

FIRMA DIGITAL

DOCUMENTO - DOCUM. ELECTRÓNICO - DOCUM. DIGITAL

DOCUMENTO: Instrumento, normalmente escrito, en cuyo texto se consigna o representa alguna cosa apta para esclarecer un hecho o se deja constancia de una manifestación de voluntad que produce efectos jurídicos

Todo documento se compone de **dos elementos:**

- . **El soporte instrumental**, que es el continente del documento
-papel: documento escrito - soporte escrito tradicional
- . **El contenido**, que es la información que se vuelca en el soporte instrumental

La unión de ambos elementos nos da como resultado el documento en el sentido que lo conocemos.

Las nuevas tecnologías han hecho aparecer el documento, no ya en soporte material, sino en un soporte virtual al que denominamos: **documento electrónico**.

Cuando en la elaboración de este documento electrónico se emplea algún proceso criptográfico se lo transforma en un **documento digital**.

Nuestro Código Civil distingue entre:

Instrumentos Públicos: deben cumplir ciertas exigencias formales, entre las que se encuentran la escritura papel, la firma y el cumplimiento de alguna formalidad o solemnidad. Hacen plena fe hasta que sean argüidos de falsos.

Instrumentos Privados: redactados sin solemnidad alguna. Existe la libertad de las formas, pero es necesario que contengan:
- escritura en papel
- firma

De allí que el documento electrónico y el documento digital no tenían hasta hace poco encuadramiento en nuestra legislación tradicional ni como documento público o privado.

DOCUM. ELECTRÓNICO - DOCUM. DIGITAL

Con la sanción de la **Ley 25506 de Firma Digital** el 14.11.2001, se ha dado reconocimiento al Documento Electrónico y al Documento Digital y se ha incorporado a la legislación argentina el principio de la equivalencia funcional.

“Artículo 6.- Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura”.

FIRMA – FIRMA ELECTRÓNICA – FIRMA DIGITAL

La **firma** es un conjunto de letras o signos que identifican a la persona que la estampa.

En el concepto tradicional la firma de un documento, ya sea este privado o público, debe efectuarse de manera manuscrita u hológrafa.

La **firma electrónica** es cualquier método o símbolo basado en medios electrónicos, utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Por su parte la **firma digital** es un forma específica de firma electrónica en la cual interviene un proceso criptográfico que cumple determinados requisitos, y que da seguridad a quien extiende esta firma. Los Españoles la llaman firma electrónica avanzada y firma electrónica reconocida.

FIRMA ELECTRÓNICA Y FIRMA DIGITAL

Con la sanción de la **Ley 25506 de Firma Digital** el 14.11.2001 se ha dado reconocimiento a la firma Electrónica y Digital y se ha incorporado a la legislación argentina el principio de la equivalencia funcional:

“Artículo 3.- Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia”

CRIPTOGRAFÍA

La criptografía es la técnica que se ocupa de transformar textos en fórmulas aparentemente ininteligibles, así como devolverlos luego a su formato original. El proceso criptográfico transforma un texto claro y legible en un mensaje cifrado al que se denomina criptograma. La criptografía es muy antigua pero la moderna criptografía utiliza algoritmos para el cifrado, existiendo dos sistemas:

SISTEMAS SIMÉTRICOS

Los primeros de estos sistemas de criptografía fueron los sistemas simétricos de “Criptografía con Clave Privada” o “Clave Única”. En estos sistemas **existe una sola clave** que sirve tanto para encriptar como para desencriptar.

SISTEMAS ASIMÉTRICOS

Con el desarrollo tecnológico aparecen los sistemas asimétricos de “Criptografía de Clave Pública”, en los que existen **dos claves diferentes** y complementarias entre sí. Cada clave es función inversa de la otra, y sólo puede descifrar lo que su par encriptó.

SISTEMAS ASIMÉTRICOS

La criptografía asimétrica fue creada a mediados de los setenta por

Diffie y Hellman, y se materializa en el sistema **RSA**
(Rivest, Hamir y Adelaman del MIT).

Actualmente existen otros sistemas asimétricos derivados:

- PGP (Pretty Good Privacy)
- PKI (Public Key Infraestructure)

SISTEMAS SIMÉTRICOS

Usando **una misma clave** se cifra y descifra el mensaje. Los dos participantes en una comunicación deben acordar la clave antes del intercambio, o enviar la clave por otro medio (mensaje por Internet y clave por TE).

Son sistemas relativamente **rápidos**.

Al existir una sola clave el sistema es mas vulnerable, por falta de un canal seguro.

No tienen capacidad de firma.

SISTEMAS ASIMÉTRICOS

Existen **dos claves** (clave pública conocida por todos y clave privada conocida sólo por el titular). Se generan automática y simultáneamente y existe una relación matemática entre ellas.

Son sistemas **lentos** por lo que suelen combinarse con los simétricos.

En la medida que la clave privada sea solo conocida por su titular no son vulnerables.

Tienen capacidad de firma.

PAR DE CLAVES O LLAVES DE LOS SISTEMAS ASIMÉTRICOS

Cada usuario debe poseer **dos claves o llaves**:

- Una **pública**: conocida por todos
sirve para encriptar
sirve para constatar la firma
- Una **privada** conocida sólo por su titular
sirve para desencriptar
sirve para firmar

Las dos claves o llaves están relacionadas matemáticamente entre si y las genera simultáneamente una sola vez el usuario con un software apropiado.

Están vinculadas a un certificado digital.

LONGITUD DE LA CLAVE

Una longitud de clave de 4 dígitos: con 10^4 : 10.000 pruebas

Una longitud de clave de 8 dígitos: con 10^8 : 100.000.000 pruebas

LONGITUD DE LA CLAVE EN bits

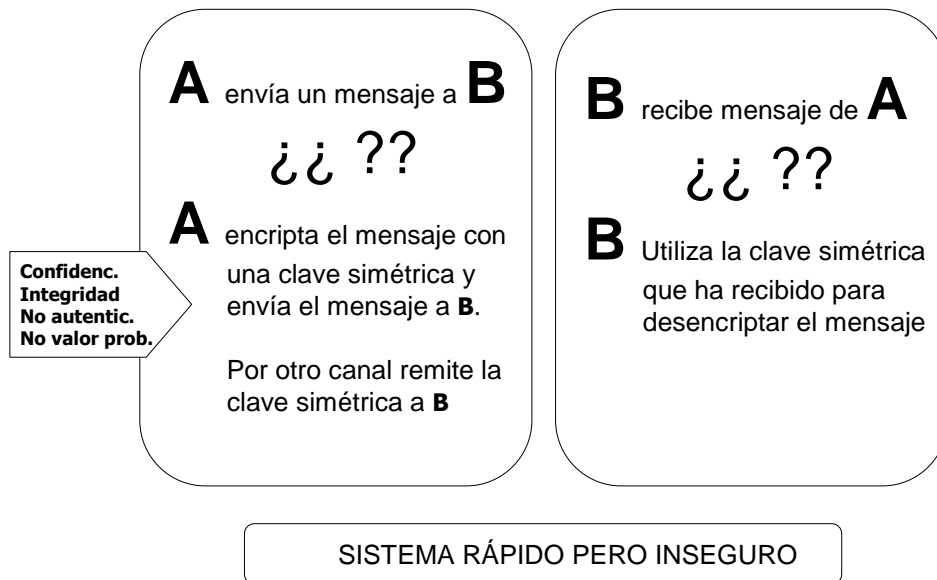
Una clave de 40 bits de longitud indica que son necesarias:

2^{40} : 1.099.511.627.776 pruebas

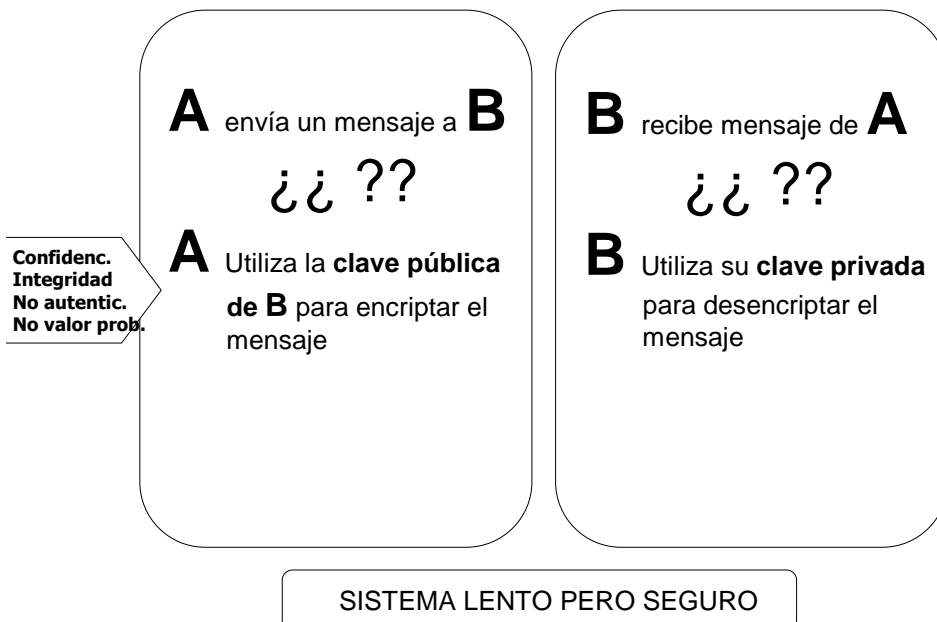
Actualmente se están utilizando claves de 2048 bits.

Se logra así la imposibilidad de un "ataque por fuerza bruta".

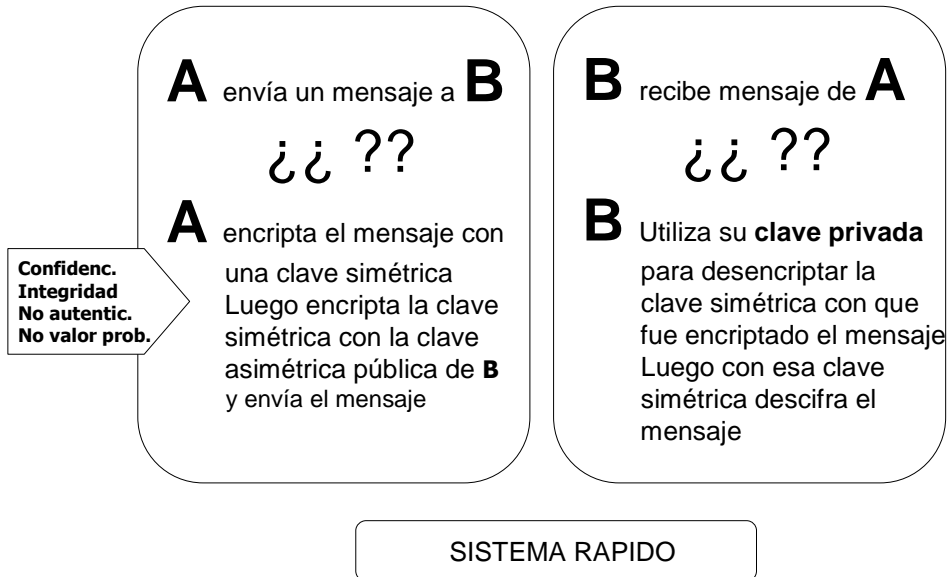
FUNCIONAMIENTO DE UN SISTEMA SIMÉTRICO



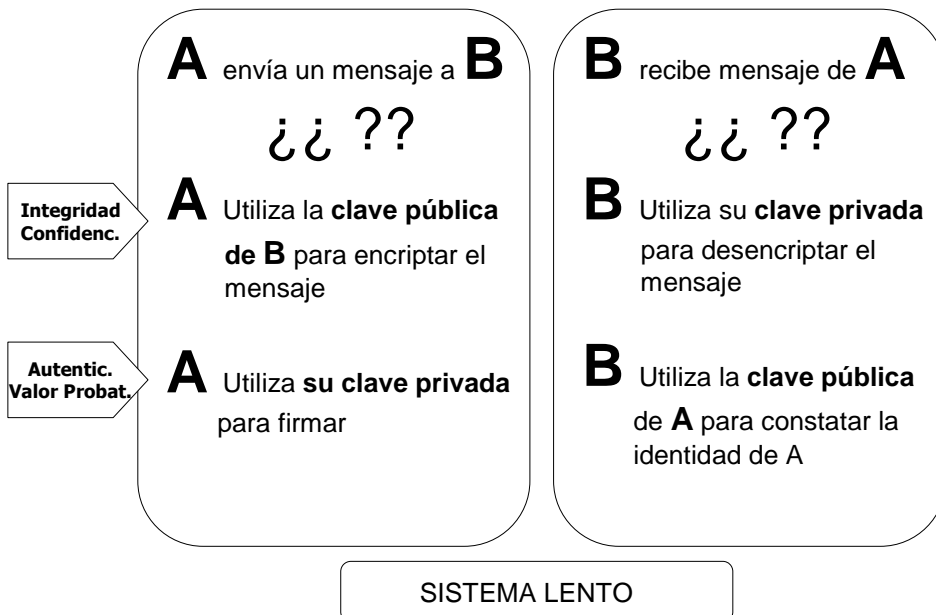
FUNCIONAMIENTO DEL SISTEMA ASIMÉTRICO



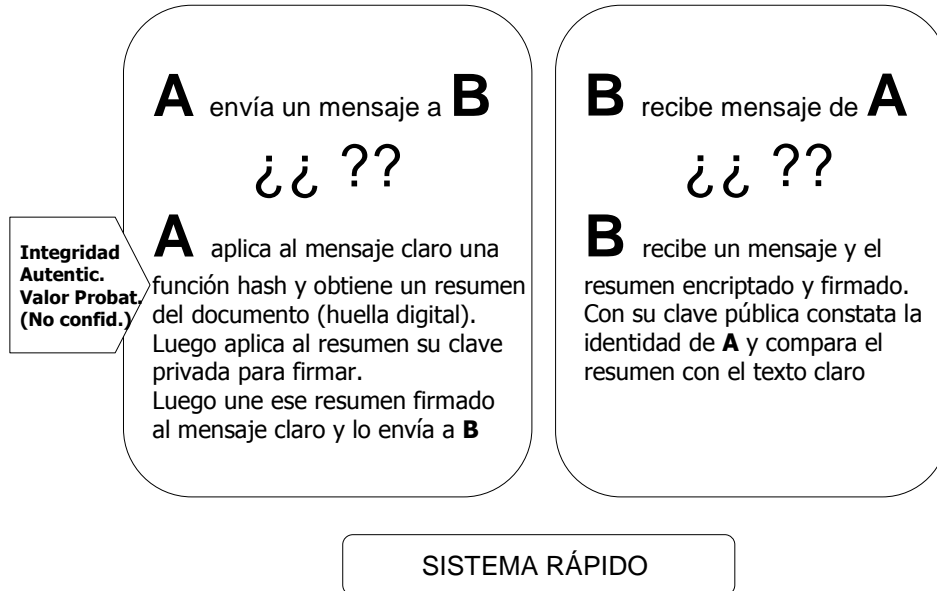
FUNCIONAMIENTO COMBINADO DEL SISTEMA SIMÉTRICO Y ASIMÉTRICO



FUNCIONAMIENTO DEL SISTEMA ASIMÉTRICO CON FIRMA

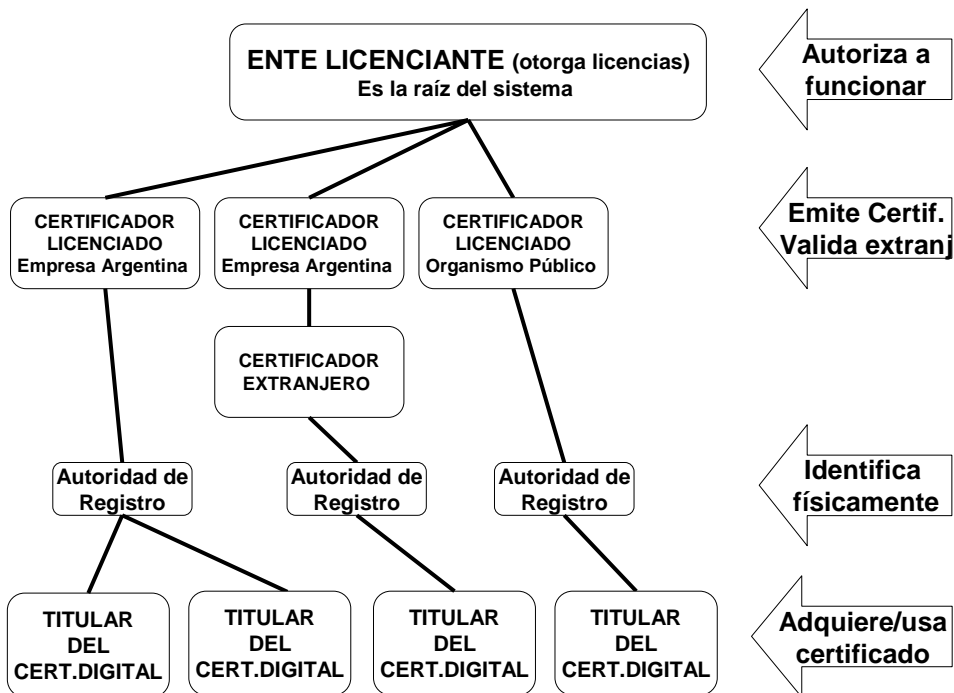


FUNCIONAMIENTO DEL SISTEMA ASIMÉTRICO CON FIRMA UTILIZANDO UNA FUNCION HASH



FUNCION HASH

- 1.- Se aplica al documento un programa que lo transforma en un extracto de longitud fija y única (**Digesto del Mensaje o Huella Digital**). Es una versión comprimida del mensaje.
- 2.- Ese Digesto se encripta con la clave privada del emisor y se agrega luego dicho digesto al mensaje completo.
- 3.- El receptor desencripta el extracto con clave pública del emisor y puede verificar que coincida con el mensaje.
De esta forma se consigue: - **autenticidad del documento**
- **integridad**
- **imposibilidad de repudio**



ESQUEMA DE SEGURIDAD

INTEGRIDAD: Prueba que la información no ha sido alterada.

AUTENTICIDAD: Garantiza que quien está del otro lado de la comunicación sea quien dice ser.

CONFIDENCIALIDAD O PRIVACIDAD: Mantiene la información privada. Los terceros no pueden ver lo datos.

VALOR PROBATORIO (NO REPUDIO): Imposibilidad de desconocer los términos de la operación llevada a cabo.

La Norma ISO/7498-92 de la International Electrotechnical Commission establece que los servicios de seguridad en el Comercio Electrónico deben garantizar estas cuatro condiciones

Al comenzarse a usar los sistemas asimétricos se planteó el problema de la prueba de la vinculación de una persona con su par de claves.

Surgió así la figura del TERCERO que certifica la vinculación de las claves con una persona a través del certificado digital.

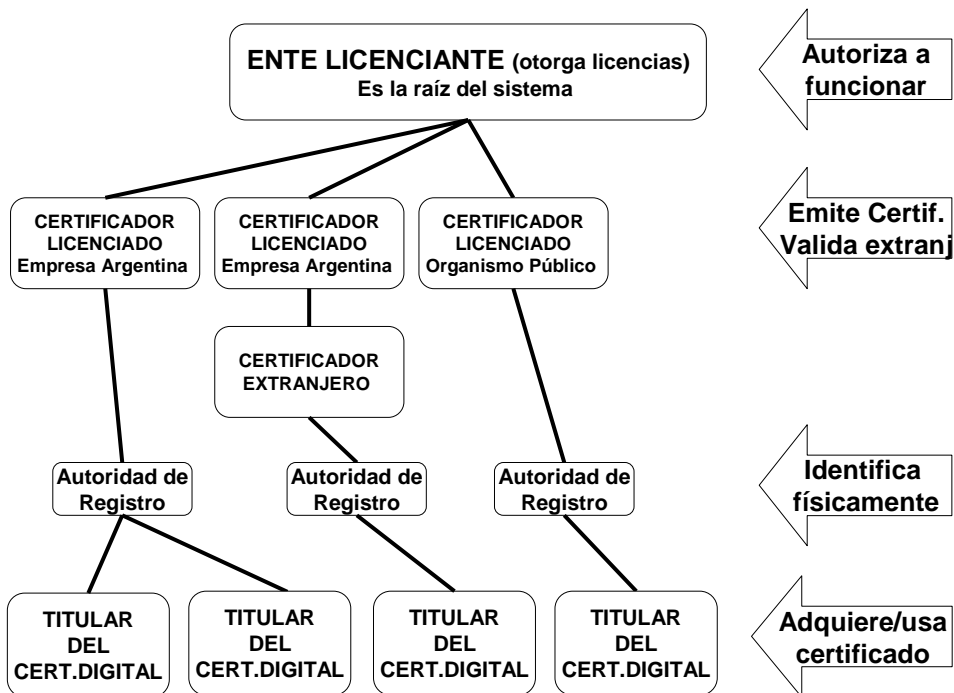
A este tercero se lo llama **Autoridad Certificante o Certificador**, y es un tercero que emite el certificado digital.

Internacionalmente existen sistemas que

- ***Exigen que los certificadores estén acreditados o licenciados por algún ente superior (raíz del sistema)***
- ***Que no exigen tal acreditación o la establecen como voluntaria (Considerando 10 de la Directiva Europea, y art.5 de la ley 59/03 de España)***

En EE.UU., cada estado tiene su propia autoridad de certificación con sus propias particularidades y alcances, ello a ha generado problemas, fundamentalmente en cuanto a la validez interestatal de las firmas digitales.

Por ello se ha creado una autoridad que constituye un puente entre todas las autoridades estatales, la **Federal Bridge Certification Authority (FBCA)**.



CERTIFICADO DIGITAL

Documento electrónico firmado digitalmente por un tercero (Autoridad Certificante) en quien se confía y que vincula una llave pública a la identidad de un usuario. Es similar a un documento de identidad

El certificado digital contiene:

- código identificador único del certificado;
- identificación y firma de la AC que expide el certificado;
- nombre y apellido y algún atributo específico del usuario;
- fecha de expiración (generalmente 1 año), límites de uso, de valor de transacciones y de responsabilidad de la AC;
- copia de la clave pública;

Emitidos en estándar X509v3.

El par de claves los genera el cliente.

La misión fundamental es permitir la comprobación que la clave pública de un usuario corresponde realmente a ese usuario.

Se envía el certificado junto con el documento firmado digitalmente.

MODELO ESPAÑOL



TIPOS DE CERTIFICADOS



SERVIDOR DE CERTIFICADOS AUTORIDAD CERTIFICANTE (CA o AC)

- Genera los certificados digitales y los envía a los usuarios
- Es depositario de los certificados digitales , almacenando las llaves publicas en Directorios públicos y en donde se puede verificar la validez de los certificados emitidos a los usuarios,
- Lleva la lista de revocación de los certificados digitales, permitiendo con ella verificar la vigencia y validez de los certificados
- La confianza en el sistema se genera básicamente por la confianza y prestigio de la AC.
- La AC debe publicar los procedimientos usados para la identificación (Prácticas de Certificación)

REVOCAION DE CERTIFICADOS DIGITALES

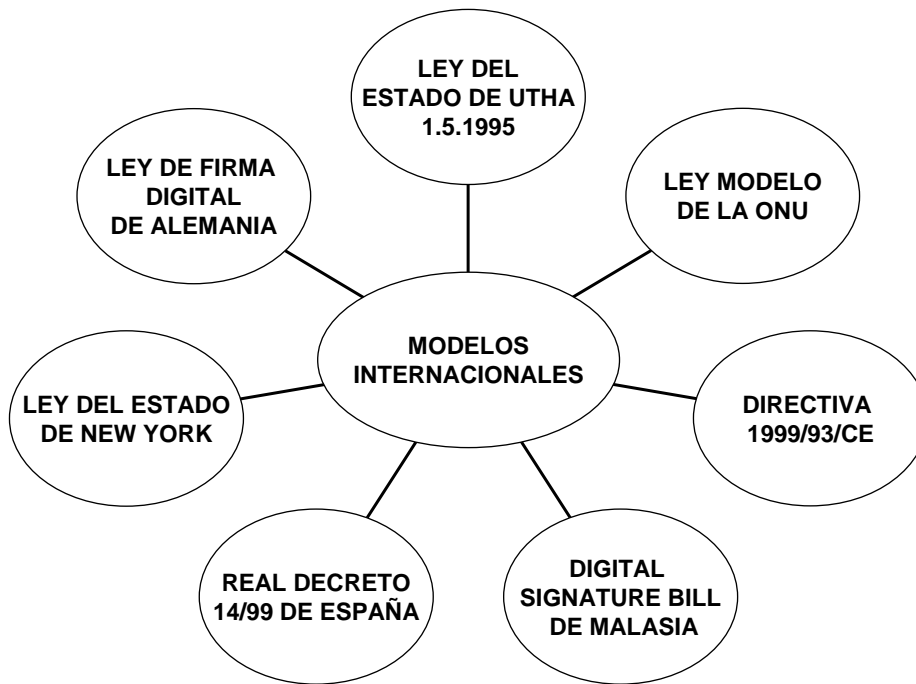
La Autoridad Certificante (CA) emite la lista de revocaciones de certificados digitales (CRL)

Las CRL son descargables de la red

Las CRL pueden ser muy extensas ya que crecen con el número de usuarios

Las CRL se actualizan periódicamente. Existe un período intermedio al que se lo denomina: **Ventana Gris**

Para solucionar el problema de las Ventanas Grises están apareciendo estándares técnicos a ese fin (OCSP - On Line Certificate Status Protocol)



LEY MODELO DE LAS NACIONES UNIDAS SOBRE FIRMA ELECTRONICA

La Ley Modelo de las Naciones Unidas para las Firmas Electrónicas fue aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en Nueva York en Marzo de 2001

La ley Modelo se elaboró a fin de brindar a los diferentes estados, un modelo legislativo uniforme, ante el riesgo de que los distintos países adoptasen criterios legislativos diferentes en relación con las firmas electrónicas, y considerando que el dictado de legislaciones uniformes en esta materia es fundamental para la interoperabilidad jurídica y técnica de cualquier sistema de firma electrónica.

Los principios fundamentales de la Ley Modelo son:

- **Equivalencia funcional**
- **Neutralidad Tecnológica**
- **Distinción entre firma electrónica simple y avanzada**

DOCUMENTO ELECTRÓNICO Y FIRMA DIGITAL EN LA LEGISLACIÓN ARGENTINA

SECTOR PÚBLICO

La **ley 24624** incorporó a la legisl. Argentina el documento electrónico con relación al Sector Público

La **Res.45/97** autorizó el empleo de la firma digital en el sector públ. y el **Decreto 427/98** dispuso la creación de la Infraestructura de Firma Digital para la Administración Publica Nacional (FDAPN)

La **Res. 194/98** de la Secretaría de la Función Pública aprobó los estándares técnicos.

SECTOR PRIVADO

El 14 de Noviembre de 2001 fue sancionada la **Ley 25506 de Firma Digital** para el Sector Privado

En Diciembre de 2002 fue dictado El **Decreto 2628** reglamentario de La Ley de Firma Digital.

Existen numerosas disposiciones que autorizan el uso del formato Electrónico o digital y la transferencia electrónica de datos
El **Decreto 658/02** autorizó la presentación de declaraciones juradas de DGI por medios electrónicos

CARACTERÍSTICAS DEL NUEVO RÉGIMEN ESTABLECIDO POR LA LEY 25506 Y REGLAMENTADO POR EL DECRETO 2628/2002

Se habilita el uso del formato electrónico y del formato digital para la celebración de actos jurídicos, así como se reconoce el empleo de la firma electrónica y de la firma digital.

La ley regula tres institutos vinculados entre si:

- **La firma electrónica**
- **La firma digital**
- **El documento electrónico o digital** -Ni la ley ni el Decreto Reglamentario hacen un claro distingio entre el documento electrónico y el documento digital, sino que lo tratan como si se tratara de un mismo instrumento

La ley distingue entre **firma digital** (art.2) y **firma electrónica** (art.5)

Artículo 2- Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose esta bajo su absoluto control.

La firma digital debe ser susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

Artículo 5- Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma Electrónica corresponde a quien la invoca acreditar su validez

Por su parte el Decreto Reglamentario (art.1) efectúa una distinción entre:

- **firma electrónica**
- **firma digital basada en certificados emitidos por certificadores no licenciados**
- **firma digital basada en certificados emitidos por certificadores licenciados**
- **firma digital basada en certificados emitidos por certificadores extranjeros (convenio reciproc.o certif. de un certif. lic. Argentino)**

Valen solo como firma electrónica y no otorgan presunción de autoría e integridad

Valen como firma digital y otorgan presunción de autoría e integridad

Se adopta conforme la tendencia internacional el “**Principio de la Neutralidad Tecnológica**”, ya que no se establece que método o tecnología resulta mas conveniente a la autenticación de los datos en formato digital.

El Decreto Reglamentario establece que la Jefatura del Gabinete de Ministros será quien apruebe los estándares tecnológicos de Infraestructura de Firma Digital en consonancia con estándares tecnológicos internacionales. Hasta que ello ocurra mantendrán vigencia los estándares establecidos en la Resolución 194/98 (art. 22 Decreto)

Se equiparan los efectos de la escritura digital y la firma digital con los de la escritura escrita y firma manuscrita, basándose en el denominado **Criterio de Equivalencia Funcional**, tal como lo recomienda la Ley Modelo de la CNUDMI.

Se establece con relación a la **firma digital una presunción iuris tantum de autoría y de integridad**, estableciendo que salvo prueba en contrario se considera que la firma digital pertenece al titular del certificado y que luego de aplicado un procedimiento de verificación a un documento digital corresponde tener al documento por no modificado desde el momento de su firma

Tal presunción no existe con relación a la firma electrónica ya que el art. 5 in fine establece que en caso de ser desconocida la firma electrónica, corresponde a quien la invoca acreditar su validez

Se da validez jurídica y fuerza probatoria a los documentos electrónicos firmados digitalmente.

El sistema de firma digital **no es aplicable**

- a) a las disposiciones por causa de muerte;
- b) a los actos jurídicos del derecho de familia;
- c) a los actos personalísimos en general;
- d) a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (art.13)

Certificadores Licenciados

Es el tercero que interviene en todo proceso de firma digital y da fé y validez al sistema

Ente público o privado que expide certificados digitales y presta otros servicios en relación a la firma digital

- Debe tener una **licencia otorgada por el ente licenciante**.
Algunos discuten la necesidad de esta acreditación obligatoria.
El fundamento de tal acreditación esta relacionado con el régimen de responsabilidad de las entidades, a fin de brindar seguridad jurídico económica al sistema y evitar que empresas sin respaldo puedan emitir certificados y en caso de conflicto no poder responder.
De allí la posibilidad de utilizar la firma electrónica (con menos requisitos y menor valor probatorio-art.5) como ocurre ya en sistemas cerrados.
- Los certificadores licenciados del sector privado prestan el servicio en régimen de competencia, pudiendo fijar libremente los aranceles
- Las licencias duran un año y pueden ser renovadas. Los certificadores licenciados pueden delegar algunas funciones en autoridades de registro

Certificado Digital

Documento digital firmado por un certificador, que vincula los datos de firma a su titular (art.13)

- **Certificado digital emitido por un certificador licenciado** Son válidos como firma digital
- **Certificado digital emitido por un certificador no licenciado** Son válidos como firma electrónica

CERTIFICADORES EXTRANJEROS

Se reconoce validez
a sus certificados
cuando:

Reúnan los requisitos de la ley y exista un convenio de reciprocidad

o

Cuando sus certificados sean reconocidos por un Certificador Licenciado Argentino y éste reconocimiento sea validado por la autoridad de aplicación

ESTRUCTURA ESTABLECIDA POR LA LEY

Autoridad de Aplicación: Subsecretaría de la Gestión Pública (conf. Decreto 409/05)

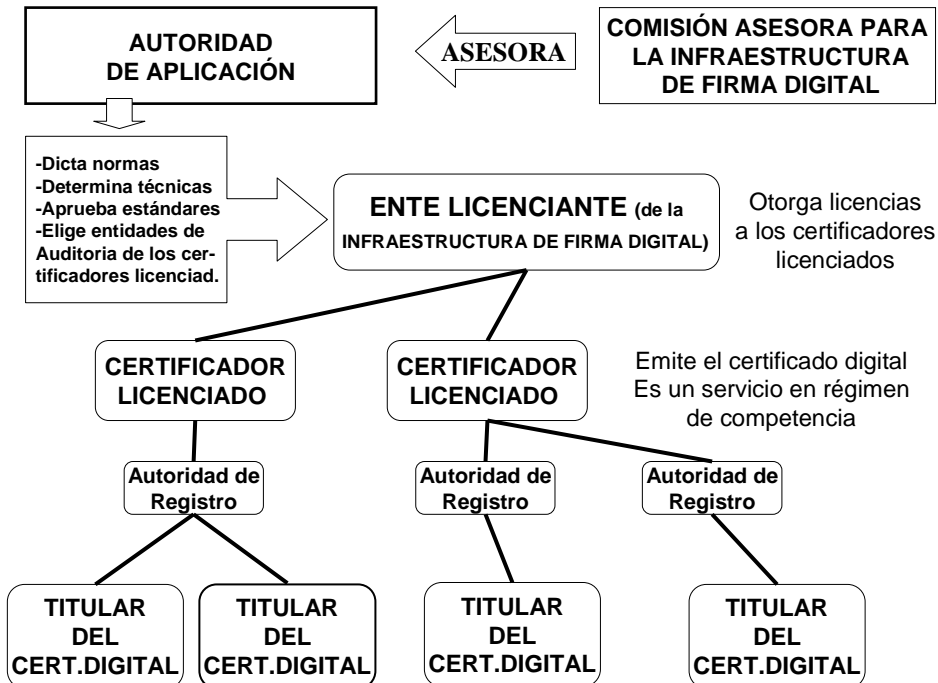
Comisión Asesora para la Infraestructura de Firma Digital: Funcionará en el ámbito de la Subsecretaría de la Gestión Pública. El Decreto 160/4 designó a sus integrantes.

Ente Administrador de Firma Digital: Órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisarlos. Es la Oficina Nacional de Tecnologías de la Información (ONTI)

Certificadores licenciados: Personas de existencia ideal, u organismos públicos que obtengan una licencia emitida por el ente administrador para actuar como proveedores de servicios de certificación.

Autoridades de Registro: Entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.

Sistema de Auditoría: Será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.



El Decreto 283/2003 dictado el 14 de Febrero de 2003 ha autorizado con carácter transitorio y hasta tanto se encuentre la Administración Pública Nacional en condiciones de emitir certificados digitales en los términos previstos en la Ley 25.506 y en su Decreto Reglamentario Nº 2628/2002, a la OFICINA NACIONAL DE TECNOLOGIAS INFORMATICAS dependiente de la SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la política de certificación vigente.

**NORMATIVA Y PROCEDIMIENTOS PARA EL
OTORGAMIENTO DE LICENCIAS HABILITANTES
A LAS AUTORIDADES CERTIFICANTES**

La ONTI el 30.12.2004 presentó un proyecto de normativa.

La Decisión Administrativa 6/2007 del 7 de febrero 2007 ha establecido el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.

Esta Decisión administrativa se complementa con 8 anexos con toda la normativa técnica.

El Decreto 1079/2005 del Gobierno de la Ciudad de Buenos Aires establece la implementación del uso de la tecnología de firma electrónica y firma digital en el ámbito del Poder Ejecutivo del gobierno de la Ciudad de Buenos Aires.