



Uso de los Certificados Electrónicos y Firma Electrónica



Ing. Gabriel Moline Mse.



Agenda

- **Introducción**
 - Nuevos paradigmas.
 - Base de la certificación electrónica
- **¿Que es un certificado electrónico?**
 - Contenido de un certificado electrónico
 - Funciones principales
 - Modelo de Confianza del Estado Venezolano
 - Tipos de Certificados
 - Sistemas de uso diario que lo implementan
- **¿Como funciona una firma electrónica?**
- **Casos de éxito en Venezuela**

Introducción

- **Internet ha cambiado la comunicación y los servicios.**
- **5.000 años de uso de la escritura**
 - La firma electrónica se convierte en un cambio de paradigma e impone repentinamente hoy día un cambio cultural de más de 5.000 años en la costumbre del uso de la escritura para otorgar validez jurídica a la expresión de la voluntad.



Introducción



Drawing by Peter Steiner © 1993 The New Yorker Magazine, Inc. All rights reserved



"On the Internet, nobody knows you're a dog."



Introducción

Base de la Certificación Electrónica



Certificado Electrónico

¿Que es un certificado electrónico?:

Es un documento electrónico validado por una autoridad, el cual permite identificar al signatario del mismo mediante un conjunto de datos que contiene, en otras palabras no es mas que un sello electrónico con atributos específicos y únicos.



Certificado Electrónico

Funciones:

- **Firmar** electrónicamente un documento
- **Identificar** el autor de un documento o solicitante de información (autenticación)
- **Encriptar** (codificar) documentos o comunicaciones



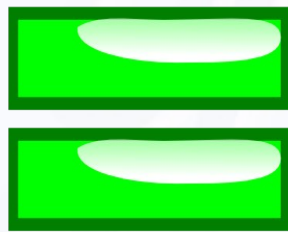
Certificado Electrónico

¿Que es un certificado electrónico (tec)?:

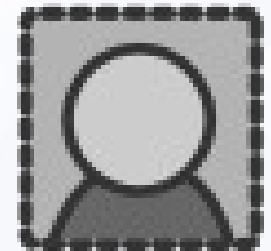
Criptografía asimétrica: Método criptográfico que usa un par de claves para el envío de mensajes.



Certificado



Privada
(Firma)



Publica

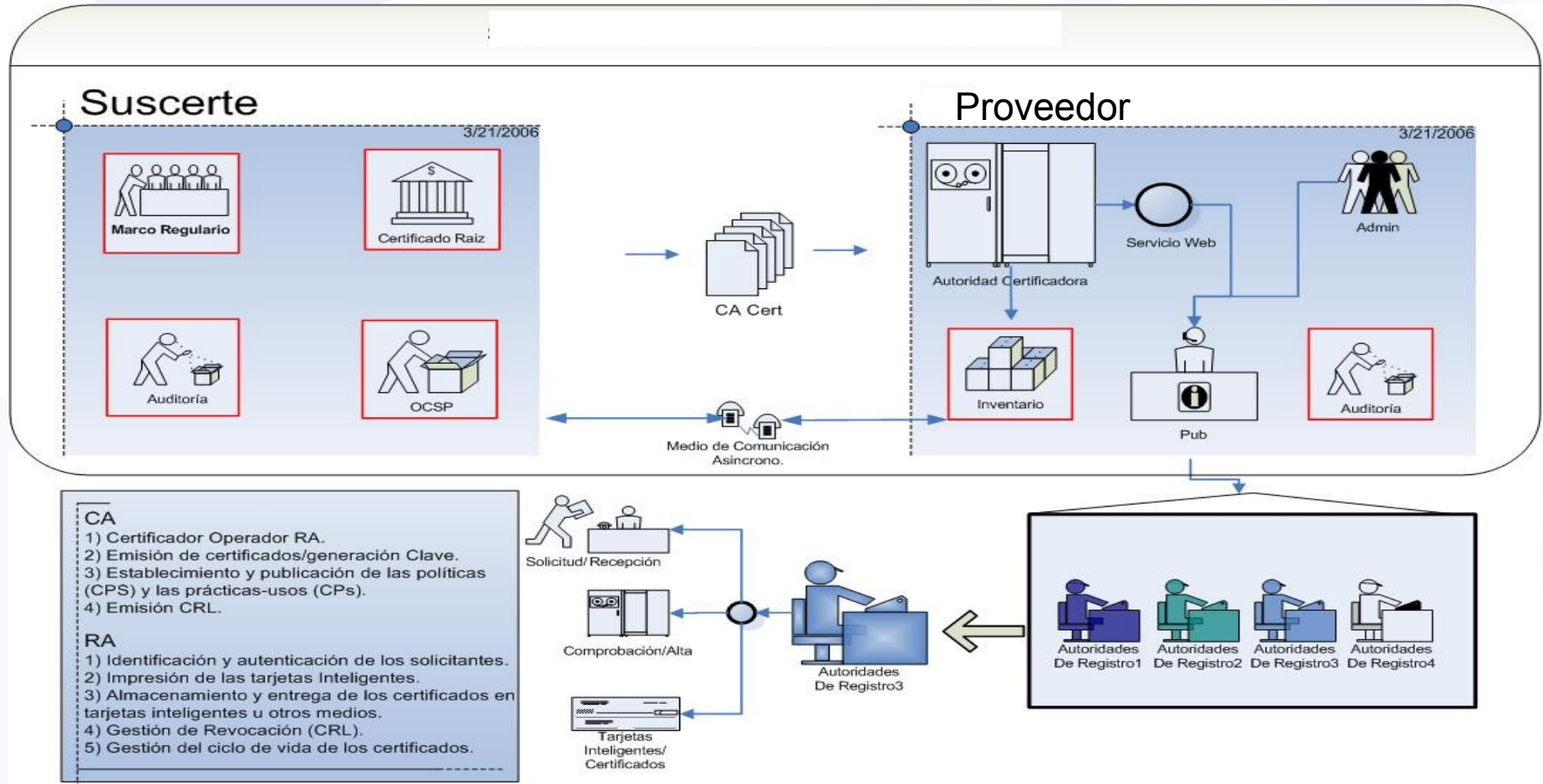
Certificado Electrónico

Almacenamiento



Certificado Electrónico

Modelo Jerárquico - Obtener un certificado Electrónico



Certificado Electrónico

Tipos de certificados actuales:

Tipo de Certificado	Características	Principales usos
Personas Naturales / Jurídicas (Hardware)	Certificados de 2048 bit, tres años vida sha1 /sha256	Firma y/o autenticación de personas naturales /jurídicas
Personas Naturales / Jurídicas (Software)	Certificados de 1024 bit, un año de vida - sha1	Firma y/o autenticación de personas naturales /jurídicas
Servidores	Certificado de 1024 y/o 2048 bit, un año de vida	Dos modelos CA criptográfica de la raíz venezolana y generados dentro de la RA
Personas Naturales Criptográficos	Certificado de 1024 y/o 2048	Utilizados para el resguardo criptográfico

Tipos de certificados futuros:

Tipo de Certificado	Características	Principales usos
Certificados de Atributos	No de Definido	Liga un determinado atributo a una identidad (certificado de clave publica)
Certificados de Colegios Profesionales	Certificados de 1024 bit, un año de vida - sha1	Firma y/o autenticación de Ejercicio Profesionales

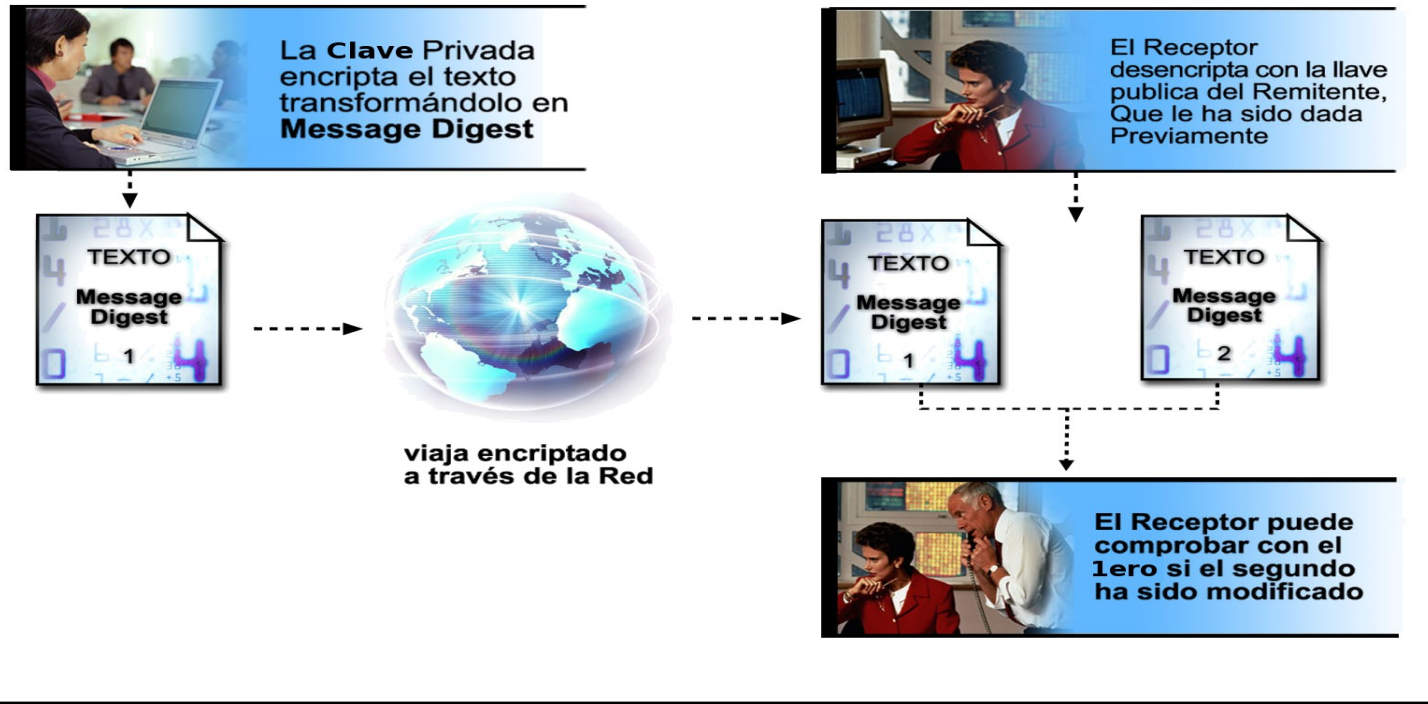
Certificado Electrónico

Sistemas de uso diario que lo implementan:

- Firma de correos electrónicos (Microsoft Outlook, Mozilla Thunderbird)
- Aplicaciones de procesamiento de palabras (Microsoft Word, OpenOffice, Acrobat Reader y Writer, StartOffice, etc.)
- Sistemas de seguimiento de documentos electrónicos
- Sistemas de autenticación en línea
- Aplicaciones en las que se manejen pagos electrónicos

Firma Electrónica

Funcionamiento de la Firma Digital



- Un ejemplo de Firma Digital:

-----BEGIN GPG SIGNATURE-----
Version: GnuPG v1.4.7 (MingW32)

```
iQEVAwUBRgmQ8LXoJ59sgHAGAQLBgf/VaeU08RA4CfqXBd0kvXNPOxL.pnb/DmCP  
ziZnHIWERD5WEYisRZBVX8MDkQnhTw35mSY3KejeeOl18SzQl1p4aapbFXXbiigB  
Yu/SfrJGZNTIp4TN0+berrZla05rcgmtzYZ+84fcVguSgyVdLRtxpqBBeEQjRIGW  
ltHFpPLMhRYMkqTVE8rIX5BT+2sTJGcU0ZKzkum+uZJzQae3NQJbSOGbqQ8pTcd8  
933FKWxXv0C5hbP2h0fpzj7TuRq40IEGUcxm1rXb5CpwKa2dujB24eFIoLlyVyNf  
bMhYeJ7BXuDMYw/Z2kITDleTZHTXPk7znmuKeAeqr5rBTkcZjIUWiQ==  
=0vpB  
-----END GPG SIGNATURE-----|
```

Firma Electrónica

¿Donde usarla?

- Firma de documentos.
- La firma y cifrado de los correos electrónicos.
- Contratación Electrónica.
- Aplicaciones Bancarias.
- Comercio Electrónico.
- Autenticación de usuarios en redes telemáticas inseguras
- Masificación de Trámites Administrativos.
- Notificaciones Electrónicas.



Firma Electrónica

Beneficios

OPERATIVOS

- No Repudio y Autenticación de documentos digitales.
- Reducción de costos en volúmenes de material utilizado para la impresión de documentos que necesiten aprobación mediante *firma manuscrita*.
- Disminución de almacenamiento en *archivos físicos*.
- Se agilizan procesos de aprobación para documentos que requieran *firma manuscrita* en *aprobación múltiple*:
 - Recepción de propuestas digitales para licitaciones.
 - Contratación y adjudicación digital.

ESTRATÉGICOS

- Se apalanca efectivamente la lucha contra la *burocracia* y la *corrupción*.
- Se Fortalece de la Seguridad *desde* el usuario basada en una infraestructura tecnológica apoyada por normativas internas y un marco legal vigente.
- Integración con PKI Nacional.
 - Fortalecimiento del Gobierno electrónico
 -

Casos de Éxito

Venezuela



AHORA ES DE TODOS

Casos de Éxito

Caso Oficina Nacional de Identificación y Extranjería (e-pasaporte).

- Inicio ejecución en marzo del 2007
- Mas de 50.000 pasaportes electrónicos emitidos a la fecha
- Venezuela se convierte en el primer país del continente americano en el empleo de tecnología de pasaporte inteligente



Caso Oficina Nacional de Identificación y Extranjería (ID Inteligente).

- Generación de 25 millones de documentos de identidad con PKI
- El tiempo de despliegue inicial abarcara a todos los venezolanos en un lapso de 3 a 5 años
- Convertirse en la AC mas grande de América
- Creación de un sistema de identificación y comunicación ciudadano estado
- Primer documento de identidad producido para el primer trimestre del 2008



Casos de Éxito

Caso Servicio Nacional Integrado de Administración Aduanera y Tributaria (RIF -Inteligente).

- Inicio de ejecución primer trimestre del 2008
- Se esperan generar 300.000 tarjetas con certificados electrónicos durante el 2008
- Se espera generar 3.000.000 de Certificado en los próximos 3 años.
- Dirigido a las personas jurídicas para su autenticación y declaración de impuestos por la Web
- Tarjeta multi-aplicación y multi-propósito



Caso Venalum Industrias Basicas (Sistema de congestión).

- Generación de certificados electrónicos para clínicas y ambulatorios
- Interconexión y autenticación entre centros clínicos y Venalum
- Se interconectaron más de 400 centros clínicos
- Reducción de costos de pólizas de seguros

Casos de Éxito

Caso Villas del Cine

- Sistema de firma de vídeos para garantizar los derechos de autor en los formatos digitales.
- Mas de 60 productoras registradas.



Caso Ministerio del poder popular para la Alimentación

- Aprobación de exportaciones de alimentos de manera electrónica
- Solicitud de aprobación de divisas para la exportación de alimentos (CADIVI)

Casos de Éxito

Otros casos de Éxito

- DISIP (División de los servicios de inteligencia y prevención)
- OCHINA (Servicio autónomo de la Oficina Coordinadora de Hidrografía y Navegación)
- Fundación Instituto de Ingeniería
- SUSCERTE

Casos en ejecución o con miras al futuro

- PDVSA (Petróleos de Venezuela)
- Metro de Caraca
- Instituto Venezolano de los seguros sociales
- CADIVI (Comisión de administración de divisas)
- CNTI (Sistema de gestion administritativa central -k2b)

Muchas Gracias...

Contacto:

Ing. Gabriel Moliné Mse.

e-mail: gmoline@suscerte.gob.ve

Tlf: +58 212 7718586

cel: +58 416 6182098

<http://www.suscerte.gob.ve>