.2 de la LFE como "la 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".*

Dos son las características básicas que se deben tener en cuenta en el uso de la firma electrónica, de una parte, hay que establecer un método seguro para asociar una clave electrónica a una persona, de forma que, utilizándola, se pueda decir que está electrónicamente firmando el documento, y de otra parte, se necesitará otro método para poder comprobar, en el otro extremo, que es esa persona realmente la que firmó el documento.

Además, se busca garantizar que el documento viaja en un entorno seguro y no puede ser leído o modificado por un tercero no autorizado, aunque lo intercepte. Esto se consigue utilizando técnicas criptográficas con el objeto de cifrar los datos.

1.2. Criptografía

Los sistemas de cifrado más conocidos son dos y, muy someramente, podemos definirlos del siguiente modo:

- *Sistema de clave simétrica o secreta:* es aquél que está formado por una sola clave que sirve tanto para cifrar como para descifrar.
- *Sistema de clave asimétrica o pública*: en este caso existen asociadas a cada firmante de un documento dos claves diferentes, una de ellas sirve para cifrar y la otra para descifrar. Estas dos claves se denominan privada y pública, la primera cifra y con la segunda se descifra lo que se ha cifrado con la primera, y ninguna de ellas lleva a la otra. Esto es, se firma con la clave privada y se descifra la firma con la clave pública[41].

La clave privada permanece secreta y la clave pública se da a conocer para poder establecer el sistema completo. En la clave privada debe quedar garantizado que no se puede descubrir por lo que suelen emplear mayores longitudes de claves, teniendo en cuenta que un algoritmo de mayor longitud es más difícil de descubrir.

1.3. Validez y eficacia jurídica de la firma electrónica

Uno de los mayores frenos con los que se encuentra el instrumento de la firma electrónica es el de que al buscar trasladar la eficacia de la firma manuscrita al entorno electrónico se plantea la falta de reconocimiento del mismo valor jurídico.

La Ley de firma electrónica en su artículo 3 establece la equivalencia funcional de la firma electrónica reconocida con la manuscrita, no basta como establecía la anterior regulación de firma electrónica[42] con que se trate de una firma electrónica avanzada sino que además habrá de estar basada en un certificado reconocido y haber sido creada por un dispositivo seguro de creación de firma.

Todo esto sin perjuicio de los efectos jurídicos que deben reconocerse a una firma electrónica que no reúna los requisitos de firma electrónica reconocida con relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

1.4. Firma electrónica de personas jurídicas

Una de las novedades más importantes que introduce la Ley de firma electrónica es la de permitir la firma electrónica de las personas jurídicas integrándolas así en el tráfico telemático y yendo más allá del régimen anterior que sólo reconocía como firmantes a las personas físicas[43].

---

[41] El documento firmado con la clave privada de una persona, es entendido, o conocido quien es el firmante, descifrando con la clave pública de esa misma persona. Lo que se cifra con la clave privada se descifra con la clave pública.

[42] Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

[43] "Art. 3. c) del Real Decreto-ley 14/1999: «Signatario»: Es la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.", mientras que el artículo 6.2 de la LFE dice que es firmante "la 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".

Éste es un caso distinto a la firma electrónica de los representantes de las personas jurídicas, supuesto ya habitual en la tradición jurídica, pues se persigue dar firma a las empresas, no a sus representantes, si bien, evidentemente, con el objeto de que así se pueda distribuir entre sus empleados.

No obstante, conviene puntualizar que ya el artículo 5.3 del Real Decreto-Ley 14/1999 apuntaba esta posibilidad en el ámbito tributario, al decir: *3. Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-Ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica*. Esta redacción venía impulsada por el manifiesto éxito de la Administración electrónica tributaria en España, y parece que la Ley ha querido extender el ámbito de actuación, tal y como recalca en su Exposición de Motivos: *Se va así más allá del Real Decreto-Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.*

De un lado, como vemos, la figura parece complicada, puesto que siempre será una persona física quien pueda firmar, electrónica o manualmente, pues la firma implica una asunción de voluntad, y, de otro lado, se pretende inyectar un mayor dinamismo y eficiencia en las relaciones telemáticas de las empresas, huyendo del exigido formalismo y las cargas que la representación tradicional, en documento público, acarrea. En este sentido, la Exposición de Motivos de la Ley resalta en su apartado I que: *El Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las Nuevas Tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones Públicas.*

En resumen, frente a la regulación del Real Decreto-Ley 14/1999, que en su artículo 3 definía al signatario únicamente como persona física, la Ley no sólo incluye la figura de la representación, sino que, además, introduce la muy novedosa figura de la firma de las personas jurídicas.

Uno de los problemas que más fácilmente se deducen del planteamiento de otorgar una firma a una persona jurídica, de la que, como decíamos, carece en el entorno tradicional obviamente, es el de la responsabilidad frente a terceros.

La Exposición de Motivos de la Ley, en este sentido, habla de varias cautelas: por un lado, dice que los solicitantes (evidentemente personas físicas) tienen que tener una legitimación especial, como se recoge en el artículo 7.1 [44], y, por otro, que se tendrán que responsabilizar de la custodia de los datos de creación de firma asociados a esos certificados, como dice el artículo 7.2 [45], además, de, finalmente, limita el uso de estos certificados a *los actos que integren la relación entre la persona jurídica y las Administraciones Públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse,* como señala el artículo 7.3 [46].

La expresión giro o tráfico ordinario pretende, según las palabras de la Exposición de Motivos de la Ley, adaptar a nuestros días lo que en la legislación mercantil española se denomina "establecimiento fabril o mercantil". No obstante, la misma Ley, consciente de la necesidad de concreción continúa intentando delimitar las actividades comprendidas en esta denominación: *se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las activida-*

[44] *Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.*

[45] *La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.*

[46] *Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.*

des de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares. En definitiva, como ya apuntábamos, se trata de un supuesto más "cotidiano" y necesariamente menos formalista que el de la representación, máxime en un entorno como el electrónico que supuestamente necesita y busca eliminar las cargas burocráticas.

La misma Ley ya señala uno de los más evidentes puntos débiles de la cuestión, al decir que: *Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.*

Continuando con el razonamiento, el problema más inmediato surge, pues, con la responsabilidad frente a terceros de los actos realizados por estas personas físicas dependientes de la persona jurídica, que no son sus representantes en el sentido tradicional del ordenamiento jurídico, pero que, en definitiva, tienen capacidad para obligar a la persona jurídica a la que, en sentido coloquial y amplio de la palabra, representan.

En definitiva, se trata de un problema de límites y de definición, que consecuentemente conlleva un grado de inseguridad jurídica muy criticado por los detractores de esta nueva figura.

1.5. Certificados electrónicos

Un certificado electrónico es un documento electrónico que vincula una clave pública, es decir, los datos de verificación de firma, a una organización o particular. Viniendo así a permitir relacionar con toda seguridad un mensaje recibido con su remitente.

El sistema de emisión de certificados electrónicos por terceras partes de confianza es la solución técnica que se ha encontrado, a nivel europeo o comunitario y nacional, vinculando estos certificados de forma segura a unos datos de verificación de firma (una clave pública, en el caso de criptografía asimétrica) e indirectamente su correspondiente dato de creación de firma (clave privada) a una persona determinada.

La LFE distingue dos clases principales de certificados electrónicos: el certificado electrónico y el certificado electrónico reconocido diferenciándose uno de otro por los requisitos que se exigen en su emisión. Para conocer estos requisitos analicemos la tabla que sigue:

CLASES DE CERTIFICADOS ELECTRÓNICOS	REQUISITOS
Certificado electrónico	✓ Firmado electrónicamente por un prestador de servicios de certificación ✓ Vincula unos datos de verificación de firma a un firmante ✓ Confirma su identidad
Certificado reconocido	✓ Expedidos por un prestador de servicios de certificación que cumpla los requisitos de: ◆ Comprobar la identidad y circunstancias personales de los solicitantes de certificados ◆ Verificar que toda la información contenida en el certificado es exacta ◆ Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado ◆ Garantizar la complementariedad de los datos de creación y verificación de firma siempre que ambos sean generados por el prestador de servicios de certificación

El contenido que al menos deben incluir los certificados reconocidos se describe en artículo 11.2 de la Ley y los recogemos en la tabla que sigue a continuación:

CONTENIDO MÍNIMO DE LOS CERTIFICADOS RECONOCIDOS

1. La indicación de que se expiden como tales
2. El código identificativo único del certificado
3. Identificación, domicilio y firma electrónica avanzada del prestador de servicios de certificación
4. Identificación del signatario:
   a) Personas físicas:
      - ◆ Nombre, apellidos, DNI o
      - ◆ Seudónimo que conste como tal de manera inequívoca
   b) Persona jurídica:
      - ◆ Denominación social
      - ◆ Código de Identificación Fiscal
5. Datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante
6. Comienzo y el fin del período de validez del certificado
7. Los límites de uso del certificado, si se establecen
8. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen

La consignación en el certificado reconocido de cualquier otra información relativa al firmante se realizará cuando sea significativo en función del fin propio del certificado y siempre que el firmante lo solicite.

1.6. Prestadores de servicios de certificación

Los sujetos que intervienen en el sistema de firma electrónica son además de los firmantes, los prestadores de servicios de certificación que son los que emiten los certificados electrónicos o reconocidos que hemos analizado en el epígrafe anterior.

Los prestadores de servicios de certificación deben formular una Declaración de prácticas de certificación que estará disponible al público de manera fácilmente accesible al menos por vía electrónica y de forma gratuita. En esta Declaración se hará constar la información que exponemos en la tabla:

DECALARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Obligaciones relativas a la gestión de los datos de:
- ◆ Creación
- ◆ Verificación de firma
- ◆ Los certificados electrónicos

Las condiciones aplicables a:
- ◆ La solicitud
- ◆ Expedición
- ◆ Uso
- ◆ Suspensión
- ◆ Extinción
  - De la vigencia de los certificados

DECALARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (continuación)

- Las medidas de seguridad técnicas y organizativas
- Los perfiles
- Los mecanismos de información sobre la vigencia de los certificados

En su caso, la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos Registros.

Las obligaciones principales de los prestadores de servicios, partiendo de la base de que los prestadores de servicios que emitan certificados reconocidos deberán cumplir las obligaciones generales de los prestadores de servicios y además unas específicas que señala el artículo 20 de la Ley de firma electrónica, veamos gráficamente cuáles son estas obligaciones:

OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

OBLIGACIONES GENERALES	No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.
	Información mínima al firmante, de forma gratuita, por escrito o por vía electrónica: ◆ Sus obligaciones. ◆ 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. ◆ Mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo. ◆ Método utilizado para comprobar la identidad del firmante u otros datos que figuren en el certificado. ◆ Condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial. ◆ 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. ◆ Demás informaciones contenidas en la declaración de prácticas de certificación.
	Mantener un Directorio actualizado de certificados que expidan.
	Servicio de consulta sobre la vigencia de los certificados rápido y seguro.
OBLIGACIONES ESPECÍFICAS DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN QUE EMITAN CERTIFICADOS RECONOCIDOS	Demostrar la fiabilidad necesaria para prestar servicios de certificación.
	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.
	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.
	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.

OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (continuación)	
OBLIGACIONES ESPECÍFICAS DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN QUE EMITAN CERTIFICADOS RECONOCIDOS	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.
	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 quince años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.
	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.
	Seguro de responsabilidad civil por importe de al menos 3.000.000 de euros que podrá ser sustituido por: ◆ Aval bancario. ◆ Seguro de caución.

La Ley establece en su artículo 30, y disposición transitoria segunda, que los prestadores de servicios de certificación deberán comunicar al Ministerio de Industria, Turismo y Comercio, sus datos de identificación, los datos que permitan establecer comunicación con el prestador, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen. Esta información deberá ser convenientemente actualizada por los prestadores de servicios de certificación (PSC) y la lista de los PSC que así lo han hecho se encuentra disponible en la dirección de Internet http://www.setsi.min.es.

Cuando un prestador de servicios de certificación vaya a cesar en su actividad debe comunicarlo con una antelación mínima de dos meses a los firmantes y a los solicitantes de los certificados de las personas jurídicas. Respecto de los certificados emitidos que estén vigentes a la fecha de su cese, los prestadores de servicios de certificación pueden bien transferir su gestión a otro prestador, siempre con el consentimiento expreso del titular del certificado y con la información previa de las características del prestador al que se tenga intención de transferir los certificados o bien extinguir su vigencia.

El régimen de responsabilidad de los prestadores de servicios de certificación se rige por las reglas generales de culpa contractual y extracontractual y recae sobre él la carga de la prueba de su actuación con diligencia.

El régimen sancionador que establece la Ley de firma electrónica diferencia entre sanciones muy graves, graves y leves y en concreto respecto de las infracciones que exponemos a continuación:

INFRACCIONES	SANCIONES
MUY GRAVES	
El incumplimiento de alguna de las obligaciones siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.	MULTA DE 150.001 € a 600.000 €
A excepción del incumplimiento de la obligación de constitución de la garantía económica.	
La expedición de certificados reconocidos sin realizar todas las comprobaciones previas cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.	
GRAVES	
El incumplimiento de alguna de las obligaciones, excepto de la obligación de constitución de la garantía cuando no constituya infracción muy grave.	MULTA DE 30.001 € a 150.000 €
La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica exigida por la Ley.	
La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en la Ley, en los casos en que no constituya infracción muy grave.	
El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de sus obligaciones si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.	
El incumplimiento por los prestadores de servicios de certificación de sus obligaciones respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la LOPD.	
La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Industria, Turismo y Comercio[47] en su función de inspección y control.	
El incumplimiento de las resoluciones dictadas por el Ministerio de Industria, Turismo y Comercio para asegurar que el prestador de servicios de certificación se ajuste a la Ley.	
LEVES	
El incumplimiento por los prestadores de servicios de certificación que no expidan certificados econocidos,de las obligaciones señaladas en el artículo 18 y las restantes de la Ley, cuando no constituya infracción grave o muy grave, excepto las contenidas en el apartado 2 del artículo 30.	MULTA DE HASTA 30.000 €

1.7. Camerfirma. Certificación digital de las Cámaras de Comercio (certificado electrónico gratuito)

1.7.1. AC Camerfirma SA.

Desde hace ya casi ocho años las Cámaras de Comercio trabajan en el ámbito de la certificación digital y la firma electrónica desde un proyecto empresarial llamado Camerfirma. Camerfirma fue creada conjuntamente con el Consejo Superior de Camaras en el 2000 con ayuda de varios socios del entorno bancario como Banesto, Caixa Galicia y Bancaja.

[47] *Tal y como venimos señalando, el Ministerio de Ciencia y Tecnología ha pasado a denominarse Ministerio de Industria, Turismo y Comercio. En este sentido, las referencias que se hagan a lo largo de este capítulo al Ministerio de Ciencia y Tecnología han de entenderse realizadas al Ministerio de Industria, Turismo y Comercio.*

Camerfirma emite certificados digitales de identidad empresarial, es decir establece siempre en sus certificados una vinculación contractual ente el titular y la entidad identificada en el certificado. La vinculación referida podría ser una vinculación de poder cuando el titular posee capacidad de representación de la entidad detallada en el certificado. En muchos casos es complejo trasladar al certificado esta capacidad de poder, principalmente debido a la gran variedad y complejidad de los poderes. Camerfirma por lo tanto decide incorporar la referencia del poder otorgado dentro de uno de los campos del certificado, de tal forma que la parte confiante sea capaz de validar si los poderes cubren los requerimientos de seguridad de una transacción electrónica concreta.

Camerfirma también ofrece otros tipos de certificados digitales: Los certificados de persona jurídica descritos por la Ley 59/2003, certificados de servidor seguro y de firma de código. Esta gama de productos cubre las necesidades de identificación electrónica empresarial necesaria para el desarrollo de servicios empresariales en redes abiertas como Internet.

El objetivo del proyecto Camerfirma por lo tanto es suministrar una identificación electrónica, ofreciendo información de la vinculación contractual entre personas físicas y jurídicas ya sea de poder o de simple pertenencia.

Para realizar estas tareas contamos con:

- *Un centro de datos propio especializado en la emisión de certificados. CPD en Ávila.*
- *Una red de Cámaras de Comercio que realizaran las labores de Autoridades de Registro.*

Las características especiales del producto son:

- **Certificados Empresariales.**
- **Certificados con perfil cualificado o reconocido** usados para la elaboración de firma electrónica avanzada. En aquellos certificados de persona física ya que el certificado cualificado o reconocido solo puede ser asociado a una persona física.
- **Certificados con amplio reconocimiento.** Para tener éxito en esta tarea tenemos que dotar a los certificados del mayor reconocimiento posible para lo cual Camerfirma ha trabajando conjuntamente con los distintos generadores de servicios electrónicos y aplicaciones.
  - Administración publica estatal.
  - Administración publica autonómica.
  - Administración Local (Ayuntamientos)
  - Navegadores (Microsoft).
- **Certificados de bajo coste** financiados por las Cámaras de Comercio

Otro de los aspectos importantes en la definición del producto es el proceso de creación y custodia de claves. En este aspecto Camerfirma elabora distintos circuitos distinguiendo el perfil del certificado, de la generación y el soporte de custodia de las claves criptográficas.

Los circuitos definidos para la elaboración de los certificados son los siguientes:

- Soporte software
  - Claves generadas por el usuario.
  - Claves generadas por el prestador del certificado.
- Soporte hardware
  - Claves generadas por el usuario.
  - Claves generadas por el prestador del certificado.

Esta información va asociada al identificativo de la política de tal forma que la aplicación conozca los aspectos sobre la generación y custodia de las claves y actuar en consecuencia.

ETIQUETA TIPO DE CERTIFICADO Y OID DE POLÍTICA	
CAM-PF-SW-KPSC	Certificado Cameral de persona física, claves almacenadas en software y generadas por el PSC 1.3.6.1.4.1.17326.10.6.2.1.1
CAM-PF-SW-KUSU	Certificado Cameral de persona física, claves almacenadas en software y generadas por el titular 1.3.6.1.4.1.17326.10.6.2.1.2
CAM-PF-HW-KPSC	Certificado Cameral de persona física, claves almacenadas en hardware y generadas por el PSC 1.3.6.1.4.1.17326.10.6.2.2.1
CAM-PF-HW-KUSU	Certificado Cameral de persona física, claves almacenadas en hardware y generadas por el titular 1.3.6.1.4.1.17326.10.6.2.2.2

Por otro lado dentro del contenido del certificado se incorporan los datos relativos a la autoridad de registro que ha realizado la validación de la información del usuario, y para los datos de representante o de persona jurídica el identificador de los poderes presentados.

Por último y para dar cumplimiento a la Ley 59/2003 se incluye un enlace a las declaraciones del titular para que este describa cualquier aspecto relevante en el uso del certificado.

Para la validación de los certificados Camerfirma pone a disposición de la parte confiante varios mecanismos entre los que se encuentran:

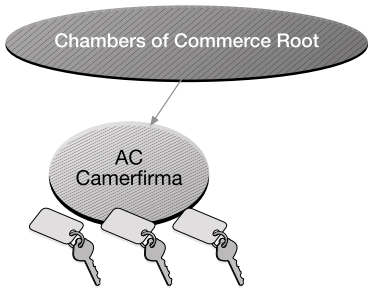
- CRL de acceso libre mediante acceso HTTP y LDAP.
- OCSP mediante el acceso a los servicios de Certiver.
- Webservice requerido por la Agencia tributaria.
- URL de revocación de Netscape.

Esta información se ofrece actualmente de forma libre y gratuita a aquellas personas que decidan confiar en los certificados emitidos por Camerfirma.

CARACTERISTICAS GENERALES DE LOS CERTIFICADOS:
Algoritmo de emisión: RSA 1024 bits
Versión x.509: V3
Uso de clave: Firma digital, Cifrado de clave, Cifrado de datos, Contrato de claves
Uso extendido de claves: Autenticación del cliente; Correo seguro
Tipo de certificado: cualificado / reconocido
Método de verificación de la identidad: presencial, realizada por personal adscrito a una organización Cameral.
Tipo de identificación para facturación: CIF IVA (VAT number as by article 28h of Directive 77/388/EEC), según artículo 28 nono de la Directiva 77/388/CEE, indicado en la extensión 1.3.6.1.4.1.17326.30.2.
Declaración del titular: el signatario puede realizar una declaración compatible con el artículo 11.3 de la Ley 59/2003 y con las políticas de certificación. El enlace a esta declaración estará contenido en la extensión bases del certificado del propio certificado (subject statment) y podrá contener declaración expresa de la indicación de autofacturación o facturación por cuenta de terceros.
Normas técnicas de referencia: RFC 3039 (IETF) y TS 101 862 (ETSI)

Para la emisión de los certificados antes referidos Camerfirma ha desarrollado una jerarquía de confianza llamada *Chambers of Commerce Root* cuya estructura se puede ver en la siguiente figura:

Jerarquía Camerfirma



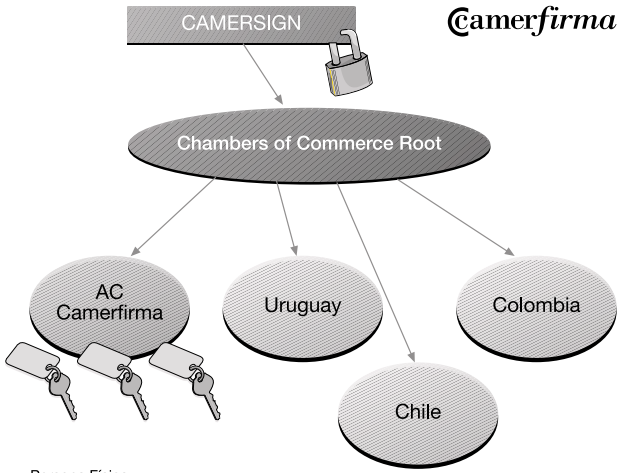
Esta jerarquía esta formada por una autoridad de certificación raíz fuente de la confianza para el resto de la estructura. Como autoridad delegada se encuentra AC Camerfirma que es la encargada de emitir certificados de identidad para la comunidad empresarial española.

Camerfirma tiene en este área un factor diferenciador fundamental que es su vocación internacional. El proyecto Camerfirma puede ser desarrollado internacionalmente en dos líneas principales:

- Primero: como parte de ampliación de la confianza al mercado latinoamericano.
- Segundo: mediante su incorporación a la Red de Confianza Cameral Europea “Chambersign”.

Nuestra visión es la comunicación electrónica segura de empresas de todo el mundo a través de una red de confianza Cameral. Esta visión encaja en el verdadero ámbito de Internet como medio de comunicación universal.

La figura anterior por lo tanto quedaría, incorporando estas nuevas áreas de desarrollo de la forma siguiente:



Camerfirma adicionalmente a la creación de certificados digitales desarrolla otra serie de áreas de negocio:

- Desarrollo e integración de aplicaciones con tecnología de Certificación digital.
- Outsourcing de PKI.
- Consultoría PKI.
- Desarrollo de productos de firma.
- Servicios de tercera parte de confianza:
  - Sellos de Tiempo.
  - Custodia de documentos.
  - Notarización de eventos electrónicos.

1.7.2. Proyecto "Hacia un Censo Digital"

La incorporación de la empresa española al uso de las Nuevas Tecnologías es una prioridad para las Cámaras de Comercio en la medida que es el principal pilar de crecimiento económico en la sociedad moderna y permite la creación de empleo sin efectos inflacionistas. En esta línea se está trabajando de una forma muy activa en actuaciones que impulsen y apoyen la incorporación y el uso de las Nuevas Tecnologías en las empresas, especialmente, en las pequeñas y medianas.

En este contexto, y dado el bajo nivel de penetración de la firma electrónica en estas empresas, la implantación de la misma constituye un elemento de gran importancia para apoyar y fomentar la incorporación de las Pymes a la Sociedad de la Información. Por este motivo se ha considerado prioritaria una actuación ambiciosa y global que ayude con eficacia a incorporar e incrementar el uso de la firma electrónica entre las empresas.

El objetivo que se propone es una acción de emisión masiva de identificadores digitales empresariales, con el objetivo de que las empresas españolas, y en especial la Pyme, puedan tener una identidad en la red. Dicha identidad estará basada en certificados digitales, y estará apoyada en el censo público de las empresas. Las Cámaras de Comercio según la Ley 3/1993[48], entre otras funciones de carácter público administrativo les corresponde llevar un censo público de todas las empresas así como de sus establecimientos, delegaciones y agencias radicados en su demarcación.

1.7.2.1. Objetivo del proyecto

El objeto del Proyecto es emitir gratuitamente 300.000 certificados digitales a empresas, desarrollando además usos de dichos certificados que estimulen el interés de las empresas y su uso creciente. Para ello, se desarrollará un programa coordinado de acciones dirigidas a un importante número de beneficiarios en los colectivos de Empresas, Pymes, micropymes y autónomos ***que impulse y apoye el uso de la certificación digital y la firma electrónica entre las empresas españolas.***

Este proyecto es una aportación fundamental de las Cámaras a la promoción de la sociedad del conocimiento, proporcionando a las empresas una herramienta básica que garantiza la seguridad en Internet. En esta misma línea se colabora con las Administraciones Públicas en la promoción de los servicios electrónicos, mediante la difusión de la certificación digital.

Actualmente 67 Cámaras participan en el proyecto, estas Cámaras actúan como autoridad de registro de Camerfirma que es la autoridad de certificación. Por esta función las Cámaras son las autoridades que validan los certificados digitales a las empresas de su demarcación.

[48] *Ley 3/1993, de 22 de marzo, básica de las Cámaras Oficiales de Comercio, Industria y Navegación.*

En esta publicación se adjunta un CD-WEB en el que se recoge toda la información para la solicitud de certificados digitales dentro del proyecto “Hacia un Censo Digital”, así como todo lo referente a sus usos y aplicaciones dentro de la vida empresarial.

El contenido de este CD-WEB es el siguiente:

CONTENIDO CD-WEB CAMERFIRMA

En el CD-WEB que se adjunta en esta publicación, se recoge toda la información necesaria para la obtención de una forma gratuita del certificado digital en sus distintas modalidades, así como toda la información y recursos para su uso.

En este CD hace referencia a los usos de los certificados Camerfirma, tanto desde el punto de vista de las Administraciones Públicas como de las propias Cámaras, además entre los usos empresariales hay que destacar la facturación electrónica. Para ello se recogen diferentes demostraciones de usos para poder observar de una manera práctica las utilidades del certificado.

LOS CERTIFICADOS DIGITALES: QUÉ SON, QUÉ PERMITEN HACER (Trámites con las Administraciones Públicas, Trámites con las Cámaras de Comercio, Usos Empresariales y Factura electrónica). MARCO LEGAL (Acceso a la ley de firma y Acceso a la directiva europea). CÓMO SE USAN (Office XP, Correo Electrónico, Ficheros Pdf, Dfirma Desktop y Servidores páginas HTML).

CERTIFICADO DE PERTENENCIA A EMPRESA (Cómo se firman los documentos, Descarga Dfirma Desktop, Solicita tu certificado y Cómo se gestiona un certificado digital). CERTIFICADO DE REPRESENTANTE / PERSONA JURÍDICA (Cómo se firman los documentos, Descarga Dfirma Desktop, Solicita tu certificado y Cómo se gestiona un certificado digital). CERTIFICADO DE FIRMA DE CÓDIGO / SERVIDOR SEGURO.

En línea con estos recursos, el CD se completa con exposición del marco legal y de las especificaciones de cada uno de los certificados digitales para empresas. Así mismo recoge enlaces de interés, y videos demostrativos tanto de firma de documentos como de pasarelas de autenticación.

2. PAGO ELECTRÓNICO

2.1. Consideraciones generales

Los llamados medios de pago electrónico son aquellos sistemas que permiten el procesamiento de órdenes de pago a través de sistemas electrónicos.

El pago electrónico no debe confundirse con la transferencia electrónica de fondos, como elemento que precede al pago electrónico pero que no siempre se concreta en él, pues puede ser una simple transacción sin objeto de pago.

En definitiva, no puede existir pago electrónico sin transferencia electrónica de fondos pero no toda transferencia electrónica de fondos es un pago electrónico.

Así, la transferencia electrónica implica una actividad económica por medios electrónicos que puede ser, además de un pago, una retirada de dinero o un depósito.

Dentro de los medios de pago electrónico encontramos distintos supuestos como son el pago mediante tarjeta, el pago por medio de cheque electrónico, el pago a través de transferencia electrónica, en el caso en el que como hemos analizado ésta tenga por fin realizar un pago, o el pago mediante dinero electrónico.

Atenderemos al pago mediante tarjeta por ser uno de los medios de pago electrónico más utilizado, pasando antes a explicar brevemente otros medios que hemos señalado.

En primer lugar y respecto de los cheques electrónicos, diremos que son instrumentos de pago que evitan el desembolso de numerario en las transacciones mercantiles. Por medio del cheque, el que lo emite, dispone de los fondos de su cuenta bancaria a favor de un tercero acreedor.

El hecho de que el cheque sea electrónico deriva de los medios a través de los que se elabore. Con este carácter, será un instrumento de pago basado en el acceso directo a una cuenta bancaria de la que es titular el usuario de aquél con el fin de realizar pagos por Internet.

En la normativa y costumbre española su uso no está extendido, en primer lugar porque su regulación exige unas formalidades concretas y también porque no existe una cultura de uso de estos medios, al contrario que en otras sociedades como la francesa o la estadounidense.

En segundo lugar, las transferencias electrónicas ya hemos comentado que pueden suponer un pago o no, y en el caso de que lo sean supone una liberación de una deuda, dado que cumple la función de pago mediante el traspaso del dinero de su cuenta de origen a la de destino.

En lo que respecta al dinero electrónico como medio de pago, no debe ocupar nuestra atención ya que en la actualidad el dinero electrónico se encuentra en fase de desarrollo existiendo varios sistemas y se encuentra recogido en distintas reglamentaciones, comunitarias y nacionales [49] pero aun es pronto para describir los cambios que traerá la utilización de un instrumento electrónico de pago que cumpla con todas las características del dinero tradicional –entre otras, anonimato y carácter fungible–, pero de forma electrónica.

Visto esto, entremos a analizar el pago electrónico realizado mediante tarjeta en el que, teniendo en cuenta el funcionamiento de la firma electrónica, vamos a estudiar el caso de que a ésta se le una la utilización de pago por medios electrónicos, con el aprovechamiento de la seguridad ofrecida por las técnicas criptográficas, que permiten que los datos de pago "viajen" seguros a través de la red y garantizan la integridad, conservación y autenticación de los documentos transmitidos, así como la identificación inequívoca de los intervinientes en la contratación, abriéndose un camino sencillo, ágil, seguro y, hoy en día, idóneo para la utilización de estas técnicas en el comercio electrónico a través de Internet.

2.2. Pago mediante tarjeta

Uno de los medios de pago electrónico más arraigados en la sociedad es el pago por tarjeta. El conocido dinero de "plástico" se presenta en una tarjeta que incorpora una banda magnética o un microchip que permite a su titular realizar una serie de operaciones, tanto con la entidad emisora, como con terceros, con objeto de llevar a cabo un pago.

El pago mediante tarjeta *no implica necesariamente que la compra del bien o el pago del servicio se esté realizando a través de Internet,* pero en el caso de que esto sea así se asimila a una venta a distancia por lo que le sería de aplicación, en lo que no esté previsto en la LCE, la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista [50] (en adelante LOCM).

La citada LOCM dispone en su artículo 46 que

> *Cuando el importe de una compra hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, su titular podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del proveedor y del titular se efectuarán a la mayor brevedad.*

[49] *En nuestro país la ley financiera ha sido aprobada mediante la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, publicada en el Boletín Oficial del Estado núm. 281, de 23 de noviembre.*

[50] *Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, publicada en el Boletín Oficial del Estado núm. 15, de 15 de enero, que ha sido modificada por la Ley 47/2002, de 19 de diciembre, publicada en el Boletín Oficial del Estado núm. 304, de 20 de diciembre.*

Esta consideración no está exenta de precauciones dirigidas a evitar el fraude por el titular de la tarjeta porque en su segundo apartado dispone que si el titular hubiese hecho el pago y pidiese después su anulación responderá ante el vendedor por los daños y perjuicios que hubiese podido causar.

2.3. Protocolos de seguridad

En el caso de las transacciones electrónicas, y como ya hemos señalado, son la desconfianza y el miedo a la falta de seguridad en el envío y recepción de la orden de pago, las principales causas que paralizan, o por lo menos no impulsan, el comercio por Internet.

Uno de los medios que tratan de evitar esta traba al comercio electrónico son los protocolos de seguridad.

Éstos son soluciones tecnológicas que buscan asegurar que los datos relativos a una transacción comercial puedan ser transmitidos al comerciante de forma segura.

Los dos protocolos de seguridad más generalizados son el SSL y el SET.

En primer lugar, el protocolo SET o *Secure Electronic Transactions,* ofrece autenticación a todas las partes implicadas, confidencialidad e integridad. Esto es así porque este protocolo de seguridad se basa en una infraestructura de clave pública que le dota de estas características.

Pese a la gran seguridad que presenta este medio tecnológico, no son pocas las dificultades que presenta en su utilización pues entre otras cosas implica la instalación de un software específico *(wallet).*

Por su parte, el protocolo de seguridad *Secure Sockets Layer, conocido como SSL,* consiste en la creación de un canal seguro de comunicación a través de Internet entre el comerciante y el comprador.

El efecto que produce es el de la autenticación del servidor, la encriptación de los datos y la integridad del mensaje que se remite a través del canal.

Las consecuencias de estos efectos son las de suponer una garantía para el comprador al autenticar al comerciante y la de que los datos se transmitan cifrados.