S A B E R E S

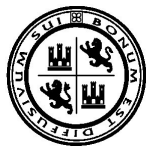
Revista de estudios jurídicos, económicos y sociales

VOLUMEN 1 ~ AÑO 2003

Separata

LA ACREDITACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA COMO SELLO DE CALIDAD

María Antonia Rodríguez Pérez



UNIVERSIDAD ALFONSO X EL SABIO
Facultad de Estudios Sociales
Villanueva de la Cañada

Avda. de la Universidad,1
28691 Villanueva de la Cañada (Madrid, España)

Saberes, vol. 1, 2003

ISSN: 1695-6311

LA ACREDITACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA COMO SELLO DE CALIDAD[*]

María Antonia Rodríguez Pérez[**]

RESUMEN: El nuevo escenario de la comunicación electrónica presenta hoy en día instrumentos técnicos que permiten garantizar la autenticidad de los interlocutores, la confidencialidad de la comunicación, la integridad de los documentos que contienen sus mensajes, la recepción de los mismos y la fecha y hora de emisión y recepción. El legislador viene esforzándose en los últimos años por crear un marco legal que dote de seguridad y eficacia jurídica las transacciones realizadas por vía telemática, lo que pasa necesariamente por la exigencia de ciertos requisitos que debe reunir la firma electrónica y los prestadores de servicios de certificación. Se pretende alcanzar así la confianza de los usuarios en un medio cuyo uso está cada vez más generalizado.

PALABRAS CLAVE: firma electrónica, certificación electrónica, entidades de certificación.

1. Concepto y caracteres

La cuestión que nos ocupa ha adquirido extraordinaria importancia en los últimos años. Las comunicaciones pueden tener lugar ahora, en un espacio no real, sino virtual. En un escenario, en el que no sólo no hay presencia de las partes, sino que los elementos que sustentan el intercambio de información, tampoco son materiales.

¿Qué hay en la comunicación electrónica? Hay al menos dos partes, públicas o privadas, que desde cualquier lugar del mundo, convienen la celebración de un contrato, o el envío de cierta información, por medios telemáticos.

---

[*] Conferencia pronunciada en la Real Academia de Jurisprudencia y Legislación el 8 de Febrero de 2001. Publicado inicialmente en http://www.uax.es/iurisuax año 2001.

[**] Master en Informática y Derecho UCM. Profesora de de Informática Jurídica. Universidad Alfonso X el Sabio. Abogada especialista en Nuevas Tecnologías.

En la mayoría de los casos, ni siquiera es necesario que se conozcan de antemano, una parte puede localizar a la otra a través de la propia red. Y pueden llegar a sostener toda la negociación y toda la relación de cumplimiento de sus respectivas obligaciones, por esta vía.

La naturaleza de este instrumento ofrece importantes ventajas, ahorro de tiempo, de desplazamientos, merma por tanto de costes, posibilidad de examinar varias ofertas simultáneamente, inmediatez en la recepción de los mensajes....

Sin embargo, desde la perspectiva jurídica, dichas ventajas no son tales si no se dan una serie de requisitos, que poco a poco el legislador intenta perfilar.

Porque, ¿cómo podemos estar seguros de que la otra parte está manifestando su verdadera identidad y no otra? Lo único que tenemos es su palabra.

Y aunque eso fuera suficiente, que puede ser mucho presumir, ¿qué garantías tenemos de que su mensaje no ha sido interceptado y alterado en el curso de la comunicación? ¿o alterada su identidad?.

No se agotan aquí las incertidumbres. El secreto de las comunicaciones es un derecho constitucionalmente reconocido (art.18.3). ¿Puede ser garantizado en la comunicación electrónica?.

¿Cuándo surgen las obligaciones? ¿se puede hacer constar la fecha y hora real en que se emitió la declaración?.

Así se presenta el nuevo escenario de la comunicación electrónica, con luces y con sombras. Pero las sombras están mitigadas hasta tal punto que son insignificantes. La técnica ofrece respuestas afirmativas a los interrogantes que he planteado. Todas ellas se resumen en la *firma electrónica*, conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge, y en la figura de los PSC Prestador de servicios de certificación que es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

En contra de lo que pudiera parecer, ya hace 8 años que se admiten documentos remitidos por vía electrónica, con idéntico valor que los tradicionales en papel.

La Ley 37/1992, de 28 de diciembre, reguladora del IVA atribuye, en su art. 88, idéntico valor a la factura emitida por vía telemática que a la tradicional en soporte papel, siempre y cuando reúna los requisitos legalmente establecidos.

Tales requisitos debían ser establecidos reglamentariamente, lo que tuvo lugar en virtud del Real Decreto 1624/1992, de 29 de diciembre de 1992, que aprueba el Reglamento del IVA y modifica, entre otros, el Real Decreto 2402/1985, de 18-12-1985, que regula el deber de expedir y entregar factura por empresarios y profesionales.

Así, establece como elementos o requisitos de las facturas y sus copias o matrices:

- Número y, en su caso, serie.
- Nombre y apellidos o denominación social y número de identificación fiscal.
- Descripción de la operación y su contraprestación total.
- Lugar y fecha de su emisión.

Observadas estas prescripciones, las facturas transmitidas por vía telemática tienen la misma validez que las originales, exigiéndose que el contenido de la factura emitida y recibida sea idéntico.

La aplicación del sistema de facturación telemática fue objeto de desarrollo mediante la Orden de 22 de marzo de 1996, en base a los principios de interés general, eficacia en la gestión empresarial y en el control administrativo, principio de integridad de los datos y reconocimiento a efectos fiscales del carácter de justificante de las facturas en soporte electrónico.

A esta Orden debemos la definición legal de factura electrónica como:

> El conjunto de registros lógicos, almacenados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos, que documentan las operaciones empresariales o profesionales, con los requisitos exigidos en el Real Decreto 2402/1985, de 18 de diciembre.

Tampoco es una novedad del año 1999 el concepto de "firma electrónica". La primera vez que encontramos esta expresión en nuestro ordenamiento, si bien a la espera de definición, es en la Ley 19/1996, de 27 de diciembre de 1996, de Presupuestos de la Generalidad de Cataluña para 1997, en la Disposición Adicional Octava, al autorizar al Departamento de Economía y Finanzas a establecer un sistema de intercambio electrónico de documentos con los proveedores de la Generalidad. Sistema que debería permitir la sustitución de documentos impresos en papel por documentos grabados en soporte electrónico y la sustitución de los sistemas de

autorización y control tradicionales por validaciones de acceso restringido o firma electrónica.

Sin embargo, 4 años antes, la Ley 30/1992, de 26 de noviembre de RJAP y PAC, al referirse en su art. 45 a la incorporación de medios técnicos en el desarrollo de la actividad de la Administración, con la pretensión última de que el ciudadano pueda relacionarse con ella por medios electrónicos, informáticos o telemáticos, había sentado algunos de los principios que deben garantizar los sistemas telemáticos de la Administración, para que los documentos emitidos por estos medios sean considerados válidos y eficaces como si de documentos originales se tratara.

Tampoco esta vez se define la firma electrónica, es más, en este caso ni siquiera se utiliza este término. Pero sí se enumera alguno de los principios que habrían de informar el desarrollo posterior de esta figura.

A saber, los principios de autenticidad, integridad, conservación y recepción.

Pues bien, en desarrollo de dicho art. 45 (L30/1992) se dictó el Acuerdo de 11 de marzo de 1998, de la Comisión Nacional del Mercado de Valores, sobre implantación del sistema CIFRA-DOC/CNMV o sistema de intercambio de información a través de línea telemática, en el que aparece la primera explicación de lo que es la firma electrónica y cómo se utiliza, al mismo tiempo que define los principios de autenticidad, confidencialidad, integridad, conservación, acuse de recibo y disponibilidad.

El ámbito de aplicación de este Acuerdo, y por ende de las relaciones en las que la CNMV puede utilizar el sistema CIFRA-DOC, se restringe a los procedimientos contenidos en la Ley 24/1998, de 24 de julio, del Mercado de Valores, la recepción de informaciones presentadas en la CNMV, enumeradas en el Anexo II del propio Acuerdo, y la atención de reclamaciones y consultas del público.

Pero por lo que ahora hace al caso, interesa destacar la definición de los principios antes enumerados y las características del sistema CIFRA-DOC basado en la firma electrónica y en el intercambio de documentos:

- Autenticidad: identificación del emisor y del receptor, y de las fechas y horas de envío y recepción.
- Confidencialidad: garantía de que ningún usuario distinto del emisor y receptor tenga acceso al documento.
- Integridad: Garantía de que cualquier alteración del contenido del documento durante la transmisión será detectada por el receptor.

- Conservación: archivo adecuado de los documentos en la CNMV que impida su pérdida o manipulación.
- Acuse de recibo: imposibilidad de rechazo del envío y garantía para el remitente de que la recepción ha tenido lugar.
- Disponibilidad: garantía de que el documento sea accesible a los usuarios autorizados.

Estas son las primeras menciones a los dos conceptos expuestos, factura electrónica y firma electrónica.

Pero son más de 40 las normas de nuestro Ordenamiento Jurídico que, o bien aluden expresamente a la firma electrónica, o bien guardan relación con ella. Así, las que tratan de:

- Comercio electrónico.
- Condiciones generales de la contratación electrónica.
- Valor del documento electrónico.
- Utilización de medios telemáticos por la Administración pública.
- Presentación telemática de declaraciones y documentos ante diferentes órganos administrativos.
- Prestadores de servicios de certificación.
- Publicidad telemática.
- Informatización y comunicación telemática entre Registros públicos, etc.
- Además de las Directivas comunitarias de firma electrónica y comercio electrónico.

Las soluciones jurídicas que propone la reciente regulación para dotar de seguridad al comercio electrónico son la *firma electrónica* y la figura del *prestador de servicios de certificación*.

Forzosamente hemos de analizar en primer lugar el Real Decreto Ley 14/1999, de 17 de septiembre, de Firma Electrónica, que debe ir acompañado de la correspondiente comparación con la Directiva 1999/93, de 13 de diciembre, de Firma Electrónica y que nos conducirá, al mismo tiempo, al estudio de la Orden de 21 de febrero del 2000 que aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

El uso de la firma electrónica, el reconocimiento de su eficacia jurídica y el régimen jurídico de los PSC establecidos en España, constituyen el

ámbito de aplicación del Real Decreto Ley 14/1999, de 17 de septiembre, de Firma Electrónica.

No altera las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Ni modifica las que regulan las funciones de las personas facultadas, con arreglo a Derecho para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

El RDL de Firma Electrónica comienza con una Exposición de Motivos que elogia el papel de España con respecto a la UE en torno a este asunto.

Se da noticia del protagonismo de nuestro país en el Consejo de Ministros de Telecomunicaciones de la Unión, celebrado el 22 de abril del año pasado, en el que se acordó adoptar una posición común respecto al Proyecto de Directiva de Firma Electrónica.

España participó activamente en el logro de la posición común sobre los elementos considerados suficientes para proteger la seguridad e integridad de las comunicaciones telemáticas en las que se utilice firma electrónica y propuso que se exigiera a los prestadores de servicios de certificación que expidan certificados reconocidos que garantizaran la determinación de la fecha y hora de la emisión o revocación del certificado. Esta iniciativa fue aceptada y está integrada en la Directiva, en su Anexo II, letra c).

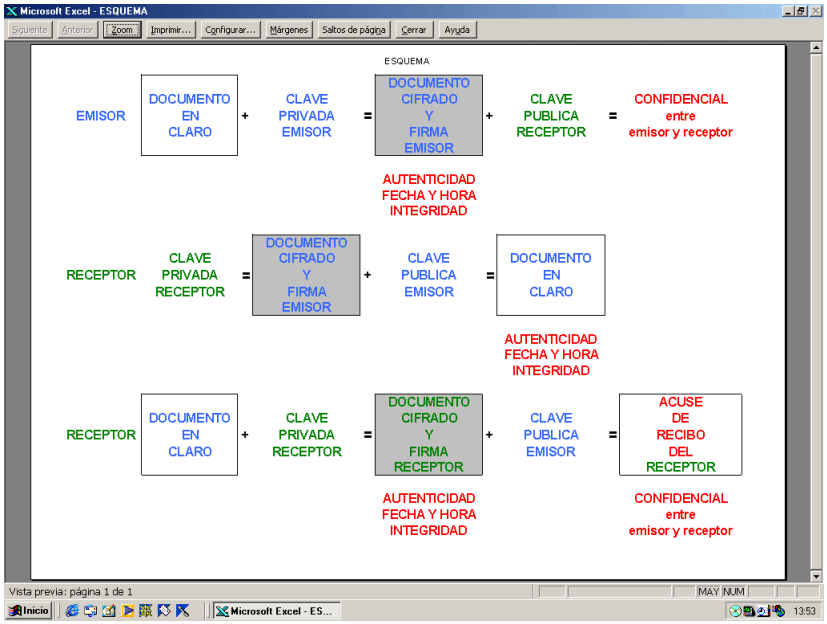
La elaboración de la Directiva estaba en marcha, pero el Gobierno español entendió que no podíamos esperar a que se dictara para luego trasponerla y optó por la vía del Real Decreto Ley, fundando la extraordinaria y urgente necesidad de dictar una norma de este tipo en:

- La existencia en España de empresas que pueden prestar servicios de certificación de firma electrónica con calidad.
- El deber de favorecer cuanto antes el desarrollo de la sociedad de la información.
- El deseo de dar a los usuarios elementos de confianza en los sistemas, de modo que éstos se difundan rápidamente.

Estas razones fueron acogidas por el Congreso, que convalidó el Real Decreto Ley 14/1999, de 17 de septiembre, de Firma Electrónica, por Resolución del 21 de octubre de 1999.

2. Funcionamiento básico

Diagrama



Es necesario conocer que nuestro sistema de Firma Electrónica se basa en claves asimétricas, de modo que cada interlocutor tiene una clave privada y otra pública. La privada sólo la conoce él. La pública puede ser conocida por todos.

La firma electrónica consiste en cifrar un resumen del contenido del documento, extraído mediante un algoritmo que asegura la unicidad del resumen con la clave privada del firmante que incluye la fecha y hora. Cualquier variación en el contenido del documento supondría un cambio en el resumen, es decir, en la firma que se obtendría al aplicar de nuevo el algoritmo.

La firma electrónica garantizará, a cualquiera que reciba el documento y que sea capaz de descifrarlo con la clave pública del firmante, la identidad del emisor y que el contenido del documento no ha sido alterado durante la transmisión, así como la fecha y hora en que ha tenido lugar su firma.

Si, posteriormente, el conjunto formado por el documento y la firma electrónica se cifra con la clave pública del destinatario, quedará

garantizado que sólo este último tendrá acceso al contenido del documento transmitido aplicando previamente para descifrarlo su clave privada.

Para el envío:

- El emisor firma electrónicamente el documento a enviar utilizando su clave privada.
- El emisor cifra el documento y la firma con la clave pública del receptor.
- El emisor envía el documento y la firma por el medio telemático establecido.

Para la recepción y su acuse de recibo:

- El receptor descifra el documento con su clave privada y obtiene el documento original y la firma del emisor.
- El receptor descrifra otra vez el documento con la clave pública del emisor y comprueba que el contenido no ha sido alterado, la identidad del emisor y la fecha y hora en que se firmó.
- El receptor firma electrónicamente el documento utilizando su clave privada.
- El receptor envía esta firma electrónica, por el medio telemático establecido, al emisor como acuse de recibo.

Utilizando así el par de claves asimétricas, quedan garantizados los *principios* que dotan a la comunicación de la seguridad necesaria:

- Autenticidad o autenticación: identificación del emisor y del receptor, y de las fechas y horas de envío y recepción.
- Confidencialidad: garantía de que ningún usuario distinto del emisor y receptor tenga acceso al documento.
- Integridad: Garantía de que cualquier alteración del contenido del documento durante la transmisión será detectada por el receptor.
- Acuse de recibo: imposibilidad de rechazo del envío y garantía para el remitente de que la recepción ha tenido lugar.

3. Efectos jurídicos

Al igual que la Directiva comunitaria, el Real Decreto Ley 14/1999 de Firma Electrónica establece que para que la firma electrónica alcance el mismo valor que la firma manuscrita, debe tratarse de una firma electrónica avanzada, basada en un certificado reconocido, producida por un dispositivo seguro de creación de firma certificado, proporcionado por un PSC acreditado que también firma el certificado reconocido. (Art. 3).

No obstante, añade el art. 3, si no reúne los requisitos anteriores, no se le niega valor jurídico ni se excluye como prueba en juicio por el hecho de ser presentada por medios electrónicos.

El alcance de este inciso deberá ser determinado por la jurisprudencia, sin embargo queda claro que si la firma reúne los requisitos mencionados tendrá el mismo valor que la firma manuscrita.

En este punto es necesario examinar las características que deben presentar dichos elementos.

3.1. *Firma electrónica avanzada*

En efecto, son dos los tipos de firma que contemplan el artículo 2 del RDL y 2 de la D, que coinciden en sus enunciados.

La definición de *firma electrónica* está informada por el principio de Autenticidad o Autenticación del signatario, persiguiendo su identificación formal.

Si al principio de autenticación añadimos el plus de integridad de los datos, la definición nos lleva al concepto de *firma electrónica avanzada*.

Así, dicen textualmente:

> a) «Firma electrónica»: Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.
>
> b) «Firma electrónica avanzada»: Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

3.2. *Certificado reconocido*

El requisito de autenticación queda garantizado por el certificado reconocido que acredita:

- La pertenencia de la clave pública a su signatario.
- La identidad del mismo.

Este extremo es el que confiere relevancia al papel del prestador de servicios de certificación (PSC) en todo este asunto.

El PSC se hace responsable frente a terceros de la veracidad de la identidad del signatario y de que el programa informático, que hace posible la firma, reúne las condiciones apropiadas para que se cumplan los principios que antes señalé.

También son dos Certificados electrónicos que pueden emitir los PSC.

El Certificado, sin adjetivos, tiene por contenido la identificación del signatario: nombre y apellidos o seudónimo que conste como tal de manera inequívoca aunque se podrá consignar otra circunstancia personal del titular, que sea significativa en relación con el fin del certificado, con su consentimiento, y los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario (clave pública del signatario).

De ahí su definición en el RDL 14/1999, art. 2.i) «Certificado: es la certificación electrónica que vincula unos datos de verificación de firma (clave pública) a un signatario y confirma su identidad».

Por su parte, el RDL 14/1999, art. 2.j) define el Certificado Reconocido del siguiente modo: «es el certificado que contiene la información descrita en el art. 8 y es expedido por un PSC que cumple los requisitos enumerados en el art. 12».

El Certificado Reconocido, que es el que necesitamos para que la firma valga jurídicamente como la manuscrita, es aquel que, además, está integrado por las siguientes especificaciones:

- La indicación de que se expiden como tales.
- El código identificativo único del certificado.
- La identificación del prestador de servicios de certificación (nombre o razón social, domicilio, dirección de correo electrónico, número de identificación fiscal y datos de identificación registral).
- La firma electrónica avanzada del prestador de servicios de certificación.

- En los supuestos en que el signatario actúa como representante de otra persona, debe indicarse el documento que acredite las facultades del signatario como representante.
- El período de validez del certificado. Éste no podrá ser superior a cuatro años, contados desde la fecha en que se haya expedido (art. 9.1.a).
- Los límites de uso del certificado, si se prevé.
- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Las causas por las que un certificado puede quedar sin efecto son las siguientes:

- Expiración del período de validez del certificado.
- Revocación por el signatario.
- Pérdida o inutilización por daños del soporte del certificado.
- Utilización indebida por un tercero.
- Resolución judicial o administrativa que lo ordene.
- Fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- Cese del prestador de servicios de certificación en su actividad salvo que, previo consentimiento expreso del signatario, sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

La pérdida de eficacia del certificado surte efecto desde:

- La expiración de su periodo de validez.
- El cese de la actividad del PSC.
- En los demás casos, desde que el PSC lo haga constar en su registro.

En cualquier caso, el PSC debe observar la máxima diligencia en la publicación de la pérdida de eficacia, dado que la demora dará lugar a responsabilidad frente al signatario y a los terceros de buena fe.

Por otra parte, el PSC puede suspender temporalmente la eficacia de los certificados si:

- Lo solicita el signatario o su representante.
- Lo ordena una autoridad judicial o administrativa.

3.3. *Dispositivo seguro de creación de firma electrónica*

Cualquiera que sea su clase, la firma electrónica es generada por un programa informático, denominado "Dispositivo de creación de firma"; programa que ejecuta su función mediante la aplicación de la clave privada del signatario.

Debe señalarse que existirá el correlativo "Dispositivo de verificación de firma" para desencriptar la firma del emisor aplicando la clave pública de éste (la del emisor).

Según el art. 19 del RDL 14/1999, a efectos del art. 2.f) del mismo cuerpo legal, para que se entienda que el dispositivo de creación de una firma electrónica es seguro, se exige:

> 1º Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.
>
> 2º Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.
>
> 3º Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.
>
> 4º Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

Del cumplimiento de estos requisitos depende que la Secretaría General de comunicaciones pueda certificar el dispositivo seguro de creación de firma electrónica, según se infiere del art. 24.1 de la Orden de 21-2-2001 que aprueba el Reglamento de acreditación de PSC y de certificación de determinados productos.

La vigencia de dicha certificación no podrá ser superior a 5 años, si bien, cabe su renovación.

El reconocimiento de tales certificados, emitidos por equivalente autoridad en el extranjero será automático sólo en el caso de que aquella pertenezca a un país de la Unión Europea. Sin embargo, si son otorgadas por países no miembros de la UE, las certificaciones de dispositivos seguros de

creación de firma electrónica serán válidas en España en virtud de Acuerdo Internacional de Mutuo Reconocimiento que sea vinculante para nuestro Estado.

El procedimiento a seguir para la obtención del certificado al que nos estamos refiriendo se explicará junto con el de acreditación de los prestadores de servicios de certificación.

3.4. *Prestador de servicios de certificación acreditado*

El último requisito, necesario para la plena validez jurídica de la firma electrónica, es que el certificado reconocido sea emitido por un PSC acreditado.

Al igual que haría la Directiva 1999/93, se establece el acceso de los PSC al mercado en régimen de libre competencia, sin sujeción a autorización previa, tanto para los establecidos en España como para los que procedan de alguno de los Estados miembros de la Unión Europea.

Las obligaciones que el RDL 14/1999 impone a los PSC consisten en:

- Poner a disposición del signatario los dispositivos de creación y verificación de firma.
- No almacenar ni copiar los datos de creación de firma, esto es, las claves privadas, salvo que el signatario lo solicite. La Directiva 1999/93 no exige esta obligación a todos los PSC, sino sólo a los que emitan certificados reconocidos.
- Informar al solicitante, antes de emitir el certificado, de su precio, condiciones de utilización, limitaciones de uso, y la forma en que el PSC garantiza su responsabilidad.
- Mantener un registro de certificados emitidos, señalando, en su caso, las razones de suspensión o pérdida de vigencia.
- Solicitar la inscripción como PSC en el Registro que a tal efecto se crea en el Ministerio de Justicia. Art. 7:

> Tienen obligación de inscribirse todos los PSC establecidos en España, para poder iniciar o continuar su actividad.
>
> Este Registro es público y podrá ser consultado por vía telemática y mediante la tradicional certificación registral.
>
> Deben constar los siguientes datos de los PSC inscritos:
> - nombre o razón social,
> - dirección web o de correo electrónico,
> - datos de verificación de su firma electrónica (su clave pública)

- si están acreditados (cuestión a la que me referiré después)y
- si pueden expedir certificados reconocidos (idem).

- En el caso de cesar en su actividad deben informar, con dos meses de antelación, al Registro de PSC y a los titulares de los certificados que hubieran emitido. Art. 13:

Al Registro deben comunicar:
- El destino ulterior de los certificados, especificando si los van a transferir o los van a dejar sin efecto.
- Si se iniciará un procedimiento de quiebra o suspensión de pagos.
- Otras circunstancias que puedan impedir la continuación de su actividad.

El Ministerio de Justicia cancelará de oficio la inscripción del PSC al cese de su actividad y se hará cargo de la información relativa a los certificados que dejen sin efecto.

A los titulares de los certificados que aún mantengan su validez deben pedir su consentimiento expreso para transferirlos a otro PSC. En otro caso deben dejarlos sin efecto.

- Responder de los daños y perjuicios causados: Art. 14.

- En el ejercicio de su actividad: cuando no cumplan las anteriores obligaciones. (Corresponde al PSC probar que actuó con la debida diligencia).
- Por el uso indebido del certificado: sólo cuando no haya consignado con claridad el límite de uso o el importe máximo de las transacciones que se pueden realizar con él.

Todo ello sin perjuicio de la protección que otorga la legislación a los consumidores y usuarios.

A los PSC que expidan certificados reconocidos se les exige además:

- Comprobar la identidad y demás circunstancias relevantes del signatario.
- Indicar fecha y hora de expedición y cese de los efectos del certificado.
- Demostrar la fiabilidad necesaria de sus servicios.
- Garantizar la rapidez y la seguridad en: la prestación del servicio, consulta al registro, extinción o suspensión de eficacia del certificado.
- Emplear personal cualificado.
- Utilizar sistemas y productos fiables que garanticen la seguridad técnica y criptográfica de los procesos de certificación.

- Tomar medidas contra la falsificación de certificados y, en su caso, garantizar la confidencialidad durante el proceso de generación de datos de creación de firma.
- Garantizar su responsabilidad patrimonial frente a los usuarios y terceros, mediante afianzamiento mercantil prestado por una entidad de crédito o un seguro de caución. Esta garantía cubrirá: Al menos, el 4 por 100 de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados. 1.000.000.000 de pesetas En caso de que no se limite el importe de las transacciones en las que puedan emplearse el conjunto de los certificados.
- Conservar, durante quince años, toda la información y documentación relativa a un certificado reconocido. Podrá realizarse por medios electrónicos.
- Informar, antes de expedir el certificado, de su precio, condiciones y límites de su uso, acreditación del PSC, procedimientos de reclamación y de resolución de conflictos. Esta información estará a disposición de terceros interesados y podrá comunicarse por medios electrónicos si las partes lo admiten.
- Utilizar sistemas fiables para almacenar certificados, de modo tal que: sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas; únicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones; pueda comprobarse la autenticidad de la información; el signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambios técnicos que afecten a los requisitos de seguridad mencionados.
- Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir.

Corresponde a la Secretaría General de Telecomunicaciones otorgar la acreditación a los PSC que cumplan los requisitos descritos.

El periodo de validez de dicha acreditación será de 4 años renovable.

La acreditación emitida por un país de la Unión Europea es reconocida por España sin más. Pero si son otorgadas por países no miembros de la UE, las acreditaciones de PSC sólo se reconocerán en virtud de Acuerdo de la UE con los mismos.

Algunos de los PSC más representativos son la Fábrica Nacional de Moneda y Timbre, mediante el proyecto CERES, la Agencia de Certificación Española ACE, el Servicio de Certificación de la Cámara de Comercio, Industria y Navegación de España CAMERFIRMA, la Fundación para el Estudio de la Seguridad de las Telecomunicaciones FESTE, Internet Publishing Services, S.L. IPSCA, ASTREA GLOBAL, VERISIGN, CERTISUR, IDENTRUS, y GLOBAL SIGN.

4. Procedimiento de acreditación y certificación

Mención singular merece la acreditación de PSC, la certificación de dispositivos seguros de creación de firma y la certificación de dispositivos de verificación de firma avanzada por cuanto tal acreditación/certificación los hace acreedores de mayor confianza por parte de los usuarios.

A esta cuestión se refiere la Orden de 21-2-2000 por la que se aprueba el Reglamento de acreditación de los PSC y la certificación de determinados productos de firma electrónica, que se propone fomentar la adopción de prácticas que garanticen la calidad y seguridad técnica de los servicios y productos de firma electrónica.

Se inaugura así un Sistema de Acreditación/Certificación que imprime un "sello de calidad" a los prestadores y productos que obtengan dicha acreditación/certificación.

El esquema competencial descansa en tres órganos diferentes: la Secretaría General de Comunicaciones, la Entidad Nacional de Acreditación y la Entidad de Evaluación.

La Secretaría General de Comunicaciones es la competente para otorgar la Acreditación/Certificación.

Ésta resolverá, fundamentalmente, en base al informe previo que ha de emitir una Entidad de Evaluación de PSC, acreditada a su vez por la ENAC (Entidad Nacional de Acreditación) u otro organismo equivalente de similares caracteres en el marco de la UE.

La Entidad de Evaluación juega un papel primordial porque obtener la Acreditación/Certificación va a depender en gran medida del sentido favorable o desfavorable de su informe.

Esa es la razón por la que un organismo superior, en este caso la ENAC, tiene que acreditar la condición de Entidad de Evaluación, atendiendo a los siguientes criterios:

- La forma en que garantizan su independencia respecto de los PSC y los fabricantes e importadores de productos de firma electrónica.
- Su competencia técnica.
- Sus locales y equipos.
- Los procedimientos de trabajo que emplean.

La ENAC otorgará la acreditación de "Entidad de Evaluación para informar sobre los PSC, sobre los productos de firma o sobre ambos", señalando su periodo de validez, y dará noticia de su otorgamiento a la Secretaría General de Comunicaciones.

Para obtener la Acreditación/Certificación es necesario cumplir una serie de requisitos diferentes en función de si se desea la Certificación de Dispositivos Seguros de Creación de Firma, la Certificación de Dispositivos de Verificación de Firma Electrónica Avanzada o la Acreditación de Prestador de Servicios de Certificación. Y en éste último caso también serán distintos los requisitos según el servicio que presten.

Recordamos a continuación dichos requisitos, la mayoría de los cuales han sido explicados anteriormente.

Requisitos a cumplir por los dispositivos seguros de creación de firma:

- Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.
- Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.
- Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.
- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

Requisitos a cumplir por los dispositivos de verificación de firma electrónica avanzada:

- Que la firma se verifica de forma fiable.

- Que el verificador puede establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.
- Que figura correctamente la identidad del signatario o, en su caso, consta claramente la utilización de un seudónimo.
- Que se verifica de forma fiable el certificado.
- Que puede detectarse cualquier cambio relativo a su seguridad.

Requisitos a cumplir por los PSC que emitan certificados:

- Poner a disposición del signatario los dispositivos de creación y verificación de firma.
- No almacenar ni copiar los datos de creación de firma, esto es, las claves privadas.
- Informar al solicitante, antes de emitir el certificado, de su precio, condiciones de utilización, limitaciones de uso, y la forma en que el PSC garantiza su responsabilidad.
- Mantener un registro de certificados emitidos.
- Inscribirse en el Registro de PSC del Ministerio de Justicia.
- Informar al Registro del Ministerio de Justicia y a los titulares de certificados del cese en su actividad, con carácter previo.
- Responder de los daños y perjuicios causados.

Requisitos a cumplir por los PSC que emitan certificados reconocidos, además de los anteriores:

- Comprobar la identidad y demás circunstancias relevantes del signatario.
- Indicar fecha y hora de expedición y cese de los efectos del certificado.
- Demostrar la fiabilidad necesaria de sus servicios.
- Garantizar la rapidez y la seguridad en la prestación del servicio, consulta al registro y extinción o suspensión de eficacia del certificado.
- Emplear personal cualificado.
- Utilizar sistemas y productos fiables que garanticen la seguridad técnica y criptográfica de los procesos de certificación.

- Tomar medidas contra la falsificación de certificados y, en su caso, garantizar la confidencialidad durante el proceso de generación de datos de creación de firma.
- Garantizar su responsabilidad patrimonial frente a los usuarios y terceros mediante afianzamiento mercantil prestado por una entidad de crédito o un seguro de caución. Esta garantía cubrirá al menos, el 4% de la suma de los importes límite de las transacciones en que puedan emplearse el conjunto de los certificados, o 1.000.000.000 de pesetas en caso de que no se limite el importe de las transacciones en las que puedan emplearse el conjunto de los certificados.
- Conservar durante 15 años toda la información y documentación relativa a un certificado reconocido. Podrá realizarse por medios electrónicos.
- Informar, antes de expedir el certificado, de su precio, condiciones y límites de uso, acreditación del PSC, procedimientos de reclamación y de resolución de conflictos. Esta información estará a disposición de terceros interesados y podrá comunicarse por medios electrónicos si las partes lo admiten.
- Utilizar sistemas fiables para almacenar certificados.
- Informar a cualesquiera usuarios de sus servicios de los criterios que se comprometen a seguir.

Requisitos a cumplir por los PSC que además presten otros servicios como:

- Consignación de la fecha y hora: se valorará: el grado de exactitud de los datos temporales que constaten, la disponibilidad de éstos para las partes, los mecanismos empleados para evitar su alteración.
- Otros servicios: fiabilidad del desarrollo de la actividad de que se trate.

El procedimiento se iniciará mediante instancia del PSC o del fabricante o importador de los dispositivos, dirigida a la Secretaría General de Comunicaciones.

Irá acompañada del Informe de Evaluación emitido por la Entidad de Evaluación.

Este informe determinará si se cumplen los requisitos, tomando como criterio: las normas que al efecto se indiquen en el DOCE, o en defecto de estas, las normas, especificaciones o recomendaciones, generalmente aplicadas en la industria, que determine la Secretaría General de Comunicaciones a propuesta de la ENAC, respetando la siguiente prelación a la hora de elegirlas:

1) Aprobadas por organismos europeos,
2) Aprobadas por Organismos internacionales,
3) Aprobadas por organismos nacionales.

Los números de referencia de estas normas serán publicados en el BOE.

En atención al contenido de estas normas se podrá reconocer distintos niveles de acreditación.

La Secretaría General de Comunicación otorgará la Acreditación/Certificación si se cumplen los requisitos y se ha aplicado el procedimiento de evaluación adecuado.

En caso contrario indicará qué procedimientos debe seguirse y qué pruebas debe realizarse.

La Secretaría General de Comunicación debe resolver la solicitud en el plazo de 6 meses, desde su entrada en el Ministerio, transcurrido el cual se entenderá estimada.

Dicha resolución será publicada en el BOE y si se trata de la Acreditación de un PSC además será notificada a la Comisión Europea.

5. Importancia de las entidades de evaluación

La importancia de las Entidades de Evaluación merece que prestemos atención a la Decisión 2000/709, de 6 de noviembre de la Comisión Europea que se dirige a los Estados miembro para que observen los criterios establecidos en ella a la hora de determinar la designación de las entidades de evaluación que informan la evaluación de los dispositivos de creación y verificación de firma electrónica.

Esta Decisión se dictó en desarrollo del art. 3.4 de la Directiva 1999/93 de Firma Electrónica para acentuar los principios de independencia y competencia técnica de las entidades de evaluación así como de su personal, de transparencia de sus prácticas, de acceso de los interesados a la información obrante en sus expedientes, de confidencialidad de dicha

información, de funcionamiento no discriminatorio y de garantía de su responsabilidad.