Taller de Criptografía Aplicada

Gestión de Certificados con OpenSSL

Andrés J. Díaz <ajdiaz@gpul.org>

Índice

¿Qué vamos a ver?

- Teoría sobre certificados, CA y RA
- Creando una CA con OpenSSL

¿Qué es un certificado digital?

Un certificado digital es un documento digital que verifica que una llave pública pertenece a una determinada persona o entidad.

Para ello se basa en:

- Criptografía de clave pública
- Firma digital
- Elementos confiantes

Certificados X.509

Los certificados digitales están definidos en el estándar X.509

Un certificado X.509 contiene:

- El nombre distinguido de la persona
- El nombre distinguido del emisor
- La clave pública de la persona
- La firma digital del emisor
- El período de validez
- El número de serie del certificado

Autoridades Certificadoras

Problema:

- No sabemos si el certificado es de quién dice ser

Soluciones:

- Redes de confianza (utilizada en PGP)
- Autoridades de certificación

Una autoridad de certificación (CA) es un organismo encargado de verificar y garantizar que un certicado pertenece a su legítimo propietario

Autoridades Raiz

Problema:

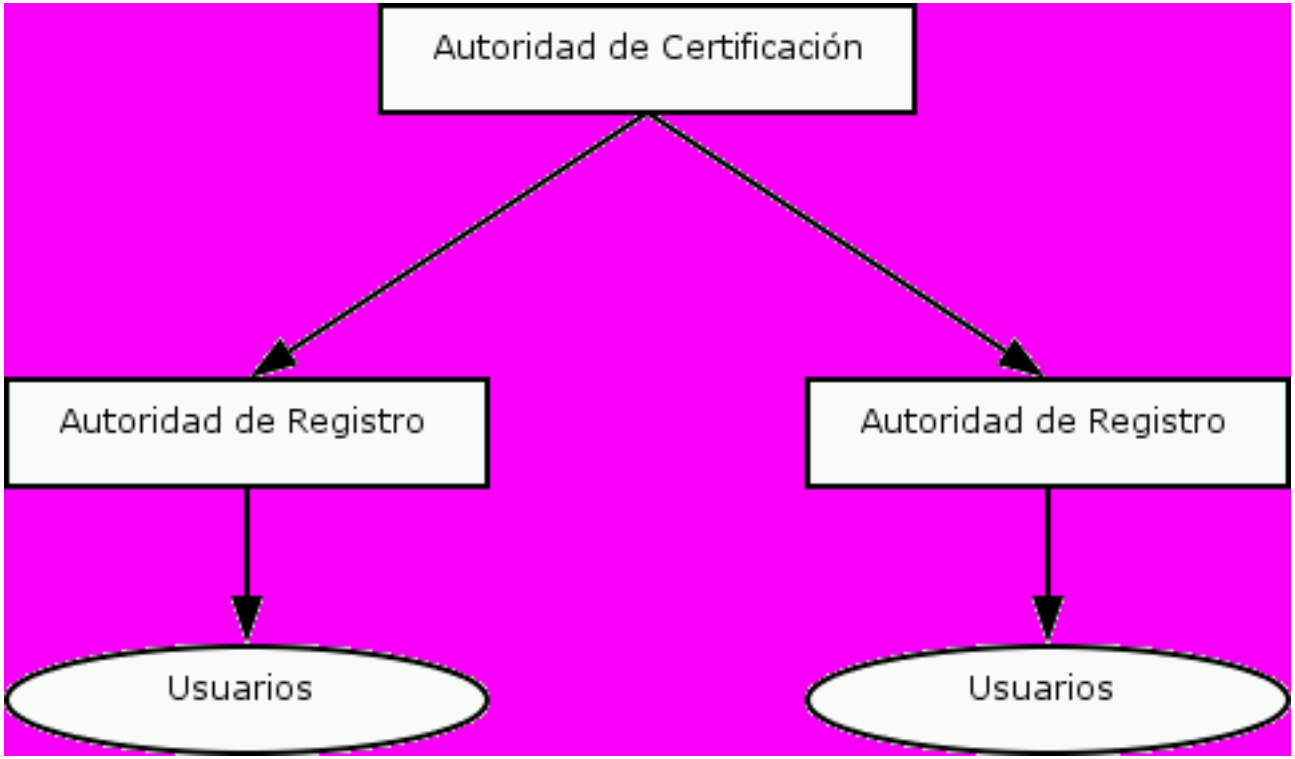
- ¿Quién verifica que la CA es quién dice ser?

Solución

- Otra CA en la que tenemos plena confianza

Una CA raiz es una CA en la que tenemos plena confianza por su reconocido prestigio, y que se firma a sí misma.

Jerarquía de la autoridades



Las autoridades de registro (RA), son CA regionales, que actú an de intermediarios entre los usuarios y la CA principal.

Diferencias con PGP/GPG (I)

En PGP:

- Cada usuario es su CA
  - Firma a las personas en quién confía
  - Otros usuarios (CAs) no tienen porqué confiar
- No hay jerarquía de CAs
  - No existe ningún «superusuario» que firme al resto
- Dependencia
  - ¡Si perdemos la clave privada estamos jodid...!
- Niveles de confianza
  - ¿Confio en los amigos de mis amigos?
  - ¿Que hacemos con las claves firmadas por terceras personas?

Diferencias con PGP/GPG (y II)

En X.509:

- Confiamos en la CA
  - ...y por tanto en todos los usuarios que haya firmado
- Las CAs (legales) confían entre sí
  - ...y por tanto confiamos en todos los usuarios certificados
- Los certificados no se limitan sólo a personas
  - Servidores, clientes, código...
- El encargado de nuestro certificado es la CA
  - Admisión de certificados
  - Autenticación del usuario
  - Distribución de certificados
  - Anulación de certificados (CRL)
  - Almacén de certificados

Tipos de certificados (I)

Según comprobación:

- Clase 1
  - Nombre, dirección y correo electrónico
- Clase 2
  - Permiso de conducir, Seguridad Social y fecha de nacimiento
- Clase 3
  - Comprobación del crédito de la persona o empresa
- Clase 4
  - Cargo de una persona en una organización (en estudio)

Tipos de certificados (y II)

Según finalidad:

- Certificados SSL para cliente
  - Identifica a un cliente frente a un servidor
- Certificados SSL para servidor
  - Identifica a un servidor frente a un cliente
- Certificados S/MIME
  - Firmado y cifrado de correo electrónico
- Certificados de firma de objetos
  - Firmado de ejecutables o porciones de código
- Certificados para CAs
  - Identifica a una CA frente a otra CA o RA

¿Cómo se anula un certificado?

Anulando un certificado

- Avisamos a nuestra CA de confianza
- La CA revoca el certificado
- LA CA publica una nueva CRL...

PROBLEMA:

- ... pero... ¡¿Cuándo publica la CA la nueva CRL?!
  - Las CRL son periódicas (cada semana, cada mes...)

SOLUCIÓN:

- OCPS (Online Certificate Status Protocol)
- SCVP (Simple Certificate Validation Protocol)

Índice

¿Qué vamos a ver?

- Teoría sobre certificados, CA y RA
- Creando una CA con OpenSSL

Estructura jerárquica

```
mkdir /etc/ssl/CA
mkdir /etc/ssl/CA/certs
mkdir /etc/ssl/CA/crl
mkdir /etc/ssl/CA/newcerts
mkdir /etc/ssl/CA/private
echo "01" > /etc/ssl/CA/serial
>/etc/ssl/CA/index.txt
```

Generando un par de claves

openssl genrsa [opciones] [tamaño]

Las opciones que usaremos:

- -aes128, -aes192,-aes256
  - Cifra la clave con un cifrado AES CBC
- -des, -des3
  - Cifra la clave con un cifrado DES o TripleDES
- -out <file>
  - Guarda la clave en formato PEM en ’file’

OJO: Formato PEM
[DEMO]

Creando un certificado autofirmado

openssl req -new -x509 -out <fsalida> -days <dias validez>
-key <clave.pri>

Esto hace:

- Coge la clave privada generada anteriormente
- Genera un certificado autofirmado X.509
- Con validez de <dias validez> dias
- Lo almacena en 'fsalida'

OJO: Formato PEM

[DEMO]

Generando un CSR

openssl req -new -out <csr.pem> -key <claveuser.pri>

Esto hace:

- Coge la clave privada del usuario (¡no de la CA!)
- Genera un CSR en formato PEM
- Lo almacena en csr.pem

[DEMO]

Configurando la CA en openssl.cnf

El fichero openssl.cnf tiene el siguiente formato:

```
[seccion]
opcion=valor
```

- Las opciones están listadas en "man ca"
- OpenSSL trae un openssl.cnf de ejemplo
- Nosotros veremos uno modificado :-P

[DEMO]

Firmando un certificado

openssl ca -in <csr> [-keyfile <cakey> -cert <cacert>]

Esto hace:

- Coge el CSR y lo firma usando:
  - La llave ’cakey’
  - El certificado ’cacert’
- Almacena el certificado firmado en el directorio ’newcerts’

[DEMO]

Revocando un certificado

openssl ca -revoke <cert> [-keyfile <cakey> -cert <cacert>]

Esto hace:

- Coge el certificado ’cert’ y lo revoca
  - Actualiza la BD de la CA
  - La revocación no es "conocida" hasta la publicación de la CRL

[DEMO]

Generando una CRL

openssl ca -gencrl

Esto hace:

- Busca en la BD de la CA los certificados revocados
- Genera una lista con los números de serie

[DEMO]

CAs en España y alrededores

Públicas:

- http://www.cert.fnmt.es
- http://www.pki.gva.es

Privadas:

- http://www.ace.es
- http://www.feste.es
- http://www.ipsca
- http://www.cacert.org

Otras:

- Universidad de Murcia
- Universidad de La Laguna

URLs

En el idioma de Shakespeare:

- http://www.openssl.org

En el idioma de Cervantes:

- http://www.argo.es/~jcea/artic/web-ssl1.htm

¡GRACIAS!

(aplausos y preguntas)