Firma digital: características esenciales y requisitos para ser Certificador Licenciado

Maltese, J. Mariano

1 — Conceptos

Se ha dicho que la firma digital es, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, un método criptográfico que asegura la identidad del remitente. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje (2).

En la página Web de la Subsecretaría de la Gestión Pública de la República Argentina (http://www.pki.gov.ar/), se afirma que "la firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen".

En el mismo sitio Web también se la define como una herramienta tecnológica que garantiza la autoría e integridad de los documentos digitales, permitiendo que estos gocen de una característica que únicamente era propia de los documentos en papel.

Asimismo, que "la firma digital no implica asegurar la confidencialidad del mensaje: un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente".

Por último, la ley 25.506 de Firma Digital de la República Argentina (LFDA), en su art. 2 la define como "al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma."

En su art. 5°, determina que debe entenderse por Firma Electrónica "al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital." Agregando que en "caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez". Sobre este aspecto probatorio volveremos mas adelante.

Por nuestra parte definiremos a la Firma Digital, a la luz de la normativa argentina, como aquel tipo de tecnología que permite determinar la autoría e integridad de un documento electrónico que, asimismo, está reconocida por una Autoridad Certificante y no admite el repudio de su titular.

Por lo cual, en sentido amplio hablaremos de "firma electrónica", y en sentido estricto de "firma digital" que es una sub especie de la firma electrónica. Ello se entenderá mejor cuando se lea el apartado "Diferencia jurídica en la República Argentina"

2 — Características esenciales

En virtud de todo lo que hemos dicho hasta ahora, nos encontramos en condiciones de afirmar que los elementos esenciales para poder hablar de Firma Digital, bajo los parámetros de la legislación argentina, entendemos que son los siguientes:

— Autoría: la tecnología utilizada debe permitir identificar al autor del documento electrónico.

— Integridad: también tiene que permitir identificar el documento original y determinar si el mismo tuvo modificaciones o no.

— Certificador Licenciado: este es uno de los requisitos mas importantes, ya que, si bien pueda determinarse la autoría e integridad del documento por medios tecnológicos, sin la existencia de la Autoridad de Certificación con licencia válidamente otorgada (o bien Certificador Licenciado) que otorgue el certificado digital para firmar digitalmente, sólo estaremos en presencia de la Firma Electrónica y no de la Firma Digital.

— No repudio: el titular del certificado digital que niega la creación del documento electrónico posee la carga de la prueba de su aseveración.

3 — Conflicto con la palabra "firma"

Uno de los aspectos preliminares a abordar cuando hablamos de "firma digital", es justamente por qué se utiliza esta palabra (firma) para designar una herramienta tecnológica que, en principio dista del concepto aceptado por la Real Academia Española (R.A.E.).

Veamos. Según podemos extractar en Internet en la página Web http://buscon.rae.es/draeI/ del Diccionario de la Real Academia Española, se designa como la palabra "firma" en sus diversas acepciones como:

1. Nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido.

2. Conjunto de documentos que se presenta a quien corresponda para que los firme.

3. Acto de firmarlos.

4. Razón social o empresa.

5. Sello (carácter peculiar o especial).

6. Autor o persona importante en el campo periodístico o artístico, especialmente literario.

Como es fácil advertir poco o nada nos dice el Diccionario de "tecnología", de "programa digital", de "criptografía", etc. entonces ¿por qué se utiliza y confunde al usuario con una expresión tan poco precisa?

De hecho, para muchas personas que no utilizan la FD están convencidas que se trata de aquellos documentos que tienen escaneada la firma ológrafa y estampada en el pie del mismo.

Seguramente el hecho que la firma ológrafa sea la que otorga "autenticidad" a un documento, derivó en la tentación de establecer para este tipo de tecnología idéntica terminología. Pero quedan ausentes el resto de los caracteres (el Certificador Licenciado, el No repudio y la certeza de "integridad" del documento), aspectos que, como hemos visto, le otorga fuerza legal a la firma digital.

En síntesis, consideramos ambigua la utilización de la palabra "firma" para referirnos a este tipo de tecnología. Entendemos que podría mencionarse genéricamente con un nombre técnico que no admita dificultad de comprensión a quien desconoce la materia.

4 — Clasificación

Según pudimos recopilar (3) este tipo de tecnología, que puede tener normativa diferente en cada país, ha sido clasificada en tres tipos distintos:

• **Simple.** Incluye un método de identificar al firmante

• **Avanzada.** Además de identificar al firmante permite garantizar la integridad del documento. Se emplean técnicas de PKI (4).

• **Reconocida.** Es la firma avanzada ejecutada con un DSCF (dispositivo seguro de creación de firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante)

Asimismo, bajo determinadas normas que definen los formatos técnicos de la firma digital, también se pueden clasificar en tres modalidades de firma:

• **Firma básica**. Incluye el resultado de operación de hash (5) y clave privada, identificando los algoritmos utilizados y el certificado asociado a la clave privada del firmante. A su vez puede ser "attached" o "detached", "enveloped" y "enveloping"

• **Firma fechada**. A la firma básica se añade un sello de tiempo calculado a partir del hash del documento firmado por una TSA (Time Stamping Authority)

• **Firma validada o firma completa**. A la firma fechada se añade información sobre la validez del certificado procedente de una consulta de CRL o de OCSP realizada a la Autoridad de Certificación.

Por último, según el dec. 2628/2002, en su art. 1° establece que podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad:

• Firma electrónica,

• Firma digital basada en certificados digitales emitidos por certificadores no licenciados,

• Firma digital basada en certificados digitales emitidos por certificadores licenciados,

• Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido

reconocidos en los siguientes casos:

1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero.

2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.

5 — Diferencia jurídica en la República Argentina

Según el Dr. Fernando Maresca (6), la legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" o "Firma Electrónica Reconocida" utilizado por la Comunidad Europea o "Firma Electrónica" utilizado en otros países como Brasil o Chile.

A su vez, sostiene el autor que para la legislación argentina los términos "Firma Digital" y "Firma Electrónica" no poseen el mismo significado. La única que se equipara en sus efectos jurídicos a la firma ológrafa es la firma digital. Asimismo, existe una diferencia respecto al valor probatorio atribuido a cada una de ellas.

En el caso de la "Firma Digital" existe una presunción "iuris tantum" en su favor; esto significa que si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la firma electrónica, en caso de ser desconocida la firma por su titular corresponde a quien la invoca acreditar su validez.

Para reconocer que un documento ha sido firmado digitalmente —existiendo en este caso una presunción "iuris tantum" en su favor— se requiere que el certificado digital del firmante haya sido emitido por un certificador licenciado (que cuente con la aprobación del Ente Licenciante).

La licencia se obtiene luego de someterse al proceso de licenciamiento cuyo objetivo es verificar la idoneidad técnica y legal del certificador para emitir certificados.

6 — Certificador Licenciado

En criptografía una Autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública (PKI). Jurídicamente es un caso particular de Prestador de Servicios de Certificación (7).

Podemos decir que, una Autoridad de Certificación o Autoridad Certificante o Certificador Licenciado es una persona que emite certificados digitales en un marco de legalidad para ser utilizado por los usuarios.

En la técnica legislativa nacional, se realiza un distingo entre el Certificador Licenciado y la Autoridad Certificante o de Certificación. Así, por ejemplo, en la **Decisión Administrativa 6/2007 de la Jefatura de Gabinete de Ministros** (DAJG N° 6/07), se establece que:

Art. 15. — Vínculo entre las Políticas de Certificación licenciadas y las Autoridades Certificantes de los certificadores. El certificador licenciado debe implementar una Autoridad Certificante por cada una de sus Políticas de Certificación licenciadas. La Autoridad Certificante Raíz emitirá un certificado digital para cada una de esas Autoridades Certificantes.

Art. 16. — De las Autoridades Certificantes de certificadores licenciados: Los certificadores licenciados emitirán certificados digitales a los suscriptores de sus Políticas de Certificación, a través de las Autoridades Certificantes que forman parte de su infraestructura tecnológica. Diferentes Autoridades Certificantes de un certificador licenciado podrán compartir la misma infraestructura tecnológica, previa aprobación por parte del ente licenciante.

En efecto, como podemos observar el certificador licenciado puede tener diversas Autoridades Certificantes según las Políticas de Certificación Licenciadas que obtuviere. Ello es así, ya que lo que se licencia son Políticas de Certificación, pudiendo un mismo Certificador tener varias licencias. En tal caso, deberá contar con tantas Autoridades Certificantes como licencias obtuviere.

Luego de estas aclaraciones, podemos definir al Certificador Licenciado como "...toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros

servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante." Así está definido por el art. 17 LFDA.

En tal sentido, para la legislación nacional los elementos fundamentales serán: 1) ser persona de existencia ideal, no bastará con la persona física (sin embargo, se debate acerca de la expresión que usa la LFDA cuando dice "registro público de contratos", ya que se entiende mayoritariamente que se está refiriendo a los escribanos, que son personas físicas), 2) prestar servicios en relación a la firma digital, y 3) contar con licencia otorgado por el ente licenciante.

En la práctica mundial, existen muchos Certificadores Licenciados (CLs) comerciales que cobran por sus servicios. Por otra parte instituciones, empresas y gobiernos pueden tener sus propias CLs y también existen CLs gratuitas.

Se suele mencionar que actúa como "tercero de confianza". El CL, por sí mismo o mediante la intervención de una Autoridad de Registro (otra persona cuya única función es corroborar la identidad del usuario y comunicarlo al CL para que ésta emita el certificado), verifica la identidad del solicitante de un certificado antes de su expedición.

En la Legislación argentina "la actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos." (art. 17 LFDA)

En los términos del art. 19 LFDA, las Funciones que cumplirá el CL son las siguientes:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

c) Identificar inequívocamente los certificados digitales emitidos;

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

1) A solicitud del titular del certificado digital.

2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.

3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.

4) Por condiciones especiales definidas en su política de certificación.

5) Por resolución judicial o de la autoridad de aplicación.

f) Informar públicamente el estado de los certificados digitales por él emitidos.

Deberá tenerse en cuenta también los motivos de cese de la actividad de los CLs. En tal sentido el art. 22 LFDA, determina tres causas: a) Por decisión unilateral comunicada al ente licenciante; b) Por cancelación de su personería jurídica; c) Por cancelación de su licencia dispuesta por el ente licenciante.

7 — Certificados por Profesión

En efecto, la LFDA otorgó especial importancia a la actividad colegiada de los profesionales a los fines de constituirse como CLs. Tuvo en miras el impacto que pudiera otorgarse a la dinámica de la utilización de la FD en el componente jurídico, contable, así como en toda la gama de inserción profesional tales como la medicina, arquitectura, ingeniería, etc.

En tal sentido, el legislador introduce novedosamente el artículo N° 18 de la LFDA, el cual reza: "Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado."

Para comprender mejor la dinámica de este apartado, tendremos que tener en cuenta que, por ejemplo, cada uno de los Colegios de Abogados de todo el país podrán oficiar como CLs para dar inicio (y continuar en algunas jurisdicciones) con la ansiada modernización del poder judicial. Así veremos más cercana y cubierta de la solvencia jurídica necesaria a la "cédula electrónica" para notificar actos procesales, o bien la presentación de "escritos por vía de firma digital", así como tantas otras funciones que permitiría este tipo de tecnología.

Otro ejemplo lo constituyen los profesionales de las ciencias económicas, quienes a través de sus Consejos Profesionales de todo el país podrán obtener certificados digitales para —entre otras actividades— realizar presentaciones ante la AFIP, o bien presentar balances y toda una gama de formularios en los Registros Públicos de Comercio o las mismas entidades de recaudación municipal, provincial o nacional, etc.

Por su parte los arquitectos ya no tendrán que soportar los engorrosos traslados de papel para registrar sus planos, dado que podrán trasladarlos digitalmente e inscribirlos en las dependencias catastrales de todo el país con la utilización de la Firma Digital.

Por último, un ejemplo de avance y claro entendimiento de lo inexorable que se avizora el uso de la tecnología en todas las ramas del saber, lo constituye el Proyecto de Reforma de La Ley de Ejercicio de la Medicina, Odontología y actividades auxiliares N° 17.132 en donde se prevé el uso de la Firma Digital para las recetas y/o prescripciones de dichos profesionales.

8 — Requisitos para brindar servicio de Certificador Licenciado

La LFDA prevé que para ser CL deberá solicitarse una licencia ante el Ente Licenciante, quien realizará auditorias para efectuar un dictamen legal y técnico. Estas licencias son intransferibles.

En estos momentos, por dec. 283/2003, desarrolla la función de Ente Licenciante la Oficina Nacional de Tecnologías Informáticas —O.N.T.I.—, dependiente de la Subsecretaría de la Gestión Publica de la Jefatura de Gabinete de Ministros de la República Argentina.

Ahora bien, es importante resaltar la sanción de la **Decisión Administrativa 6/2007 de la Jefatura de Gabinete de Ministros** (DAJG N° 6/07) de fecha 7 de febrero de 2007.

Desde hace varios años, quienes nos desempeñamos como profesionales del derecho vinculados a las nuevas tecnologías, estamos aguardando el efectivo lanzamiento de la firma digital como herramienta de trabajo cotidiano. Sin embargo, por cuestiones estrictamente reglamentarias, hasta el presente año resultó imposible hacer uso de este instrumento en los términos de la ley de Firma Digital.

Con el dictado de la DAJG N° 6/07, se completó el plexo normativo estableciéndose el marco aplicable al otorgamiento y revocación de las licencias, a los certificadores que así lo soliciten.

En tal sentido, las personas de existencia ideal, y en particular los Consejos y/o Colegios Profesionales de todo el país ya se encuentran en condiciones de iniciar el trámite correspondiente que les permitirá proveer certificados digitales a sus miembros.

De esta forma, tanto la institución como sus integrantes estarán en condiciones de firmar documentos digitales y realizar transacciones comerciales con el respaldo jurídico que proporciona la ley.

El art. 13 de la DAJG N° 6/07 determina que los componentes de la Infraestructura de Firma Digital de la República Argentina son:

a) el ente licenciante y su Autoridad Certificante Raíz,

b) los certificadores licenciados, incluyendo sus Autoridades Certificantes y sus Autoridades de Registro,

c) los suscriptores de los certificados digitales de esas Autoridades Certificantes y

d) los terceros usuarios de esos certificados.

En nuestro régimen, a diferencia de lo que ocurre en otras partes del mundo, el mismo ente licenciante administra la Autoridad Certificante Raíz (art. 14, DAJG N° 6/07).

9 — Niveles de prestación

Según lo establece la normativa argentina de Firma Digital podríamos resumir los niveles de prestación en los siguientes:

a. Autoridad Certificante con Equipos Propios.

Se trata de la posibilidad de certificar la identidad de la persona que solicita una firma digital, y emitir los certificados digitales, contando con la tecnología adecuada para poder satisfacer todo el servicio. En este supuesto el mismo interesado sería Autoridad Certificante y de Registro.

b. Autoridad Certificante sin Equipos Propios (tercerización).

En iguales términos que el anterior, pero con la diferencia que se tercerizaría la confección del certificado ya que la tecnología no sería propia. El certificado figuraría emitido por el interesado, pero técnicamente lo confecciona un tercero.

c. Autoridad de Registro.

Sólo se brinda el servicio de identificar a la persona que solicita una firma digital. Luego la confección de los certificados está a cargo de un tercero (Autoridad Certificante). El certificado figurará emitido por el mismo tercero. No requiere tener equipos propios, ni tercerizar su procesamiento, ya que no se emitirá el certificado a su nombre.

10 — Trámites para el licenciamiento

Como fue mencionado, la DAJG N° 6/07 completó el andamiaje normativo necesario para establecer los requisitos que deben cubrir los aspirantes a brindar el servicio de Certificador Licenciado.

En sus ocho Anexos la Decisión mencionada establece:

— Requisitos para el licenciamiento de certificadores

— Requisitos Mínimos para Políticas de Certificación

— Perfil Mínimo de Certificados y Listas de Certificados Revocados

— Contenidos Mínimos del Resumen de la Política de Certificación y del Manual de Procedimientos de Certificación para Suscriptores

— Contenidos Mínimos de los Acuerdos con Suscriptores

— Contenidos Mínimos de los Términos y Condiciones con Terceros Usuarios

— Montos de aranceles y garantías

— Contenidos Mínimos de la Política de Privacidad

Los Anexos técnicos respectivos se podrán obtener del siguiente Link http://infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/125115/decadm6-2007-anexo.pdf

En efecto, la legislación nacional establece requisitos formales genéricos (Estatuto social, inscripción tributaria, etc.) y otra serie de obligaciones específicas de la materia. Entre otros, ellos son:

— Política de Certificación

— Manual de Procedimientos de Certificación

— Acuerdo con suscriptores

— Acuerdos con terceros, en caso de tercerización de servicios

— Acuerdos entre el certificador y autoridad registrante

— Pólizas de seguro — Otros seguros y garantías

— Políticas y medios de comunicación con los suscriptores

— Información publicada por el certificador conforme normativa vigente.

— Política de Certificación

— Manual de Procedimientos de Certificación

— Direcciones, protocolos y medios para acceder a la información que se publica, certificados, lista de certificados revocados.

Certificados y perfil de certificados

— Plan de Cese de Actividades

— Plan de Seguridad

— Plan de Contingencia

— Descripción de la plataforma tecnológica

Como se puede advertir el trámite de Licenciamiento para CLs tiene su complejidad, aunque con la debida experiencia e idoneidad se podrá estar en condiciones de brindar un servicio adecuado para el complejo mundo de transacciones que exige una modernización permanente.

11 — Conclusión

Existen momentos en la historia de los hombres que los mismos acontecimientos que fomentan la trascendencia de los hechos no son advertidos por los contemporáneos.

Le ocurrió a los reyes, gobernantes y autoridades máximas de todas las épocas. ¿Cuánto hubiera dado el hombre más poderoso de la tierra por superar un momento de dolor físico con sólo tomar una pastilla? Hoy en día con la fórmula de la aspirina atacamos varios focos al mismo tiempo, solucionando así problemas que en el pasado podrían llevar a la misma muerte.

Sin embargo, ¿conocemos la fórmula del ácido acetilsalicílico? definitivamente, en mi caso, no. ¿Necesito conocerla para beneficiarme? la respuesta personal también es no. Entonces, ¿por qué sin conocer el funcionamiento y la composición la ingiero sin reparos en mi cuerpo? es sencillo: tengo confianza en los resultados de la aspirina.

Con la Firma Digital sucede algo similar. Falta mayor confianza en la tecnología para realizar transacciones, notificaciones, y todo tipo de acto jurídico, con la misma confianza que nos genera el soporte en papel.

O ¿acaso a un contrato le desconfiamos cuando vemos todas las firmas estampadas en el mismo?, ¿no pensamos que ese papel que sostiene el acuerdo de partes puede perderse, romperse, robarse, destruirse por el tiempo, etc., etc.? Si concebimos que todos estos hechos pueden ocurrir, ¿por qué le pedimos a la Firma Digital mayor seguridad que al papel?

Vuelvo al inicio; cuando existen hechos que cambian la forma de ver las cosas, de pensar, de sentir, el seguir en el mismo lugar, sin cambiar, implica exponerse a los golpes más crudos de la adversidad, ya que el tiempo no espera a nadie, y la superación en el ser humano es una exigencia natural de su propio espíritu.

Este artículo tiene por intención, brindar una breve información de los principios básicos de la Firma Digital, así como explicar sucintamente los requisitos para brindar el servicio de Certificador Licenciado, pero fundamentalmente dejar en claro que el mundo ya nos lleva varios años a los argentinos beneficiándose de muchos avances tecnológicos. No pretendamos que esos avances se detengan, o bien estaremos como aquel loco que quería que todo a su alrededor mejorase diametralmente sin él realizar ningún tipo de cambio.

(1) Abogado, egresado de la Universidad de Buenos Aires. Director de Consultores Jurídicos, Estudio de Abogados especialistas en Derecho Informático. Director de la Consultora Informático Jurídica (C.I.J.) y Director de la Comisión de Hábeas Data de la Asociación Argentina de Derecho para la Sociedad de la Información (AADeSI). Ex — Profesor de Derecho Económico II (Concursos y Quiebras) en la Facultad de Ciencias Económicas de la U.B.A. Actual Docente en la materia Elementos de Derecho Comercial en la Facultad de Derecho y Cs. Sociales de la U.B.A. Profesor invitado por diversas universidades y colegios de abogados para disertar y dar clases especiales. Redactor de numerosos artículos publicados en revistas especializadas y otros medios virtuales.

(2) http://es.wikipedia.org

(3) http://es.wikipedia.org

(4) La tecnología PKI (Public Key Infrastruture) permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

(5) En informática, Hashing es un método para resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo. Técnicamente, la Firma Digital de un documento es el resultado de aplicar cierto algoritmo matemático,

denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

(6) "LA INFRAESTRUCTURA DE FIRMA DIGITAL", Por el Dr. Fernando Maresca. Artículo hecho llegar por el autor.

(7) http://es.wikipedia.org