

La Firma Electrónica y los Servicios de Certificación.

De: Guillermo Díaz Bermejo.

guillermo.diaz@hispadata.com

Fecha: Diciembre 2007.

Origen: Noticias Jurídicas.

1. Introducción

Los rápidos avances tecnológicos y la dimensión mundial de Internet han hecho que, primero las empresas y después los ciudadanos y la administración, estén haciendo cada vez mas uso de las telecomunicaciones y de las nuevas tecnologías. Está siendo verdaderamente espectacular el crecimiento de las transacciones telemáticas que se vienen realizando con contenido económico.

El fuerte desarrollo de la sociedad de la información y de los elementos positivos que de ella se derivan, nos está llevando a una sociedad del conocimiento. Pero, en esta nueva sociedad llena de redes telemáticas abiertas y al alcance de cualquier ciudadano que tenga una conexión a Internet, aun existe mucha desconfianza respecto a la seguridad de las comunicaciones y más aun a la certeza jurídica de las transacciones comerciales.

Aquí podríamos preguntarnos ¿es segura la red para realizar transacciones con contenido económico y jurídico? Evidentemente la seguridad total no existe, pero entiendo que no deberíamos preocuparnos por ello, ya que en el comercio ordinario a pié de calle y en las transacciones convencionales tampoco existe seguridad plena.

Lo que si es una realidad es que la red se inició con sencillas páginas Web a un mínimo coste y con escasos niveles de seguridad. Mas adelante se fueron introduciendo medios de marketing, sistemas de pago, transacciones aun rudimentarias, pero con poco nivel de seguridad. Pero hoy en día podemos afirmar que existen implantados sistemas capaces de garantizar altos niveles de seguridad en la red, mayores incluso que en el negocio tradicional, ya que además de protección frente a riesgos, cubierta por entidades de seguros, existen mecanismos de seguridad que permiten el acceso a ciertos usuarios, sistemas de control de accesos, defensas contra hackers, etc.

Y, ha sido precisamente la utilización de las nuevas tecnologías en las transacciones comerciales y los inconvenientes que se planteaban desde el punto de vista jurídico, lo que ha llevado a los legisladores a la creación de sistemas seguros que garanticen la autenticidad, la integridad y la confidencialidad de los datos que se transmiten a través de la red.

La evolución tecnológica y la dimensión mundial de la red hicieron necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación y en esta dirección el gran reto fue encontrar un sistema electrónico alternativo que sirviera para sustituir a la firma manuscrita y que a la vez cumpliera sus mismas funciones, es decir, asegurar la identidad de las partes contratantes, y vincularlas en cuanto a las declaraciones de voluntad que realizaran, o lo que es lo mismo, al contenido del contrato.

La fórmula se ha encontrado en la "firma electrónica" y en los proveedores de "servicios de certificación". Consiste en un instrumento generado por documento electrónico relacionado con la herramienta de firma en poder del usuario, y que es capaz de permitir la comprobación de la procedencia y de la integridad de los mensajes intercambiados y ofreciendo bases para evitar su repudio. Con ello se alcanza el vínculo contractual o la autenticidad de un documento al igual que si se tratara de una firma manuscrita.

Marco jurídico:

Directivas Comunitarias:

- 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 Diario Oficial nº L 013 de 19/01/2000 P. 0012-0020.

Leyes Orgánicas:

- [Ley Orgánica 6/1985](#), de 1 de Julio, del Poder Judicial. Artículo Doscientos treinta.
- [Ley Orgánica 15/1999](#), de 13 de diciembre, de Protección de Datos de Carácter Personal.

Leyes:

- [Ley 11/2007](#), de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- [Ley 30/1992](#), de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- [Ley 24/2001](#), de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden social. Título V. de la acción administrativa. Capítulo XI. Acción administrativa en materia de seguridad jurídica preventiva. Sección VIII. Incorporación de técnicas electrónicas, informáticas y telemáticas a la seguridad jurídica preventiva.
- [Ley 24/2001](#), de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social. Título IV. Normas de gestión y organización administrativa. Capítulo III. Procedimientos. Artículo 68. Modificaciones de la Ley 30/1992, de Régimen Jurídico de las

Administraciones Públicas y del Procedimiento Administrativo Común para impulsar la administración electrónica.

- [Ley 34/2002](#), de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- [Ley 11/2002](#), de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
- DISPOSICIÓN ADICIONAL DECIMOSÉPTIMA, de la Ley 53/2002, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social. Modificación de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.
- Ley 53/2002, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social. Título I, Capítulo II Impuestos indirectos. Sección 1ª Impuesto del Valor Añadido. Artículo 4 Modificación de la Ley 37/1992, de 28 de diciembre, del IVA. Capítulo VII Régimen especial aplicable a los servicios prestados por vía electrónica.
- [Ley 59/2003](#), de 19 de diciembre, de firma electrónica.
- Anteproyecto de Ley de Impulso de la Sociedad de la Información, que persigue la adaptación de la firma electrónica en los procesos de negocios.

Reales Decretos-Ley:

- [Real Decreto Ley 14/1999](#), de 17 de septiembre, por el cual se regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

Reales Decretos:

- [Real Decreto 263/1996](#), de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.
- [Real Decreto 994/1999](#), de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- [Real Decreto 1114/1999](#), de 25 de junio, por el que se adapta la Fábrica Nacional de Moneda y Timbre a la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.
- [Real Decreto de 1289/1999](#), de 23 de julio, de creación de la Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías en España.
- [Real Decreto 111/2000](#), de 28 de enero, por el que se modifican determinados artículos del Reglamento General de Recaudación, aprobado por Real Decreto 1648/1990, de 20 de diciembre, en materia de ingresos correspondientes a declaraciones prestadas por vía telemática.

- [Real Decreto 1317/2001](#), de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, en materia de prestación de servicios de seguridad, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas.
- [Real Decreto 1029/2002](#), de 4 de octubre, por el que se establece la composición y el régimen de funcionamiento del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información.
- [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.
- [Real Decreto 292/2004](#), de 20 de febrero de 2004, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimientos de concesión.
- [Real Decreto 421/2004](#), de 12 de marzo, por el que se regula el Centro Criptológico Nacional.

Ordenes Ministeriales:

- [Orden de 13 de abril de 1999](#) por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre la Renta de las Personas Físicas.
- [Orden de 26 de julio de 1999](#) por la que se regulan las bases de datos y ficheros automatizados de carácter personal existentes en la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.
- Orden del 21 de diciembre de 1999 por la que se fijan los umbrales estadísticos de asimilación definidos en el artículo 28 del reglamento (CEE) 3330/91 del consejo y se autoriza la presentación de declaraciones intrastat por vía telemática.
- [Orden de 20 de enero de 1999](#) por la que se establecen las condiciones generales y el procedimiento para la presentación telemática de las declaraciones-liquidaciones mensuales de grandes empresas.
- [Orden de 21 de febrero de 2000](#) por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de Firma Electrónica.
- [Orden de 28 de febrero de 2000](#) por la que se establecen las condiciones generales y el procedimiento para la renovación y revocación del certificado de usuario X 509 V3 expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda al amparo de la normativa tributaria.
- [Orden de 26 de septiembre de 2000](#) por la que se establece el sistema para la presentación telemática por Internet de los documentos de circulación utilizados en la gestión de los impuestos especiales.

- [Orden de 21 de diciembre de 2000](#) por la que se establecen las condiciones generales y el procedimiento para la presentación telemática por Internet de las declaraciones correspondientes a los modelos 117,123,124,126,128,216,131,310,311,193,198,296 y 345.
- [Orden de 11 de Diciembre de 2001](#) por la que se regulan los ficheros de datos de carácter personal de la FNMT-RCM.
- [Orden de 21 de febrero de 2000](#) por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.
- [Orden ECO/2579/2003, de 15 de septiembre](#), por la que se establecen normas sobre el uso de la firma electrónica en las relaciones por medios electrónicos, informáticos y telemáticos con el Ministerio de Economía y sus Organismos adscritos.
- [Orden HAC/1181/2003, de 12 de mayo](#), por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.
- [Orden PRE/1551/2003, de 10 de junio](#), por la que se desarrolla la disposición final primera del 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.

2. La Firma Electrónica

Definición

La Directiva 1999/93/CE del Parlamento Europeo y del Consejo de la Unión Europea, creó un marco jurídico para la firma electrónica y para determinados servicios de certificación, con el fin de garantizar un adecuado funcionamiento del mercado comunitario y además formuló la necesidad de buscar acuerdos transfronterizos para garantizar la interoperabilidad a nivel mundial.

Esta Directiva pretende mantener un marco jurídico coherente en toda la Comunidad, conscientes de que ese marco claro aumentará la confianza en las nuevas tecnologías. Igualmente contribuye al uso y al reconocimiento legal de la firma electrónica. Es importante alcanzar el equilibrio entre las necesidades de los consumidores, de las empresas y de la propia administración y además de todo ello, para contribuir a la aceptación general de los métodos de autenticación electrónica, debe de garantizarse la admisibilidad de la firma electrónica como prueba en procedimientos judiciales de los estados miembros.

Para incrementar la confianza de los usuarios en sus comunicaciones y en el comercio electrónico, los proveedores de servicios de certificación deberán de observar las normativas sobre protección de datos y el respeto de la intimidad.

Esta Directiva entiende por "firma electrónica".los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación..." (Artículo 2.1).

Igualmente distingue la "firma electrónica" de la denominada "firma electrónica avanzada", un especie de firma electrónica "cualificada", y la define como "...la firma electrónica que cumple con los siguientes requisitos: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; y d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable." (Artículo 2.2).

La firma electrónica avanzada comúnmente la conocemos como "firma digital". Desde el punto de vista jurídico, esta distinción resulta importante, pues los efectos jurídicos de una firma electrónica serán equiparables a los de la firma manuscrita únicamente cuando se trate de una firma electrónica avanzada o firma digital artículo 5).

La Ley española 59/2003, de firma electrónica, en su artículo 3, define igualmente la firma electrónica de este modo:

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Funcionamiento (Conceptos de PKI)

La firma electrónica se instrumenta mediante un sistema de "criptografía asimétrica".

Conviene que invirtamos unas pocas líneas en explicar qué es la criptografía, para mejor comprensión de los lectores que en principio se supone tienen formación jurídica, pero no técnica.

La criptografía es la rama de las matemáticas que estudia el cifrado de información legible e información que no puede ser leída directamente, al tener que ser descifrada. La criptografía es el arte de cifrar y de descifrar los mensajes intercambiados entre un emisor y un receptor.

Los sistemas de criptografía utilizados en las tarjetas digitales, utilizan un algoritmo asociado a una llave para convertir un mensaje inicial en un mensaje codificado que no puede ser decodificado más que mediante un algoritmo de decodificación asociado a una llave de descifrado.

Existen dos esquemas clásicos de encriptación: La simétrica que obliga a al emisor y receptor del mensaje a utilizar la misma clave para encriptar y desencriptar el mismo (como por ejemplo el criptosistema DES, *Data Encryption Standard*, desarrollado por IBM), y la encriptación *asimétrica* o criptográfica de claves públicas que está basada en el concepto de pares de claves, de forma que cada uno de los elementos del par (una clave) puede encriptar información que solo la otra componente del par (la otra clave) puede desencriptar.

El par de claves se asocia con un solo interlocutor, así un componente del par (la clave privada) solamente es conocida por su propietario mientras que la otra parte del par (la clave pública) se publica ampliamente para que todo el mundo pueda verla (en este caso destaca el famoso criptosistema RSA cuyas iniciales son las de sus creadores: Rivest, Shamir y Adelman). Esta clave pública es dada por un tercero que es el conocido como "*autoridad de certificación*".

El sistema se compone de cuatro etapas:

1. A cada usuario se le asigna una clave pública.
2. Igualmente, cada usuario posee una clave privada que sólo él conoce, y que puede cambiar cuantas veces desee.
3. Se crea un directorio de claves públicas accesibles al público general.
4. El usuario de la red envía sus mensajes con la clave pública del destinatario encriptada con su clave privada. El destinatario sólo podrá abrir el mensaje con la clave pública junto con su clave privada.

Es un método que habitualmente se viene utilizando con total aceptación de los usuarios, ya que garantiza adecuadamente la seguridad y la confidencialidad de lo que se transmite.

Podemos decir por tanto, que la firma electrónica es un bloque de caracteres que se añade a un documento o fichero para acreditar quien es su titular (autenticación) y también para detectar que no haya habido ninguna manipulación subsiguiente de los datos (integridad). En la firma el titular utiliza el código personal que el solo conoce (criptografía asimétrica) y esto es lo que impide que después se pueda negar su autoría (no revocación o no repudio). De este modo el titular de la firma queda vinculado por el documento emitido e igualmente la validez de la firma podrá ser averada por cualquier persona que disponga de la clave pública de titular.

Para la firma electrónica "*escrita*" se necesitará un pad o dispositivo de firma electrónica que sea capaz de capturar o registrar la firma escrita y todos sus aspectos, tales como tiempo, presión y trazado. También necesitará un programa capaz de codificar la firma electrónica de modo seguro y asimétrico en un documento electrónico con poder probatorio. El sistema que utilice habrá de ser capaz de captar la firma escrita de modo que, en caso de juicio, y a pesar de tratarse de una firma electrónica, un grafólogo pueda verificar su autenticidad.

Al realizar una firma electrónica, el sistema informático del titular introduce un algoritmo sobre el documento a firmar obteniendo un extracto de longitud determinada y específico para este documento de modo que si se produjere una mínima modificación posterior, se generaría un extracto totalmente diferente y por ello, no se correspondería con el original que firmó el titular. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits, se somete seguidamente a un cifrado mediante la clase secreta del titular.

El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA. Con el se obtiene un extracto final cifrado con la clave privada del autor, que se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

Ahora, una vez realizada la firma electrónica habrá de determinarse su validez y para ello el software del receptor, previa introducción en el mismo de la clave pública de remitente (obtenida a través de una Autoridad de Certificación), descifrará el extracto cifrado del autor y a continuación calculará el extracto hash que le correspondería al texto del mensaje y, si el resultado coincide con el extracto anteriormente descifrado, se considera válida; en caso contrario significaría que el documento ha sufrido una modificación posterior y por tanto no es válido.

Ventajas

- Mediante la firma electrónica se suprime el choque de medios, es decir, se evita la impresión en papel para la firma y se protegen adecuadamente los datos transmitidos.
- Se facilita la identificación tanto del emisor del mensaje como del receptor.
- Como la firma es intransferible, la firma electrónica escrita es una forma de identificación que al contrario que las contraseñas y llaves no se puede robar ni olvidar.
- La firma es sin duda un acto voluntario y además permite que el contenido de los mensajes lanzados a la red, sea irrevocable y no repudiable.
- La firma es un proceso reconocido por todos que da constancia de un acuerdo voluntario.

- El sujeto firmante no tiene que ser socio de ninguna compañía certificadora para poder utilizar la firma electrónica escrita.
- La firma capturada mediante la firma electrónica escrita puede ser examinada por expertos grafólogos (comparando, por ejemplo, la firma electrónica contra otra realizada sobre papel).

Desventajas

El sistema por sí solo no es infalible y los riesgos no se pueden eliminar en su totalidad, y por ello es necesario utilizar un adecuado sistema de distribución de claves públicas.

De otra parte, el sistema de distribución deberá estar debidamente protegido y debe ser administrado por una persona o entidad autorizada expresamente para ello.

3. Certificados de Seguridad Electrónicos

Concepto

Para generar confianza en el usuario, el entorno Internet ha de ser seguro. Por ello los estados han venido trabajando para resolver esos problemas hasta llegar a definir lo que ya podemos llamar "identidad digital". Esto es algo así como un DNI o identificador digital único dentro de la red que permite a su poseedor ser identificado como tal dentro de la misma.

Los certificados electrónicos son dispositivos que posibilitan el almacenamiento de diversos datos relativos al propietario de los mismos (datos personales, claves, etc) y permiten identificarlo en la red, garantizando tanto la emisión de los datos, como su recepción, la integridad de la información transmitida, la confidencialidad y lo más importante, el no repudio de la transacción.

En el marco jurídico comunitario, los certificados de seguridad han sido expresamente definidos como: "...la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta..." (Artículo 2.9 de la Directiva 1999/93/CE).

La Ley 59/2003 de Firma Electrónica, en su [a href="http://noticias.juridicas.com/base_datos/Admin/I59-2003.t2.html#a6">](http://noticias.juridicas.com/base_datos/Admin/I59-2003.t2.html#a6) artículo 6, nos da el siguiente concepto: Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. El firmante es 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.

Estos certificados deben ser emitidos por las *autoridades de certificación*, también conocidas con el nombre de *proveedores de servicios de certificación*. Al igual que existe una firma electrónica general y otra cualificada, en el caso de los certificados de seguridad se habla también de *certificados ordinarios* y *certificados reconocidos*. Éstos últimos son certificados que ofrecen mayores garantías, ya que reúnen una serie de requisitos que aumentan su seguridad:

El artículo 11 de la referida Ley nos dice que como mínimo un certificado reconocido incluirá los siguientes datos:

1. La indicación de que se expiden como tales.
2. El código identificativo único del certificado.
3. La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
4. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
5. La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
6. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
7. El comienzo y el fin del período de validez del certificado.
8. Los límites de uso del certificado, si se establecen.
9. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

1. Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.
2. Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
3. 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.

4. Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Utilidades del Certificado de Seguridad Electrónico

El certificado de seguridad electrónico puede ser utilizado para muchas aplicaciones, desde la firma de documentos hasta la identificación dentro de una organización. Un certificado de seguridad es una identidad digital, y por tanto como identidad, sirve entre otros, para los siguientes usos:

1. Firma digital. El certificado de seguridad se utiliza para firmar todo tipo de documentos digitales, desde simples e-mails hasta los más complejos contratos mercantiles. Esto implica garantía de no repudio, de conocimiento inequívoco de quien es el emisor del documento y de la integridad del documento, es decir, que el documento firmado es el original y que nadie ha modificado su contenido después de su firma. También es usado para firmar ciertas operaciones, como por ejemplo, formalizar una orden de transferencia que se pueda realizar en un *home-banking*, esto da la garantía a las partes de que dicha orden de transferencia sólo la puede realizar el titular, y la entidad bancaria guarda la prueba de dicha orden y capacidad.
2. Seguridad en la comunicación. El certificado sirve para codificar una comunicación entre dos personas, haciendo que toda la información transmitida sea confidencial. Con ello se garantiza que cualquier documento enviado por una persona a otra estará cerrado y sólo podrá ser abierto por su legítimo destinatario. A su vez es igualmente aplicable cuando el emisor o bien el receptor no son una persona sino un servidor de Internet, y por tanto, la información enviada o recibida de este servidor estará codificada con el fin de que sólo el auténtico receptor pueda leerla. Un ejemplo de ello lo tenemos en la mayoría de páginas Web donde se nos pide el número de una tarjeta de crédito para efectuar un pago. Están utilizando certificados digitales, y con ello garantizan que solo el comercio podrá acceder a la información del número de la tarjeta de crédito (para verificar que dicho comercio realiza la transacción de forma segura, se puede ver que se cierra el candado situado en la parte inferior de los navegadores, que normalmente está abierto).
3. Seguridad entre las partes: Uno de los problemas se plantean es el de que a veces no estamos seguros de que el receptor sea realmente quien dice ser y por lo tanto el emisor puede tener dudas acerca de si enviar una información o no. Aquí es donde la autoridad de certificación que es la parte de confianza tiene un papel importante puesto que certifica a este como el auténtico receptor. Un caso específico es el de los servidores Web, muchas veces podemos tener dudas acerca de si la página Web que estamos consultando pertenece realmente a la empresa que creemos. La consulta del certificado digital que pueda tener esta Web nos va a certificar que realmente esta Web pertenece a la empresa.

4. Identificación ante un acceso restringido. Hasta ahora en el momento de entrar en un espacio digital restringido se utilizaba el par *login + password*, sistema con un nivel de seguridad muy bajo. Todo indica que el siguiente sistema de identificación será el certificado digital. En el momento de entrar en Intranets, accesos a una red local, a un servidor determinado, o incluso a aplicaciones específicas, la tecnología utilizada será la del certificado de seguridad electrónico. En estos momentos, la mayoría de los grandes fabricantes del sector de las tecnologías de la información está trabajando en adaptar sus productos a esta tecnología. Un caso a resaltar es el de la administración: uno de los grandes obstáculos que ha tenido hasta hoy la administración para su completo desarrollo en la red, y en concreto en la puesta a disposición de los ciudadanos a través de Internet de un conjunto de servicios y trámites, era la necesidad de garantizar la identidad del administrado. En distintos servicios, es básico el poder garantizar esta, puesto que la información que ha de dar la administración para un completo desarrollo de este trámite es confidencial, como por ejemplo la consulta previa al pago de multas. Esta utilidad del certificado digital, más la necesidad del no-repudio por parte de la administración y del administrado está llevando a estas a implantar dicha tecnología en su relación con los administrados.
5. Firma de software. El certificado digital es utilizado para firmar *software*. Esto permite a la entidad que va a utilizar el *software* garantizar que este es el original, conocer quien lo ha creado, y muy importante, que con posterioridad a su firma, nadie lo ha modificado. Esto garantiza que dicho *software* no contiene virus, y si los contiene, es el propio creador del *software* quien los ha incorporado, pudiendo ir en contra de este con una prueba firmada.

Clases de Certificados

Certificados de Servidor

El Certificado de Servidor aporta a un WEB SITE la característica de seguridad y confianza necesaria para poder entablar cualquier tipo de relación con los potenciales usuarios. Es el elemento necesario para poder aprovechar la gran vía de negocio que supone el comercio a través de Internet con la máxima rentabilidad y seguridad. Los Certificados de Servidor permiten incorporar el protocolo SSL (*Secure Socket Layer*) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos personales, datos de tarjetas de crédito, números de cuenta, passwords, etc. Cobra especial importancia dentro del área del comercio electrónico, donde la seguridad de los datos es la principal barrera para el desarrollo de este sistema.

Certificados para WAP

Los Certificados WAP permiten a las WEB comerciales existentes y de nueva creación la realización de transacciones seguras con los consumidores móviles. Los nuevos portales basados en transacciones móviles seguras expandirán el comercio electrónico entre los usuarios móviles y los WEB SITES dedicados al comercio. Los servidores WAP necesitan proporcionar seguridad y confianza a los usuarios potenciales. Esta es la base para que se establezca una contraprestación que satisfaga a ambas partes. Los Certificados WAP permiten mantener conexiones seguras basadas en encriptación y autenticación con dispositivos de telefonía móvil.

Certificados Personales

Otorgan seguridad a los correos electrónicos basados en un *standard S/MIME*. Podrá firmar o cifrar los mensajes de correo para asegurarse de que sólo el receptor designado sea el lector de nuestro mensaje.

CAs Corporativas

Es la solución óptima para las empresas que quieran disponer de un sistema de generación de cualquier tipo de Certificado para sus usuarios (trabajadores, proveedores, clientes, etc.) y servidores. Una CA Corporativa puede generar cualquier tipo de certificado, ya sean Certificados Personales, de Servidor, para WAP, para firmar Código e incluso para IPSec-VPN. En función del tipo de funcionalidad que se le quiera dar a la CA se deberá escogerse un diferente tipo de CA Corporativa.

Certificados para firmar Código

El Certificado para la Firma de Código, permitirá a un Administrador, Desarrollador o Empresa de Software firmar su Software (ActiveX, Applets Java, Plug-ins, etc.) y Macros, y distribuirlo de una forma segura entre sus clientes.

Certificados para IPSec-VPN

Los Certificados para VPN son los elementos necesarios para que la empresa aproveche las cualidades y ventajas de la utilización de las VPNs de un modo plenamente seguro. Las VPNs surgen como consecuencia de la creciente demanda de Seguridad en las comunicaciones ya sea entre Router-Router o Cliente-Servidor. La apertura de las redes corporativas a empleados remotos (con gran importancia en el caso del Teletrabajo, sucursales, business, partners o clientes.

Ventajas

Mediante la utilización de los certificados electrónicos, tanto las transacciones electrónicas como cualquier otra clase de transmisión de información a través de Internet, estará más protegida, originándose de esta forma una mayor

confianza y seguridad en los usuarios en relación con los contenidos de los mensajes enviados y recibidos.

Su mayor ventaja es la certeza que produce sobre la identificación de la persona que envía un determinado mensaje, ya que autentifica fehacientemente la identidad del emisor.

Validez de los Certificados de Seguridad

a) Vigencia

Los certificados de seguridad son válidos por un período de tiempo determinado: en el propio certificado hay que indicar la fecha y hora del comienzo y la extinción de su validez. La duración del período de validez de los certificados no debe ser demasiado extensa, pues, en este caso, las claves protegidas se encuentran expuestas a mayores riesgos de ser copiadas, apropiadas o utilizadas ilegítimamente por terceros.

Algunos países, limitan la duración máxima de los certificados entre tres y cinco años. Una firma electrónica sólo será válida si se expidió dentro del período de validez del certificado de seguridad correspondiente. En caso de que la firma electrónica haya sido expedida fuera de este período, las transacciones celebradas utilizando dicha firma carecen de seguridad jurídica.

En España, la Ley 59/2003 reseña como causa de extinción de la vigencia de un certificado, las siguientes

1. Expiración del período de validez que figura en el certificado.
2. Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
3. Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.
4. Resolución judicial o administrativa que lo ordene.
5. Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
6. Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
7. Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del

certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

8. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

b) Revocación

Por regla general, los certificados serán revocados una vez que cumplan el período temporal de validez por el cual fueron creados. Sin embargo, también cabe la posibilidad de que el certificado sea objeto de una revocación anticipada, generalmente cuando la clave privada ha sido puesta en peligro (perdida o extraviada), por lo que puede ser utilizada por personas no autorizadas o para fines ilegítimos.

Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

1. Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
2. Resolución judicial o administrativa que lo ordene.
3. La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c y g del artículo 8.1.
4. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación. Los certificados perderán su validez desde el momento mismo en que concurra alguna de las causas de revocación, si bien, en algunos casos, se requiere que dicha revocación sea debidamente publicada por el proveedor de servicios.

4. Servicios de Certificación

La identidad en la Red está basada en la existencia de las terceras partes de confianza, que son las entidades que verifican y dan fe de la identidad de los internautas. Los Servicios de certificación son entidades cuyo fin es el de

verificar la identidad y otros datos relevantes de una persona para que ésta pueda identificarse en la Red.

Existen diferentes entidades de certificación que emiten certificados de seguridad para personas, para empresas, para colectivos, para colegios profesionales, para universidades o para entes públicos. Entre otros tenemos los siguientes prestadores: *AC Abogacía, ANCERT (Agencia Notarial de Certificación), ANF AC, Autoritat de Certificació de la Comunitat Valenciana (ACCV), Banesto CA, Camerfirma, CATCert, CERES (Fábrica Nacional de Moneda y Timbre), CICCOP, Dirección General de la Policía y de la Guardia Civil, Firmaprofesional S.A., Izempe SA, Telefónica Empresas...*

Resulta evidente que los certificados emitidos por cada prestador suelen estar vinculados a determinados colectivos de usuarios. Así, por ejemplo, un DNI electrónico emitido por la Policía será inicialmente aceptado para realizar trámites con la administración pública, mientras que un certificado emitido por un Colegio profesional (AC Abogacía) será aceptado como instrumento electrónico que identifique al colegiado respecto a su actividad profesional, o un certificado de las cámara de comercio (Camerfirma) será aceptado por las empresas adheridas en sus transacciones comerciales.

Estas entidades, son la parte fiable que acredita la ligazón entre una determinada clave y el usuario propietario de la misma y actúan como una especie de notario electrónico que garantiza la veracidad de la información puesta en la red. En definitiva, son los órganos encargados de otorgar confianza en la infraestructura de las claves públicas, ya que resulta absolutamente necesario confiar en una tercera parte de toda solvencia que garantice la identificación de una persona física o jurídica a través de una clave pública.

Conforme al artículo 2.11 de la Directiva 1999/93/CE los Proveedores de Servicios de Certificación (PSCs), son "...la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica También son conocidos como *prestadores de servicios de certificación o entidades de certificación*.

El artículo 2 de la Ley 59/2003 los define como la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Los servicios de certificación podrán ser prestados tanto por instituciones públicas como privadas, sin que para ello deba solicitarse una licencia previa. No obstante, los servicios de certificación deberán cumplir con ciertos requisitos y obligaciones que se exponen a continuación.

Obligaciones

Conforme a los artículos 17 a 21 de la Ley 59/2003, podemos clasificar las obligaciones a que están sujetos los prestadores de servicios de certificación, del siguiente modo:

a) Obligaciones generales

Los PSCs que deseen emitir cualquier clase de certificado, deberán cumplir las siguientes obligaciones de carácter general:

- comprobar la identidad y demás datos personales del solicitante
- facilitar al signatario el dispositivo de creación y verificación de firma
- no almacenar ni copiar los datos de creación de firma del solicitante
- antes de la emisión del certificado, deberán informar al solicitante sobre el precio, condiciones de uso y limitaciones del certificado
- mantener un registro público de los certificados emitidos
- en caso de cese de su actividad, deberán comunicarlo este hecho con la debida antelación (mínimo dos meses) a los titulares de los certificados
- estar inscritos en el Registro de Prestadores de Servicios de Certificación

b) Obligaciones específicas

Además de las citadas obligaciones generales, los PSCs que emitan certificados reconocidos deberán cumplir las siguientes obligaciones específicas:

- indicar la fecha y hora de la expedición y/o revocación del certificado
- demostrar fehacientemente la fiabilidad de sus servicios
- garantizar rapidez y seguridad en la prestación de sus servicios
- contar con empleados cualificados para los servicios ofertados
- utilizar sistemas y productos fiables que garanticen la seguridad técnica de la certificación
- contar con medidas para prevenir la falsificación de certificados
- utilizar sistemas fiables y seguros de almacenamiento
- disponer de recursos económicos suficientes, que sirvan de garantía frente a una eventual responsabilidad por daños y perjuicios causados negligentemente
- conservar durante un período de tiempo (generalmente 15 años) la información relativa al certificado emitido, para el caso de que dicha información pueda ser utilizada como prueba en algún procedimiento judicial o administrativo.

El conjunto de obligaciones citadas (generales y específicas) tiene como objetivo proporcionar seguridad y confianza en la prestación de los servicios de certificación y servir de garantía de calidad del servicio.

Responsabilidad

Conforme al artículo 23 de la Ley 59/2003, como principio de carácter general, los PSCs responden civilmente por los daños y perjuicios que pudieran causar a

sus usuarios o a terceros cuando actúen con negligencia en el cumplimiento de sus obligaciones. Los PSCs son responsables, por tanto, no sólo frente al titular del certificado sino también frente a cualquier tercero que se vea perjudicado por actos u misiones de los PSCs. Se trata de una la responsabilidad subjetiva contractual y extracontractual.

Además, una vez revocado el certificado los PSCs seguirán estando sujetos a responsabilidad en cierta medida. Ni la normativa comunitaria ni la doctrina han fijado un criterio claro para esclarecer el alcance de esta responsabilidad. Por un lado, se considera que los PSCs deben estar sujetos a una responsabilidad limitada. Esto es, los PSCs responderían únicamente de los daños y perjuicios que causaran por el incumplimiento negligente de la obligación de publicar la revocación del certificado o de la obligación de inscribirlo en el registro de certificados del PSC, con lo cual, el titular acabaría asumiendo todos los riesgos derivados de un posible robo o extravío de la clave. Por otro lado, se intenta extender la responsabilidad de los PSCs para que respondan también por las posibles utilizaciones ilegítimas de la clave de firma.

Límites de la responsabilidad

Entre los límites a la responsabilidad de los PSCs que admite la doctrina se encuentran los siguientes:

Límites de uso:

Los PSCs podrán limitar su responsabilidad emitiendo el certificado únicamente para un uso determinado (ciertos ámbitos, transacciones, operaciones, etc). Con esta limitación, el PSC no será responsable cuando el certificado se utilice más allá de la finalidad para la cual fue expedido.

Esta limitación debe establecerse de forma expresa, clara e inequívoca en el propio certificado, facilitando con ello que los terceros conozcan la limitación existente.

Limites de cuantía:

Estos límites se dirigen a proteger a los PSCs, limitando su responsabilidad a un importe máximo relacionado con el valor de las transacciones realizadas utilizando el certificado.

En este sentido, los PSC tienen dos opciones:

1. establecer que el certificado sólo sea utilizado en transacciones que no excedan de una determinada cuantía. Por ejemplo, emisión de un certificado que sólo puede ser utilizado en operaciones cuyo monto no exceda de 24 millones de euros.

Inconveniente: El certificado puede ser utilizado en una gran cantidad de operaciones de distinto tipo, siempre que no se superaran los límites cuantitativos establecidos, por lo cual, la responsabilidad del PSC se incrementa.

2. establecer que el certificado sólo pueda utilizarse hasta una determinada cantidad máxima con independencia de las transacciones que se realicen. Por ejemplo, un certificado válido hasta que se cubra la cantidad total de 24 millones de euros.

Inconveniente: Si bien los derechos de los PSCs se encuentran más protegidos, ésta limitación perjudica los intereses de los usuarios de los certificados, pues éstos deberán estar controlando en todo momento el valor total de las operaciones realizadas con el certificado.

5. Conclusión

El objetivo de la firma electrónica es que ésta sirva para producir los mismos efectos que la firma manuscrita. Por tanto, debe reunir los requisitos de integridad y autenticidad, así como garantizar la imposibilidad de rechazo o repudio del contenido firmado. Cualquier firma electrónica no puede ser equiparada de forma absoluta a una firma manuscrita.

Para que ello ocurra, la firma electrónica debe cumplir ciertos requisitos:

1. debe tratarse de una firma electrónica avanzada;
2. la firma debe basarse en un certificado reconocido;
3. la firma debe haber sido producida por un dispositivo seguro de creación de firma;

La normativa comunitaria impone a los Estados miembros la obligación de reconocer plenamente los efectos jurídicos y validez de la firma electrónica, siempre y cuando ésta cumpla los requisitos previamente citados (Art. 5.1 de la Directiva 1999/93/CE).

Es importante recordar que si la firma electrónica cumple los requisitos citados, ésta también podrá ser utilizada como medio de prueba en cualquier procedimiento judicial.

En España, la Ley 59/2003 viene a regular la firma electrónica, su eficacia jurídica y la prestación de los servicios de certificación.

Guillermo Díaz Bermejo.

Hispadata Solutions, S.L.

guillermo.diaz@hispadata.com