LA FIRMA ELECTRÓNICA

Por: Alfredo Alejandro Reyes Krafft. Doctor en Derecho por la Universidad Panamericana. Director jurídico de e-business en BBVA Bancomer. Presidente de la Asociación Mexicana de Internet. (México)

Sumario:
Introducción.- Panorama Internacional.- La firma autógrafa.- La firma electrónica.- Criptografía.- La Infraestructura de Clave Pública.- Reformas al Código de Comercio en materia de firma electrónica en México.

LA FIRMA ELECTRÓNICA
INTRODUCCIÓN:

No deja de ser curioso que la 'firma electrónica' pueda casualmente sintetizarse en el acrónimo 'FE' que es precisamente algo de lo que, por desgracia, aun hace mucha falta para creer y, por lo tanto, confiar en el uso de las nuevas tecnologías.

La contratación y el comercio electrónico representan una nueva modalidad constitutiva de obligaciones, no hablamos de una nueva fuente de la obligación, sino de una nueva forma de expresión de la voluntad derivada de los avances tecnológicos que hoy en día facilitan la transmisión electrónica de mensajes de datos agilizando fundamentalmente las transacciones jurídicas comerciales.

Esta nueva forma de contratar plantea problemas como la ausencia del soporte en papel y de la firma autógrafa que acredita la autenticidad y le otorga validez al documento; ante esta situación se cuestiona la validez del documento emitido y contenido en un soporte electrónico.

El 29 de mayo del año 2000, se publicó en el Diario Oficial de la Federación el Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal (ahora Código Civil Federal), del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor:

La legislación existente hasta esa fecha, requería para la validez del acto o contrato del soporte de la forma escrita y la firma autógrafa, para vincular a las partes en forma obligatoria.

Las reformas y adiciones al CÓDIGO CIVIL FEDERAL se centraron en el reconocimiento a la celebración de actos jurídicos a través de medios electrónicos, ópticos o de cualquier otra tecnología, añadiéndose los “medios tecnológicos” como medio idóneo para expresar el consentimiento. Es importante resaltar que se estableció una equivalencia funcional entre el consentimiento expresado por medios tecnológicos y la firma autógrafa “siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta”.

Se reconoció en el CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador: La fiabilidad del método para generar, comunicar, recibir o archivar la información (que pueda conservarse sin cambio), su atribución a las personas obligadas y la posibilidad de acceder a ella en ulteriores consultas. Asimismo y para que la información generada, comunicada, recibida o archivada por medios electrónicos se considere como original (para su conservación o presentación) deberá acreditarse que dicha información se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta

En el CODIGO DE COMERCIO se definió el concepto “Mensaje de Datos” como la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

Respecto de la obligación a los comerciantes de conservar por un plazo mínimo de 10 años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y

obligaciones , en el caso de mensajes de datos se requerirá que el contenido de la información se haya mantenido íntegro e inalterado a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Economía deberá emitir una Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

Se estableció una presunción en materia mercantil, salvo pacto en contrario, de que el mensaje proviene del emisor (atribución a la persona obligada) si ha sido enviado: i) Usando medios de identificación, tales como claves o contraseñas de él (para lo que se requerirá de un previo acuerdo entre las partes), o ii) Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

En materia mercantil, al igual que en la civil, cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta.

Y se reconoce como prueba a los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada

Se reformó la LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR para reconocer la utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren los proveedores con los consumidores, dando las bases sobre las cuales habrán de realizarse dichas operaciones (confidencialidad, certeza, seguridad en la información proporcionada al consumidor, etc.), previendo sanciones administrativas para el caso de que los proveedores no cumplan con dichas disposiciones.

De lo anterior resulta necesario hacer las siguientes consideraciones:

Para que un mensaje de datos en el que se consignen contratos, pueda considerarse legalmente válido, es necesario asegurar que la información en él contenida reúna las siguientes características:

INTEGRIDAD:
Entendida en dos vertientes, la primera respecto de la fiabilidad del método para generarla, comunicarla, recibirla o archivarla. Y la segunda como la forma de garantizar que la información en él contenida no fue alterada. Al respecto la Secretaría de Economía elaboró una Norma Oficial Mexicana que establece los requisitos que deben observarse para la conservación de mensajes de datos, con fundamento en lo dispuesto por el artículo 49 segundo párrafo del Código de Comercio.

El martes 19 de marzo del 2002 se firmó el texto final de la NOM, el cual fue publicado el DOF el día 4 de junio del 2002, para su entrada en vigor se requiere de existencia de infraestructura y publicación de aviso en el Diario Oficial de la Federación.

ATRIBUCIÓN:
Es la forma en que podemos garantizar que las partes que se obligan en la relación jurídica son quienes dicen ser y expresan su voluntad libre de vicios.

Esta atribución a las personas obligadas en la relación jurídica que se pretende formalizar en un mensaje de datos, no es más que una “FIRMA ELECTRÓNICA”, la cual puede ser de dos tipos:

SIMPLE definida como los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos (partiendo de la presunción, en materia mercantil, de que el mensaje ha sido enviado usando medios de identificación como claves o contraseñas por ambas partes conocidas, para lo cual se requerirá de un acuerdo previo y firmado en forma autógrafa por las partes) o

AVANZADA que podemos conceptuar como la firma electrónica que permite la identificación del firmante y ha sido generada bajo su exclusivo control que vincula exclusivamente al mismo con el mensaje de datos al que se adjunta o se asocia, lo que permite que sea detectable cualquier

modificación ulterior de éste (entendida como proceso electrónico que permite al receptor de un mensaje de datos identificar formalmente a su autor, mismo autor que mantiene bajo su exclusivo control los medios para crear dicha firma, de manera que esté vinculada únicamente a él y a los datos a que se refiere el mensaje, permitiendo detectar cualquier modificación ulterior al contenido del mismo, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento.

Para esto se hizo necesaria la legislación federal relativa a la firma electrónica "avanzada" en la que se regule la actividad de los prestadores de servicios de certificación, a los propios certificados de firmas electrónicas, así como la admisibilidad y forma de presentar como prueba en juicio a los mensajes de datos firmados y se establecieran los requisitos técnicos necesarios para su conservación en una NOM para tales efectos, procurando preservar la independencia tecnológica.

ACCESIBILIDAD:
Se refiere a que el contenido de un mensaje de datos en el que se consignen contratos, pueda estar disponible al usuario (emisor, receptor, juez, auditor, autoridades, etc.) para ulterior consulta, siempre y cuando reúna las dos características anteriormente anotadas. Para ello será necesario establecer, en la legislación federal que al efecto deberá emitirse, la forma de presentar a "los usuarios" estos mensajes de datos, la cual podría hacerse previa certificación de atribución e integridad por parte del prestador de servicios de certificación.

Es importante recalcar que el medio físico a través del cual el contenido de un mensaje de datos se pone a disposición del usuario puede ser diferente de aquél en que se creó, ya que se debe garantizar la integridad del mensaje de datos, no del medio físico que lo contiene. Esto es, que el mensaje puede estar contenido en el disco duro de una computadora y ponerse a disposición del usuario en un diskette, el copiarse a ese medio físico distinto al en que fue creado no lo hace de ninguna manera perder integridad.

El objeto del presente trabajo consiste en presentar una breve exposición doctrinal que sirva de marco conceptual al DECRETO DE REFORMAS AL CÓDIGO DE COMERCIO EN MATERIA DE FIRMA ELECTRÓNICA, que el pasado 26 de noviembre del 2002 fue aprobado en la Cámara de Diputados por 422 votos a favor y 1 abstención, el cual, en proceso legislativo fue aprobado por el Senado de la República el 8 de abril del 2003, por unanimidad (85 votos a favor) y será vigente 90 días después de su publicación en el DOF (29 de agosto de 2003).

El mismo adopta básicamente la ley modelo sobre firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) introduce en la legislación mexicana el concepto de firma electrónica fiable o avanzada y complementa la parte relativa a Mensaje de Datos detallando conceptos como Intermediario, Acuse de Recibo, Copia, Error, etc.

Establece el uso voluntario y la posibilidad de convenir cualquier método de firma que determinen las partes, obviamente bajo la responsabilidad de uso del Firmante. Incorpora la figura del Prestador de Servicios de Certificación, quien como tercero confiable estará investido de la facultad de validar, por su probidad y su tecnología (no fé pública), el proceso de emisión, identificación y atribución de firmas electrónicas. Pueden ser:

- Notarios o Corredores Públicos
- Empresas Privadas
- Instituciones Públicas

Reconoce como Autoridad Registradora Central a la Secretaría de Economía (además de Banco de México y la Secretaría de la Función Pública) y no descuida el reconocimiento y validez de los cerificados extranjeros

LA FIRMA ELECTRÓNICA
PANORAMA INTERNACIONAL

Actualmente entre los países que cuentan con una legislación en materia de Firma electrónica podemos enumerar a los siguientes:

ALEMANIA (El 13 de junio de 1997 fue promulgada la Ley sobre Firmas Digitales y el 7 de junio del mismo año, fue publicado su Reglamento. Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Bundesgesetzblatt - BGBl. Teil I S. 876 vom 21. Mai 2001). Published 16 May 2001. Official Journal Nº 22, 22 May 2001. In Force 22 May 2001).

ARGENTINA (El 17 de marzo de 1997, el Sub-Comité de Criptografía y Firma Digital, dependiente de la Secretaría de la Función Pública, emitió la Resolución 45/97 -firma digital en la Administración Pública- el 14/12/2001 Ley de Firma Digital para la República Argentina 25/506.

BELGICA : Loi fixant certaines règles relatives au cadre juridiqe pour les signatures électroniques et les services de certification (Moniteur belgue du 29 septembre 2001). Loi introduisant l´utilisation de mohines de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, 20 octobre 2000. Belgisch Staatsblad, 22/12/200. Moniteur Belge.

C.E.E. (Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica..- Decisión de la Comisión, de 6 de noviembre de 2000, relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica (2000/709/CE).

CANADÁ (British Columbia Bill 13-2001, The Electronic Transactions Act).

COLOMBIA (Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación)

CHILE (2002 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación).

DINAMARCA: Act 417 of 31 May 2000 on Electronic Signatures. Bill L 229. Executive Order on Security Requirements etc. for Certification Authorities. Executive Order Nº 923 of 5 October 2000. Executive Order on Reporting of Information to the National Telecom Agency by Certification Authorities and System Auditors. Executive Order Nº 922 of 5 October 2000.

ESPAÑA (Real Decreto Ley 14/1999 sobre Firmas Electrónicas. Septiembre de 1999, Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos 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. -Ley de Servicios de la Sociedad de Información-) El Proyecto de Ley de firma electrónica, de 20 de junio de 2003 , ha introducido diversas modificaciones respecto del vigente Real Decreto ley 14/1999 de firma electrónica. Tras su ratificación por el Congreso de los Diputados, se acordó someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto, entre los puntos mas importantes que considera están: Promoción de Autorregulación de la Industria, Concepto de Firma Electrónica Reconocida, Time stamping, Declaración de prácticas de certificación, Documento Nacional de Identidad Electrónico y el más debatido, Certificados para Personas Morales, un caso distinto a la firma electrónica de los representantes de las personas morales, pues se persigue dar firma a las empresas, no a sus representantes, si bien, evidentemente, con el objeto de que así se pueda distribuir entre sus empleados.

FRANCIA : Décret nº 2001-272 du 30 mars 2001 pris pour l´application de l´article 1316-4 du code civil et relatif à la signature électronique. Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l´informtion et relative à la signature électronique.

IRLANDA: Electronic Commerce Act, 2000 (Number 27 of 2000)

ITALIA (El 15 de marzo de 1997, fue publicado el “Reglamento sobre: Acto, Documento y Contrato en Forma Electrónica” aplicable a las diversas entidades de la Administración Pública, el 15 de abril de 1999 las reglas técnicas sobre firmas digitales y el 23 de enero del 2002 la ley sobre firma electrónica).

JAPÓN (1/04/2001 Ley sobre firma electrónica y Servicios de Certificación).

LUXEMBURGO : Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiment électronique et à la création du comité "commerce électronique". Projet de règlement grand-ducal portant determination d´un système d´accréditation des organismes de certification et d´inspection, ainsi que des laboratoires d´essais et d´étalonnage et portant création de l´Office Luxembourgeois d´Accréditation et de Surveillance, d´un Comité de´accréditation et de´un Recueil national des auditeurs qualité et techniques. Texte amendé suite aux avis de la Chambre de commerce et de la Chambre des métiers.

PANAMÁ (3/08/2001 Ley 43 de Comercio Electrónico).

PORTUGAL: Decree-Law 290-D/99.

REINO UNIDO: Electronic Communications Act, 2000.

SUECIA: Qualified Electronic Signatures Act (FSF 2000:832)

En este trabajo analizaremos la legislación de algunos de los países que consideramos representativos.

ESTADOS UNIDOS

La primera ley en materia de Firma Digital en el Mundo fue la denominada “Utah Digital Signature Act”, publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos.

Su objetivo es facilitar mediante mensajes electrónicos y firmas digitales las transacciones. Procurar las transacciones seguras y la eliminación de fraudes. Establecer normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos, en coordinación con otros Estados.

Su ámbito de aplicación son las transacciones mediante mensajes electrónicos, su confiabilidad, así como las firmas digitales.

Esta ley, define a la Firma Digital como la “transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación.”

Al Criptosistema Asimétrico, como aquel “algoritmo o serie de algoritmos que brindan un par de claves confiable.”

Al Certificado, como aquel registro basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite.
En cuanto a la Supervisión y al control, estos recaen sobre la División, quien actúa como autoridad certificadora. También formula políticas para la adopción de las tecnologías de firma digital y realiza una labor de supervisión regulatoria.
La emisión de los certificados corre a cargo de la autoridad certificadora que ha sido acreditada
Se equipara el valor probatorio de un mensaje de datos que uno en papel siempre y cuando contenga una firma digital confirmada mediante la clave pública contenida en un certificado que haya sido emitida por una autoridad certificadora autorizada.
No se contempla el reconocimiento de certificados extranjeros, solo se menciona que la División puede reconocer la autorización emitida por Autoridades Certificadoras de otros Estados.
No contempla sanciones.

ABA: El Comité de Seguridad de la Información, de la División de Comercio Electrónico, de la American Bar Association, emitió, en agosto de 1996, la "Guía de Firmas Digitales".

NCCSL: El 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme, elaboró la "Uniform Electronic Transactions Act" (UETA), la cual se aprobó el 30 de julio de 1999.

El 4 de agosto del 2000 se aprobó la "Uniform Computer Information Transactions Act" (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana.

PRESIDENCIA: El 30 de junio el 2000 se emite la "Electronic Signatures in Global and National Commerce Act" (E-Sign Act.) vigente a partir del 1 de octubre del 2000 (otorgando a la firma y documento electrónico un estatus legal equivalente a la firma autógrafa y al documento en papel).

LATINOAMERICA :

COLOMBIA

En Colombia existe la Ley de Comercio Electrónico en Colombia (Ley 527 de 1999)

Su objetivo es la reglamentación y la definición del acceso y el uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, además del establecimiento de las Entidades de Certificación.

Su ámbito de aplicación es el uso de firmas digitales en mensajes de datos

Define como Firma Digital, al valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Como Mensaje de Datos a la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

Como Entidad de Certificación a aquella persona que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

En cuanto a la Supervisión y al control, estas recaen sobre las Entidades de Certificación autorizadas por la Superintendencia de Industria y Comercio.

Se equipara el valor probatorio de un mensaje de datos que uno en papel siempre y cuando contenga lo siguiente:
1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Si da Reconocimiento a Certificados Extranjeros

Las sanciones serán impuestas por la Superintendencia de Industria y Comercio de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, estas van de la Amonestación a la Revocación de la Autorización.

PERU

En Perú existe la Ley No. 27269 Ley de Firmas y Certificados Digitales (2000)

Su Objetivo es utilizar la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Su Ámbito de Aplicación son aquellas Firmas electrónicas que, puestas sobre un mensaje de datos puedan vincular e identificar al firmante, y garantizar su integridad y autenticación.

Define como Firma Digital aquella que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

Como Certificado Digital a aquel documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Por su parte la Entidad de Certificación es aquella que cumple con la función de emitir o cancelar certificados digitales.

Existe una Entidad de Registro o Verificación que es la encargada de recolectar y comprobar la información del solicitante del Certificado, además identifica y autentica al suscriptor de firma digital y acepta y autoriza las solicitudes de emisión y cancelación de certificados digitales.

La Supervisión y el Control, corren a cargo de la autoridad administrativa designada por el Poder Ejecutivo.

Las Entidades de certificación intervienen en la emisión de certificados y pueden asumir las funciones de entidades de registro o verificación.

Las Entidad de Certificación deberán de contar con un Registro.

Esta ley no establece el Valor probatorio de la Firma Electrónica.

Para que un Certificado Extranjero sea reconocido, este debe contar con el aval de una Entidad nacional

No existen Sanciones

VENEZUELA

Ley sobre Mensajes de Datos y Firmas Electrónicas (2001)

Su Objetivo es otorgar y reconocer eficacia y valor jurídico al mensaje de datos, a la firma electrónica y a toda información inteligible en formato electrónico.

Su Ámbito de Aplicación son los mensajes de datos y firmas electrónicas.

Define a la Firma Electrónica como aquella información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Como Mensajes de Datos a toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Como órgano de control, existe la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Los Proveedores de Servicios de Certificación, son los que emiten los certificados

La firma tendrá valor probatorio cuando vincule al signatario con el mensaje de datos y se pueda atribuir su autoría.

Cuando los certificados extranjeros estén garantizados por un proveedor de servicios de certificación acreditado, tendrán la misma validez y eficacia jurídica

Las Sanciones para los proveedores de servicios de certificación van de entre 500 a 2,000 Unidades Tributarias.

EUROPA

ESPAÑA

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

Su objetivo es establecer una regulación sobre el uso de firma electrónica, atribuyéndole eficacia jurídica, además de establecer lineamientos para los prestadores de servicios de certificación.

Su Ámbito de Aplicación son las firmas electrónicas, su eficacia jurídica y la prestación al público de servicios de certificación.

Define a la Firma electrónica como un conjunto de datos, en forma electrónica, ajenos 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.

Define también a la Firma Electrónica Avanzada como aquella que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

Como certificado aquella certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

Como Prestador de Servicios de Certificación a aquella persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

La supervisión corre a cargo del Ministerio de Fomento a través de la Secretaría General de Comunicaciones.

Existe un Registro de Prestadores de Servicios de Certificación en el Ministerio de Justicia, en el que se solicita su inscripción antes de iniciar actividades.

Cuando la firma electrónica avanzada esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá Valor probatorio

Para otorgarle Reconocimiento de certificados extranjeros, estos deben cumplir los siguientes requisitos:

a) 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.
b) Que el certificado esté garantizado por un prestador de servicios de la Unión Europea que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica.
c) 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.

Las Sanciones son impuestas conforme a los siguientes parámetros:

a) Por la comisión de infracciones muy graves, se impondrá multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción o, en caso de que no resulte posible aplicar este criterio lo constituirá el límite del importe de la sanción pecuniaria.

b) La reiteración de dos o más infracciones muy graves, en el plazo de cinco años, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.
c) Por la comisión de infracciones graves, se impondrá multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquéllas o, en caso de que no resulte aplicable este criterio o de su aplicación resultare una cantidad inferior a la mayor de las que a continuación se indican, esta última constituirá el límite del importe de la sanción pecuniaria.
d) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 2.000.000 de pesetas (12.020,23 euros).

Instrucción sobre el Uso de la Firma Electrónica de los Fedatarios Públicos

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. -Ley de Servicios de la Sociedad de Información-)

Proyecto de Ley de Firma Electrónica: Promoción de Autorregulación de la Industria, Concepto de Firma Electrónica Reconocida, Time stamping, Declaración de prácticas de certificación, Documento Nacional de Identidad Electrónico y Certificados para Personas Morales.

LA DIRECTIVA DE LA UNIÓN EUROPEA

La Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica (1999)

Su Objetivo es garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, instituyendo un marco jurídico homogéneo y adecuado para la Comunidad Europea, y definiendo criterios que fundamenten su reconocimiento legal.

Su Ámbito de aplicación se limita al reconocimiento legal de la firma electrónica y establece un marco jurídico para determinados servicios de certificación accesibles al público.

Define a la Firma electrónica a la realizada en forma digital integrada en unos datos, ajena a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:

1. Estar vinculada al signatario de manera única;
2. Permitir la identificación del signatario;
3. Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control
4. Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Como Dispositivo de creación de firma a los datos únicos, como códigos o claves criptográficas privadas, o un dispositivo físico de configuración única, que el signatario utiliza para crear la firma electrónica.

El Dispositivo de verificación de firma son los datos únicos, tales como códigos o claves criptográficas públicas, o un dispositivo físico de configuración única, utilizado para verificar la firma electrónica.

El Certificado reconocido es el certificado digital que vincula un dispositivo de verificación de firma a una persona y confirma su identidad, y que cumple con los requisitos establecidos en el Anexo Y de la ley.

El Proveedor de Servicios de Certificación es la persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica.

La Comisión ejerce la supervisión con ayuda del Comité de Firma Electrónica, de carácter consultivo, compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

Los Estados miembros velarán porque la firma electrónica sea considerada como firma que cumple los requisitos legales de una firma manuscrita y produce los mismos efectos que la manuscrita cuando cumpla con los requisitos establecidos en ley.

Los Estados miembros velarán porque los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país tengan la misma validez que un local cuando cumplan con los siguientes requisitos:

1. El proveedor de servicios de certificación cumple los requisitos establecidos en la presente Directiva y ha sido acreditado en el marco de un sistema voluntario de acreditación establecido por un Estado miembro;
2. Un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones del Anexo II, avala el certificado en la misma medida que los suyos propios;
3. El certificado o el proveedor de servicios de certificación están reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

No establece Sanciones

ORGANIZACIONES INTERNACIONALES
ONU

La organización de las Naciones Unidas por conducto de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNDUMI, mejor conocida por sus siglas en inglés UNCITRAL), con sedes tanto en Nueva York como en Viena, se compone por 37 países. Funciona desde 1968, elaborando múltiples convenciones, además de reglas de arbitraje, modelos de contratos, de clásulas contractuales y guías jurídicas, pero sobre todo Leyes Modelo como la de Arbitraje (adoptada por México en 1992), Comercio Electrónico (adoptada en México en el 2000) y Firma Electrónica (adoptada por nuestro país en el 2003).

En la sesión del día 12 de diciembre de 2001, fue aprobada por el pleno de la 85ª Sesión Plenaria de la Asamblea General la Ley Modelo sobre las Firmas Electrónicas.
Toda vez que esta Ley Modelo es la que ha sido mas aceptada a nivel internacional, sus puntos mas importantes serán analizados mas adelante.

OCDE
En marzo de 1997, la Organización para la Cooperación y el Desarrollo Económico publicó su recomendación para el establecimiento de políticas sobre Criptografía, sin embargo solo establece una serie de lineamientos que se sugiere a los gobiernos adoptar al momento de legislar en materia de firma digital y de Entidades Prestadoras de Servicios de Certificación.

LA FIRMA AUTÓGRAFA

No existe en nuestro Derecho, una teoría sobre la firma, sus elementos, consecuencias o su concepto y las pocas referencias que existen son obras de Derecho Notarial .

“En Roma, existía la Manufirmatio, que consistía en una ceremonia en que leído el documento por su autor, o el funcionario, se colocaba desenrollando y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre, signo, o una o tres cruces, por el autor o el funcionario en su nombre, haciéndolo seguidamente los testigos. Más que in requisito, la Manufirmatio era en sí misma parte del espectáculo solemne en que se realizaba el acto”

En la Edad Media, se inscribía una cruz a la que se le añadían diversas letras y rasgos. Estos signos se utilizaban como firma. Debido a que no sabían leer ni escribir, los nobles remplazaron esta práctica con el uso de sellos.

“La diferenciación entre “firmas” y “signos” hizo que se empezase a entender que aquellas eran, más que simples “signos”, la inscripción manuscrita del nombre o de los apellidos. En ese tiempo, pocas eran las personas que sabían leer y escribir, por lo que generalmente los particulares estampaban en los documentos que suscribían diversos signos o sellos, la extensión de la instrucción y el desenvolvimiento de las transacciones comerciales, hicieron que la firma fuera adquiriendo la importancia y uso que con el transcurso del tiempo se fue consgrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona.”

Según el Diccionario de la Real Academia, la firma es el 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.

Si se considera a la firma como un conjunto de signos, podemos distinguir que esta tiene una doble función por un lado el hecho de que vincula a la persona con el acto jurídico, esto es, se torna IDENTIFICADORA de la persona, puesto que determina su personalidad, así como sus derechos y obligaciones sobre el convenio de que se trata. Sin embargo este método no es totalmente fiable puesto que el mismo podría ser falsificado y su autoría deberá ser comprobada por un perito.

Existe también la AUTENTICACION que consiste en “el proceso por medio del cual se revelan algunos aspectos de la identidad de una persona.” Es decir el autor además de expresar su consentimiento, y toma como suyo el mensaje.

Así, la firma autógrafa se utiliza para expresar el consentimiento de las partes sobre un contrato en particular, sin embargo su uso no se encuentra regulado en ninguna legislación, su utilización se ha venido dando a lo largo de los años.

CARACTERÍSTICAS DE LA FIRMA

La firma autógrafa tiene las siguientes características:

IDENTIFICATIVA: Sirve para identificar quién es el autor del documento.

DECLARATIVA: Significa la asunción del contenido del documento por el autor de la firma. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.

PROBATORIA: Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.

ELEMENTOS DE LA FIRMA .-

Al respecto es necesario distinguir entre:

ELEMENTOS FORMALES.- Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la misma:

La firma como signo personal. La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

El animus signandi. Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento, que no debe confundirse con la voluntad de contratar, como señala Larrieu.

ELEMENTOS FUNCIONALES. Tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función:

Identificadora. La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. La identidad de la persona nos determina su personalidad a efectos de atribución de los derechos y obligaciones. La firma manuscrita expresa la identidad, aceptación y autoría del firmante. No es un método de autenticación totalmente fiable. En el caso de que se reconozca la firma, el documento podría haber sido modificado en cuanto a su contenido -falsificado- y en el caso de que no exista la firma autógrafa puede ser que ya no exista otro modo de autenticación. En caso de duda o negación puede establecerse la correspondiente pericial caligráfica para su esclarecimiento.

Autenticación. El autor del acto expresa su consentimiento y hace propio el mensaje:

Operación pasiva que no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado.

Proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo.

La firma es el lazo que une al firmante con el documento en que se pone , el nexo entre la persona y el documento. Para establecer ese lazo, la firma no necesita ni ser nominal ni ser legible; esto es, no requiere expresar de manera legible el nombre del firmante; en una palabra no requiere aptitud para desempeñar aquella función identificativa de la firma a la que nos referíamos en párrafos anteriores, que señalaba Carnelutti y de la que los “informáticos” han hecho propia, pero que ni antes ni mucho menos ahora los documentos escritos acostumbran a cumplir; los documentos, en efecto, no suelen indicar mediante la firma quien es su autor (ni quienes son las demás personas que en ellos intervienen), sino que lo hacen en su encabezamiento (inscriptio, praescriptio), o en el cuerpo del documento; a lo que quiero llegar y polarizando hacia la firma electrónica, es que la función identificativa de la firma es una exigencia de la contratación a distancia y no de los conceptos tradicionales de documento y firma.

La firma, al constituir el lazo o nexo de la persona con el documento, debe ser documental y personal y ha de haber sido puesta en el documento por el firmante “en persona” . La idea anterior suele expresarse como “manuscritura” (escritura con la propia mano, del puño y letra del suscribiente), pero se debe ampliar a cualquier otra “grafía” puesta en el documento por el firmante mismo, es decir a toda “autografía”, de ahí el término de “firma autógrafa”. Es decir, lo que resulta destacar es la actuación del firmante mismo en el documento y en éste orden de ideas la “manuscritura” puede ser sustituida por cualquier otra “grafía” del firmante que necesariamente haya de ser personal, como hasta ahora viene ocurriendo con la huella digital pero no por otra grafía que pueda ser impuesta por un tercero o por procedimientos que permitan a terceros imponerla.

El uso mercantil y bancario han ido orientándose a que la “firma” pueda estamparse por medios mecánicos como pueden ser el facsímil y las máquinas de firma, para poder considerarla se requiere de un acuerdo previo entre las partes en el que se haga constar que el “supuesto firmante” asume la responsabilidad. Por lo anterior, en lo particular, cuestiono el denominativo de firma al símbolo estampado por un tercero por medio de facsímil o “máquinas de firma”.

Resumiendo, la función primordial de la firma no es entonces la identificación del firmante, sino la de ser el instrumento de su declaración de voluntad, que exige esa actuación personal del firmante en la que declara que aquello es un documento y no un proyecto o un borrador, que el documento está terminado y declara que el firmante asume como propias las manifestaciones, declaraciones o acuerdos que contiene.

Algunos autores consideran que la firma como exteriorización de la declaración de voluntad de una persona es imprescindible en los documentos comerciales, no es un mero requisito, la cual precisa de una actuación personal del firmante, una actuación física, corporal del firmante mismo, porque solo así puede ser instrumento de su declaración de voluntad. En éste sentido no estoy de acuerdo, ya que considero que si la firma es la exteriorización de la declaración de voluntad de una persona, ésta exteriorización puede hacerse por otro medio, como pudiera ser el electrónico siempre que la haga el firmante o legalmente se atribuya a él. Y aquí retomo lo comentado en párrafos anteriores sobre la función identificativa de la firma, pero ahora con el calificativo de electrónica, pues ésta sí requiere de identificación del autor para dar certeza de que es él y no un tercero quien declara su voluntad, de ahí el concepto de UNICITRAL de "equivalente funcional de la firma".

En cuanto al concepto de equivalencia funcional de la firma y a manera de resumen, resulta de utilidad el siguiente cuadro que refleja la distinción entre la firma autógrafa y la firma electrónica:

	FIRMA AUTÓGRAFA	**FIRMA ELECTRÓNICA**
ELEMENTOS FORMALES.-		
La firma como signo personal.	X	X
El *animus signandi*, voluntad de asumir el contenido de un documento.	X	X
ELEMENTOS FUNCIONALES		
Función Identificadora, relación jurídica entre el acto firmado y la persona que lo ha firmado.	X	X
Función de Autenticación. El autor del acto expresa su consentimiento y hace propio el mensaje	X	X
INTEGRIDAD		X
ACCESIBILIDAD		X

FIRMA ELECTRÓNICA

Existen muchas definiciones de Firma Electrónica, sin embargo consideramos que la mas completa es la establecida por la UNCITRAL:

Por “firma electrónica” se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

El documento electrónico o informático, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica. La seguridad en el comercio electrónico es fundamental para su desarrollo. En un flujo de transacciones en donde las partes ya no tienen contacto ‘físico’, ¿cómo pueden asegurarse de la identidad de aquel con quien están realizando una operación? e, incluso, ¿cómo pueden tener la certeza de que la información intercambiada no ha sido robada, alterada o conocida por personas ajenas?

La firma electrónica, técnicamente, es un conjunto o bloque de caracteres que viaja junto a un documento, fichero o mensaje y que puede acreditar cuál es el autor o emisor del mismo (lo que se denomina autenticación) y que nadie ha manipulado o modificado el mensaje en el transcurso de la comunicación (o integridad).

Es aquél conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico (es decir, contenido en un soporte magnético ya sea en un disquete, algún dispositivo externo o disco duro de una computadora y no de papel), que permite identificar a su autor, es decir que es el conjunto de datos, en forma electrónica, anexos 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.

La Firma Electrónica permite identificar a la persona que realiza la transacción, es decir, proporciona el servicio de autentificación (verificación de la autoridad del firmante para estar seguro de que fue él y no otro el autor del documento) y no de repudio (seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones asignadas en él).

Quizás la parte que más nos interesa a los usuarios es la garantía de detección de cualquier modificación de los datos firmados, proporcionando una integridad total ante alteraciones fortuitas o deliberadas durante la transmisión telemática del documento firmado. El hecho de la firma sea creada por el usuario mediante medios que mantiene bajo su propio control (clave privada protegida, contraseña, datos biométricos, tarjeta chip, etc.) asegura la imposibilidad de efectuar de lo que se conoce como “suplantación de personalidad”.

En otras palabras podríamos definir a la Firma electrónica como el conjunto de datos, en forma electrónica, anexos 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. La debilidad en cuanto al emisor y al receptor radica en la posible suplantación de la identidad de alguno de ellos por parte de elementos ajenos al sistema.

FIRMA ELECTRÓNICA AVANZADA

Según la UNCITRAL, para que una firma electrónica sea considerada como fiable debe cumplir con lo siguiente:

a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante

c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Con lo anterior es factible garantizar:

Autenticación, para asegurar la identidad de la persona con la que se está comerciando.

Autorización, para asegurar que a esa persona es la indicada para llevar a cabo una operación concreta.

Privacidad, para garantizar que nadie mas va a ver los intercambios de datos que se lleven a cabo.

Integridad, para asegurar que la transmisión no sea alterada en ruta o en almacenaje

No Repudiación, para garantizar que quien envía el mensaje no puede negar que lo envió el."

EQUIVALENCIA FUNCIONAL

El reto mas importante fue equiparar la firma electrónica a la firma autógrafa, dándole los mismos atributos y la misma validez jurídica.

Según la Ley Modelo, "Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje".

La firma electrónica entonces será fiable si hay acuerdo entre las partes para su uso (intercambio de claves y contraseñas), ahora bien, por disposición de ley y salvo prueba en contrario se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo anterior "si:

a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma."

De esta manera se pretende que la documentación consignada por medios electrónicos otorgue un grado de seguridad equivalente al del papel, junto con su característica principal, mayor confiabilidad y rapidez

NEUTRALIDAD TECNOLÓGICA

Con el paso del tiempo la tecnología avanza a pasos agigantados, no podemos limitar el cumplimiento de las disposiciones de ley a una determinada tecnología, porque no sería justo para las demás y esto limitaría el desarrollo tecnológico.

La propia UNCITRAL, sobre el particular establece que: "Convencida de que la armonización tecnológicamente neutral de ciertas normas relativas al reconocimiento jurídico de las firmas electrónicas y el establecimiento de un método para evaluar de un modo tecnológicamente neutral la fiabilidad práctica y la idoneidad comercial de las técnicas de firma electrónica darán una mayor certidumbre jurídica al comercio electrónico."

El reto es que estas reformas puedan lograr un equilibrio entre el proceso mas dinámico, que es la tecnología, con el mas lento, que es la creación de leyes.

PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

Según la UNCITRAL, un Prestador de Servicios de Certificación, es aquella persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

Es un tercero confiable que acredita el vínculo existente entre una clave y su propietario. Además extiende un certificado de firma electrónica el cual está firmado con su propia clave, para así garantizar la autenticidad de la información.

La existencia de diversos Prestadores de Servicios de Certificación, permitirá que sea el propio usuario quien elija a aquella Entidad que le proporcione mayor confianza y/o seguridad.

CERTIFICADOS

Según la Ley Modelo el Certificado es todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma (clave privada).
Es un archivo que incorpora la clave pública de un sujeto y la relaciona con su clave privada.
Su validez consiste en que es la propia Agencia de Certificación o un agente, persona física, dependiente de él, quien actuando como tercero confiable, verifica la identidad de el firmante y da certeza a cualquier otra sobre tal información.

OBLIGACIONES DE LAS PARTES:

OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

a) Actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas. A esto se le llama Declaratoria de Prácticas de Certificación y constituye el límite de Responsabilidad frente al Usuario y Firmante del Prestador de Servicios de Certificación;

b) Actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho el firmante en relación con el certificado o que estén consignadas en él sean exactas y cabales;

c) Proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

i) La identidad del prestador de servicios de certificación;

ii) Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) Proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

i) El método utilizado para comprobar la identidad del firmante;

ii) Cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma (clave privada) o el certificado;

iii) Si los datos de creación de la firma (clave privada) son válidos;

iv) Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) Si existe un medio para que el firmante dé aviso de que los datos de creación de la firma (clave privada) no estén o puedan no estar en su poder;

vi) Si se ofrece un servicio para revocar oportunamente el certificado;

e) Proporcionar un medio para que el firmante dé aviso de que los datos de creación de la firma (clave privada) no estén o puedan no estar en su poder y, cuando se ofrezcan servicios de Registro de Certificados cerciorarse de que existe un servicio para revocar oportunamente el certificado;

f) Utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido estos.

OBLIGACIONES DEL FIRMANTE

Cuando puedan utilizarse datos de creación de firmas (clave privada) para crear una firma con efectos jurídicos, cada firmante deberá:

a) Actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma (clave privada);

b) Sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación, o en cualquier caso esforzarse razonablemente, para dar aviso en caso de que:
i) el firmante sepa que los datos de creación de la firma (clave privada) han quedado en entredicho; o
ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma (clave privada) hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el certificado o que hayan de consignarse en él son exactas y cabales.

OBLIGACIONES DE LA PARTE QUE CONFIA
a) Verificar la fiabilidad de la firma electrónica; o
b) Cuando la firma electrónica esté refrendada por un certificado:
i) Verificar la validez, suspensión o revocación del certificado; y
ii) Tener en cuenta cualquier limitación en relación con el certificado.

LA CRIPTOGRAFÍA

ANTECEDENTES

Criptografía es la ciencia de la seguridad de la información aunque muchas veces ha sido descrita como el arte o la ciencia de la escritura secreta. Por medio de ella se puede almacenar o transmitir información en una forma tal que permite ser revelada únicamente a aquellos que deben verla. La palabra viene del griego kryptos, que significa “oculto”. La criptografía está relacionada con el criptoanálisis, que es la práctica de violar los intentos de esconder información y es parte de la criptología, donde se incluye la criptografía y el criptoanálisis.

El origen de la criptografía data de el año 2000 AC., con los egipcios y sus jeroglíficos. Los jeroglíficos estaban compuestos de pictogramas complejos, donde sólo el significado completo podría ser interpretado por algunos. El primer indicio de criptografía moderna fue usado por Julio César (100 AC. a 44 AC.), quien no confiaba en sus mensajeros cuando se comunicaba con los gobernadores y oficiales. Por esta razón, creó un sistema en donde los caracteres eran reemplazados por el tercer caracter siguiente del alfabeto romano. No solo los romanos, sino los árabes y los vikingos hicieron uso de sistemas de cifrado.

Gabriel de Lavinde hizo de la criptografía una ciencia más formal cuando publicó su primer manual sobre Criptología en 1379.
Samuel Morse. El Código Morse, desarrollado en 1832, aunque no es propiamente un código como los otros, es una forma de cifrar las letras del alfabeto dentro de sonidos largos y cortos.

En tiempos modernos, la criptografía se ha convertido en una compleja batalla entre los mejores matemáticos del mundo y de los ingenieros en sistemas computacionales. La habilidad de poder almacenar de manera segura y de transferir la información ha dado un factor de éxito en la guerra y en los negocios.

Dado a que los gobiernos no desean que ciertas entidades entren y salgan de sus países para tener acceso a recibir o enviar información que puede comprometer y ser de interés nacional, la criptografía ha sido restringida en muchos países, desde la limitación en el uso, la exportación o la distribución de software de conceptos matemáticos que pueden ser usados para desarrollar sistemas criptográficos.

De cualquier manera, el Internet ha permitido que todas estas herramientas sean distribuidas, así como las tecnologías y técnicas de criptografía, de tal manera, que al día de hoy, la mayoría de los sistemas criptográficos avanzados están en dominio público.

La criptografía incluye técnicas como esconder texto en imágenes y otras formas de esconder información almacenada o en tránsito.

Simplificando el concepto, hoy en día la criptografía se asocia más a convertir texto sencillo a texto cifrado y viceversa. La Criptografía se ocupa de dar solución a los problemas de identificación, autenticación y privacidad de la información en los sistemas informáticos. Debido a la naturaleza de un medio no físico, no resultan útiles los métodos tradicionales de sellar o firmar documentos, con propósitos comerciales o legales.

En lugar de esto, dentro de la información digital que se desea proteger, debe colocarse algún tipo de marca codificada que sirva para identificar el origen, autenticar el contenido y asegurar la privacidad ante posibles intrusos. La protección de la privacidad utilizando un algoritmo simétrico, como por ejemplo el contenido en el estándar DES (Data Encryption Standard), es sencillo en redes pequeñas, pero requiere el intercambio de la clave secreta de encriptación entre cada una de las partes. En la medida en que han proliferado las redes, el intercambio seguro de las claves secretas se ha vuelto costoso e inadecuado. Por tanto, el empleo aislado de esta solución, es inadecuado para grandes redes de comunicación. El estándar DES sufre una desventaja adicional: requiere que se comparta el conocimiento de la Clave Privada. Cada persona debe confiar en la otra respecto de la custodia de la clave secreta común y, además, no transmitírsela a nadie más. Teniendo en cuenta que el usuario debe tener diferentes claves para cada una de las personas con las que se quiere comunicar, debe compartir con cada una de ellas una de sus claves secretas. Esto significa que desde el punto de vista de la implantación práctica, solamente se puede establecer una comunicación segura entre personas que tengan alguna relación previa.

Por tanto, los aspectos fundamentales que DES no cubre son la autenticación y el no repudio. El hecho de que la clave secreta sea compartida implica que cada una de las partes no puede estar absolutamente segura de lo que la otra ha hecho con la misma. Incluso, una de las partes puede, maliciosamente, modificar los datos sin que un tercero pueda determinar la verdadera identidad del remitente ni quién es el culpable de la alteración. La misma clave que hace posible comunicaciones seguras puede ser empleada para crear documentos falsificados en nombre del otro usuario.

ALGORITMOS
Un Algoritmo en general es la serie de reglas que no pueden ser ambigüas y deben tener una meta clara. Los algoritmos pueden ser expresados en cualquier lenguaje, desde el inglés al francés, hasta lenguajes de programación de computadoras.

Los algoritmos criptográficos son la base para construir aplicaciones y protocolos de encripción.

Existen dos tipos generales de algoritmos basados en claves que son: Simétricos y Asimétrico.

ALGORITMO DE ENCRIPCIÓN SIMÉTRICO
Cuando la clave que va a encriptar el mensaje puede ser calculada desde la clave para desenciptar y viceversa se le conoce como algoritmo simétrico. En muchos de los algoritmos asimétricos, la clave de encripción y para desencriptar es la misma. Estos algoritmos requieren que el emisor y el receptor tengan la misma clave antes de comunicarse. La seguridad de un algoritmo simétrico realmente recae en la clave. El divulgar la clave significa que cualquiera puede encriptar o desencriptar la información. La clave tiene que mantenerse en secreto tanto tiempo como la comunicación se quiere mantener en secreto.

ALGORITMO DE ENCRIPCIÓN ASIMÉTRICO
Los algoritmos asimétricos o también llamados de clave pública son diseñados de tal manera que una clave se usa para encriptar y una diferente para desencriptar. Esto ocasiona que teniendo la clave para desencriptar, no se puede calcular la clave de encripción. Estos algoritmos son llamados de “clave pública” porque la clave para encripción se puede publicar. Un completo desconocido puede usar la clave para encriptar el mensaje, pero sólo una persona puede desencriptar el mensaje. En estos sistemas, la clave de encripción es llamada clave pública y la clave para desencriptar se llama clave privada.

MÉTODOS DE ENCRIPCIÓN
En las siguientes páginas se hablará de los algoritmos criptográficos más importantes usados hoy en día para la seguridad. Cada uno de los algoritmos es identificado por un nombre, un propósito, un rango de clave y por la fecha de creación.

Todos los algoritmos tienen uno o más propósitos:

A) Encripción
Se usan simplemente para encriptar comunicación. Tanto el emisor como el receptor encriptan y decriptan el mensaje usando el mismo algoritmo.

B) Firmas Digitales
Existen muchos algoritmos de firma electrónica. Todos ellos son algoritmos de clave pública con información secreta para firmar documentos e información pública para verificar las firmas. Muchas veces al proceso de firmado se le llama encriptar con una clave privada y la verificación se le llama desencriptar con una clave pública, pero esto es sólo verdadero para el algoritmo usado por RSA.

C) Hashing y Digest
Un algoritmo de hashing es una función matemática que toma una cadena de longitud variable y la convierte a una cadena de longitud fija. Es una manera de obtener una huella digital de los datos. Si se necesita verificar un archivo que pertenece a cierta persona se manda un valor de hashing para comprobarlo. Esto es muy usado en transacciones financieras. El algoritmo de hashing genera un valor para el mensaje.

El Digest es la representación del texto en forma de una cadena de dígitos, creado con una fórmula de hashing de una sola dirección. El encriptar un digest de un mensaje con una clave privada, genera una firma digital.

ALGORITMOS DE ENCRIPCIÓN
RSA
Propósito: Encripción y Firma Digital
Rango de clave: 1024 bits para uso corporativo y 2048 para claves valuables
Fecha de Creación: 1977

RSA es un sistema de encripción y autenticación que usa un algoritmo desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman.

El algoritmo RSA es el más usado en Internet dado a que es parte de los navegadores como Netscape e Internet Explorer, así como de muchos otros productos.

Los problemas de autenticación y protección de la información en grandes redes de comunicación fueron analizados en 1976, en el plano teórico, por Whitfield Diffie y Martin Hellman, en un trabajo en el que explicaron sus conceptos respecto del intercambio de mensajes sin necesidad de intercambiarse claves secretas. La idea fructificó en 1977 con la creación del Sistema Criptográfico de Clave Pública RSA, por parte de Ronald Rivest, Adi Shamir y Len Adleman, por aquel entonces profesores del Instituto de Tecnología de Massachusetts (M.I.T.). En lugar de emplear una sola clave para encriptar y desencriptar datos, el sistema RSA emplea un par combinado de claves que desarrolla una transformación en un solo sentido. Cada clave es la función inversa de la otra, es decir, lo que una hace, sólo la otra puede deshacerlo. La Clave Pública en el sistema RSA es publicada por su propietario, en tanto que la Clave Privada es mantenida en secreto. Para enviar un mensaje privado, el emisor lo encripta con la Clave Pública del receptor deseado. Una vez que ha sido encriptado, el mensaje sólo puede ser descifrado con la Clave Privada del receptor. Inversamente, el usuario puede encriptar datos utilizando su Clave Privada. Es decir, las claves del sistema RSA pueden ser empleadas en cualquier dirección. Esto sienta las bases para la firma digital. Si un usuario puede desencriptar un mensaje con la Clave Pública de otro usuario, éste debe, necesariamente, haber utilizado su Clave Privada para encriptarlo originariamente. Desde el momento que solamente el propietario puede utilizar su propia Clave Privada, el mensaje encriptado se transforma en una especie de firma digital, un documento que nadie más ha podido crear.
Bajo RSA se desarrolló el algoritmo estándar de firmas digitales para correos S/MIME

Funcionamiento del RSA
Los números enteros (el 0, 1, 2... y sus opuestos -1,-2, etc.) tienen una estructura algebraica determinada con las operaciones que todos conocemos, el producto y la suma. Esta estructura es la de anillo conmutativo y una de sus características es la existencia de un elemento neutro respecto al producto, que es la unidad. En este anillo existen dos divisores de la unidad (el número 1), el 1 y el -1.

Dados dos números enteros, p y q, es posible encontrar otros dos, c y r tales que $p = q.c + r$. A c se le suele llamar cociente y a r resto. Particularmente, existe un r tal que $r < |q|$.
Cuando r es cero, entonces decimos que q es un factor de p.

Fijado un entero q, existen |q| restos posibles: 0, 1, 2,....,|q-1| y es definible una relación de equivalencia: Dos enteros m y n son equivalentes si y sólo si m-n es un múltiplo de q. Esto es lo mismo que decir que tanto m como n tienen el mismo resto, o que m es congruente con n módulo q, y lo simbolizaremos por $m = n \pmod q$. El conjunto de las clases de equivalencia forma a su vez un anillo y tendremos tantas como restos posibles.

Decimos que d es el máximo común divisor de dos números p y q cuando es el factor más grande de p y q: $d = m.c.d\ (p,q)$.
Dos números p y q son primos entre sí, cuando $m.c.d\ (p,q) = 1$.

Un número p es primo cuando siempre que exista un factor q tal que $p = q.k$ entonces k es un divisor de la unidad (dicho en pocas palabras, sólo se puede dividir por él mismo).

Cualquier número q es un producto de primos y este producto es único (salvo divisores de la unidad).

Existe un número infinito de primos, no hay una fórmula para obtenerlos y su distribución no se puede determinar por métodos numéricos.

DSA
Propósito: Firmas Digitales
Rango de clave: 56 bits
Fecha de Creación: 1994

El Digital Signature Algorithm (DSA) fue publicado por el Instituto Nacional de Tecnología y Estándares (NIST) en el estándar llamado Digital Signature Standard (DSS) que es parte de gobierno de los Estados Unidos. DSS fue seleccionado por el NIST con ayuda del NSA (National Security Agency) para ser el estándar de autenticación digital del gobierno de los Estados Unidos a partir de Mayo 19 de 1994.

DSA está basado en el problema de logaritmos discretos y se deriva de sistemas criptográficos propuestos por Schnorr y ElGamal. Es únicamente para autenticación.

Diffie-Hellman (DH)
Propósito: Firmas Digitales
Rango de clave: 1536 bits
Fecha de Creación: 1976

Este fue el primer algoritmo de clave pública inventado. Tiene su seguridad en la dificultad de calcular logaritmos discretos infinitamente. DH se usa principalmente para distribución de claves. Es usado para generar claves secretas, mas no se usa para encriptar ni decriptar.

DES
Propósito: Encripción
Rango de clave: 56 bits
Fecha de Creación: 1976

El Data Encryption Standard (DES) conocido también como el Algoritmo de Encripción de Datos (DEA) ha sido un estándar por cerca de 20 años. Aunque muestra signos de que tiene mucho tiempo, se ha desempeñado muy bien a través de años de criptoanálisis y es aún seguro contra los adversarios.

DES es un bloque cifrado, encriptando los datos en bloques de 64 bits. DES es un algoritmo simétrico, el mismo algoritmo se usa para encriptar y desencriptar.

La clave tiene un tamaño de 56 bits, la clave usa un número de 56 bits y puede ser cambiado a cualquier hora. La seguridad recae directamente en la clave.

Otros algoritmos de Encripción:
- 3DES y ya se está implementando el AES (Advanced Encryption Standard).
- RC2
- RC4
- RC5
- ECC (Critpografía de Curva Elíptica)

MD5
Propósito: Hashing (Digestión de documentos digitales)
Rango de clave: 128 bits
Fecha de Creación: 1992

MD5 es una función de hashing de una sola dirección, produciendo un resultado de 128 bits. Después de un proceso inicial, MD5 procesa el texto insertado en bloques de 512 bits, divididos en 16 bloques de 32 bits. El resultado de el algoritmo son 4 bloques de 32 bits, que juntos forman un bloque de 128 bits.

Otros algoritmos de hashing:
- SHA-1

ESTÁNDARES ABIERTOS:
No hay que olvidar que utilizar estándares abiertos para la generación y utilización de firmas digitales permite :

Interoperabilidad entre diferentes plataformas en redes heterogéneas
Sectores Comercial, Financiero, Gobierno, TIC.
Interoperabilidad con empresas e instituciones internacionales
TLCAN, todos estamos conectados, reconocer comprobantes multinacionales.
Ambientes competitivos que benefician a los clientes.
Precios, servicios, calidad.
Implementación de soluciones probadas y seguras.
Outsourcing. No hay que inventar nada. Enfoque a procesos y servicios propios.
Evita tecnologías patentadas.
Riesgos de obsolescencia y especialización.
Implantación libremente disponible (open source) así como implantaciones comerciales.
Extensible – se puede usar en el futuro, cuando surgen aplicaciones nuevas.

Las pautas que apoyan a los estándares abiertos :

WebTrust para Autoridades de Certificación: Tiene la cobertura de áreas específicamente definidas por el AICPA/CICA, para auditar las prácticas de negocio de AC, integridad de servicio (incluso ciclo de vida de llaves y actividades de administración de certificados) y controles ambientales de AC. Fue diseñado expresamente para los exámenes de actividades de negocios de AC.

Federal Bridge CA (FBCA): El FBCA es el elemento que une las Autoridades de Certificación de agencias que por otra parte no se podrían conectar en un PKI sistemáticamente federal. El FBCA funciona como un 'puente' no jerárquico que crea un camino de su dominio hasta el dominio de la agencia que publicó el certificado, de modo que los niveles de aseguramiento honrado por PKIs puedan ser reconciliados.

American National Standards Institute (ANSI): el ANSI X9F5 Política de Certificado y Firma Digital desarrolla el X9.79 PKI Prácticas y Marco de Política (X9.79) estándar para la comunidad de servicios financieros.

American Bar Association's Information Security Committee (ABA-ISC): Han desarrollado las Pautas de Evaluación PKI (PAG) que se dirigen a las exigencias legales y técnicas para Autoridades de Certificación.

EU (European Commission) Electronic Signature Directive: La directiva proporciona un marco común para firmas electrónicas. Armonización de los aspectos: legal, confianza, y técnico. Propone un marco para los estandares abiertos en proporcionar la base para la realización, revisión de cuentas y acreditación.

European Telecommunications Standards Institute (ETSI): El objetivo principal del ETSI es apoyar la armonización global proporcionando un foro en el cual todos los jugadores clave, puedan contribuirse activamente. El ETSI es oficialmente reconocido por la Comisión Europea y la secretaría de EFTA.

Internet Engineering Task Force (IETF): El IETF es una comunidad internacional abierta de diseñadores de red, operadores, vendedores e investigadores preocupados por la evolución de la arquitectura y la operación del Internet. Escribieron un documento (RFC2459) cuyo objetivo es desarrollar un perfil para facilitar el uso de certificados X.509 dentro de las aplicaciones de Internet y PKI.

Microsoft Program: Microsoft inició un programa de PKI usando los principios y criterios de WebTrust para Autoridades de Certifición para auditar y revisar las autoridades de certificación de raíz en el Windows XP.

Identrus: Identrus es una red global de instituciones financieras que proporciona un marco legal, empresarial al tradicional PKI y técnico a los estándares que permiten a los bancos servir a sus

clientes de negocio. Estas actúan como terceras partes de confianza para el comercio electrónico en el que intervienen algunas instituciones financieras.

Componentes de PKI	Estandares Abiertos	Pautas de PKI
Symmetric Encryp. Algorithms		
DES, CAST, Triple-DES, RC2 y IDEA encryption	FIFS PUB, ANSI X.392, X.9.52, RFC 2144, 2268, ISO/IEC 9979	✓
Digital Signature Algorithms		
RSA, DSA, ECDSA	PKCS #1, FIPS PUB 186-2, ANSI X9.30	✓
One-Way Hash Functions		
SHA-1, MD5, MD2, RIPEMD-160	FIPS PUB 180-1, ANSI X9.30, RFC 1321, 1319, ISO/IEC 10118-3:1998	✓
Key Exchange Algorithms		
RSA, Diffie-Hellman, SPKM	RFC 1423, PKCS #1, #3, IEEE P1363, RFC 2025	✓
Symmetric Integrity Techniques		
MAC, HMAC	FIPS PUB 113, X9.19, RFC 2104	✓
Certificate Management		
PKIX, SEP, PKCS	RFC 2510, 2511	✓

INFRAESTRUCTURA DE CLAVE PÚBLICA

PKI (Public Key Infraestructure) es una arquitectura de seguridad que ha sido desarrollada para proveer de un nivel mayor de confidencialidad al intercambiar información en Internet.

El término PKI puede llegar a ser muy confuso, incluso para personal técnico, ya que puede significar varias cosas diferentes. Por un lado, PKI puede significar métodos, tecnologías y técnicas que juntas proveen de una infraestructura segura. Por otro lado, puede significar el uso de claves públicas y privadas para autenticarse y verificación de contenido. Una infraestructura de PKI debe ofrecer a los usuarios de los siguientes beneficios:

- Confirmación de la integridad y calidad de la información enviada y recibida electrónicamente
- Confirmación de la fuente y destino de esa información
- Seguridad en el tiempo de la información
- Confirmación de la privacidad de la información

Estas facilidades son realizadas usando una técnica matemática llamada criptografía de clave pública que usa un par de claves criptográficas para verificar la identidad del emisor (firma) y/o asegurar la privacidad (encripción).

Dentro de los componentes más importantes de PKI se encuentran:
- Agencias Certificadoras (CA)
- Agencias de Registro (RA)
- Protocolos de Administración de Certificados (CMP)
- Repositorios de Certificados
- Servidores “Time Stamp” (TSA)

Las CA tienen un conjunto de políticas operativas que describen la implantación y apoyo a las políticas de seguridad, condensadas en un detallado documento conocido como la Declaración de Prácticas de Certificación (CPS). Estas políticas incluyen: Procedimientos Verificación de Identidad, Rango de Usuarios a Certificar, Ciclo de Vida de un certificado, etc. Constituyen la limitación de responsabilidad de la Agencia Certificadora frente a sus usuarios.
La lista de Revocación de Certificados (CRL) permite conocer la validez de un certificado, al verificar que no se encuentre en esa lista.

CONCEPTO DE CLAVE PÚBLICA
La criptografía de clave pública usa un par de claves criptográficas. Si una clave sirve para encriptar la información, entonces únicamente la otra clave puede decriptar la información. Si se conoce una de las claves no se puede fácilmente calcular la otra. Por consiguiente, en un sistema de clave pública se tiene lo siguiente:

- Una clave pública: Que se hace público – se encuentra a disposición de todos.
- Una correspondiente (y única) clave privada: Que se debe mantener en secreto y no se comparte a los demás.

Por medio de estos conceptos, podemos asociar los siguientes conceptos básicos:

- Autenticación: Asegurarse que la entidad que envió los datos es quien dice ser.
- Integridad: Asegurarse que la información no fue alterada (intencionalmente o sin intención) entre el emisor y el receptor o entre el momento que fue generado y el momento recibido.
- Confidencialidad: Asegurarse que no cualquier entidad puede tener acceso a esa información que fue generada intencionalmente para una sola entidad.

La clave Pública usada para Encriptar

Una persona en Internet usa la clave pública de otra cuando requiere enviar información confidencial. La información que será enviada estará encriptada usando una clave simétrica única, la cual será encriptada por la clave pública. Esta doble Encripción permite hacer el proceso más rápido, teniendo que encriptar con la clave pública únicamente la clave simétrica única de menor tamaño que la información. Se puede proveer de la clave pública al emisor o puede ser obtenida directamente del directorio donde ha sido publicada.

La clave Privada usada para Desencriptar

Una clave privada es usada para desencriptar la clave simétrica única y así desencriptar la información que ha sido encriptada por la clave pública correspondiente. La persona usando la clave privada puede asegurar que la información que recibe únicamente puede ser vista por ella pero no puede asegurar la identidad del emisor del mensaje.

La clave Privada para Firmar

Si el emisor desea proveer una verificación de que es realmente esa persona, se usa una clave privada para firmar digitalmente el mensaje. A diferencia de una firma con la que firmamos papeles legales, la firma electrónica es diferente cada vez que se realiza. Un valor matemático único, determinado por el contenido del mensaje es calculado usando un algoritmo de “hashing” o “digestión” para después este valor sea encriptado con la clave privada, creando así la firma electrónica para este mensaje. El valor encriptado viene adjunto al mensaje o en un archivo por separado junto con el mensaje. La clave pública correspondiente a la clave privada puede ser enviada junto con el mensaje como parte de un certificado.

La clave Pública para Verificar Firmas

El receptor de un mensaje firmado digitalmente usa la clave pública de la otra persona para verificar la firma realizando los siguientes pasos:

1. La clave pública es usada para desencriptar el valor que el emisor envió calculado en base al mensaje.
2. Usando el mismo algoritmo de hashing o digestión, realiza el cálculo matemático del mensaje.
3. El valor resultante es comparado con el valor recibido por el emisor. Si los valores concuerdan, el receptor sabe que la persona controlando la clave privada corresponde a la clave pública que envió la información. De esa manera también se asegura que la información no ha sido alterada desde que fue firmada.
4. Si un certificado de clave pública fue recibido con la información, entonces es validado con la Autoridad Certificadora que generó el certificado para asegurar que el certificado no ha sido falsificado y que la identidad del controlador de la clave privada es genuina.
5. Finalmente, si es posible, se revisa la lista de certificados revocados en la Autoridad Certificadora para validar que el certificado el válido.

Para encriptar información que será almacenada para uso propio (únicamente la persona que encripta la información podrá leerla) se usa la clave pública propia para poder desencriptar la información más adelante con la clave privada.

Es muy importante aclarar que la generación de las claves invariablemente debe partir del propio usuario, en la práctica el usuario baja una aplicación programada para generar el par de claves, conserva su clave privada y el requerimiento de certificación junto con su clave pública lo presenta ante una agencia de certificación o agente de ésta, se identifica y le genera un certificado.

CERTIFICADOS DIGITALES

Un certificado es información con respecto a la clave pública que ha sido firmada por una Autoridad Certificadora (CA). La información normalmente encontrada en el certificado, actualmente se basa en el estándar X.509 v3. Los certificados dentro de éste estándar incluyen información de la identidad del propietario de la clave privada, el tamaño de la clave, el algoritmo usado y el algoritmo de hashing asociado, vencimiento y las acciones que se pueden realizar con este certificado.

El certificado es esencial para PKI toda vez que permite asociar a una persona determinada una clave pública y por ende su privada. Esto es, el propio requermiento de certificación que incluye algunos datos del solicitante constituye el antecedente del certificado.

EL ESTÁNDAR X. 509 V 3

El estándar X.509 inicialmente fue publicado por el ITU-T X.509 o ISO/IEC/ITU 9594-8 en 1988. Varios campos fueron agregados al paso del tiempo hasta su estandarización en Junio de 1996 con la versión 3.

El grupo PKIX ha tomado este estándar y ha trabajado en desarrollar el “RFC 2459, Internet X.509 Public Key Infraestructure Certificate and Certificate Revocation List” Dentro de este documento se define lo que debe contener el certificado, los campos que el certificado contiene son:

- Número de serie del Certificado emitido por la Autoridad Certificadora
- Algoritmo usado por la Autoridad Certificadora que valida el Certificado
- Nombre de la autoridad generadora del Certificado
- Validez del Certificado
- Nombre del Propietario del Certificado
- Clave pública del Propietario y Algoritmo usado
- Extensiones Usadas
- Firma Digital de la Autoridad Certificadora
- Algoritmo de Firma Digital que fue usado por la Autoridad Certificadora

Este tipo de estándares son dinámicos y conforme avanza la tecnología se van actualizando, actualmente se trabaja en el desarrollo de la versión 4.

AGENCIAS CERTIFICADORAS Y REGISTRADORAS
Los certificados son generados por una Agencia Certificadora (CA), la cual puede ser cualquier entidad confiable que certifica la identidad de a quién se entrega un certificado. Una compañía puede generar certificados para sus empleados, o una universidad a sus alumnos, o una ciudad a sus habitantes. De manera de prevenir la generación de certificados falsificados, el CA debe tener un certificado de un CA de mayor nivel para asegurar la validez de sus certificados (normalmente la certificadora / registradora de mayor nivel se le denomina ARC: Autoridad Registradora Central, la cual debe custodiar el certificado raíz y garantizar la unicidad de las claves).

Dado a que el CA debe revisar su propia identidad, algunas empresas deciden actuar como CA de sus propios miembros y empleados.

Una agencia certificadora genera las claves públicas y una agencia registradora almacena los certificados poniendo a disposición de cualquier usuario las claves públicas y lleva actualizada una lista de revocación de los certificados.

RECOMENDACIONES DEL USO DE PKI
Dentro del Uso de PKI, podemos hacer las siguientes recomendaciones:

COMPROMISO DE CLAVE PRIVADA DE USUARIO
En el dado caso de que la clave privada sea comprometida, ya sea por robo o pérdida, el certificado digital deberá ser revocado para evitar el mal uso de la clave. De esta manera se deberá generar un nuevo certificado.

COMPROMISO DE CLAVE PRIVADA DE AGENCIA CERTIFICADORA
Si la clave privada de la Agencia Certificadora es comprometida, todos los certificados validados y generados por esa agencia certificadora tendrán que ser revocados, ya que la clave que ha sido comprometida puede ser usada para poder generar nuevos certificados. En este caso se debe revocar todos los certificados incluyendo el de la agencia certificadora.

EXPIRACIÓN DEL CERTIFICADO
Un certificado siempre tiene un tiempo de vida finito, es decir, una fecha de vencimiento.
Es posible tramitar certificados de forma electrónica, esto es sin requerir la presencia del titular y esto pudiera hacerse en tanto el certificado anterior esté vigente pues con esta firma electrónica el titular genera la solicitud del nuevo certificado.

DISPOSITIVOS FÍSICOS PARA EL ALMACENAMIENTO DE CERTIFICADOS
Existen diferentes dispositivos para el almacenamiento de certificados, desde certificados personales hasta certificados de autoridades certificadoras.

	Dispositivo de almacenamiento	Ventajas	Desventajas
Chip Card	Se almacenan en una tarjeta inteligente	•Se pueden utilizar en cualquier lado •Dispositivo de almacenamiento más seguro	•Es caro ya que se requieren lectoras especiales •La tecnología aún no es accesible para todos los usuarios
Browser	Se almacena en el la computadora del cliente modificando localmente la configuración del Browser del cliente	•Es el certificado más barato	Únicamente se puede utilizar desde la computadora donde se almacenó el certificado localmente
Servidor	Se almacena en un servidor	El cliente puede accesarla a través de una clave desde cualquier computadora.	•Dependencia total de un solo servidor •Cliente se autentica sin certificado

Un Smart Card o Chip Card es un dispositivo con forma de tarjeta de crédito con un chip en su interior. Un Smart Card requiere de un lector para poder hacer uso de él.

La clave privada (PKI) de un usuario puede ser almacenada en un Smart Card donde internamente todas las funciones criptográficas se realizan, incluyendo firma digital, y decripción de las claves de sesión.

Las Smart Cards son pequeñas, fáciles de transportar y difíciles de replicar. Las aplicaciones que usan esta tecnología van desde identificación de telefonía móvil a controles de televisión por satélite. Las Smart Cards tienen sus desventajas como los demás productos. Conectar los lectores a los sistemas puede consumir mucho tiempo. Un estudio realizado por militares de Estados Unidos indica que aproximadamente se instala y configura un lector en 30 min.

Otra opción para almacenar la clave privada pudieran ser los Smart Tokens
Los Smart Tokens usan una tecnología idéntica a las Smart Cards, con la diferencia de su forma y su interfase. Los Smart Tokens son del tamaño de una clave de auto o de la casa y usan el Universal Standard Bus (USB) como interfase.

Los Smart Tokens basados en USB dan ventajas en los escenarios de IT. Los lectores no son necesarios dado a que los smart tokens se conectan directamente a los puertos USB que se encuentran en la mayoría de los sistemas de cómputo actuales.

De todos los dispositivos de autenticación, los llamados “Smart” son los que son aceptados y usados para su integración con aplicaciones PKI dado a que pueden dar autenticación “siempre activa”.

Para las Agencias Certificadoras, existen las tarjetas de almacenamiento de certificados, de tal manera que el certificado se almacena dentro de la tarjeta y no en el disco duro. El certificado digital se respalda en dos “Smart Cards” o “Tokens” de una manera que el certificado se divide dentro de los dispositivos para que el certificado no sea almacenado o custodiado por una sola entidad. Algunas de estas tarjetas cumplen con el Estándar Federal de Proceso de Información (FIPS 140-1 Nivel 3), el cual elimina cualquier información dentro de la tarjeta en caso de que se intente abrir para obtener el certificado digital.

LA FIRMA ELECTRÓNICA
EN MEXICO

Era muy importante para nuestro país, completar la legislación existente en materia de comercio electrónico con la de Firma Electrónica. La razón por la cual estas disposiciones no fueron incluidas en las reformas publicadas el 29 de mayo del 2000, fue que la UNCITRAL, aún no tenía aprobada la Ley Modelo respectiva, por lo que la Comisión de Comercio de la LVII Legislatura, decidió posponer su incorporación con el fin de no crear una Ley que fuera a presentar inconsistencias con la Ley Modelo y que atentara con el correcto desarrollo comercial a nivel internacional.

En el año de 2001, y una vez aprobada por la UNCITRAL, la Ley Modelo de Firmas Electrónicas, la Comisión de Comercio y Fomento Industrial de la LVIII Legislatura, decidió completar la legislación existente a fin de otorgar seguridad jurídica a todas aquellas empresas que ya estaban utilizando firma electrónica.

Es claro que los negocios no esperan, la realidad era que tanto empresas privadas como algunos órganos del gobierno como el propio Banco de México, utilizaban ya sistemas de Firma Electrónica para realizar transacciones.

Dicha legislatura realizó, los días 5 y 6 de Septiembre del 2001, el Foro "Avances en la Legislación en materia de Comercio Electrónico" bajo el siguiente programa:

Tema	**Ponente**	**Organismo**
El internet en México	Lic. Alejandro Rodríguez	Asociación Mexicana de la Industria Publicitaria y Comercial en Internet
La legislación Vigente a Nivel nacional	Lic. Philip Bienvenu y Dr. Alfredo Reyes K	Asociación de Banqueros de México
Norma de Conservación de Mensajes de Datos	Lic. Sergio Carrera	Secretaría de Economía
Firmas Electrónicas en su ámbito legal	Lic. Luis Manuel Mejan	Grupo Gilce
Firmas Electrónicas en su ámbito técnico	Mat. Ignacio Mendivil	Director General de Seguridata
Panorama Internacional	Lic. José Ma. Abascal	Representante de México ante la ONU
Factura Electrónica	Lic. Ramón López Castro	Miembro del Grupo Gilce
Delitos Informáticos	Lic. Luis Manuel Ramírez Perches	L. Ramírez y Asociados, S.C.
Posibles Modificaciones a la Constitución	Lic. Luis Vera Vallejo	Amiti
Nombres de Dominio	Lic. Arturo Azuara	Nic México
Páginas de Internet	Ing. Alejandro Diego	Director General de Interware
Legislación en materia de propiedad Industrial e Intelectual	Lic. Flor Ma. Cuellar	Coordinadora del Proyecto E-Commerce Gobierno de Guanajuato

El principal objetivo del foro fue identificar el contexto en el que se desenvuelve el comercio electrónico, las problemáticas mas recurrente, las demandas de los usuarios de esta nueva práctica comercial, así como la forma mas conveniente en que la legislación pueda coadyuvar para generar las condiciones necesarias de seguridad jurídica y facilitación comercial.

Resultado de éste foro se integró un Grupo de Trabajo con representantes con la activa participación de las empresas privadas y organizaciones tanto del sector privado, el público y el académico, el día 15 de mayo de 2002, después de casi un año de trabajo, el Dip. Diego Alonso Hinojosa Aguerrevere, Presidente de la Comisión, presentó la Iniciativa de Reformas y Adiciones al Código de Comercio, en materia de Firma Electrónica.

Este decreto consiste en la reforma de 30 artículos, modificándose el Título Segundo denominado “Del Comercio Electrónico”, del Capítulo Primero denominado “De los mensajes de datos”, la

creación de un Capítulo Segundo intitulado “De las Firmas”, un Capítulo Tercero “De los Prestadores de Servicios de Certificación” y un Capítulo Cuarto “Reconocimiento de Certificados y Firmas Electrónicas Extranjeros”.

Para efectos académicos, para el análisis presentaremos un cuadro comparativo entre la reforma del 29 de mayo del 2000 y la del pasado 29 de agosto del 2003, con un breve comentario al margen:

REFORMA 29 DE MAYO 2000	REFORMA 29 DE AGOSTO 2003
Artículo 49.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.	**Artículo 49**.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

No se modificó

LIBRO SEGUNDO DEL COMERCIO EN GENERAL	LIBRO SEGUNDO DEL COMERCIO EN GENERAL
Artículo 80.- Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.	**Artículo 80**.- Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

No se modificó

TITULO II DEL COMERCIO ELECTRONICO	TÍTULO SEGUNDO DEL COMERCIO ELECTRÓNICO CAPÍTULO I DE LOS MENSAJES DE DATOS
Artículo 89.- En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará mensaje de datos.	**Artículo 89.-** Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte. Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del

	Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa. En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones: **Certificado:** Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica. **Datos de Creación de Firma Electrónica:** Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante. **Destinatario:** La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje. **Emisor:** Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario. **Firma Electrónica:** Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio. **Firma Electrónica Avanzada o Fiable:** Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica. **Firmante:** La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa. **Intermediario:** En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él. **Mensaje de Datos:** La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología. **Parte que Confía:** La persona que, siendo o no el Destinatario, actúa sobre la base de un

	Certificado o de una Firma Electrónica. **Prestador de Servicios de Certificación:** La persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide los Certificados, en su caso. **Secretaría:** Se entenderá la Secretaría de Economía. **Sistema de Información:** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos. **Titular del Certificado:** Se entenderá a la persona a cuyo favor fue expedido el Certificado.

El primer párrafo es reiterativo, pues el Código de Comercio es Federal. Se pretende tener en cuenta su origen internacional

Se incluyen para interpretación los principios de Neutralidad Tecnológica, (no privilegiar a determinada tecnología) Compatibilidad Internacional (cumplir con estándares internacionales) y Equivalencia Funcional (la firma electrónica deberá ser funcionalmente equivalente a la autógrafa), el principio de Autonomía de la Voluntad se explica en el art. 78 C. de Com.

Se incluyen definiciones, es de hacer notar la modificación a la definición de mensaje de datos a la que se le quitó el término de comunicación, ya que este constituye un proceso de envío y recepción de información (resultaba reiterativa).

Los datos de creación de firma equivalen a la clave privada

Es importante la distinción que se hace de firma digital, ya que ésta es aquella firma electrónica que se realice con tecnología digital.
Es importante considerar que existe la posibilidad de que un mensaje de datos pueda ser generado automáticamente en una computadora (sin intervención humana, ejemplo mensajes de autorespuesta), estos se considerarán emitidos o recibidos por la persona en cuyo nombre se haya programado la computadora.

La definición de intermediario es tan amplia que permite considerar al operador de redes como tal, pero está restringido a un mensaje de datos en lo particular.

RECONOCIMIENTO JURÍDICO DE LOS MENSAJES DE DATOS

	Artículo 89 bis. No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.

Parece reiterativo con el tercer párrafo del artículo anterior, pero se refiere a que los mensajes de datos no deben ser objeto de discriminación, deberán ser tratados sin disparidad alguna respecto de los documentos consignados sobre papel.

ATRIBUCIÓN DEL MENSAJE DE DATOS

Artículo 90.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado: I.- Usando medios de identificación, tales como claves o contraseñas de él, o II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.	**Artículo 90.** Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado: I. Por el propio Emisor; II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere

	automáticamente.

Se incluyó a los enviados por el propio emisor o persona facultada para enviar a nombre de él el Mensaje (figura de Intermediario)
Es importante relacionar con el art. 95

PRESUNCIÓN DE ENVÍO Y DEBIDA DILIGENCIA

	Artículo 90 bis. Se presume que un Mensaje de Datos ha sido enviado por el Emisor y, por tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia, cuando: I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste, o II. El Mensaje de Datos que reciba el Destinatario o la Parte que Confía resulte de los actos de un Intermediario que le haya dado acceso a algún método utilizado por el Emisor para identificar un Mensaje de Datos como propio. Lo dispuesto en el presente artículo no se aplicará: I. A partir del momento en que el Destinatario o la Parte que Confía haya sido informado por el Emisor de que el Mensaje de Datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia, o II. A partir del momento en que el Destinatario o la Parte que Confía tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor. Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas.

Se adiciona como presunción, salvo prueba en contrario, de procedencia del mensaje de datos la aplicación de procedimientos previamente convenidos o envío por intermediario con claves o procedimiento del emisor (ej. e-mail de la secretaria a nombre del jefe).

Es importante hacer notar que el cumplimiento de los requisitos de fiabilidad establecidos en el art. 97 hacen presumir que se actuó con la debida diligencia en la verificación de identidad del emisor.

Los adverbios “debida diligencia” son de difícil aplicación en nuestro derecho

Es importante relacionar también con el art. 95

MOMENTO DE RECEPCIÓN DEL MENSAJE DE DATOS

Artículo 91.- El momento de recepción de la información a que se refiere el artículo anterior se determinará como sigue: I.- Si el destinatario ha designado un sistema	**Artículo 91.** Salvo pacto en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará como sigue:

de información para la recepción, ésta tendrá lugar en el momento en que ingrese en dicho sistema, o II.- De enviarse a un sistema del destinatario que no sea el designado o de no haber un sistema de información designado, en el momento en que el destinatario obtenga dicha información. Para efecto de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos.	I. Si el Destinatario ha designado un Sistema de Información para la recepción de Mensajes de Datos, ésta tendrá lugar en el momento en que ingrese en dicho Sistema de Información; II. De enviarse el Mensaje de Datos a un Sistema de Información del Destinatario que no sea el Sistema de Información designado, o de no haber un Sistema de Información designado, en el momento en que el Destinatario recupere el Mensaje de Datos, o III. Si el Destinatario no ha designado un Sistema de Información, la recepción tendrá lugar cuando el Mensaje de Datos ingrese en un Sistema de Información del Destinatario. Lo dispuesto en este artículo será aplicable aun cuando el Sistema de Información esté ubicado en un lugar distinto de donde se tenga por recibido el Mensaje de Datos conforme al artículo 94.

Es importante considerar la designación del sistema de información que va a “recibir” el mensaje y el concepto de “ingreso” a ese sistema de información, es decir a partir del momento en que puede ser procesado el mensaje en ese sistema de información.

MOMENTO DE EXPEDICIÓN DEL MENSAJE DE DATOS

	Artículo 91 bis. Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido cuando ingrese en un Sistema de Información que no esté bajo el control del emisor o del intermediario.

En este caso es importante recalcar el concepto de control, es decir a partir del momento en que ya no puede el emisor “manipular” el mismo.

ACUSE DE RECIBO

Artículo 92.- Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerará que el mensaje de datos ha sido enviado, cuando se haya recibido el acuse respectivo. Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente.	**Artículo 92.** En lo referente a acuse de recibo de Mensajes de Datos, se estará a lo siguiente: I. Si al enviar o antes de enviar un Mensaje de Datos, el Emisor solicita o acuerda con el Destinatario que se acuse recibo del Mensaje de Datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante: a) Toda comunicación del Destinatario, automatizada o no, o b) Todo acto del Destinatario, que baste para indicar al Emisor que se ha recibido el Mensaje de Datos. II. Cuando el Emisor haya indicado que los efectos del Mensaje de Datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el Mensaje de Datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo en el plazo fijado por el Emisor o dentro de un plazo razonable atendiendo a la naturaleza del negocio, a partir del momento del envío del Mensaje de Datos; III. Cuando el Emisor haya solicitado o acordado con el Destinatario que se acuse recibo del Mensaje de Datos,

	independientemente de la forma o método determinado para efectuarlo, salvo que: a) El Emisor no haya indicado expresamente que los efectos del Mensaje de Datos estén condicionados a la recepción del acuse de recibo, y b) No se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio. El Emisor podrá dar aviso al Destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el Emisor reciba acuse de recibo del Destinatario, se presumirá que éste ha recibido el Mensaje de Datos correspondiente; IV. Cuando en el acuse de recibo se indique que el Mensaje de Datos recibido cumple con los requisitos técnicos convenidos o establecidos en ley, se presumirá que ello es así.

Es importante recalcar que el uso de “acuse de recibo” se debe de acordar entre las partes (la ley no puede imponerlo).

El acuse de recibo no necesariamente debe hacerse por la misma vía (se puede acusar recibo por correo o teléfono).

El último párrafo se refiere a mensajes que requieren un protocolo de comunicación determinado (ej. EDIFACT)

FORMA ESCRITA Y FIRMA

Artículo 93.- Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta. En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.	**Artículo 93.** Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente. Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes. En los casos en que la Ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de Mensajes de Datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Es importante la distinción entre forma escrita y firma, toda vez que la forma escrita no requiere de atribución.

Pero no podrá firmarse aquello que no está escrito (íntegro y accesible).

ORIGINAL

	Artículo 93 bis. Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la Ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos: I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar. Para efectos de este artículo, se considerará que el contenido de un Mensaje de Datos es íntegro si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

En relación a mensajes de datos el original no es el soporte en el que por primera vez se consigna la información (en éste orden de ideas todos los que recibe un destinatario serían copia) lo que se busca es encontrar su equivalente funcional en el sentido de reducir posibilidad de alteración, es decir integridad.

Por otro lado también aclarar que el medio que contiene el mensaje de datos puede variar y no así el propio mensaje de datos (ej. Diskette o CD o Disco Óptico).

La evaluación de la integridad o grado de integridad requerida debe establecerse en función del caso concreto (no necesariamente se requerirá de PKI de acuerdo con lo establecido por la NOM de Conservación de Mensajes de Datos, podría convenirse otro método dependiendo del caso particular, por ejemplo la conservación de mensajes de e-mail que formalizan acuerdos por importes menores que no justifican la intervención de un prestador de servicios de certificación).

Otro caso pudiera ser el acuse de recibo o la certificación al final del mensaje de datos de la fecha y hora de envío o recepción, no afectan su calidad de documento íntegro.

LUGAR DE ENVÍO Y RECEPCIÓN DE UN MENSAJE DE DATOS

Artículo 94.- Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo.	**Artículo 94.** Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo: I. Si el Emisor o el Destinatario tienen más de un establecimiento, su establecimiento será el

	que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal, y II. Si el Emisor o el Destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

La ubicación de los sistemas de información es indiferente, el Código prevé un criterio más objetivo: el establecimiento de las partes.

ERROR Y DUPLICADO

	Artículo 95. Conforme al artículo 90, siempre que se entienda que el Mensaje de Datos proviene del Emisor, o que el Destinatario tenga derecho a actuar con arreglo a este supuesto, dicho Destinatario tendrá derecho a considerar que el Mensaje de Datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia. El Destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el Mensaje de Datos recibido. Se presume que cada Mensaje de Datos recibido es un Mensaje de Datos diferente, salvo que el Destinatario sepa, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo Mensaje de Datos era un duplicado.

Relacionar con el art. 90 y 90 bis, sobre todo en lo relativo a la presunción de que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas (art. 97)

	CAPÍTULO II **DE LAS FIRMAS**

IGUALDAD DE TRATAMIENTO DE LAS TECNOLOGÍAS PARA LA FIRMA

	Artículo 96. Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica.

Su objeto es no limitar la fuerza vinculatoria del NIP

CUMPLIMIENTO DEL REQUISITO DE FIRMA Y SU FIABILIDAD.

	Artículo 97. Cuando la Ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte

	apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos. La Firma Electrónica se considerara Avanzada o Fiable si cumple por lo menos los siguientes requisitos: I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante; II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante; III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

En PKI los Datos de creación de firma son la CLAVE PRIVADA.

Otro método para garantizar la fiabilidad de una firma sería el acuerdo entre las partes y se deja abierto para cualquier método

DIFUSIÓN DEL CUMPLIMIENTO DEL REQUISITO DE FIABILIDAD

	Artículo 98. Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97. La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado

Lo anterior para evitar malos entendidos entre el cliente y su PSC (esto es independiente de la difusión de las practicas de certificación adoptadas por el PSC)

PROCEDER DEL FIRMANTE

	Artículo 99. El Firmante deberá: I. Cumplir las obligaciones derivadas del uso de la Firma Electrónica; II. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma; III. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en

	relación con el Certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas. El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo, y IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

Los datos de creación de firma (clave privada) obran en poder del firmante y el se hace responsable de su uso frente al PSC.

Insisto en que los adverbios “debida diligencia” son de difícil aplicación en nuestro derecho

	CAPÍTULO III **DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN**

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

	Artículo 100. Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría: I. Los notarios públicos y corredores públicos; II. Las personas morales de carácter privado, y III. Las instituciones públicas, conforme a las leyes que les son aplicables. La facultad de expedir Certificados no conlleva fe pública por sí misma; así, los Notarios y Corredores Públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información

La inclusión como Prestadores de Servicios de Certificación a fedatarios no es nueva en nuestra legislación:
Las modificaciones al Código Civil de mayo del 2000 establecen que cuando un acto jurídico deba otorgarse en escritura publica, se prevé que los notarios podrán ..generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos, o de cualquier otra tecnología..para lo cual el notario deberá hacer constar en la escritura que al efecto se otorgue, los elementos a través de los cuales se atribuye dicha información a las partes otorgándola conforme se establece en la legislación notarial.

En las Reformas al Código de Comercio de mayo del 2000 el artículo 30 bis.- La Secretaría certificará los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio, así como la de los demás usuarios del mismo, y ejercerá el control de estos medios a fin de salvaguardar la confidencialidad de la información que se remita por esta vía.
Artículo 30 bis 1.- Cuando la autorización a que se refiere el artículo anterior se otorgue a notarios o corredores públicos, dicha autorización permitirá, además, el envío de información por medios electrónicos al Registro...

El día 18 de septiembre del 2000, la entonces Secretaria de Comercio y Fomento Industrial publicó el acuerdo que establece los lineamientos para la operación del Registro, en donde menciona el modo de operación del Registro Público de Comercio mediante un sistema denominado Sistema Integral de Gestión Registral (SIGER). El sistema cuenta con un módulo Web, a través del cual se operan vía remota los subsistemas de registro y de consulta, el cual podrá ser utilizado por los fedatarios públicos autorizados para tal efecto. La Dirección General de Normatividad Mercantil habilitará a las autoridades certificadoras para emitir los certificados digitales u otros medios de identificación de los notarios.

Con fecha 17 de enero de dos mil dos, se publicó en el Diario Oficial de la Federación el Acuerdo por el que se establecen las disposiciones que deberán observar las dependencias y los organismos descentralizados de la Administración Publica Federal, para la recepción de promociones que formulen los particulares en los procedimientos administrativos a través de medios de comunicación electrónica, así como para las notificaciones, citatorios, emplazamientos, requerimientos, solicitudes de informes o documentos y las resoluciones administrativas definitivas que se emitan por esa misma vía. En dicho acuerdo ya se contempla, en los apartados decimocuarto y decimoséptimo, que se otorgarán plenos efectos a los certificados electrónicos que sean emitidos por los notarios, que sean utilizados e los tramites electrónicos que se harán a través de Tramitanet, sistema electrónico de tramites.

En este mismo acuerdo se establece que para Dependencias Públicas y Organismos descentralizados de la Administración Pública Federal la Secretaría de Función Pública fungirá como Autoridad Registradora Central

PERSONAS MORALES DE CARÁCTER PRIVADO

	Artículo 101. Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior, contendrán en su objeto social las actividades siguientes: I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica; II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación; III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y emitir el Certificado, y IV. Cualquier otra actividad no incompatible con las anteriores.

Atendiendo el esquema de operación, estas actividades corresponden a las funciones principales de el Agente Certificador, la Agencia Certificadora y la Agencia Registradora.

Se pretende profesionalizar los servicios de los Prestadores de Servicios de Certificación.

ACREDITACIÓN POR LA SECRETARÍA

	Artículo 102. Los prestadores de servicios de certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad. A) Para que las personas indicadas en el artículo 100 puedan ser prestadores de servicios de certificación, se requiere acreditación de la Secretaría, la cual no podrá

	ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los prestadores de servicios de certificación que comprueben la subsistencia del cumplimento de los mismos: I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación; II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad; III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y con medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros; IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio; V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría; VI. Establecer por escrito su conformidad para ser sujeto a Auditoria por parte de la Secretaría, y VII. Registrar su Certificado ante la Secretaría. B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Al respecto hay que tomar en consideración lo establecido en el transitorio **TERCERO:** En lo que se refiere al artículo 102, dentro de los doce meses siguientes a la entrada en vigor de las reglas generales a que se refiere el artículo anterior, el plazo de 45 días a que se refiere el mismo, será de 90 días.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

	Artículo 103. Las responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes.

Independientemente de lo establecido por el artículo 98 los PSC deben firmar contrato con el cliente en donde este se atribuyen las operaciones que se realicen con su firma electrónica y se definan las responsabilidades y sus limitaciones de las PSC, esto es, como y en base a que certifican la identidad del solicitante, sus elementos de seguridad, etc.

PROCEDER DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

	Artículo 104. Los Prestadores de Servicios de

	Certificación deben cumplir las siguientes obligaciones: I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante; II. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica; III. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad; IV. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten. El contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría; V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación; VI. En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos; VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica; VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y IX. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar: a) La identidad del Prestador de Servicios de Certificación; b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado; c) Que los Datos de Creación de la Firma eran

	válidos en la fecha en que se expidió el Certificado; d) El método utilizado para identificar al Firmante; e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado; f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación; Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y g) Si se ofrece un servicio de terminación de vigencia del Certificado.

Definición de sus principales obligaciones

AUTORIDAD REGISTRADORA CENTRAL

	Artículo 105. La Secretaría coordinará y actuará como autoridad Certificadora, y registradora, respecto de los Prestadores de Servicios de Certificación, previstos en este Capítulo.

IES BANXICO

	Artículo 106. Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras.

Para instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores (ej: CECOBAN)

Considerando lo establecido en el transitorio **CUARTO**, el Banco de México, en el ámbito de su competencia, regulará y coordinará a la autoridad registradora central, registradora y certificadora, de las instituciones financieras y de las empresas mencionadas que presten servicios de certificación.

PROCEDER DE QUIEN CONFÍA EN EL CERTIFICADO

	Artículo 107. Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para: I. Verificar la fiabilidad de la Firma Electrónica, o II. Cuando la Firma Electrónica esté sustentada por un Certificado: a) Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y b) Tener en cuenta cualquier limitación de uso

	contenida en el Certificado.

CERTIFICADOS DIGITALES

	Artículo 108. Los Certificados, para ser considerados válidos, deberán contener: I. La indicación de que se expiden como tales; II. El código de identificación único del Certificado; III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría; IV. Nombre del titular del Certificado; V. Periodo de vigencia del Certificado; VI. La fecha y hora de la emisión, suspensión y renovación del Certificado; VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

Esta estructura no es limitativa**.**

VIGENCIA DEL CERTIFICADO

	Artículo 109. Un Certificado dejará de surtir efectos para el futuro en los siguientes casos: I. Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Antes de que concluya el periodo de vigencia del Certificado, podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación; II. Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado; III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado; IV. Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la Ley, situación que no afectará los derechos de terceros de buena fe, y V. Resolución judicial o de autoridad competente que lo ordene.

Se establece un límite máximo de vigencia de dos años, acorde con prácticas internacionales

SANCIONES

	Artículo 110. El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo,

	previa garantía de audiencia, y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Suspensión temporal o definitiva de sus funciones mas la responsabilidad civil o penal en que incurra, en su caso.

RESPONSABILIDAD CIVIL Y PENAL DEL PRESTADOR

	Artículo 111. Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

EJECUCIÓN DE LAS SANCIONES

	Artículo 112. Las autoridades competentes harán uso de las medidas legales necesarias, incluyendo el auxilio de la fuerza pública, para lograr la ejecución de las sanciones y medidas de seguridad que procedan conforme a esta Ley. Incluso, en los procedimientos instaurados se podrá solicitar a los órganos competentes la adopción de las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte.

PRESTADOR SUSTITUTO

	Artículo 113. En el caso de que un Prestador de Servicios de Certificación sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los Certificados que haya expedido pasarán, para su administración, a otro Prestador de Servicios de Certificación que para tal efecto señale la Secretaría mediante reglas generales.

	CAPÍTULO IV **RECONOCIMIENTO DE CERTIFICADOS Y FIRMAS ELECTRÓNICAS EXTRANJEROS**

FIRMAS ELECTRÓNICAS EXTRANJERAS

	Artículo 114. Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos: I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado

	la Firma Electrónica, y II. El lugar en que se encuentre el establecimiento del prestador de servicios de certificación o del Firmante. Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título. Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente. A efectos de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente. Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable

No se quiso limitar el concepto “grado de fiabilidad equivalente”, por lo que para determinarlo se podrá estar a lo establecido en el Código o a las convenciones internacionales aplicables.

PRUEBA

Artículo 1205.- Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.	**Artículo 1205**.- Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.

No se modificó

Artículo 1298-A.- Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.	**Artículo 1298-A**.- Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

No se modificó

	TRANSITORIOS **PRIMERO.** El presente Decreto comenzará su vigencia 90 días después de su publicación en el Diario Oficial de la Federación. **SEGUNDO.** Dentro del plazo de 90 días posteriores a la entrada en vigor del presente Decreto, el Ejecutivo emitirá las reglas generales a que se refieren las presentes disposiciones. **TERCERO.** En lo que se refiere al artículo 102, dentro de los doce meses siguientes a la entrada en vigor de las reglas generales a que se refiere el artículo anterior, el plazo de 45 días a que se refiere el mismo, será de 90 días. **CUARTO.** Por lo que se refiere al artículo 106, el Banco de México, en el ámbito de su competencia, regulará y coordinará a la autoridad registradora central, registradora y certificadora, de las instituciones financieras y de las empresas mencionadas que presten servicios de certificación.

Es importante comentar que la Secretaría de Economía está trabajando en la elaboración de Lineamientos para la Acreditación de Prestadores de Servicios de Certificación, un Reglamento del Código de Comercio en materia de firma electrónica y en las Reglas Generales a que se refiere el Código de Comercio. Al respecto para consultar los avances se puede consultar el sitio: http://www.firmadigital.gob.mx/

BIBLIOGRAFÍA

ACOSTA ROMERO, Miguel;
“Nuevo Derecho Mercantil”;
Editorial Porrúa;
Primera Edición;
15 de agosto del 2000.

Adams, Carlisle & Lloyd, Steve
Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations
USA; New Riders Publishing, 1999
ISBN: 1-57870-166-x

Lawrence Lessig.
El Código y otras leyes del ciberespacio.
Editorial Taurus es digital.
España 2001.

Schneier, Bruce
Secrets & Lies: Digital Security in a Networked World
USA; Wiley, 2000
ISBN: 0-471-25311-1

King, Christopher; Dalton, Curtis
Security Architecture: Design, Deployment & Operations
USA; RSA Press, 2001
ISBN: 0-07-213385-6

REYES KRAFFT Alfredo;
La firma electrónica y las entidades de certificación.
Ed. Porrua;
México 2003

Russel, Ryan; Cunningham, Stace
Hack Proofing your Network: Internet Tradecraft
USA; Syngress, 2000
ISBN: 1-928994-15-6

STROKE PAUL,
“La Firma Electrónica”
Editorial Cono Sur,
España,2000

Documentos

Schneier, Bruce
Why Cryptography is Harder than it looks?
Counterpane Systems, 1997

Francesc A. Baygual (Roca Junyent Abogados):
De la 'FE' a la 'FEA':¿más de lo mismo?
REDI: Revista Electrónica de Derecho Informático.
Número 44. ISSN 1576-7124

Estudio comparativo de algunas leyes internacionales relativas a la firma digital elaborado durante el año 2001 y publicado en el Boletín de Política Informática número 4. Coordinado por Guillermina González Durand Subdirectora de Análisis Jurídicos y Administrativos y Sandra Gómez Pérez, especialista del departamento de análisis jurídicos en informática de la Dirección de Políticas y Normas en Informática del INEGI

Internet

Cryptography FAQ
http://www.faqs.org/faqs/cryptography-faq/

International Association for Cryptologic Research
http://www.iacr.org/

Request for Comments
http://www.ietf.org/rfc.html

ActivCard
http://www.activcard.com

Aladdin Knowledge Systems
http://www.ealaddin.com

GemPlus
http://www.gemplus.com

Rainbow Technologies
http://www.rainbow.com

RSA Security
http://www.rsasecurity.com

Vasco
http://www.vasco.com