Universidad
Carlos III de Madrid

Grupo CoSec · *Dpto. Informática*

Universidad Carlos III de Madrid

Firma digital y PKI. OpenSSL

Prácticas de Criptografía y Seguridad Informática
Curso 2019/2020

Práctica en Linux

Responsable: Pablo Martín

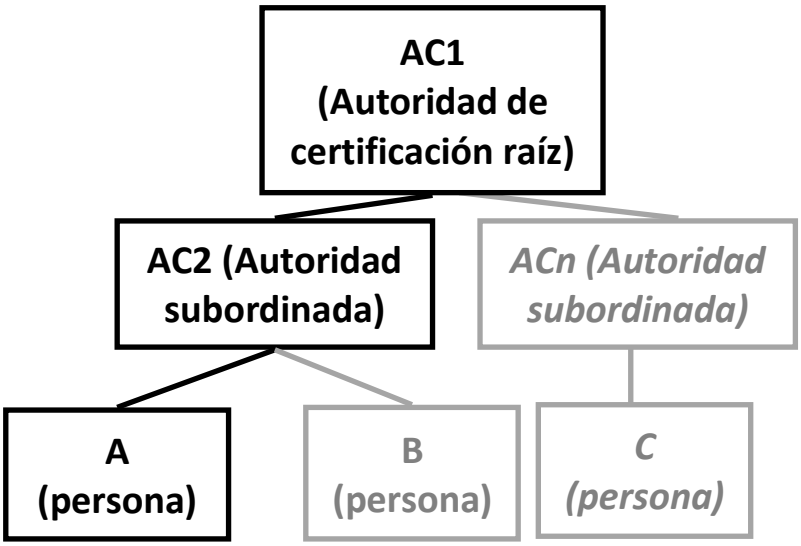
El objetivo de esta práctica es comprender los **fundamentos** sobre los que se basan las **infraestructuras de clave pública**. Particularmente, los objetivos concretos son los siguientes:

1- Comprender los **pasos** necesarios para que una **Autoridad emita un certificado**.

2- Entender **qué papel juegan** los **certificados** en la **firma y verificación** de documentos.

Para alcanzar estos objetivos, en esta práctica cada grupo de alumnos se convierte en una **AUTORIDAD DE CERTIFICACIÓN RAÍZ** (como puede ser en el mundo real, la Fábrica Nacional de Moneda y Timbre). Dicha Autoridad (AC1), por cuestiones organizativas (por ejemplo, para tener una delegación en cada comunidad autónoma) tiene varias **AUTORIDADES DE CERTIFICACIÓN SUBORDINADAS** (AC2,…, ACn), las cuales se dedican a emitir certificados de clave pública a las personas (A, B, C).

El conjunto de todas estas Autoridades conforma una **INFRAESTRUCTURA DE CLAVE PÚBLICA** (en inglés, PKI).



Para limitar la carga de trabajo, en esta práctica sólo se gestionará la autoridad raíz (AC1), una única autoridad subordinada (AC2) y una persona (A).

Parte en Linux

Descripción general y preparación del entorno

Importante: OpenSSL es un paquete criptográfico disponible en Linux, por ejemplo en Ubuntu. Preste atención a los cambios que se van produciendo en el directorio en el que se ejecutan los comandos indicados. La práctica se puede realizar también en Windows con comandos muy similares

Recomendación: Abra una consola para cada una de las entidades (3 en total) y manténgalas abiertas durante toda la sesión.

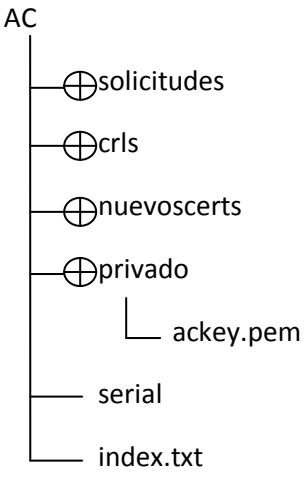
Para organizar el desarrollo de la práctica, **cree tres carpetas**, una cada para entidad: AC1, AC2 y A.

```
# practica> mkdir AC1 AC2 A
```

Para emitir los certificados, las Autoridades utilizan una POLÍTICA de certificación. Copie los ficheros que contienen estas políticas `openssl_AC1.cnf` y `openssl_AC2.cnf` (disponibles en Aula Global) **en el directorio `AC1` y `AC2` respectivamente.** Analice los ficheros `openssl_ACx.cnf dados`, comparándolos entre sí y con el fichero de configuración por defecto, el cual se encuentra en `/etc/ssl/openssl.cnf`.

Antes de comenzar la práctica, modifique los ficheros de políticas de tal forma que el nombre de sus AC sea AC1-*XXXXX* y AC2-*XXXXX*, donde *XXXXX* son los cinco últimos dígitos de su identificador de alumno en la Universidad.

La estructura de los directorios y archivos quedará en un principio como sigue:



Configuración de AC1 (Autoridad de Certificación raíz)

Los comandos de OpenSSL necesarios para la realización de la práctica son:

- `ca`: permite crear y gestionar una Autoridad de Certificación basada en el modelo de confianza jerárquico.
- `req`: permite crear y gestionar peticiones de emisión de certificados X.509.
- `x509`: permite gestionar certificados X.509.
- `verify`: permite verificar certificados X.509.

1. Genere la estructura de directorios necesaria para AC1 e inicialice los ficheros `serial` e `index.txt`.

```
# AC1> mkdir solicitudes crls nuevoscerts privado
# AC1> echo '01' > serial
# AC1> touch index.txt
```

2. Genere un par de claves RSA junto con el certificado autofirmado por AC1. Estudie los cambios producidos en el directorio AC1.

```
# AC1> openssl req -x509 -newkey rsa:2048 -days 360 -out
ac1cert.pem -outform PEM -config openssl_AC1.cnf
```

Se pide un passphrase para crear la clave privada de AC1, que habrá que recordar cuando queramos utilizarla.

```
# AC1> openssl x509 -in ac1cert.pem -text -noout
```

Configuración de AC2 (Autoridad de Certificación subordinada)

3. Genere la estructura de directorios necesaria para AC2 e inicialice los ficheros `serial` e `index.txt`.

```
# AC2> mkdir solicitudes crls nuevoscerts privado
# AC2> echo '01' > serial
# AC2> touch index.txt
```

4. Genere un par de claves de RSA junto con una solicitud de emisión de certificado y "envíesela" a AC1. Estudie los cambios producidos en el directorio AC2.

```
# AC2> openssl req -newkey rsa:2048 -days 360 -out ac2req.pem -
outform PEM -config openssl_AC2.cnf
```

Al igual que antes en AC1, se pide un passphrase que habrá que recordar cuando se utilice la clave privada de AC2

```
# AC2> openssl req -in ac2req.pem -text -noout
# AC2> cp ac2req.pem ../AC1/solicitudes
```

Generación del certificado de AC2 por AC1

5. Verifique la solicitud de emisión de certificado "enviada" por AC2.

```
# AC1> openssl req -in ./solicitudes/ac2req.pem -text -noout
```

6. Genere el certificado de AC2 y "envíeselo" (en el proceso, cambie el nombre del nuevo certificado - actualmente `01.pem` - a `ac2cert.pem`, ya que AC2 tiene configurado en su fichero de configuración este último nombre). Estudie los cambios producidos en el directorio AC1.

```
# AC1> openssl ca -in ./solicitudes/ac2req.pem -notext -
extensions v3_subca -config openssl_AC1.cnf
```

AC1 utiliza su clave privada para crear el certificado de AC2, por lo que se pide el passphrase de AC1.

```
# AC1> cp ./nuevoscerts/01.pem ../AC2/ac2cert.pem
```

Generación de las claves de A y su solicitud de emisión de certificado para AC2

7. Para la entidad A, genere un par de claves de RSA junto con una solicitud de emisión de certificado y "envíeselas" a AC2 (en el proceso de generación de solicitudes de emisión de certificado, rellene todos los campos que se le soliciten e indique que el país es "ES", que la provincia es "MADRID", que la organización es "UC3M", que el nombre común es *XXXXX (según lo indicado anteriormente)*, y que su email es su dirección de correo de estudiante). Estudie los cambios producidos en el directorio A.

```
# A> openssl req -newkey rsa:1024 -days 360 -sha1 -keyout
Akey.pem -out Areq.pem
```

Al igual que antes, se pide un passphrase que habrá que recordar cuando se quiera utilizar la clave privada de A.

```
# A> openssl req -in Areq.pem -text -noout
```

```
# A> cp Areq.pem ../AC2/solicitudes
```

Generación del certificado de A por AC2

8. Compruebe la solicitud de emisión de certificados "enviada" por A.

```
# AC2> openssl req -in ./solicitudes/Areq.pem -text -noout
```

9. Genere el certificado de A y "envíeselo" de vuelta (en el proceso, cambie el nombre del nuevo certificado - actualmente `01.pem` - a `Acert.pem`).

```
# AC2> openssl ca -in ./solicitudes/Areq.pem -notext -config
./openssl_AC2.cnf
```

AC2 utiliza su clave privada para crear el certificado de A, por lo que se pide el passphrase de AC2.

```
# AC2> cp ./nuevoscerts/01.pem ../A/Acert.pem
```

10. Estudie los cambios producidos en el directorio AC2 y compruebe el certificado resultante:

```
# A> openssl x509 -in Acert.pem -text -noout
```

Verificación del certificado de A

11. Obtenga una copia auténtica de los certificados de clave pública de AC1 y AC2 y verifique el certificado de A (para ello necesitara concatenar los certificados de AC1 y AC2 en un único fichero).

```
# A> cp ../AC1/ac1cert.pem ./
# A> cp ../AC2/ac2cert.pem ./
# A> cat ac1cert.pem ac2cert.pem > certs.pem
# A> openssl verify -CAfile certs.pem Acert.pem
```

Si todo es correcto, marcará un OK al ejecutar el último comando

Uniendo el certificado y la clave privada para firmar en aplicaciones habituales (Word / correo electrónico)

12. Exporte el certificado de A, su clave privada y la concatenación de los certificados de AC1 y AC2 al formato PKCS12.

```
# A> openssl pkcs12 -export -in Acert.pem -inkey Akey.pem -
certfile certs.pem -out Acert.p12
```

Se solicita el passphrase de A para exportar su clave privada, y un nuevo passphrase para el certificado .p12

Cuestiones

a. ¿Para qué se usa el fichero “serial”?

b. ¿Para qué se usa el fichero “index.txt”?

c. ¿Podría AC2 crear su certificado utilizando el paso 2 de este guión?

d. Si su grupo de prácticas se convirtiera en una Autoridad de Certificación de verdad, explique **razonadamente** (i.e. ventajas, inconvenientes, otras alternativas razonables, etc.) qué valor le pondría a cada uno de los siguientes parámetros de su política de certificación: default_days, default_crl_days, countryName

Navegador Web

La Autoridad Pública de Certificación CERES de la FNMT-RCM

13. Acceda a su página web http://www.cert.fnmt.es/home.

14. Consulte el manual de solicitud de certificado de persona física, accesible en esta dirección web:

    http://www.cert.fnmt.es/documents/10445900/10528353/solicitud_certificado_persona_fisica.pdf

15. Consulte el documento de "Declaración General de Prácticas de Certificación" https://www.sede.fnmt.gob.es/documents/10445900/10536309/dgpc.pdf

Cuestiones

e. ¿Qué es CERES, qué tipo de certificados ofrece y cuáles son los servicios que oferta?

f. ¿Cuando se inicia el procedimiento para solicitar un certificado de clave pública de persona física, dónde se generan las claves pública y privada?

g. ¿Puede el usuario elegir el tamaño de las claves que se acreditarán en dicho certificado?

h. ¿Para qué sirve la dirección de correo solicitada durante el proceso de generación de la solicitud de dicho certificado?

i. ¿Qué es necesario presentar en la oficina de registro y con qué propósito una vez se ha solicitado el certificado de clave pública de persona física a través de Internet?

j. ¿Qué condiciones se le exigen al usuario para poder descargar correctamente el certificado de clave pública de persona física?

k. ¿Se realiza una copia de seguridad de las claves privadas ("Datos de creación de firma") de la Autoridad de Certificación de la FNMT-RCM?

l. ¿Cómo se distribuye la clave pública de las AC a las partes que confían y que tamaño tienen las claves y que algoritmos utilizan?

m. Los pasos que tiene que seguir un ciudadano para obtener un certificado de clave pública emitido por la Fábrica Nacional de Moneda y Timbre vienen resumidos en la siguiente tabla. Rellene la tabla, que sirve para relacionar cada uno de esos pasos con los realizados en esta práctica: para cada paso de ese proceso, indique en qué punto de esta práctica se ha realizado.

Paso	**Descripción**	**Punto de este guión en que se ha realizado**
1	Crear un par de claves (pública y privada) y envío de la solicitud de certificado	
2	Personarse en una oficina de registro	
3	Generación del certificado de clave pública de acuerdo a las políticas	
4	Descargarse el certificado	

Navegador Web

Certificados de servidor Web – visión del cliente

16. Abra una pestaña del navegador y acceda al servicio de Aula Global o Campus Global de la UC3M.
17. Abra otra pestaña del navegador y acceda a la página web principal del buscador Google.

Cuestiones

n. Averigüe cuál es el certificado ofrecido para asegurar la conexión con el protocolo TLS por parte de la UC3M. ¿Cuál es la cadena de certificación?

o. Averigüe cuál es el certificado ofrecido para asegurar la conexión con el protocolo TLS por parte de Google. ¿Cuál es la cadena de certificación?

Certificados de servidor Web – visión del servidor

18. Lea este tutorial acerca de cómo crear un certificado auto-firmado para servidor web y su instalación en Apache Web Server para ofrecer conexiones cifradas con el protocolo TLS/SSL:
    a. http://linuxconfig.org/apache-web-server-ssl-authentication
19. Abra en otra pestaña del navegador la página web https://letsencrypt.org/ y averigüe qué anuncia. Estudie qué ofrece y cómo funcionaría.

Cuestiones

p. ¿Cuáles serán las ventajas principales de los certificados de servidor emitidos por “Let’s Encrypt”?

Documentación

Aquí se listan algunos recursos que pueden utilizarse en caso de duda:

- Manual de OpenSSL en Linux: `man openssl`
- Página web oficial de OpenSSL: http://www.openssl.org