



MIPPCOEXIN

Certificados de Firma Electrónica

By PROCERT.NET.VE

Base Legal.

Ley Especial Contra Delitos Informáticos.

Ley Sobre Mensajes de Datos y Firmas Electrónicas.

Providencia Administrativa SUSCERTE N° 004-10.

Ley Infogobierno.

Oponible a
Terceros.

Reconocimiento
Gubernamental.



Prueba Legal de
Transacciones.

Sustitución
Comprobante
Físico.

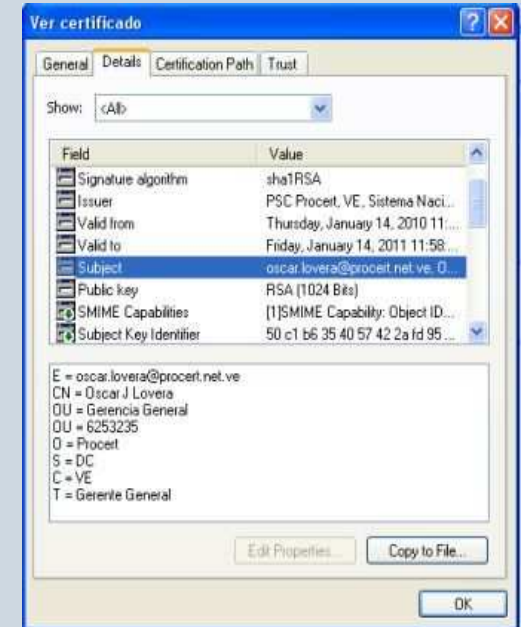
Base Legal.

Ley/Código	Gaceta Oficial	Fecha
Ley Orgánica de Seguridad de la Nación	N° 37.594	18-12-2002
Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo	N° 39.912	30-04-2012
Ley Sobre Mensajes de Datos y Firmas Electrónicas	N° 37.148	28-02-2001
Ley Especial Contra Delitos Informáticos	N° 37.313	30-10-2001
Ley de Interoperabilidad	N° 39.945	15-06-2012
Ley de Infogobierno	N° 40.274	17-10-2013

Certificado Electrónico.

- Autenticación
 - Sabemos quién nos ha enviado el mensaje o documento electrónico.
 - La clave privada identifica la entidad firmante.
- Integridad
 - Una vez firmado, el contenido del mensaje no puede ser modificado.
 - La clave privada identifica la entidad firmante.
- No Repudio
 - El signatario o usuario no puede negar la autoría del mensaje firmado.
 - Sólo la entidad firmante posee su clave privada, y ha firmado dicho documento porque contiene el hash del mismo.
- Disponibilidad
 - Que la información sea disponible para su ulterior consulta.
- Prueba Legal
 - Amparado en Ley.

Vista del Certificado



Funcionamiento. El certificado – Proceso para su emisión.



Suministro de
información.

C.I.

Doc. Empresa

RIF

Poder

Gaceta

Asambleas

Recibo de
Servicio



Validación
Documental
Identidad



Generación de
claves
criptográficas
Emisión

•Funcionamiento. El certificado – Ciclo de Vida.



Activo.

Validado por medio de la LCR y el OCSP.

Obliga al signatario.

Es validable por terceros.

Autoría.

No repudio.

Autenticación.



Suspendido

Validado por medio de la LCR y el OCSP.

Puede ser activado.

Preventivamente e aparece como suspendido.

Obliga al signatario

Es validable por terceros.



Revocado

Por cumplimiento del plazo.

Por revocación de clave.

Obliga al signatario.

Aparece en la LCR y el OCSP como Revocado.

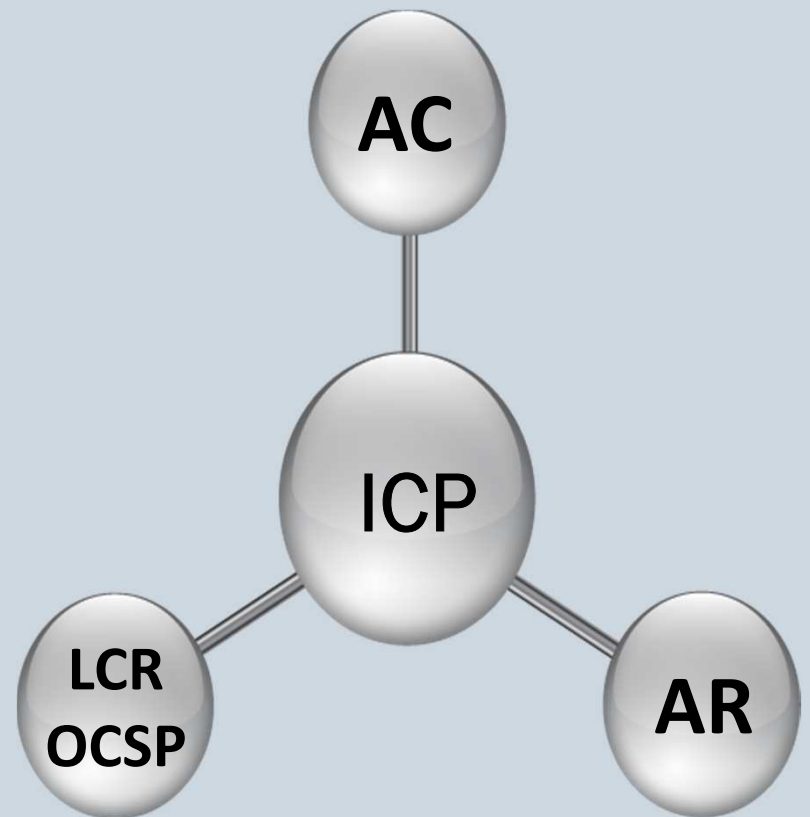
Es validable por terceros.

Certificados Electrónicos

- Emitidos por un Proveedor de Servicios de Certificación (PSC) acreditado ante SUSCERTE.
- Los certificados de empleados y funcionarios sirven para firmar documentos electrónicos, correo electrónico, autenticarse ante sistemas y cifrar correos electrónicos.
- El algoritmo de firma es SHA-256.
- La longitud de clave es de 2048.
- Vigencia de 1 año.
- Generados en Venezuela.
- Regulados legalmente.

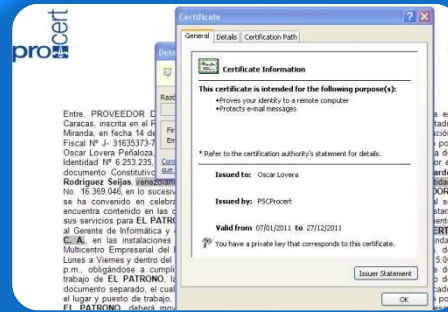
Infraestructura de Clave Pública (ICP)

- Autoridad de Certificación (AC)
 - Maneja Ciclo de Vida de Certificados.
 - Opera Conforme a Estándar X.509 V3
- Protocolo X.509 V3
 - Establece Estándar de Operación ICP.
 - Lista Certificados Revocados (LCR).
 - On Line Certificate Status Protocol (OCSP).
- Autoridad de Registro (AR)
 - Establece Identidad de Usuarios.
 - Crea Registro de Usuarios.
 - Aprueba junto a la AC los Certificados.



La Firma Electrónica es Visible en Varios Formatos:

.doc, .txt, .jpg., .pdf, .gif., .ppt, .bmp



usar un algoritmo de firma SHA-256 y una longitud de clave del certificado de 2048

veedor de Certificados (PROCERT), C.A. queda a sus órdenes a los fines de dar asesoría y productos de certificación electrónica y seguridad de TI, los cuales le permiten minimizar la ocurrencia de eventos y adicionalmente dar cumplimiento al marco legal venezolano.

procert Digitally signed by
Oscar Lovera
DN: c=VE, st=DC,
o=Procert, ou=6253235,
ou=Gerencia General,
cn=Oscar Lovera,
email=oscar.lovera@pro
cert.net.ve
Date: 2011.10.06
08:41:21 -0430'