Cómo aplicar la nueva normativa sobre la firma electrónica

Fernando Ramos Suárez - Legalia

Real Decreto Ley 14/1999 de 17 de septiembre sobre Firma Electrónica

El gran intercambio electrónico de información que en la actualidad se esta produciendo gracias al avance de las Nuevas Tecnologías, constituye una poderosa herramienta que está destinada a producir enormes cambios en las relaciones sociales y económicas. La educación, la cultura, el comercio, el trabajo etc. son campos de nuestra vida que están ampliamente influenciados por el flujo de la información, es por tanto imprescindible dotar de una infraestructura que garantice un trafico jurídico mercantil seguro.

En este sentido estamos experimentando en la actual sociedad de la información un profundo cambio que nos lleva hacia el ocaso de la civilización del papel, de la firma manuscrita y por consiguiente del monopolio de la escritura en la realidad documental. Esta revolución se esta produciendo en parte con la nueva entrada en vigor del Real Decreto Ley 14/1999 de 17 de septiembre sobre Firma Electrónica (en adelante RDL)

A través de este RDL se persigue establecer una regulación clara de la Firma Electrónica, que le otorgue igual eficacia jurídica que la firma manuscrita. Para la consecución de este objetivo es requisito sine qua non la intervención en el proceso de las terceras partes de confianza o Thrusted Third Parties (TTP). Por tanto es contenido obligado de la Ley establecer un régimen jurídico aplicable a las TTP o a los prestadores de servicios de certificación.

Con la llega del EDI (Electronic Data Interchange) en los años ochenta, se introduce la necesidad de que una tercera parte intervenga en las relaciones comerciales entre empresas. La función de esta tercera parte es dar fe de que las transacciones electrónicas de datos se han producido.

La extensión de la informática y la expansión de las redes de ámbito mundial, ha hecho incrementar los peligros para la información que circula y se almacenada en los sistemas informáticos. Por ello la Sociedad de la Información ha realizado un esfuerzo considerable para garantizar la seguridad de dichas redes telemáticas.

En este sentido se han aportado una serie de soluciones, propuestas por los organismos de normalización, para evitar los posibles ataques y operaciones ilegales a los que pueden estar sometidas las redes telemáticas. Estas soluciones consisten en dotar a las redes telemáticas de una serie de servicios de seguridad que utilizan en su mayoría técnicas criptográficas como herramienta básica. La encriptación podemos decir que está basada en dos componentes: un algoritmo y una clave. Actualmente se han podido desencriptar algoritmos de 40 bits en no mucho tiempo, siendo por tanto imprescindible para una comunicación segura la utilización de un algoritmo que admita una clave de 128 bits, dichos algoritmos son muchísimo más seguros pero también más lentos, por ello hay que encontrar un termino medio en la aplicación de dichos mecanismos de seguridad.

Hay dos tipos de encriptación, la encriptación simétrica que obliga a los dos interlocutores (emisor y receptor) del mensaje a utilizar la misma clave para encriptar y desencriptar el mismo (como por ejemplo el criptosistema `DES¿ desarrollado por IBM, Data Encryption Standard), y la encriptación asimétrica o criptografía de claves públicas la cual está basada en el concepto de pares de claves, de forma tal 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 sólo interlocutor, así un componete 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 todos la conozcan (en este caso destaca el famoso criptosistema RSA cuyas iniciales son las de sus creeadores Rivest, Shamir y Adelman).

Según el documento de la ISO (International Standard Organization) que describe el modelo de referencia OSI, presenta en su parte 2 una Arquitectura de seguridad. (`Information Processing Sistems. OSI Reference model- Part 2: Security Architecture¿. ISO/IEC IS 7498-2, Jul. 1988). Según esta arquitectura de seguridad para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes servicios de seguridad:

- Autenticación de entidad.
- Control de acceso.
- Confidencialidad de los datos.
- No repudio.

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del modelo de referencia OSI los siguientes mecanismos de seguridad:

Cifrado:

Utilizando sistemas criptográficos simétricos o asimétricos.

Control de acceso:

Mecanismo que se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee..

Firma digital:

Supone el cifrado con una componente secreta del firmante, de la unidad de datos. La firma digital descrita por la OSI utiliza un esquema criptográfico asimétrico. La firma se obtiene a través de una cadena que contiene el resultado de cifrar con RSA, aplicando la clave privada del firmante, a una versión comprimida del texto a firmar. Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, luego comprime el texto original recibido con igual función que el emisor y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene la garantía de que el texto no ha sido modificado. A través de este mecanismo se pueden garantizar casi todos los servicios de seguridad determinados por la ISO.

Pero aquí no acaban los problemas ya que en todos estos procedimientos de encriptación asimétrica existe un punto débil. Supongamos por ejemplo, que un usuario A quiere enviar un mensaje cifrado a otro usuario B. En una comunicación anterior un tercer usuario C, ha conseguido engañar a A y le ha hecho creer que la clave pública de B es una que él le ha proporcionado. Cuando A envíe su mensaje cifrado con la clave pública , C podrá interceptarlo y descifrarlo. El problema se resuelve gracias a un intermediario cuya clave pública es conocida por todos los interesados y en el cual todos confían. Cuando alguien necesita de una clave de otro usuario se la solicita al intermediario, que la envía en un mensaje firmado lo que garantiza la validez de la clave. En Internet estos intermediarios serán unos programas ejecutandose en unos ordenadores, los cuales son denominados

servidores de claves o Autoridades de Certificatión.

¿Que es una firma digital? ➦

Un firma digital, es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrica), a la que sólo el tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio). De esta forma, el autor queda vinculado al documento de la firma. Por último la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

¿Como se realiza una firma digital? ➦

El software del firmante aplica un algoritmo hash sobre el texto a firmar, obteniendo un estracto de longitud fija, y absolutamente específico para ese mensaje. Un mínimo cambio en el mensaje produciría un extracto completamente diferente, y por tanto no correspondería con el que originalmente firmó el autor. Los algoritmos hash más utilizados son el MD5 ó SHA-1. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits (según el algoritmo utlilizado), se somete a continuación a cifrado mediante la clave secreta del autor. El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA. De esta forma obtenemos un extracto final cifrado con la clave privada del autor el cual 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.

¿Como se comprueba la validez de la firma digital? ➦

Como he comentado antes es necesario la clave pública del autor para poder verificar la validez del documento o fichero. El procedimiento sería el siguiente: el software del receptor previa introducción en el mismo de la clave pública del remitente (obtenida a través de una autoridad de certificación), descifraría el extracto cifrado del autor, a continuación calcularía el extracto hash que le correspondería al texto del mensaje, y si el resultado coincide con el extracto anteriormente descifrado se consideraría válida, en caso contrarío significaría que el documento ha sufrido una modificación posterior y por tanto no es válido.

Hasta este momento hemos conseguido la autenticación del documento, su integridad y la imposibilidad de repudio del mismo por parte del autor. Através de otros mecanismos como por ejemplo los que utiliza el SET (Secure Electronic Transfer protocol) se conseguiría obtener los servicios de seguridad que la ISO destaca como primordiales para la seguridad en las redes telemáticas. Sin embargo existe un punto débil que ya he destacado anteriormente. Si todos estos medios de seguridad están utilizando el procedimiento de encriptación asimétrico, habrá que garantizar tanto al emisor como al receptor la autenticación de las partes, es decir que estas son quienes dicen ser, y sólo a través de autoridad de certificación (CA Certification Authority) podrá corregirse dicho error, certificando e identificando a una persona con una determinada clave pública. Estas autoridades emiten certificados de claves públicas de los usuarios firmando con su clave secreta un documento , valido por un período determinado de tiempo, que asocia el nombre distintivo de un usuario con su clave pública.

¿Que es una Autoridad de Certificación? ➦

Es esa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actuaría como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información. Sin embargo ¿quién autoriza a dicha autoridad?, es decir, ¿como sé que la autoridad es quién dice ser?, ¿deberá existir una autoridad en la cuspide de la piramide de autoridades certificadoras que posibilite la autenticación de las demás?.

Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser fiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que certifique la validez de su clave. Esta solución da origen a diferentes niveles o jerarquías de CAs.

En cuanto a los Certificados, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.

Contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un Registro (repository), considerado como una base de datos a la que el público puede acceder directamente en línea (on-line) para conocer acerca de la validez de los mismos. Los usuarios o firmantes son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante.

La Autoridad Certificante puede emitir distintos tipos de certificados:

1. Certificados de identificación: identifican y conectan un nombre a una clave pública.
2. Certificados de autorización: ofrecen otro tipo de información correspondiente al usuario, como por ejemplo la dirección comercial, antecedentes, catálogos de productos, etc.
3. Otros certificados colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para dar fe de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido.
4. Otros certificados permiten determinar día y hora en que el documento fue digitalmente firmado (Digital time-stamp certificates).

El interesado en operar dentro del esquema establecido por la ley, deberá, una vez creado el par de claves, presentarse ante la autoridad certificante (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita 'firmar' el documento de que se trate. Por ejemplo, para realizar una operación financiera de importancia con un banco, éste puede requerir al interesado un certificado del que surja, además de la constatación de su identidad, el análisis de sus antecedentes criminales o financieros. Esto quiere decir que la firma digital del interesado sólo será aceptada por la otra parte si cuenta con el certificado apropiado para la operación a realizar.

Los Repository o Registros son la base de datos a la que el público puede acceder on-line para conocer la validez de los certificados, su vigencia o cualquier otra circunstancia que se relacione con los mismos. Dicha base de datos debe incluir, entre otras cosas, los certificados publicados en el repositorio, las notificaciones de certificados suspendidos o revocados publicadas por las autoridades certificantes acreditadas y los archivos de autoridades certificantes autorizadas y todo otro requisito exigido por la Ley. Para ser reconocido, el repositorio debe operar bajo la dirección de una autoridad certificante acreditada.

Es por tanto objeto de esta ley el regularizar la actividad de dichas autoridades o proveedores de servicios de certificación. Con ello se consigue regularizar en España la actividad que desde hace unos meses viene siendo desarrollada por estos organismos.

A parte de llenar este vacío legal este RDL nos proporciona una mayor seguridad en las comunicaciones on line y remueve los obstáculos en el comercio electrónico transfronterizo, a través de la homologación de certificados. Con la Firma Electrónica se permite asegurar la identidad electrónica tanto de la persona física como de la jurídica. Aporta un marco legal idoneo para las relaciones entre el consumidor, la empresa y la administración. De esta forma se establece el punto de partida para el desarrollo del Comercio Electrónico.

Analizando la Ley por encima vemos que tiene por objeto regular el uso de la Firma Electrónica, el reconocimiento de su eficacia jurídica, así como regularizar a las autoridades u organísmos en la actividad de servicios de certificación. Para ello, define el concepto de Firma Electrónica, establece sus efectos jurídicos y regulariza la situación legal de los prestadores de dichos servicios de certificación.

Puntos a tener en cuenta en la aplicación de la ley. ➦

Los ocho puntos a tener en cuenta en la ley de Firma electrónica son los siguientes:

1. Diferencias entre Firma Electrónica y Firma Digital.

   El RDL distingue entre firma electrónica y firma electrónica avanzada. Por Firma Electrónica se entiende `aquel 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. Mientras que la Firma Electrónica avanzadaserá `aquella firma electrónica que permite la identificación del signatario y ha sido creada por medios que este mantiene bajo su exclusivo control, de manera que esta vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos¿. La diferencia estriba en que en esta última se permite identificar de forma fehaciente al signatario mientras que en la otra no, otorgándole iguales efectos jurídicos que en la firma manuscrita. Por tanto en ésta última definición de firma electrónica ha de intervenir necesariamente la figura de la Autoridad de Certificación.

   Por otro lado la diferencia entre Firma Electrónica y Firma digital estribaría en que esta última denominación se utiliza para las firmas electrónicas basadas en criptografía de clave pública mientras que la otra se utiliza para cualquier tipo de firma electrónica. Por tanto tendríamos un concepto amplio de fiirma electrónica y otro restringido o para una determinada técnica como es la infraestructura de clave pública.

2. Autoridad de Certificación.

El Real Decreto las define como `Prestadores de servicios de certificación¿ y según el artículo 2.k) son aquellas personas físicas o jurídicas que expiden certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

Como ya he mencionado antes, son aquellos órganos encargados de otorgara confianza en una infraestructura de clave pública. Desde el punto de vista de una infraestructura de clave pública es necesario confiar en una tercera parte solvente que te pueda garantizar o te otorgue la confianza necesaria para poder identificar a una persona física o jurídica con una determinada clave pública.

Los requisitos de dichas autoridades de certificación se establecen en la presente ley regulando de esta forma una actividad que venía siendo desarrollada sin ningún tipo de normativa en España.

3. Que es un Certificado.

Según el RDL se entiende por Certificado `la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad¿. A su vez la ley define otro tipo de certificado, Certificado Reconocido ` es el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12 `. Con esta distinción se quiere diferenciar los certificados genéricos de aquellos otros que son oficiales o capaces para ser utilizados en cualquier transacción electrónica de e-commerce. De esta forma un certificado reconocido producido por un dispositivo seguro de creación de firma, produciría los efectos jurídicos señalados en el artículo 3 cuando vaya unido a una firma electrónica avanzada.

Dentro de los servicios de certificación de estas Autoridades se encuentran la emisión de distintos tipos de certificados. Por poner un ejemplo podemos citar los tipos de certificado de la ACE (Agencia de Certificación Electrónica, constituida por Telefónica en un 40% y con la participación de la banca representada por CECA, SERMEPA, y 4B con un 20% respectivamente).

En los servicios de certificación X509 de ACE se ofrecen distintos tipos de certificados:

1. Certificado de Navegador, Intranets/Extranets.

   Este tipo de certificados permiten firmar digitalmente los documentos, garantizando la autenticidad y el no repudio de los mismos. Además da la posibilidad de cifrar la información (encriptación) de tal forma que sólo el receptor pueda descifarlos y tener acceso a su contenido, garantizando su integridad y confidencialidad. Por ultimo otorgaría también la facultad de securizar y autentificar la identidad en el control de acceso de los usuarios de Intranets/Extranets.

2. Certificado de Servidor Seguro. Garantizan la identidad del servidor y posibilitan las comunicaciones seguras y privadas con clientes, socios, proveedores u otras personas.
3. Certificado de firma de Software. Garantizan la identidad del fabricante y la integridad del contenido.

   A su vez ACE dispone de cuatro categorías distintas de certificados dependiendo de la naturaleza de la entidad que realiza la validación de las peticiones y por el tipo de verificación de los datos del suscriptor del certificado.

   - Categoría 0: No existe validación de datos para la identificación del

suscriptor por lo que se recomienda su utilización para control de acceso a Intranets y Extranets. La validez de la firma de documentos no está garantizada para terceros, es decir sería la definición antes apuntada de certificado genérico, pues no ha existido un procedimiento seguro de generación de firma ya que no se identificaron de forma consistente los datos de los suscriptores.

- Categoría 1: La validación realizada por ACE o por alguna de las Entidades Registro Colaboradoras privadas.
- Categoría 2. La validación del suscriptor la realiza una entidad de carácter público como una Cámar Oficial de Comercio, un ayuntamiento o un Colegio Oficial que se ha constituido como Entidad de Registro Colaboradora pública.
- Categoría 3. En esta categoría interviene, en fase de validación de datos, un fedatario público como un Notario homologado como Entidad Registro Colaboradora.

Las tarifas de precios de estos certificados no es desorbitante, sino al contrario, facilita el comercio electrónico estableciendo un precio entre las 2.000 pta y las 7.000 pta según el certificado y según la Entidad que lo verifique.

Con respecto al certificado de navegador necesario para poder firmar electrónicamente contratos u ofertas de compra de determinados productos o servicios, vemos que podemos conseguir el efecto de no repudio, que no se producía con el pago a través de SSL (Según la ley del comercio minorista, en su artículo 46 establece la posibilidad que tiene el titular de una tarjeta de crédito de anular el cargo producido en su cuenta cuando la tarjeta no hubiese sido presentada directamente o identificada electrónicamente). Se podría pensar que el certificado está en el navegador y que por tanto podría ser usurpado del mismo consiguiendo así la firma digital del usuario, para ello se establecen distintos mecanismos de seguridad que llevan a securizar de forma eficiente el certificado en el navegador. No obstante podemos decir que ACE esta suscribiendo acuerdos con importantes compañías del sector informático, como BULL, para mejorar la seguridad en la administración por el suscriptor del certificado. Este tipo de acuerdos, hace pensar en la posibilidad de que se integre el certificado en una smartcard de forma que exista mayor seguridad en la Infraestructura de Calve Pública. También recientemente a suscrito un acuerdo con FESTE (Federación Española para la seguridad en las Telecomunicaciones Electrónicas, autoridad de certificación avalada por los notarios y corredores de comercio, es decir, por los fedatarios de las operaciones mercantiles) estableciendo las bases para ser una entidad de certificación multiservicio consiguiendo responder a casi todas las situaciones que pueden presentarse en el e-commerce.

4. Valoración de la seguridad en una Infraestructura de Clave Pública.

   Para evaluar la seguridad de una infraestructura de clave pública debemos hacernos tres preguntas.

   ¿Que sé?, ¿Que tengo? y ¿Quién soy?.

   Con respecto al certificado de navegador seguro, sabría un PIN para acceder a mi clave privada instalada en el naveagador (¿que se?). Si exportase la clave a un disquete tendría el disquete en mi posesión (que tengo) aunque lo ideal sería que pudiese disponer de una smart card o tarjeta chip en la que introducir mi certificado de forma que el nivel de seguridad aumente en el sentido que nadie puede poseer esta misma tarjeta y además conocer el PIN. Con respecto a la última pregunta ¿Quién soy?, nos encontraríamos con el nivel más alto de seguridad si además de

tener tarjeta y el PIN añadimos cualquier parte del cuerpo que sea capaz de identificarme como por ejemplo la huella dactilar o el iris del ojo. Sería utilizar por tanto procedimientos biométricos que aportarían una mayor confianza a la Infraestructura de clave pública.

5. Efectos jurídicos de la Firma Electrónica.

Los efectos jurídicos de la Firma Electrónica son los descritos por el artículo 3 del RDL. En concreto señala los efectos jurídicos para la firma avanzada, estableciendo que siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá los siguientes efectos jurídicos:

- Respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel
- Será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

A parte de establecer los efectos jurídicos, establece una presunción para la adquisición de los efectos jurídicos antes nombrados. Señala dos requisitos que se presumen necesarios para que una firma avanzada tenga efectos jurídicos:

- Debe ser emitida con un certificado reconocido.
- El certificado reconocido debe ser expedido por un prestador de servicios de certificación acreditado.
- El dispositivo de creación de firma deberá encontrarse certificado con arreglo a lo establecido en el artículo 21, es decir, por entidades de evaluación acreditadas, las cuales aplicarán las normas técnicas cuyos números de referencia hayan sido publicados en el Diario Oficial de las Comunidades Europeas o en el Boletín Oficial del Estado. Se reconoce por tanto, la eficacia de los certificados sobre dispositivos seguros de creación de firma expedidos por Estados miembros de la Unión Europea.

No obstante y a pesar de establecerse estos requisitos para obtener los mencionados efectos jurídicos, se señala en el apartado 2 del art. 3 que aunque no reúna los requisitos señalados no será motivo de denegación de estos efectos jurídicos por el mero hecho de presentarse en forma electrónica.

1. Como obtener un certificado recocido.

Un Certificado se puede obtener bien directamente de la Autoridad de Certificación, o a través de otras empresas que se hayan constituido como Entidades colaboradoras en el registro de cerificados.

Para la emisión de un certificado es preciso la identificación del usuario frente a la Autoridad de Registro o una Entidad colaboradora en el Registro. Según el certificado solicitado se deberá presentar la documentación requerida, como por ejemplo el DNI, las escrituras de constitución de la Sociedad o cualquier otro documento oficial necesario.

La Autoridad de Registro y las ECR se encargan por tanto de identificar de manera inequívoca a los usuarios para que, posteriormente, éstos puedan obtener los certificados.

El procedimiento es el siguiente:

1. El usuario presenta la documentación bien de forma on-line o físicamente según

el nivel de seguridad, se verifica la identidad y se proporciona un ID o identificador y un Password.

2. Usuario procede con el ID y la Pasword a realizar la solicitud on-line a la Autoridad de Certificación (como por ejemplo ACE) y ésta tras verificar los datos que el solicitante le proporciona (ID, Password) emite el certificado.
3. La solicitud se realiza por tanto de forma on-line y las claves se generan automáticamente en el mismo ordenador desde el que se realiza la solicitud. La clave pública se enviaría posteriormente a la Autoridad de Certificación (también de forma automática).
4. El usuario podrá a partir de entonces firmar a través de su clave privada que está guardada de forma segura en el disco duro del ordenador. Para la firma será requerido un PIN o password de acceso a la clave privada firmándose el documento y adjutando a su vez el certificado de clave pública que está convenientemente firmado por la autoriadad de certificación, en este caso ACE.

Sin embargo puede surgir el problema de la movilidad de mi clave privada y certificado, para ello se establece la posibilidad de exportarse a un disquete. No obstante, la forma ideal será la incorporación del mismo en una smartcard cumpliéndose entonces las dos primeras preguntas que nos hacemos para valorar la seguridad de un criptosistema de clave pública; ¿Qué sé? el PIN o Password y ¿qué tengo? la smartcard. Recientemente la empresa RSA Security de la mano de una consultora española ha presentado sus productos en Madrid para la implantación en la empresa española y crear una infraestructura de clave pública, bien privada para el organigrama interno de la empresa o bien publica para el comercio entre empresas o e-business. De entre los distintos productos que presentó llamaba la atención un producto llamado TOKEN que consistía en la introducción tanto en el disco duro del ordenador como en la smartcard de una clave aleatoria que cambiaba cada minuto reforzándose por tanto el sistema de seguridad, ya que no solo necesitabas saber el PIN y estar en el ordenador de la persona sino que necesitabas el TOKEN, especie de aparato parecido al busca personas, en el que te aparece en una pantalla digital la password que debes introducir tras el PIN.

Por último destacar la posibilidad de revocación de los certificados en caso de perdida o sustracción, de forma que si tienes algún problema siempre puedes revocarlo y dejarlo sin efecto evitando así, que otras personas puedan firmar por ti y vincularte a una determinada relación contractual. La revocación de certificados permite que un certificado que es válido y está en vigor, deje de serlo. La petición de revocación puede iniciarla la Autoridad de Registro (AR o RA Registration Authority) o el propio usuario. Si la petición la realiza la RA se informa al usuario de que su certificado ha sido revocado. Si la petición la realiza el usuario la RA debe verificar la identidad del usuario. Los casos en que puede existir revocación pueden ser distintos, ya sea bien porque los datos han dejado de ser válidos, la clave privada ha sido comprometida o bien porque el certificado ha dejado de tener validez dentro del contexto para el que había sido emitido.

1. Equivalencia de Certificados u homologación en la UE.

Con respecto a la equivalencia de certificados de Estados que no sean miembros de la Unión Europea el artículo 10 establece una serie de requisitos o condiciones:

1. Que el prestador de servicios reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica y haya sido acreditado conforme a un sistema voluntario establecido en un Estado miembro de la Unión Europea.
2. Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla con los requisitos establecidos en la normativa comunitaria sobre firma electrónica.

3. Que el certificado o el prestador de servicios estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

1. Las Autoridades de Fechado Digital o Time Stamping Authorities.

Las autoridades de fechado digital vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante referenciado. Esta autoridad puede ser individual, es decir prestar exclusivamente estos servicios o puede ser parte de una gama de servicios relacionados con las Autoridades de Certificación.

Las autoridades de fechado digital (TSA Time Stamping Authority) proporcionan una prueba de existencia de una cierta información en un momento dado. El mecanismo de fechado digital proporciona una semántica del tipo `antes de¿: corrobora la evidencia de que el documento existía antes del instante de sellado, y garantiza que no se ha modificado con posterioridad.

Por tanto, permiten al verificador determinar fehacientemente si la firma digital fue ejecutada dentro del período de validez del certificado, previenen fechados fraudulentos antes o después del fecha consignada e impiden alterar el contenido del documento posteriormente al instante de firma.

Para concluir quisiera resaltar el momento al que estamos asistiendo, donde los antiguos métodos de comercio están siendo llevados a la era de las nuevas teologías. Conceder efectos jurídicos a la firma electrónica significa poder trasladar al espacio electrónico la eficacia de los negocios jurídicos tradicionales, en definitiva supone un paso más hacia la escalada mundial por alcanzar un mercado global donde todos los operadores puedan libremente comerciar entre sí con seguridad jurídica. Paso, en el que se ven involucrados todos los gobiernos mundiales, en donde la Unión Europea juega un importante papel. Es por tanto de elogiar el esfuerzo realizado por el legislador español en la redacción del actual Real Decreto Ley sobre Firma Electrónica, ya que con ello sienta las bases para que el comercio electrónico comience su andadura. Ahora debemos coger el relevo y comenzar poco a poco (despacio pero sin pausa) la carrera continua hacia la tan ansiada aldea global.

23 de Marzo de 2001