

FIRMA DIGITAL: Aspectos Técnicos y Legales

Temario

- Conceptos básicos
- Funcionamiento
- Marco normativo en la Argentina
- Aplicaciones

CONCEPTOS BÁSICOS

Problemática Actual

- ❖ No es posible determinar con certeza el autor.
 - ❖ Un documento electrónico es fácilmente alterable.
 - ❖ Puede ser objeto de repudio.
-  No permite reemplazar totalmente al papel.

Objetivo

- Poder enviar un documento firmado a través de medios electrónicos de manera que ese documento cuente, por lo menos, con las mismas características técnicas de seguridad y legales que tiene un documento firmado hológrafamente.
- Resumen: Modelar digitalmente las mismas características de un documento con firma hológrafa.

Qué necesitamos ...

- ❖ Atribuir el documento a su autor (una persona) en forma fehaciente (*autenticar al autor*).
- ❖ Verificar la no alteración del contenido del documento luego de que fue firmado (*integridad del contenido*).
- ❖ Garantizar el NO REPUDIO.

Firma Digital – Definición Técnica

- ❖ La firma digital es una solución tecnológica que permite **autenticar el origen y verificar la integridad del contenido** de un mensaje de manera tal que ambas características sean demostrables ante terceros.

Firma Digital - Propiedades

- ❖ Autenticidad: Poder atribuir el documento únicamente a su autor de forma fidedigna, de manera de poder identificarlo.
- ❖ Integridad: Estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- ❖ Exclusividad: Garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.
- ❖ No repudio: Garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.

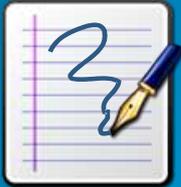
Qué se puede firmar

- ❖ Datos enviados a través de un formulario web.
- ❖ Una imagen, fotos o música.
- ❖ Un base de datos.
- ❖ Un disco rígido, un CD o un DVD.
- ❖ Una página o un sitio de Internet.
- ❖ Una transacción electrónica o un e-mail.
- ❖ Una hoja de cálculo o un documento de texto.
- ❖ El código fuente de un programa o un software.
- ❖ Uno o varios archivos en general.

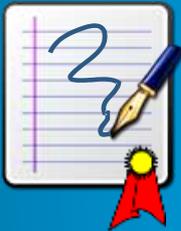
Qué no es una Firma Digital

- ❖ Una firma digitalizada (una firma manuscrita escaneada).
- ❖ Una contraseña o password.
- ❖ Un sistema biométrico.
- ❖ Un sistema de autenticación: este requisito sólo no alcanza.
- ❖ Una firma electrónica.
- ❖ Un documento encriptado (solo se garantiza la confidencialidad).

Medidas de Seguridad



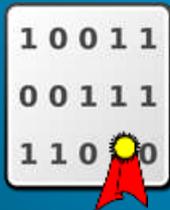
Documento no firmado ni cifrado
Sin protección ni seguridad.



Documento firmado pero no cifrado
Autenticidad – Integridad - No Repudio.



Documento cifrado pero no firmado
Confidencialidad.

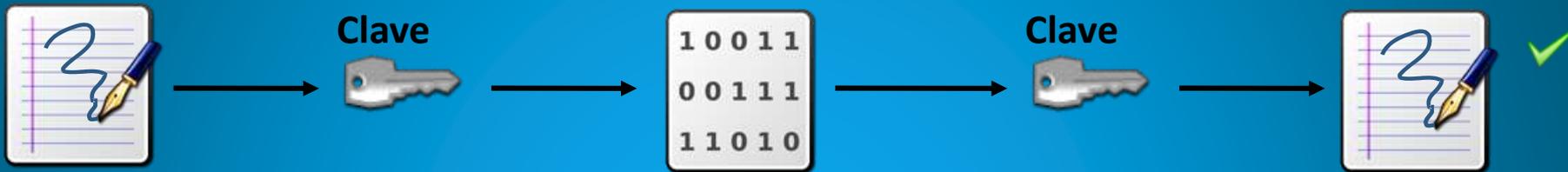


Documento firmado y cifrado
Todas las características anteriores.

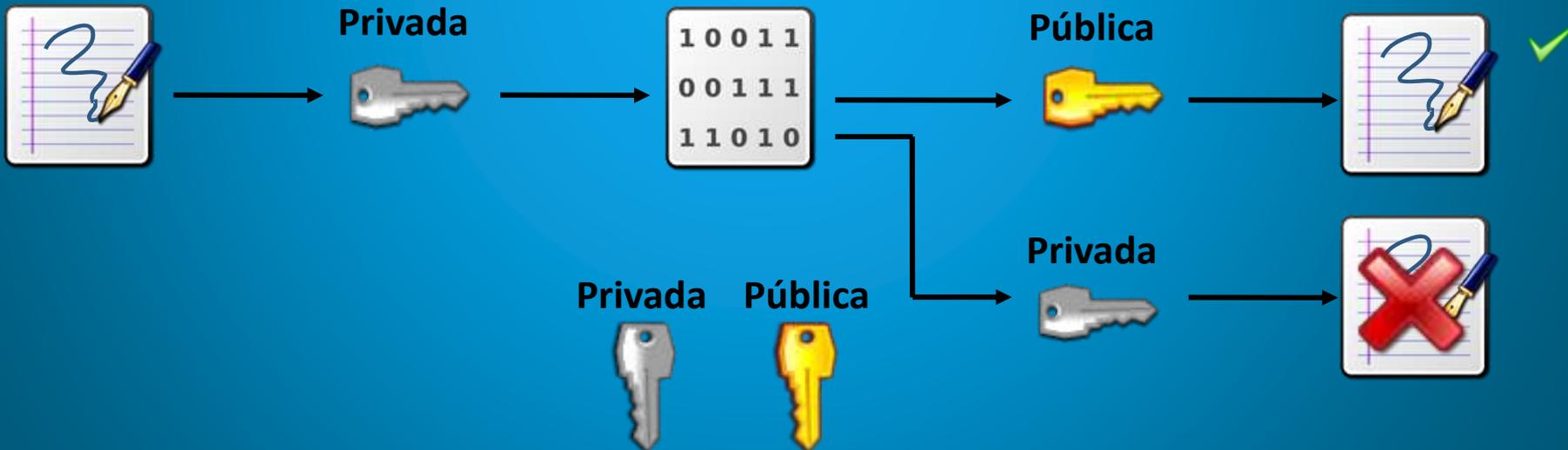
FUNCIONAMIENTO

Criptografía

Criptografía Simétrica

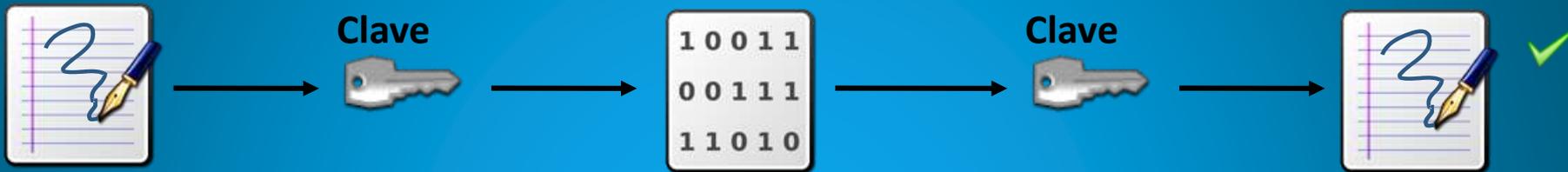


Criptografía Asimétrica

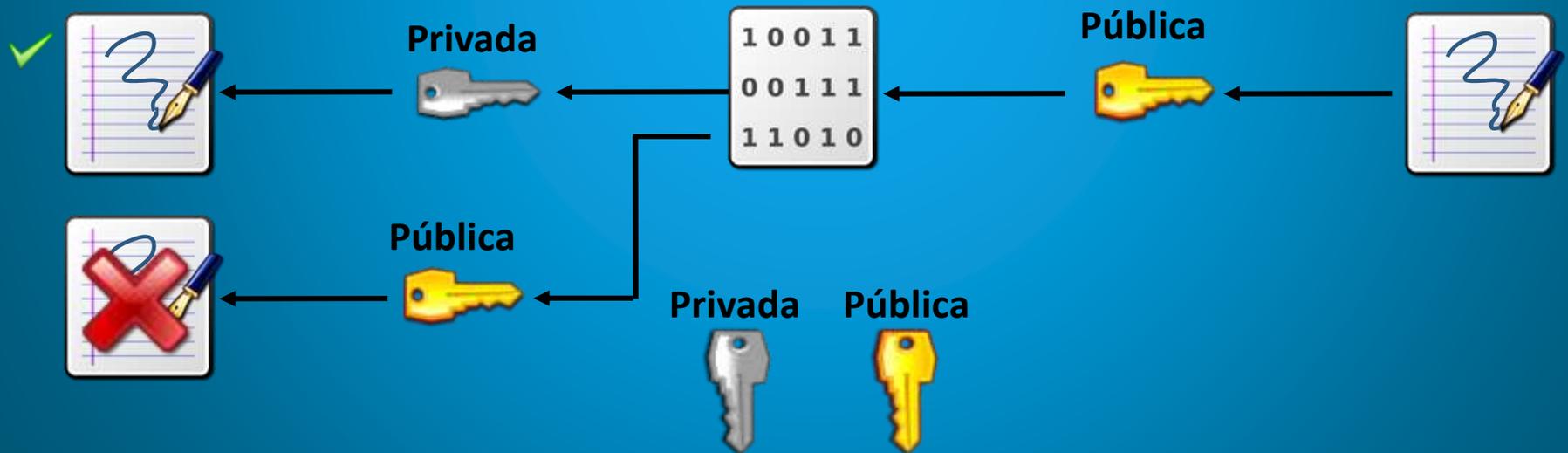


Criptografía

Criptografía Simétrica



Criptografía Asimétrica



Esquema RSA

ESQUEMA RSA

$p = 13069322402100655460372905860955471125556555722027918271400496820543230709995361923026449726342667352298135532444657556071721709079499346407281185886210303$

$q = 11543291706304854991282053266556482345340381283249361938035635072123140767619879947055794178155878831076988621881878883273530930538636731138191162287228337$

CLAVE PÚBLICA:

$n = p * q$

$= 150863000891192741319840914668544464467514371784439070450576744919329592611912795422903481515108819664757442760567137259505878925100335308535018685795925041443616170203299241549726752965481817691505256855094549856968833483708744362754719215241945330731$

$e = 5$

CLAVE PRIVADA:

$d = e^{-1} \text{ mod } ((p-1)(q-1))$

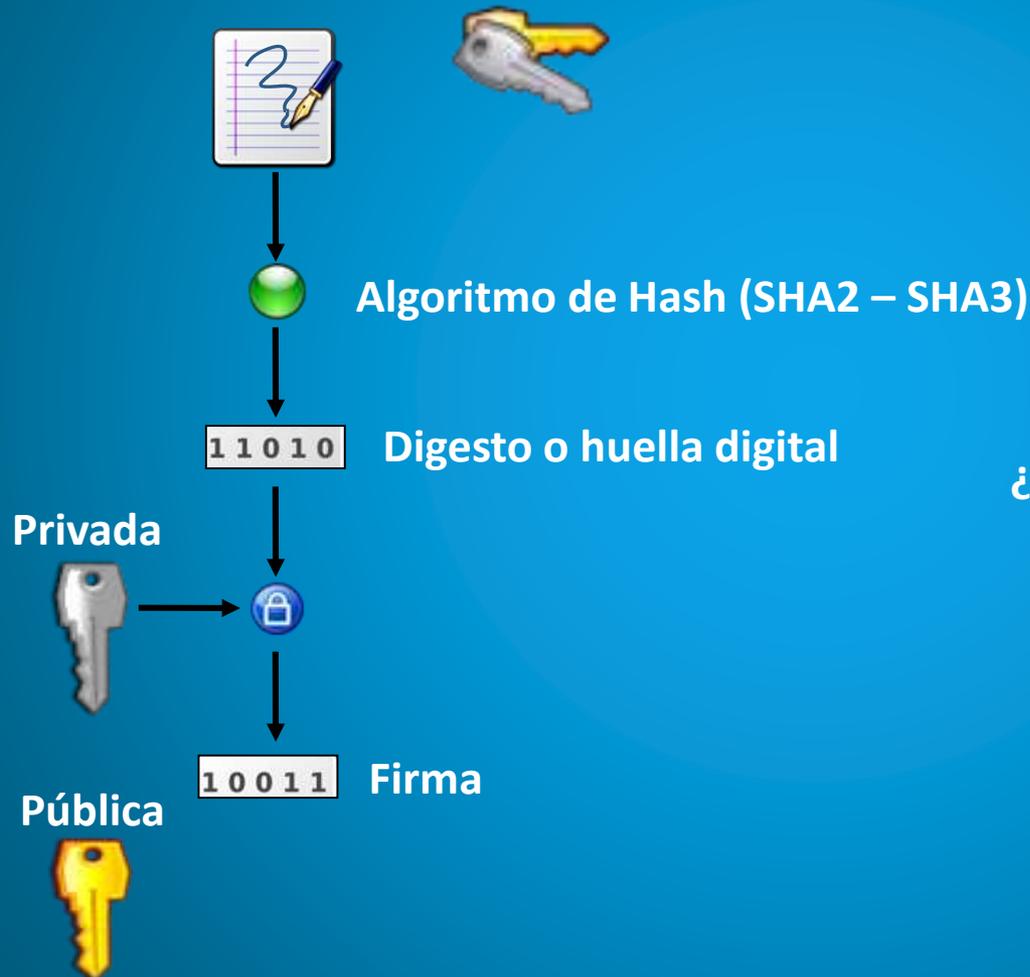
$= 603452003564770965279363658674177857870057487137756281802306979677318370447651181691613926060435278659029771042268549038023515700401341234140074743183700067324008247191155159579070501814113387178273006311257361683347763269349066990051396531992163328742$

Firma Digital: Procedimiento

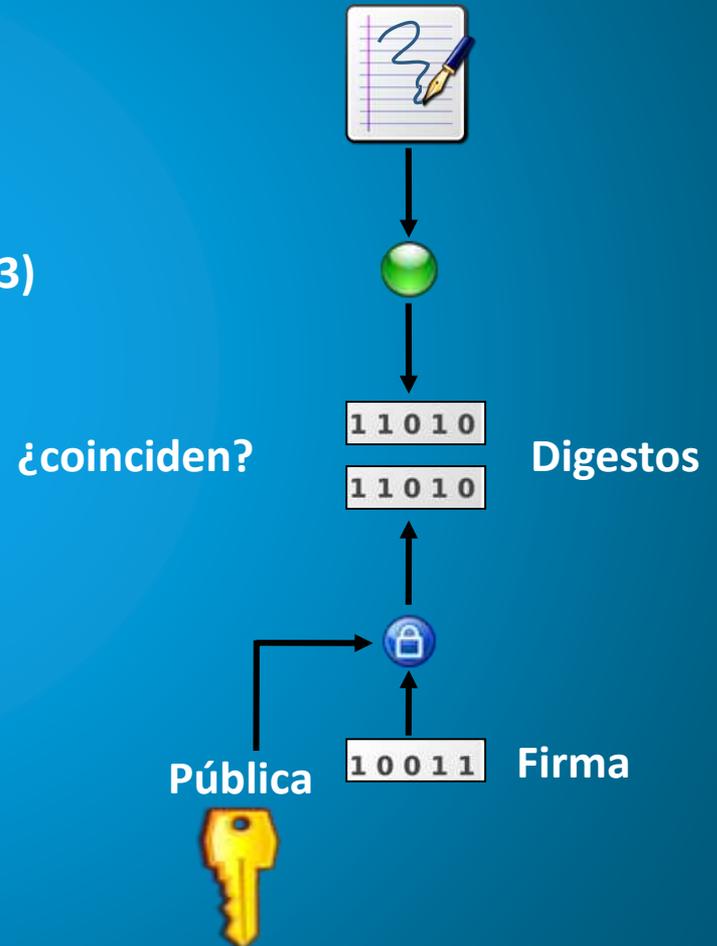


Firma Digital: ¿Como funciona?

Quando se Firma



Quando se Verifica

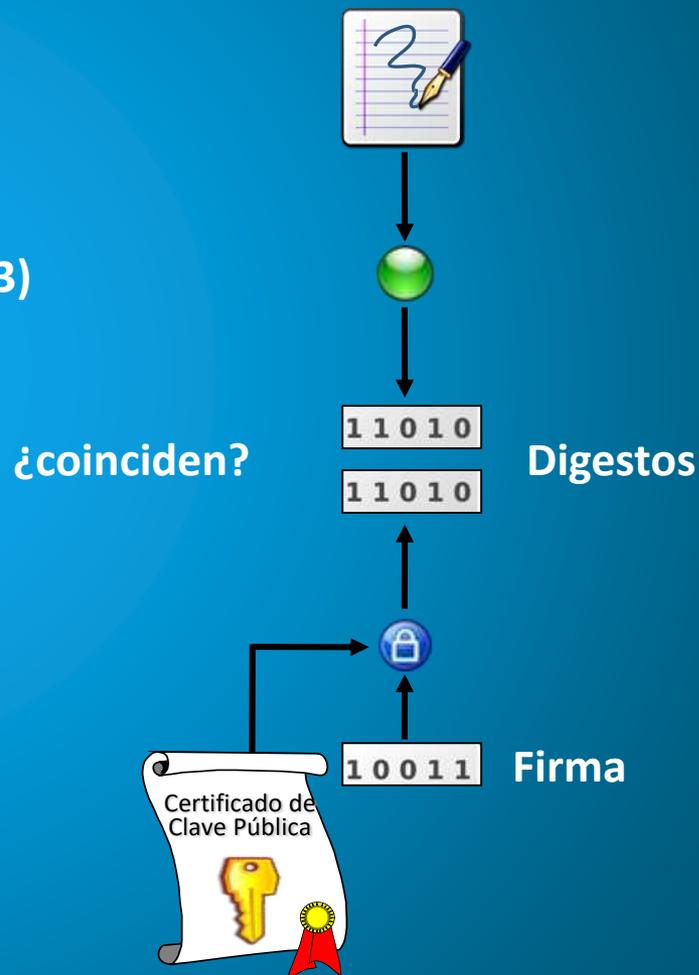


Firma Digital: ¿Como funciona?

Quando se Firma



Quando se Verifica



Certificado de Clave Pública

El Certificador da fe que el Sr. JUAN LOPEZ es titular de la clave pública:

3081 8902 8181 00ED 254C B8AD
D8D4 F35B 4A35 D885 1876 9BA9
DD10 6F2C 4539 ER53 9Y53 3856

....

....

33FC A825 BE50 4976 03C2 07B4
2943 72BF 165B 8B02 0301 0001

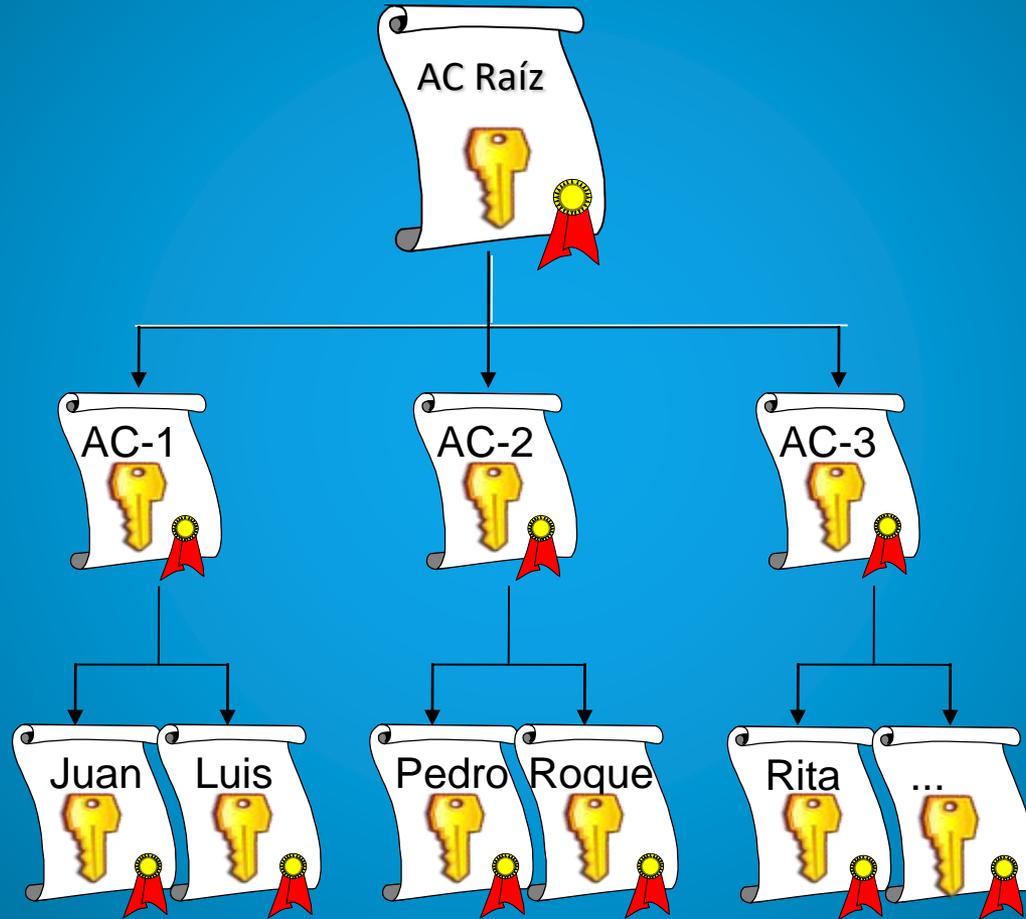
Válido entre: 01/01/2011 y 31/12/2012

No. de serie: 1001

(Firma digital del Certificador)



Jerarquía de AC's



Certificado- Definición

- ❖ Los certificados de clave pública son documentos digitales firmados digitalmente por una Autoridad Certificante que vinculan la clave pública de una persona a sus datos de identidad.

AC - Definición

- ❖ Las *Autoridades Certificantes o Certificadores* son terceras partes confiables que dan fe de la veracidad de la información incluida en los certificados que emiten.

Infraestructura de Firma Digital (PKI)

Se define *Infraestructura de Firma Digital o Infraestructura de Claves Públicas* como el conjunto de normas jurídicas, hardware, software, bases de datos, redes, estándares tecnológicos, personal calificado y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones), mediante el uso de certificados digitales como herramienta, se identifiquen entre sí de manera segura al realizar transacciones en redes, especialmente Internet, permitiendo además dotar de autoría e integridad a los documentos digitales.

Consideraciones

Algunas consideraciones para usuarios de certificados:

- ❖ La clave privada es generada, almacenada y utilizada en la estación de trabajo del usuario.
- ❖ Se debe proteger la clave privada, para esto se deben utilizar mecanismos de autenticación (ej: contraseñas, etc.).
- ❖ La Autoridad Certificante NO tiene forma de acceder a la clave privada, por lo tanto no puede restaurarla si se pierde; en este caso el titular deberá revocar su certificado.
- ❖ No es necesario un certificado por cada documento a firmar digitalmente.
- ❖ La firma digital no se puede imprimir.

Sistema de Firma Digital

Hay 4 actores principales:

- ❖ Quien firma (el suscriptor).
- ❖ Quien(es) necesita(n) verificar la firma.
- ❖ Quien testimonia que una firma digital pertenece a una cierta persona.
- ❖ Quien controla el Sistema.

Marco Normativo

Escenario Nacional

Ley N° 25.506 de Firma Digital

- ❖ Establece una Infraestructura de Firma Digital Nacional.
- ❖ Autoridad de Aplicación: Secretaría de Gobierno de Modernización.
- ❖ Certificadores Licenciados: Sistema de acreditación obligatorio.
- ❖ Firma digital: presunción de autoría e integridad, salvo prueba en contrario.
- ❖ Principio de equivalencia funcional.
- ❖ Firma electrónica: se modifica la carga probatoria.
- ❖ Despapelización del estado.
- ❖ Neutralidad tecnológica.
- ❖ Reconocimiento de certificados extranjeros.
- ❖ Protección de datos del suscriptor del certificado.

Normativa complementaria

- ❖ Decreto N° 2.628/02:
Reglamenta la ley de firma digital.
- ❖ Decreto N° 561/16:
Sistema de Gestión Documental Electrónica.
- ❖ Decreto 892/17:
Crea la AC MODERNIZACION – Plataforma de firma digital remota.
- ❖ Resolución N° 399E/16:
 - ❖ Establece el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.
 - ❖ Establece una Política Única de Certificación común a todos los Certificadores Licenciados.
 - ❖ Los certificados emitidos por los Certificadores Licenciados son interoperables.

Firma Digital - Definición

- ❖ Es el resultado de aplicarle a un documento digital un *procedimiento matemático* que requiere *información de exclusivo conocimiento* del firmante, encontrándose ésta bajo su *absoluto control*.
- ❖ Debe ser susceptible de verificación por terceras partes, de manera tal que dicha verificación permita simultáneamente identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Firma Digital – Requisitos Legales

- ❖ Autenticidad: Poder atribuir el documento únicamente a su autor de forma fidedigna, de manera de poder identificarlo.
- ❖ Integridad: Estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- ❖ Exclusividad: Garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.
- ❖ No repudio: Garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.
- ❖ Validez: Haber sido producida con un certificado emitido por un Certificador Licenciado.

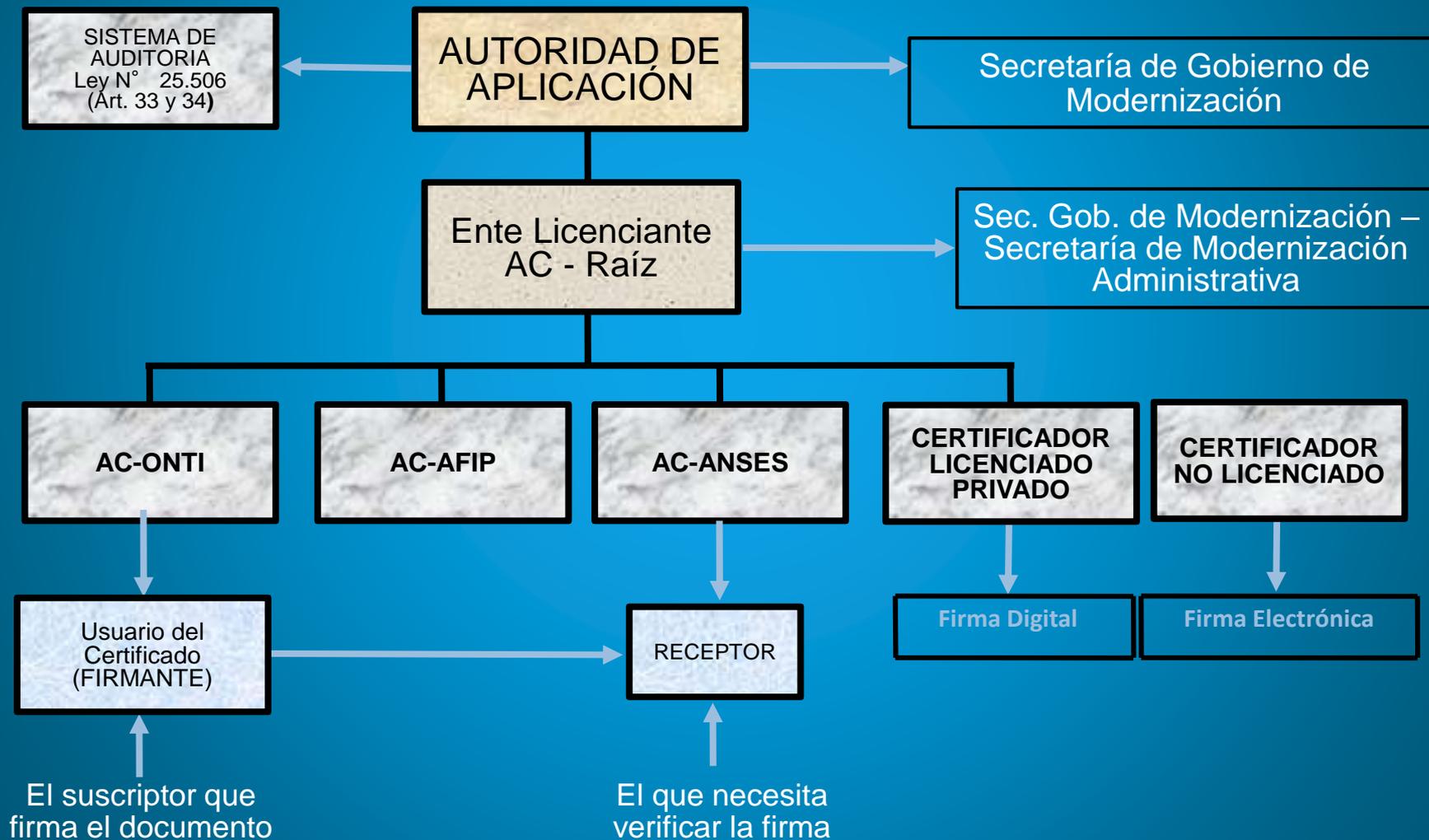
Certificado Digital - Definición

- ❖ Se entiende por Certificado digital al documento digital firmado digitalmente por un Certificador, que vincula los datos de verificación de firma a su titular.
- ❖ Los certificados de firma digital deben ser emitidos por un Certificador Licenciado cuya licencia este certificada por el Ente Licenciante.

Certificador Licenciado - Definición

- ❖ Se entiende por Certificador Licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante.

Infraestructura de Firma Digital (PKI)



APLICACIONES

Aplicaciones

- ❖ Presencia de la Administración en la red.
- ❖ Publicación de información segura en la red.
- ❖ Consulta de información personal a través de Internet.
- ❖ Notificaciones oficiales (Boletín Oficial).
- ❖ Remisión de información vía correo electrónico.
- ❖ Compras electrónicas.
- ❖ Inscripción y trámites en línea.
- ❖ Realización de cualquier trámite a través de Internet.
- ❖ Acceso a aplicaciones informáticas de gestión por ciudadanos y empresas.
- ❖ Expedientes digitales.
- ❖ Mejorar la comunicación entre dependencias de una administración pública y entre distintas administraciones.

Aplicaciones en el Estado

APN

CERTIFICADO DE ANTECEDENTES PENALES

Registro Nacional de Reincidencias
Ministerio de Justicia

Aplicaciones en el Estado

- Aplicación

A los ciudadanos que, ejerciendo su derecho de HABEAS DATA, solicitan sus antecedentes penales.

De existir alguna información, se le brinda la respectiva copia de los datos emanados del Poder Judicial; de lo contrario se le otorga un Certificado que acredita dicha ausencia.

Aplicaciones en el Estado

- Firma Digital

Aquellos ciudadanos que tramitan sus certificados de antecedentes y no registran antecedentes penales reciben dicha documentación firmada digitalmente.



Trámite: P1431039

**CONSTANCIA DE EMISION DE
CERTIFICADO DE ANTECEDENTES PENALES**
Art. 8 inciso f) LEY Nro. 22.117
Art. 52 C.P. (Modificado por Ley 23.057)

SE DEJA CONSTANCIA que : JUAN PEREZ

NACIONALIDAD Argentina, FECHA DE NACIMIENTO 20/10/1980

DOCUMENTO D.N.I. 23.444.666

NO REGISTRA ANTECEDENTES PENALES a informar por esta Repartición.

Se expide el presente a los efectos de ser presentado ante las autoridades que correspondan.

Buenos Aires, 19 de mayo de 2006

Firmado conforme Ley 25.506 por : Francisco Vallejos
Coord. Noche - Area At. Usuario

La presente constancia acredita la emisión del Documento Digital correspondiente al Certificado de Antecedentes Penales conforme los términos de la Ley 25.506, el Decreto 2628/2002 y el Decreto 283/2003, siendo su código de Trámite: P1431039 y Código de seguridad: 6C430647AA625626F86F6A69B1F04EF3062F7A50. A efectos de su verificación, acceda a la siguiente dirección: www.direc.jus.gov.ar/certificado.asp

Código de seguridad



6C430647AA625626F86F6A69B1F04EF3062F7A50

Certificado de Antecedentes Penales



Trámite: P1431039

**CONSTANCIA DE EMISION DE
CERTIFICADO DE ANTECEDENTES PENALES**

Art. 8 inciso f) LEY Nro. 22.117

Art. 52 C.P. (Modificada por Ley 23.057)

SE DEJA CONSTANCIA que : JUAN PEREZ

NACIONALIDAD Argentina, FECHA DE NACIMIENTO 20/10/1980

DOCUMENTO D.N.I. 23.444.666

NO REGISTRA ANTECEDENTES PENALES a informar por esta Repartición.

Se expide el presente a los efectos de ser presentado ante las autoridades que correspondan.

Buenos Aires, 19 de mayo de 2006

Firmado conforme Ley 25.506 por : Francisco Vallejos
Coord. Noche - Area At. Usuario

Código de seguridad



6C430647AA625626F86F6A69B1F04EF3062F7A50

Certificado de Antecedentes Penales

Aplicaciones en el Estado

- Verificación

Consulta de Certificados de Antecedentes
Penales con Firma Digital

Los ciudadanos pueden verificar la validez de aquellos certificados de antecedentes que hayan sido firmados digitalmente.

Acceder al sitio web del Registro.

www.dnrec.jus.gov.ar/certificado.asp

Consultar el certificado conforme Ley 25.506, Decreto 2.628/2002 y Decreto N° 283/2003 (Firma Digital).



Aplicaciones en el Estado

SISTEMA DE RETIRO VOLUNTARIO

OFICINA NACIONAL DE EMPLEO PÚBLICO

Aplicaciones en el Estado

- Aplicación

Sistema de Retiro Voluntario

Antes de proceder a la realización de un contrato o nombramiento, se debía verificar la no inscripción en el REGISTRO DEL PERSONAL ACOGIDO AL SISTEMA DE RETIRO VOLUNTARIO.

Organismos involucrados :

Oficina Nacional de Empleo Público.

Unidades de Recursos Humanos del Sector Público Nacional.

Aplicaciones en el Estado

R.R.H.H.

Manual



Mesa de Entradas

Manual

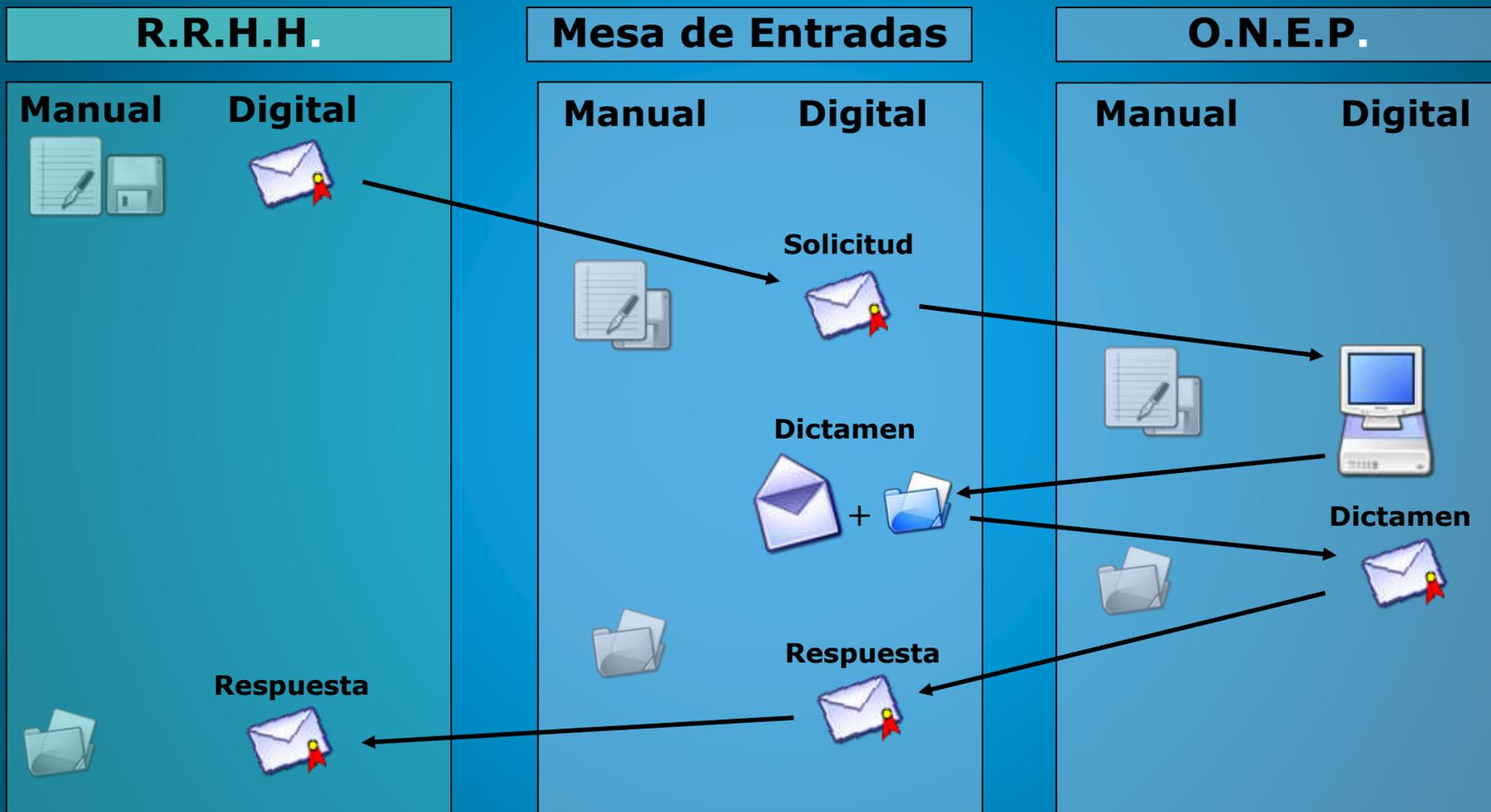


O.N.E.P.

Manual



Aplicaciones en el Estado



Aplicaciones en el Estado

- Resultados

Indicadores

Tiempo promedio de respuesta : menos de 1 hora.
15 organismos involucrados.

Principales ventajas

Eficiencia y agilidad.
Economía de recursos.
Seguridad y respaldo.
Feedback inmediato.

Constitución de Autoridades de Registro

- **ADMINISTRACIÓN PÚBLICA NACIONAL**

El área de Recursos Humanos cumplirá las funciones de Autoridad de Registro (Dec. N° 2.628/02 art. 39).

- Nota emitida por la Autoridad competente del Organismo al Director Nacional de la ONTI, constituyendo:
 - La Autoridad de Registro en el Organismo
 - Designando al/los Responsables de Autoridad de Registro en el área de RRHH

En caso de necesitar constituir una Autoridad de Registro adicional en un área diferente de RRHH, la máxima Autoridad del Organismo deberá emitir y justificar la misma (Dec. N° 2.628/02 art. 39)

- Notas asignando las funciones de
 - Oficial de Registro
 - Responsable de Soporte Técnico de Firma Digital

En caso de Oficiales de Registro en un área diferente de RRHH, el Responsable de la Autoridad de Registro deberá emitir y justificar la misma

Constitución de Autoridades de Registro

- **SECTOR PÚBLICO**

Surge del artículo 35 del Decreto Reglamentario Nº 2628/02 que el Certificador podrá delegar funciones en Autoridades de Registro y detalla sus responsabilidades.

- Nota emitida por la Autoridad competente del Organismo al Director Nacional de la ONTI, constituyendo:
 - La Autoridad de Registro en el Organismo
 - Designando al/los Responsables de Autoridad de Registro
- Notas asignando las funciones de
 - Oficial de Registro
 - Responsable de Soporte Técnico de Firma Digital

Autoridad de Registro

Autoridad de Registro
(Organismo)



Roles y funciones

- **Responsable de la Autoridad de Registro**

Responsable legal y nexo formal para las comunicaciones entre el Certificador y la AR.

- **Oficiales de Registro**

Validación de identidad y de otros datos de los solicitantes y suscriptores de certificados, registrando las presentaciones y trámites que les sean formulados por éstos

- **Responsable de Soporte Técnico de Firma Digital**

- Instruir a los usuarios de la AR en la tramitación de los servicios provistos por el Certificador
- Responsable de la difusión dentro del Organismo del uso y aplicabilidad de la Firma Digital
- Asistir técnica y procedimentalmente a solicitantes o suscriptores en la tramitación de los servicios provistos por el Certificador y en el manejo de la operatoria de la tecnología de firma digital de las distintas aplicaciones que requieran su uso.

Política de Certificación

Podrán ser suscriptores de los certificados emitidos por la Autoridad Certificante de la Oficina Nacional de Tecnologías de Información:

- Las personas humanas que desempeñen sus funciones en entes públicos.
- Las personas humanas que realicen trámites con el estado por medio de alguna aplicación Informática que requiera el uso de firma digital (la Autoridad de Registro encargada del proceso de registración debe haber sido previamente autorizada por la AC-ONTI).

Implementación - Criterio

- ❖ Contar con un marco legal adecuado.
- ❖ Generar confianza en la firma digital por medio de la capacitación de los Recursos Humanos.
- ❖ Redefinir procesos administrativos y protocolos.
- ❖ Contar con la infraestructura tecnológica necesaria.
- ❖ Desarrollar aplicaciones que fomenten el uso de la firma digital.

Autoridad Certificante de Firma Digital del Ministerio de Modernización

Muchas Gracias

Consultas

consultapki@modernizacion.gob.ar