



ECUADOR
UNIVERSIDAD
INTERNACIONAL
SEK



SEGURIDAD DE DATOS

Ing. José Luis Medina



Firma Electrónica



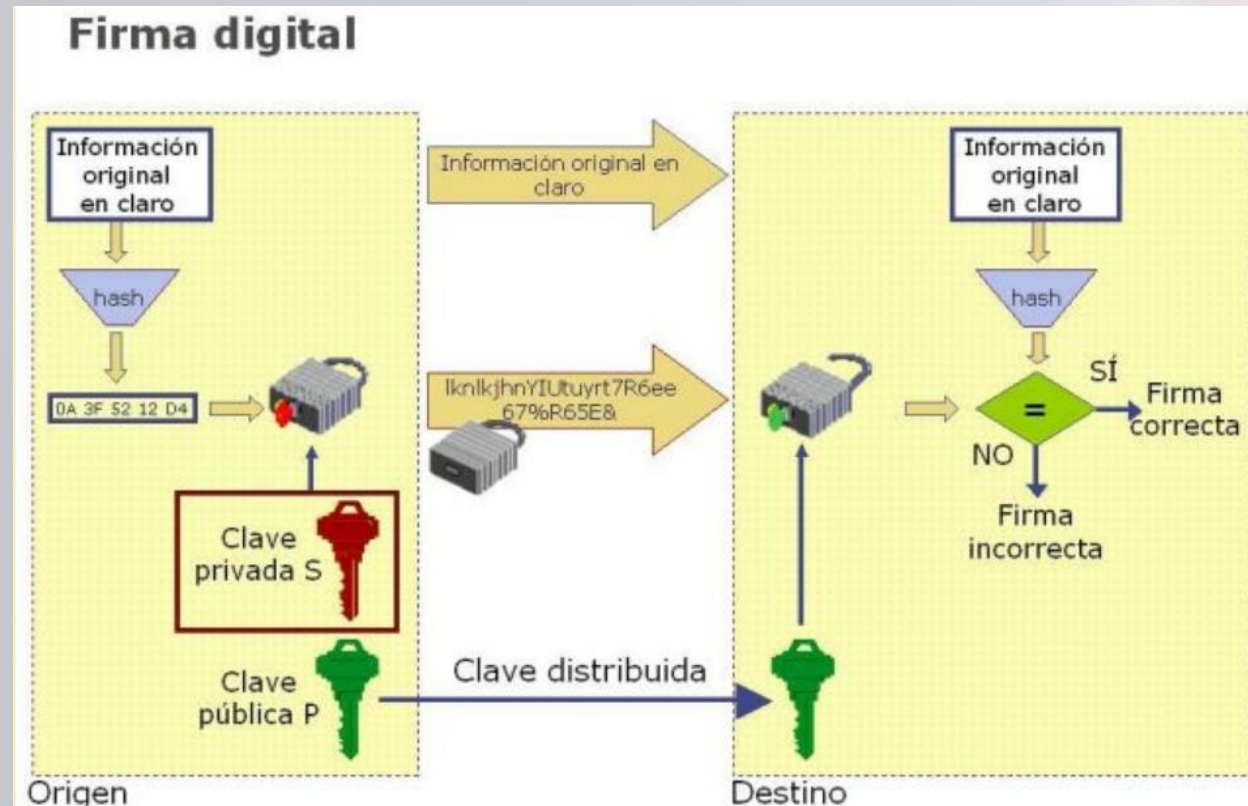
Firma Electrónica

- Según Wikipedia, es un **concepto jurídico**, equivalente electrónico a la firma manuscrita donde la persona acepta el contenido de un mensaje electrónico a través de cualquier medio electrónico válido.
- Según la ley de comercio electrónico en el Ecuador, son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo y que puedan ser usados para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos

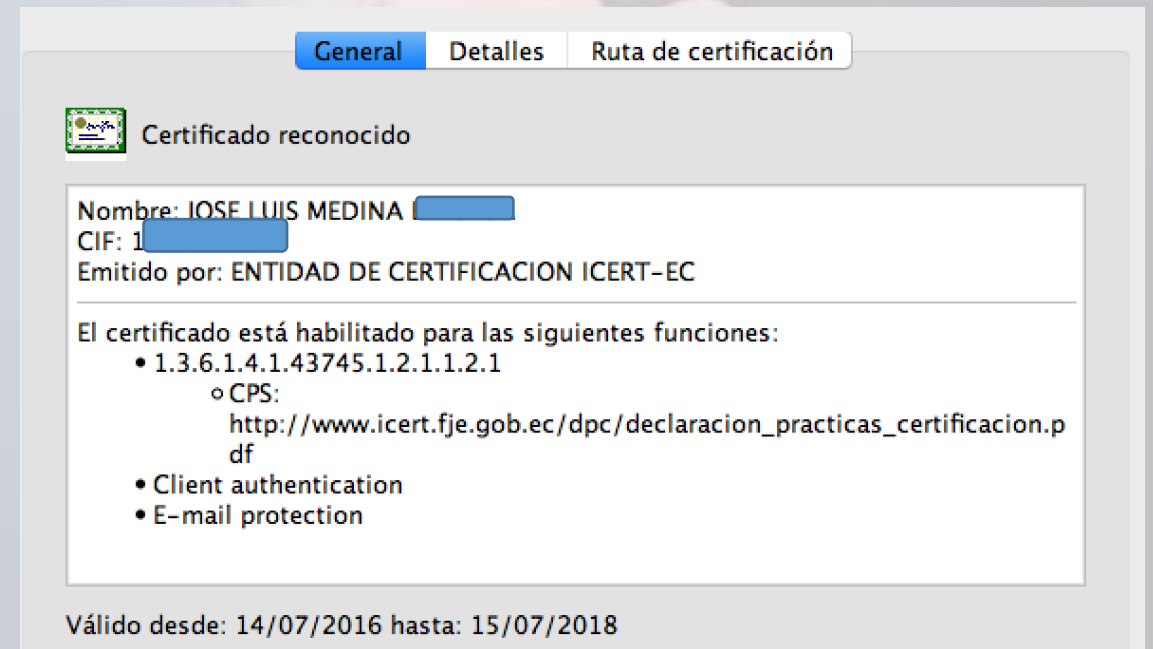
- La Firma Electrónica tendrá igual **validez** que la firma manuscrita, para ello se reconocerá los mismos efectos jurídicos que la firma manuscrita.
- Migrar al concepto de cero papel
- Añadir confianza en la firma de un documento, para ello quien firma el documento acepta el contenido del mismo y cuando lo firma confirma quien dice que es



- La firma electrónica se basa en el principio de clave pública, para ello en la generación de certificados digitales se crean dos claves pública y privada
- El firmante del documento utiliza su clave privada
- El receptor accede al documento mediante la clave pública correspondiente y con eso evidencia quien es el firmante de dicho documento



- La firma electrónica se basa en un certificados digitales v3
- Un certificado digital son similares a tarjetas de identificación y estos son emitidos por una **Entidad de Certificación CA** o **Infraestructura de Clave Pública PKI**
- El certificado posee información acerca de la entidad certificadora además contiene la pareja de claves públicas y privada además de toda la información necesaria como fecha de emisión y expiración del certificado.



Certificados Digitales

Certificado

General Detalles Ruta de certificación

Mostrar: Sólo campos versión 1

Campo	Valor
Versión	V3
Número de serie	2f 73 6c 2c 1b a8 8e eb
Algoritmo de firma	sha256RSA
Emitido por	ENTIDAD DE CERTIFICACION ICERT-EC, SUBDIRECCION NAC
Válido desde	Thu, 14 Jul 2016 19:32:25 +0000 UTC
Válido hasta	Sun, 15 Jul 2018 19:32:25 +0000 UTC
Emitido a	JOSE LUIS MEDINA [REDACTED], QUITO, EC
Clave pública	RSA (2048 Bits)

Certificado

General Detalles Ruta de certificación

Mostrar: Sólo extensiones

Valor
Client authentication (1.3.6.1.5.5.7.3.2),E-mail protection (1.3.6.1.5.5.7.3.4)
Subject Type=End Entity,Path Length Constraint=None
[1]Certificate Policy:, Policy Identifier=1.3.6.1.4.1.43745.1.2.1.1.2.1, [1,1]...
[1]Authority info access, Access method = OCSP (1.3.6.1.5.5.7.48.1), Ac...
[1]CRL distribution point, Distribution point name:, Full name: http://...
KeyID=2f 22 7a f8 5e 6d 94 8e 6a 40 14 37 c7 6e 6b 72 e9 3a c2 3f
10 fc 99 8e 78 01 8f 91 f0 45 47 b5 36 96 09 bd af 24 53 c5
RFC822 Name=medinajl@gmail.com,Other Name:,Principal Name=171133...
Digital signature,Non repudiation (c0)

Certificado

General Detalles Ruta de certificación

Información del certificado

El certificado está habilitado para las siguientes fu

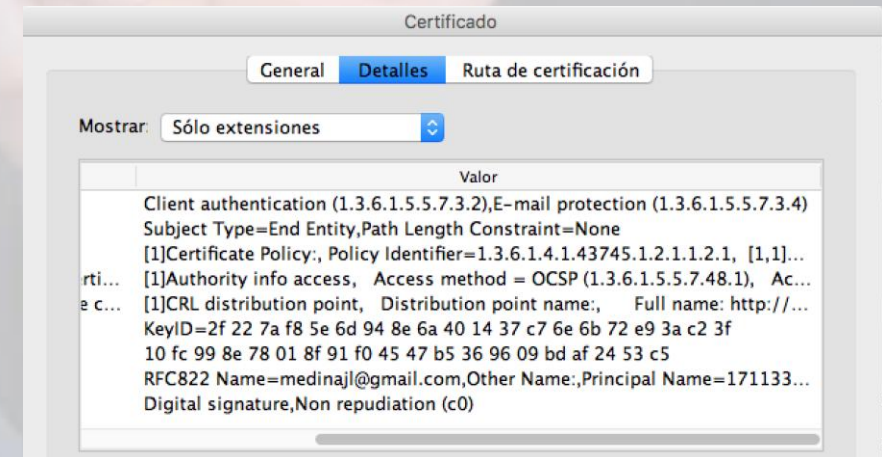
- 2.5.29.32.0
 - CPS:
<http://www.icert.fje.gob.ec/dpc/declarac>
- All application policies

Emitido a: ENTIDAD DE CERTIFICACION ICERT-EC

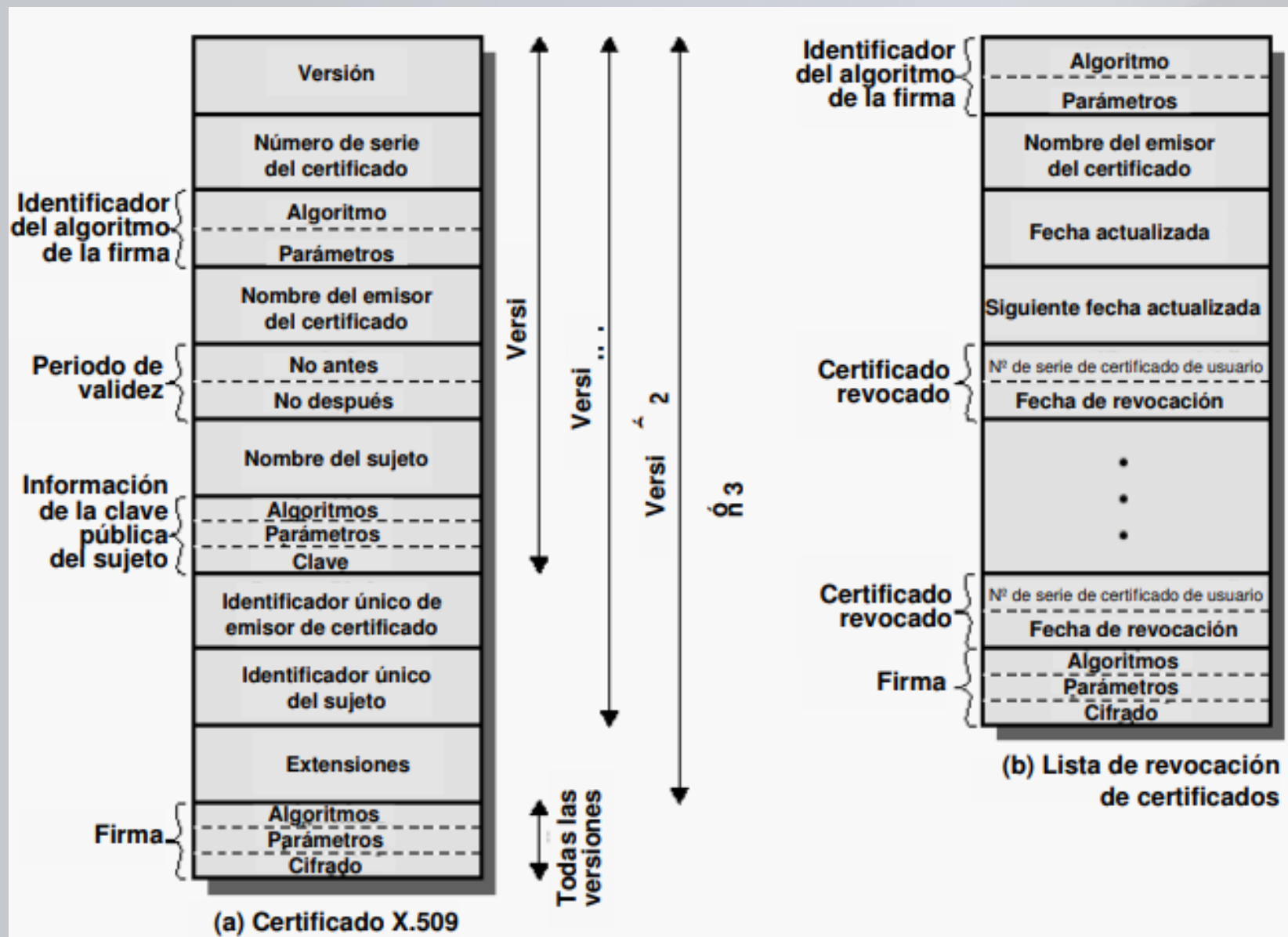
Emitido por: ICERT-EC ENTIDAD DE CERTIFICACION RAIZ

Válido desde: 16/10/2014 hasta: 15/10/2034

- La manera en que se **garantiza** la identidad de las partes es a través de un **certificado digital** emitido a la persona
- Un **certificado digital**, es un documento emitido y firmado por la **autoridad de certificación**, el mismo que confirma la identidad de la persona natural o jurídica, vinculada con una llave pública asociada a la llave privada
- Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido
- Los certificados digitales se emiten a:
 - Personas
 - Servidores
 - Entidades Jurídicas



Versión del certificado	Versión 3
Núm. de serie del certificado	<i>Generado por la CA, único</i>
Algoritmo de firma del certif.	sha1withRSAEncryption
Nombre X.500 del emisor	c=ES, o=Empresa, cn= Autoridad de Certificación
Periodo de validez	desde dd/mm/aa hasta dd'/mm'/aa'
Nombre X.500 del sujeto	c=ES, o=Empresa, cn=José Pérez
Clave pública del sujeto	AC:46:90:6D:F9:.....
Uso de la clave	Firma digital, cifrado de clave
Uso de la clave mejorado	Autenticación en W2000
Identificador claves CA	Identifica el par de claves utilizado para firmar el certificado
Identificador claves usuario	Identifica el par de claves asociado a la clave pub. en el certif.
Punto de distribución CRLs	HTTP://servidor/ruta/nombre.crl (publicación en web)
Firma de la AC	Firma del certificado por la CA



- Dentro de los **estados** de los certificados digitales tenemos:
- **Emisión** (certificado válido, generalmente 2 años)
- **Caducado** (expiración del periodo de validez, se requiere la renovación del certificado)
- **Revocación de certificados** (puede pasar que la clave privada asociada al certificado se haya visto comprometida, es decir robada, extraviada o sustraída, puede pasar que el titular del certificado lo revoque por cambio de datos, puede ser revocado por la CA)
- **Suspensión del certificado** (revocación temporal)

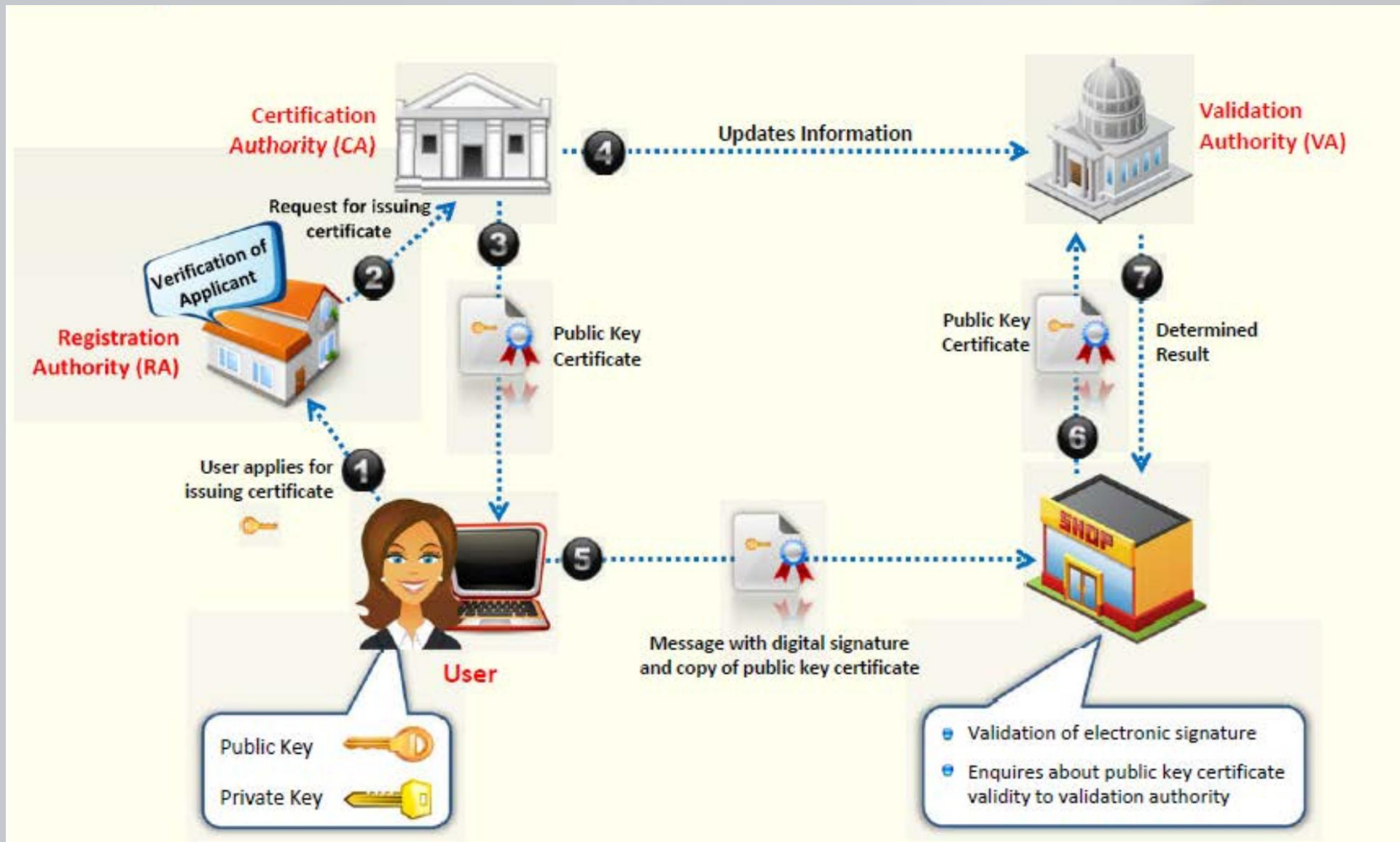
Infraestructura de Clave Pública - PKI

- Es un conjunto de hardware, software, gente, políticas y procedimientos que permiten crear, manejar, distribuir, usar, almacenar y revocar certificados digitales
- Para la creación de una PKI es importante la definición de:
 - **DPC** (Descripción de prácticas de certificación)
 - **PCs** (Políticas de certificados)

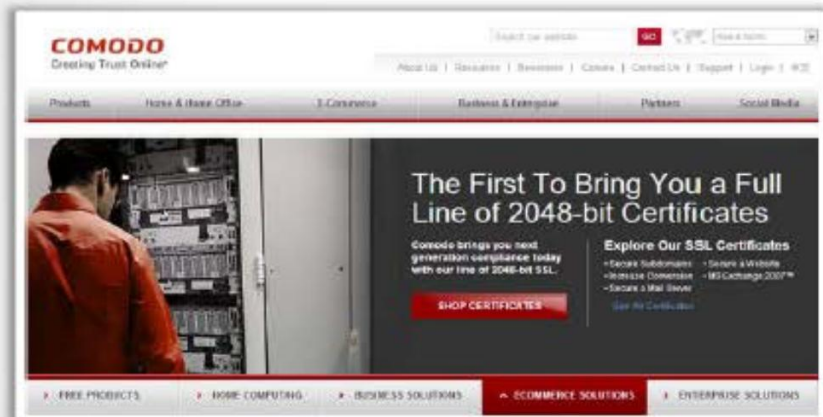


- Una **infraestructura de clave pública** tiene los siguientes componentes:
 - Autoridad de Certificación (CA-Raiz)
 - Autoridad de Certificación Subordinada (CASub)
 - Autoridad de Registro (RA)
 - Autoridad de Validación (VA)
 - Autoridad de Sellado de Tiempo (TSA)
 - Certificados Digitales
 - Personas





Entidades de Certificación Mundiales



COMODO
Creating Trust Online

Search for products

Products Home & Home Office E-Commerce Business & Enterprise Partners Social Media

The First To Bring You a Full Line of 2048-bit Certificates

Comodo brings you next generation compliance today with our line of 2048-bit SSL.

Explore Our SSL Certificates

- Secure Subdomains
- Secure Websites
- Wildcard Domains
- Secure Mail Server

[See All Certificates](#)

[SHOP CERTIFICATES](#)

FREE PRODUCTS HOME COMPUTING BUSINESS SOLUTIONS E-COMMERCE SOLUTIONS ENTERPRISE SOLUTIONS

<http://www.comodo.com>



thawte

Contact Us • 1-888-484-2863 Chat sales@thawte.com Change Country

Products Partners Support Resources My Account

The most visible sign of web site security

Show your customers your site is safe with Extended Validation SSL.

[Learn more](#)

Buy Certificates

- SSL Certificate
- Code Signing

White Paper

Understanding SSL Certificates

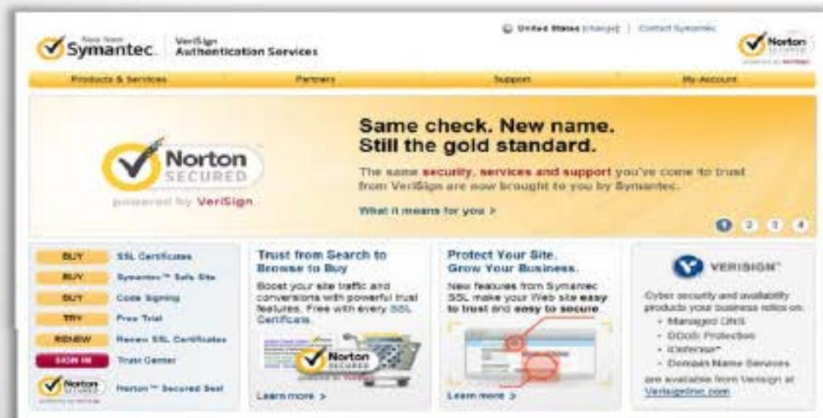
Manage Multiple Certificates

Manage certificates across any size organization with ease!

Not all SSL is the Same

Compare Thawte to other SSL providers and see the difference!

<http://www.thawte.com>



Symantec Norton Authentication Services

Products & Services Partners Support My Account

Same check. New name. Still the gold standard.

The same security, services and support you've come to trust from VeriSign are now brought to you by Symantec.

What it means for you

Trust from Search to Browse to Buy

Boost your site traffic and conversions with powerful trust features. Free with every SSL Certificate.

Protect Your Site. Grow Your Business.

New features from Symantec SSL make your Web site easy to trust and easy to secure.

Go Wild!

Buy Now

VERISIGN

Cyber security and availability products your business relies on.

- Managed DNS
- DDoS Protection
- SecureMail
- Domain Name Services

See availability from VeriSign at [VeriSign.com](#)

<http://www.symantec.com>



Entrust

SECURITY ON: SSL

Entrust Discovery

Find, inventory and manage ALL certificates across ALL your systems and environments

[Go Wild!](#)

Buy Now

EV Multi-Domain SSL Certificates

From \$373/year

EV Multi-Domain SSL Certificates

From \$249/year

Advantage SSL Certificates

From \$186/year

Standard SSL Certificates

From \$155/year

Go Wild!

Buy Now

EV Multi-Domain SSL Certificates

From \$373/year

EV Multi-Domain SSL Certificates

From \$249/year

Advantage SSL Certificates

From \$186/year

Standard SSL Certificates

From \$155/year

<http://www.entrust.net>

Entidades de Certificación - Locales



ICERT - EC
ENTIDAD DE CERTIFICACIÓN
Consejo de la Judicatura



Inicio Quienes Somos Productos Servicios Marco Normativo Atención al Público Centro de Descargas Tarifas

Trámites en Línea

Inicio



Acuerdo Ministerial No. 012-2016

Se dispone el uso de certificados de persona natural para uso de servidores públicos. Entra en operación a partir del Lunes 24/10/2016 << ver más >>

Trámites en Línea: Reactivación Certificado, Registro Empresa o Institución, Solicitud de Certificado, Revocatoria Certificado, Renovación Certificado, Suspensión Certificado



Bienvenidos a nuestra Compañía

SecurityDATA
La Firma Electrónica del Ecuador

La Forma más Segura de tener TU FIRMA ELECTRÓNICA



Atención ininterrumpida de Lunes a Viernes de 8:00 a 19:00
Sábados de 9:00 a 13:00

SECURED BY Entrust SSL *VERIFY



BANCO CENTRAL DEL ECUADOR

Inicio Quienes Somos Marco Normativo Firma Electrónica Servicios Relacionados Centro de Descargas Contáctenos



ágil

Firma electrónica

Noticias



Obténlo también en las oficinas del Registro Civil

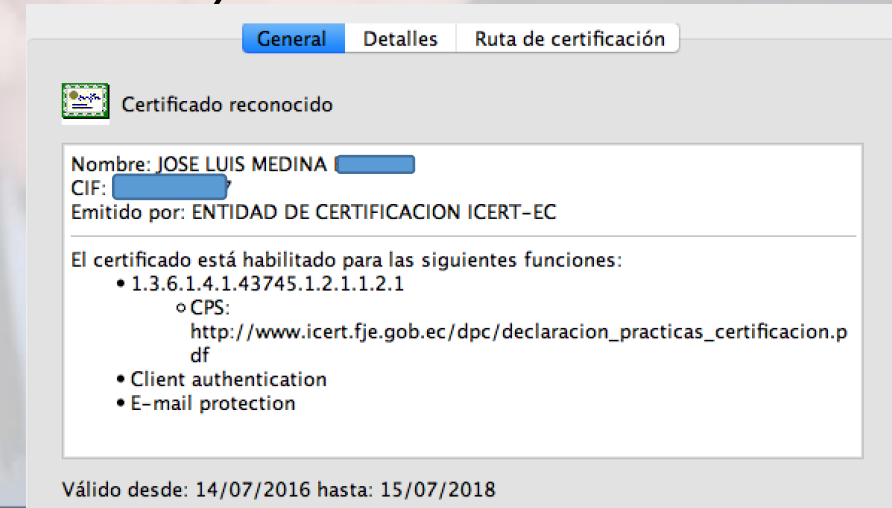
Certificado Digital de Firma Electrónica

En Quito, Guayaquil, Cuenca, Loja, Ibarra, Coca, Ambato, Manta, Tulcán, Esmeraldas, Santo Domingo, Quevedo, Machala, Salinas, Galápagos y Portoviejo.



Ciclo de vida de los certificados

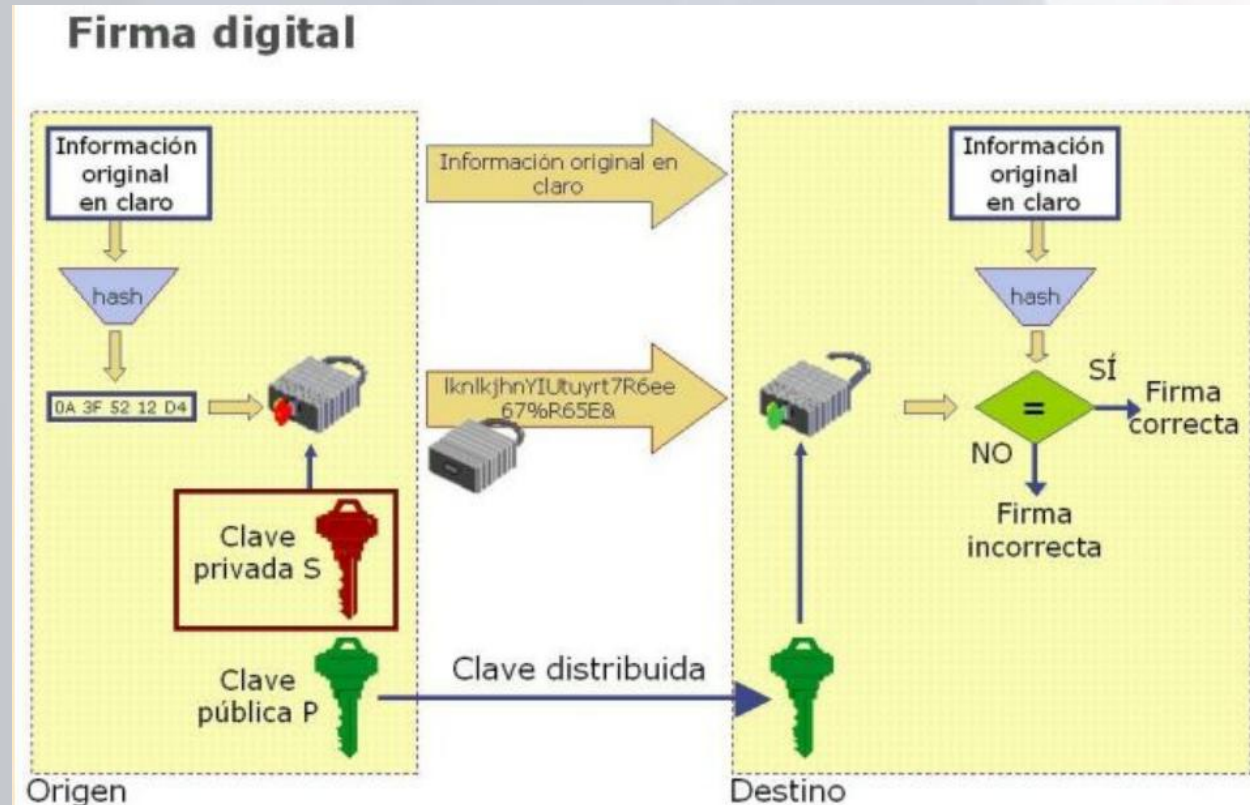
- Una entidad de certificación es un **tercero de confianza**, para ello como entidad se encarga de **validar la información de la persona que realiza la solicitud** de generación de un certificado digital
- En la entidad de certificación se realizan las siguientes operaciones que forman parte del ciclo de vida de un certificado:
 - Solicitud - **por parte del solicitante** (persona – usuario)
 - Validación de la información
 - Creación del certificado
 - Almacenamiento de las claves
 - Revocación del certificado



- La función de la **CA-Raíz** es de la creación del **primer certificado** que dará vida al funcionamiento de toda la entidad de certificación
- Por razones de seguridad este componente **NO** está online
- La generación del primer certificado válido es a través de una ceremonia de generación de claves
- A través del primer certificado se pueden firmar los certificados para las demás autoridades de registro, validación, etc.
- Para mejorar el tipo de encriptación se utilizan **HSMs**



- A través de la **Autoridad de Validación**, se revisa la existencia y validez de un certificado, esto a través del protocolo **OCSP** (Online Certificate Status Protocol), este revisa las **CRLs** (Certificate Revoked List) emitidas y publicadas por la Entidad de Certificación



- A través de la **Autoridad de Estampado de Tiempo**, es la entidad que certifica la fecha y hora en la cual el documento fue firmado electrónicamente.

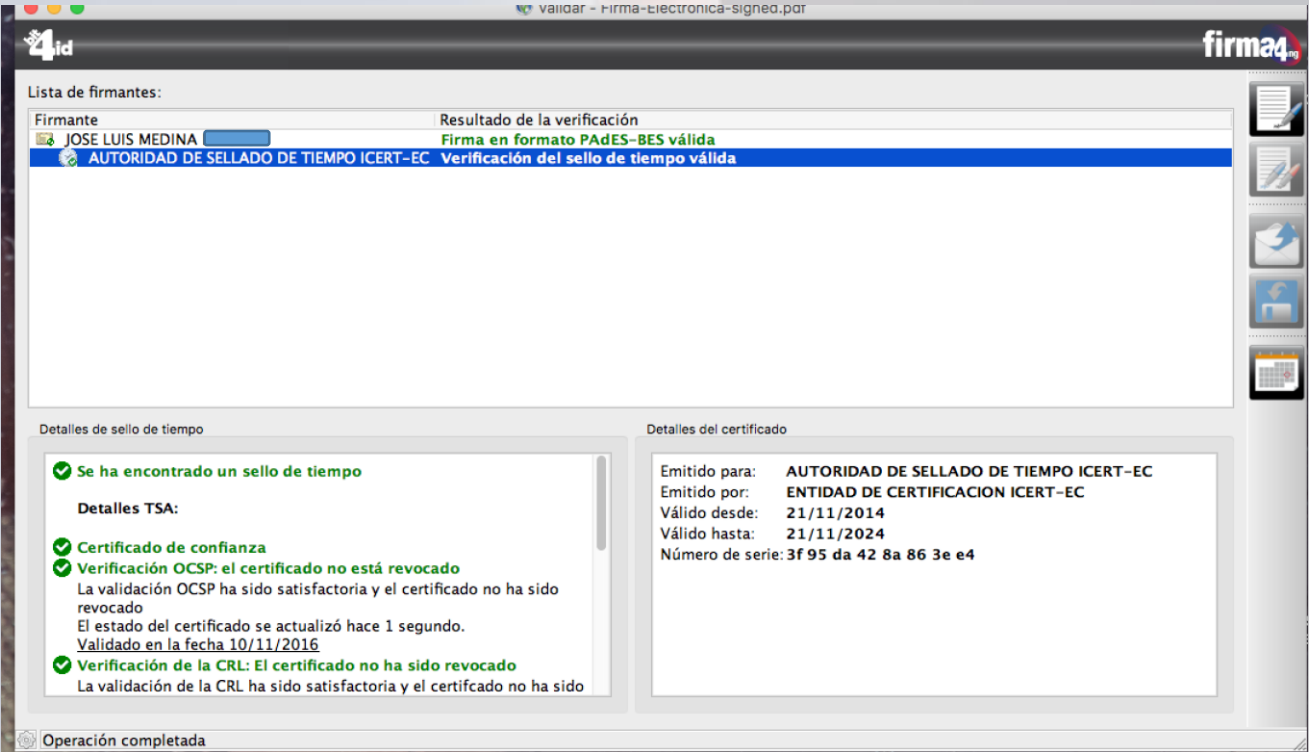


Imprimir documento persona validada

Es importante tener en cuenta el procedimiento para la parte de la solicitud, la misma que puede realizarse una vez la certificación reconocida, posteriormente y después de la validación del habilitante se procede a crear un certificado digital, en el formato PAdES-BES, válido para la firma pública y privada que servirá mucho para el firmado de documentos.

Saludos,

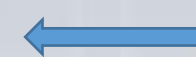
Digitally signed by
JOSE LUIS MEDINA
EC
José Luis Medina



```
jose Luis@themordor:~$ gpg --list-key
/home/jose Luis/.gnupg/pubring.kbx
-----
pub   rsa2048 2018-01-25 [SC] [expires: 2020-01-25]
uid           [ultimate] Jose Luis Medina <[redacted]@gmail.com>
sub   rsa2048 2018-01-25 [E] [expires: 2020-01-25]

jose Luis@themordor:~$ gpg --sign mensaje.txt
jose Luis@themordor:~$
```

```
-rw-r--r--  1 jose Luis_jose Luis  441 Apr 20 22:43 mensaje.txt.gpg
```



Firmado de documento

Importación de clave pública

```
root@themordor:~# gpg --keyserver pgp.mit.edu --search-key [redacted]@gmail.com
gpg: data source: http://pgp.mit.edu:11371
(1)   Jose Luis Medina
      Jose Luis Medina <[redacted]@gmail.com>
      2048 bit RSA key [redacted], created: 2018-01-25, expires: 2020-01-25
Keys 1-1 of 1 for "[redacted]@gmail.com". Enter number(s), N)ext, or Q)uit > 1
gpg: key [redacted]: public key "Jose Luis Medina <[redacted]@gmail.com>" imported
gpg: Total number processed: 1
gpg:         imported: 1
```

Verificación de la Firma

```
root@themordor:~# gpg --verify /home/jose Luis/mensaje.txt.gpg
gpg: Signature made Sat 20 Apr 2019 10:42:58 PM -05
gpg:         using RSA key [redacted]
gpg: Good signature from "Jose Luis Medina <[redacted]@gmail.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:         There is no indication that the signature belongs to the owner.
Primary key fingerprint: [redacted]
root@themordor:~#
```

Bibliografía

- PCs y DPC, Consejo de la Judicatura Ecuador
- RAMIO, Aguirre Jorge, Libro Electrónico de Seguridad Informática y Criptografía, Versión 4.1 de 1 de marzo de 2006, http://www.criptored.upm.es/guiateoria/gt_m001a.htm