



Laboratorio PKI (1ª Fase)

SRDSI

Jose Ángel Gumiel

Índice

A.- Introducción.....	2
B.- Puesta en marcha	2
1.- Crear la estructura	2
2.- Inicialización de ficheros	3
3.- Completar el fichero de configuración	3
4.- Generar la clave	3
5.- Generar una CRL vacía	4
6.- Generar la clave y el certificado para un servidor OCSP	4
7.- Conclusiones	4
C.- Emisión de un certificado.....	4
D.- Revocación de un certificado	5
E.- Validación de un certificado (OCSP responder)	6
F.- Exportar certificado y clave privada	7
G.- Dedicación	7

A.- Introducción

En esta práctica se creará una infraestructura de claves públicas (PKI), compuesta por una autoridad de certificación (CA) que emita y verifique certificados.

Una PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

Las comunicaciones con seguridad PKI no requieren del intercambio de ningún tipo de clave secreta para su establecimiento, por lo que se consideran muy seguras si se siguen las políticas de seguridad pertinentes.

B.- Puesta en marcha

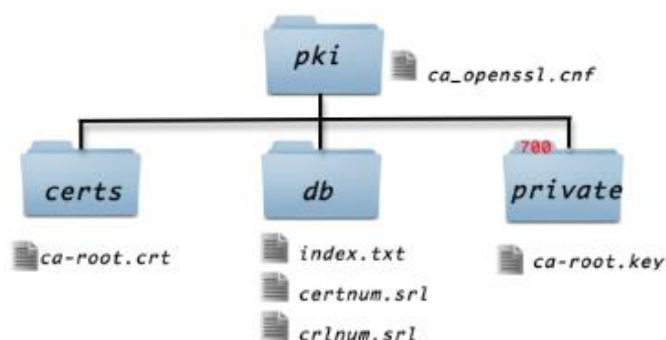
En los siguientes apartados se describirá el proceso seguido para la puesta en marcha de la PKI.

1.- Crear la estructura

El primer paso es conocer cómo se van a organizar los directorios en la PKI para almacenar la información que se vaya generando.

```
LXTerminal
Archivo Editar Pestañas Ayuda
root@srdsi:~# mkdir pki
root@srdsi:~# cd pki/
root@srdsi:~/pki# mkdir certs
root@srdsi:~/pki# mkdir db
root@srdsi:~/pki# mkdir private
root@srdsi:~/pki# cd private
root@srdsi:~/pki/private# openssl rand -hex 8 > ca-root.key
root@srdsi:~/pki/private# cd ..
root@srdsi:~/pki# cd db
root@srdsi:~/pki/db# nano index.txt
root@srdsi:~/pki/db#
```

Se ha decidido mantener la siguiente estructura de directorios:



Por seguridad es recomendable que a la carpeta “*private*” sólo pueda acceder el administrador de la máquina, y que sólo éste tenga permisos de lectura y escritura.

2.- Inicialización de ficheros

Hay que inicializar tres ficheros, todos pertenecientes a la carpeta “db”.

- *certnum.srl* y *crlnum.srl*. Se inicializan con valores hexadecimales aleatorios. Para ello se puede usar el siguiente comando “*openssl rand -hex 8 > nombre-fichero*”.
- *index.txt*. Se crea el fichero. Se puede hacer desde un editor de consola como “nano”.

3.- Completar el fichero de configuración

Existe un archivo de configuración que evita tener que introducir manualmente algunos datos. Además también guarda las rutas de los directorios, para mantener una coherencia, y datos sobre la CA que se va a crear, como por ejemplo el dominio, la empresa, la nacionalidad...

4.- Generar la clave

La CA tiene que tener una clave, y ésta contendrá alguna información básica sobre la propia autoridad de certificación. En el siguiente paso se crea la clave.

```
root@srdsi:~/pki# openssl req -new -nodes -keyout /root/pki/private/ca-root.key
-out /root/pki/certs/ca-root.crt -config /root/pki/ca_openssl.cnf
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/root/pki/private/ca-root.key'
-----
root@srdsi:~/pki#
```

Todo certificado válido, ha de ser emitido por una CA reconocida, que garantiza la validez de la asociación entre el tenedor del certificado y el certificado en sí. En este caso no se cuenta con ninguna CA que vaya a firmar el certificado, pero una CA se puede validar a sí misma.

El siguiente paso consiste en “autofirmar” la clave.

```
root@srdsi:~/pki/db# openssl req -new -nodes -keyout /root/pki/private/ca-root.key -out /root/pki/
/certs/ca-root.crt -config /root/pki/ca_openssl.cnf
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/root/pki/private/ca-root.key'
-----
root@srdsi:~/pki/db# openssl ca -selfsign -in /root/pki/certs/ca-root.crt -out /root/pki/certs/ca
-root-selfsigned.crt -config /root/pki/ca_openssl.cnf -extensions ca_ext
Using configuration from /root/pki/ca_openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 16604037402897526365 (0xe66d640bc501ae5d)
        Issuer:
            countryName             = ES
            stateOrProvinceName     = VI
            organizationName        = FISS
            organizationalUnitName   = Seguridad
            commonName              = SecuID
        Validity
            Not Before: Mar  7 15:30:40 2016 GMT
            Not After : Mar  7 15:30:40 2017 GMT
        Subject:
            countryName             = ES
            stateOrProvinceName     = VI
            organizationName        = FISS
            organizationalUnitName   = Seguridad
            commonName              = SecuID
```

En la imagen se ve como la CA que emite el resultado es la misma CA que firma su propio certificado. Al final del proceso se firma el certificado con éxito y se actualiza la base de datos.

5.- Generar una CRL vacía

El acrónimo CRL significa “Certificate Revocation List”. Va a contener los certificados de la CA que han sido revocados, conjunto información como la fecha en la que fue rechazado y la razón que eso haya ocurrido.

```
root@srdsi:~/pki# nano ca_openssl.cnf
root@srdsi:~/pki# openssl ca -gencrl -out /root/pki/certs/crl-ca-root.pem -config
enssl.cnf
Using configuration from /root/pki/ca_openssl.cnf
root@srdsi:~/pki#
```

6.- Generar la clave y el certificado para un servidor OCSP

Se elabora una petición y se firma el certificado con la clave privada de la PKI. La generación de la clave es igual que la que se ha hecho en el paso 4, y la firma del certificado se hace con la clave de la CA.

El resultado es la creación del archivo “*certificado-ca-ocsp.crt*” que se guarda en la carpeta “*certs*” y el fichero “*clave-privada-ca-ocsp*” en el directorio “*private*”.

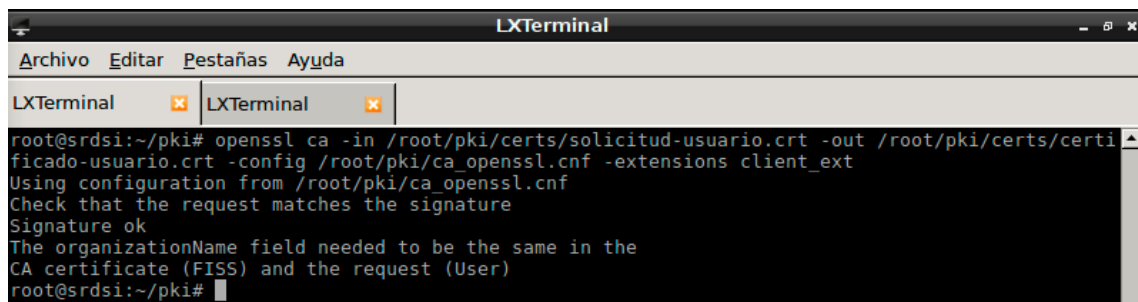
7.- Conclusiones

Se ha conseguido con éxito la implementación de una infraestructura de claves públicas. Ésta puede ahora gestionar los certificados, de forma que podrá emitir nuevos certificados y revocar certificados que estuvieran en curso.

A continuación se mostrará cómo realizar algunas de las tareas comunes de la CA.

C.- Emisión de un certificado

El primer caso que se ha probado es solicitar un certificado para una organización con un nombre distinto al de la CA.



```
LXTerminal
Archivo Editar Pestañas Ayuda
LXTerminal LXTerminal
root@srdsi:~/pki# openssl ca -in /root/pki/certs/solicitud-usuario.crt -out /root/pki/certs/certi
ficado-usuario.crt -config /root/pki/ca_openssl.cnf -extensions client_ext
Using configuration from /root/pki/ca_openssl.cnf
Check that the request matches the signature
Signature ok
The organizationName field needed to be the same in the
CA certificate (FISS) and the request (User)
root@srdsi:~/pki#
```

Al intentar certificar al usuario la CA no deja proceder. De hecho al abrir el certificado que se crea, éste está vacío.

Se realiza el mismo paso con un certificado que tiene como organización la misma que la CA.

```

root@srdsi:~/pki# openssl req -new -nodes -out /root/pki/solicitud-usuario3.crt -keyout /root/pki/private/clave-privada-usuario3.key
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/root/pki/private/clave-privada-usuario3.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:VI
Locality Name (eg, city) []:Bilbao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FISS
Organizational Unit Name (eg, section) []:Seguridad
Common Name (e.g. server FQDN or YOUR name) []:SecuID
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:

```

En este punto se ha creado una clave nueva. En el siguiente paso se certificará por la CA.

```

root@srdsi:~/pki# openssl ca -in /root/pki/certs/solicitud-usuario3.crt -out /root/pki/certs/certificado-usuario3.crt -config /root/pki/ca_openssl.cnf -extensions client_ext
Using configuration from /root/pki/ca_openssl.cnf
Check that the request matches the signature
Signature ok

```

Aquí ha empezado el procedimiento, en la siguiente imagen se observa cómo ha ido la operación.

```

Certificate is to be certified until Mar  7 18:48:43 2017 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@srdsi:~/pki#

```

Se ha emitido el certificado con éxito.

D.- Revocación de un certificado

Existen ya dos certificados emitidos “certificado-usuario2.crt” y “certificado-usuario3.crt”. A continuación va a ser revocado el “certificado-usuario2”.

```

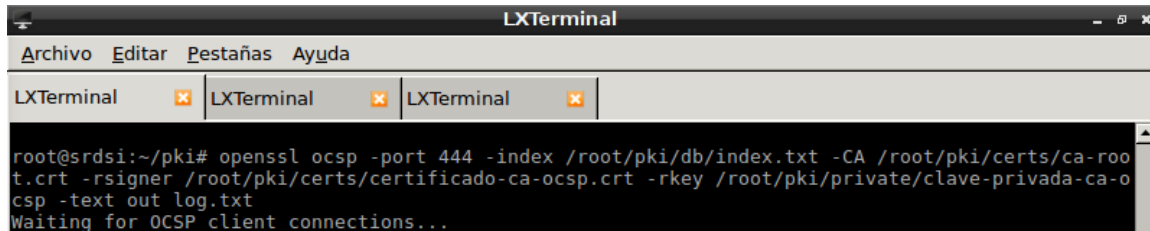
LXTerminal
Archivo Editar Pestañas Ayuda
LXTerminal LXTerminal
root@srdsi:~/pki# openssl ca -revoke /root/pki/certs/certificado-usuario2.crt -crl_reason keyCompromise -config /root/pki/ca_openssl.cnf
Using configuration from /root/pki/ca_openssl.cnf
Revoking Certificate 68DD234C238A115A.
Data Base Updated
root@srdsi:~/pki#

```

Se ha revocado el certificado del usuario y los cambios se han guardado en la base de datos.

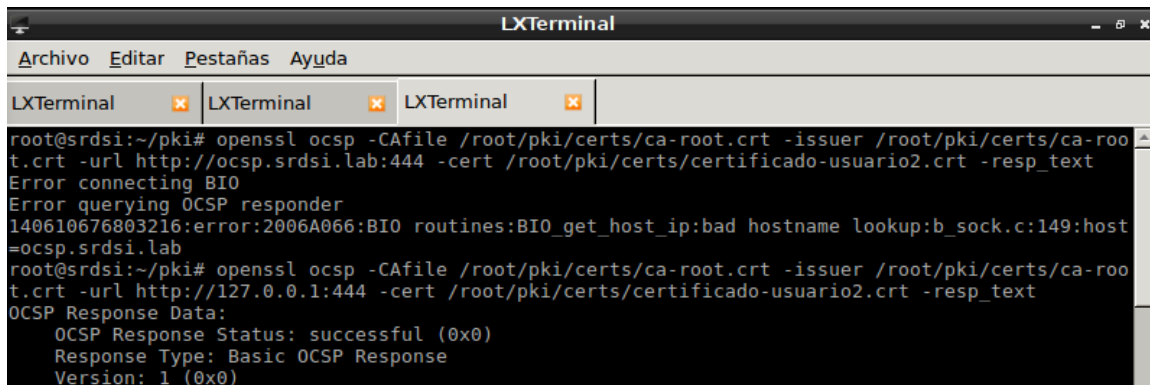
E.- Validación de un certificado (OCSP responder)

En una pestaña del terminal hay que iniciar el servidor OCSP. Éste se quedará a la espera de clientes que se conecten.



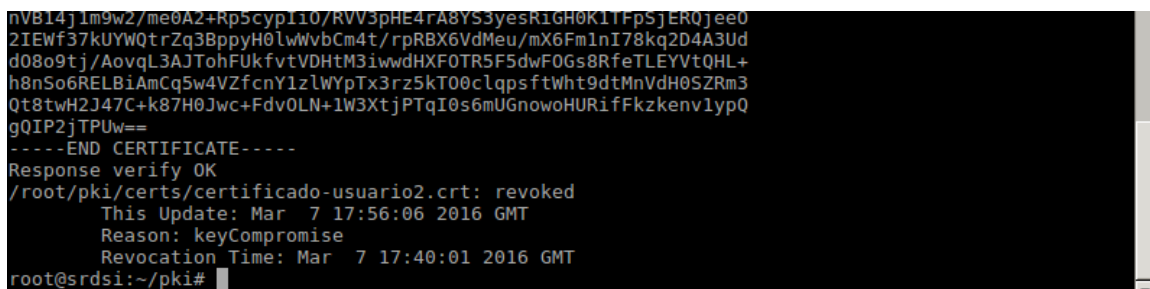
```
LXTerminal
Archivo Editar Pestañas Ayuda
LXTerminal LXTerminal LXTerminal
root@srdsi:~/pki# openssl ocsp -port 444 -index /root/pki/db/index.txt -CA /root/pki/certs/ca-root.crt -rsigner /root/pki/certs/certificado-ca-ocsp.crt -rkey /root/pki/private/clave-privada-ca-ocsp -text out log.txt
Waiting for OCSP client connections...
```

En otra pestaña se le hace una petición.



```
LXTerminal
Archivo Editar Pestañas Ayuda
LXTerminal LXTerminal LXTerminal
root@srdsi:~/pki# openssl ocsp -CAfile /root/pki/certs/ca-root.crt -issuer /root/pki/certs/ca-root.crt -url http://ocsp.srdsi.lab:444 -cert /root/pki/certs/certificado-usuario2.crt -resp_text
Error connecting BIO
Error querying OCSP responder
140610676803216:error:2006A066:BIO routines:BIO_get_host_ip:bad hostname lookup:b_sock.c:149:host=ocsp.srdsi.lab
root@srdsi:~/pki# openssl ocsp -CAfile /root/pki/certs/ca-root.crt -issuer /root/pki/certs/ca-root.crt -url http://127.0.0.1:444 -cert /root/pki/certs/certificado-usuario2.crt -resp_text
OCSP Response Data:
  OCSP Response Status: successful (0x0)
  Response Type: Basic OCSP Response
  Version: 1 (0x0)
```

El servidor emite una respuesta. Lo interesante se encuentra en la siguiente imagen. Hay que tener en cuenta que el “certificado-usuario2” estaba revocado.



```
nVB14j1m9w2/me0A2+Rp5cyp1i0/RVV3pHE4rA8YS3yesR1GH0K1TFpsJERQjee0
2IEWf37kUYWQtrZq3BppyH0lwVbCm4t/rpRBX6VdMeu/mX6Fm1nI78kq2D4A3Ud
d08o9tj/AovqL3AJTohFukfvtVDHtM3iwwdHXF0TR5F5dwF0Gs8RfeTLEYVtQHL+
h8nSo6RELBiAmCq5w4VZfcnY1zlwYpTx3rz5kT00clqpsftWht9dtMnVdH0SZRm3
Qt8twH2J47C+k87H0Jwc+Fdv0LN+1W3XtjPTqI0s6mUGnowoHURifFkzkenvlypQ
gQIP2jTPUw==
-----END CERTIFICATE-----
Response verify OK
/root/pki/certs/certificado-usuario2.crt: revoked
  This Update: Mar  7 17:56:06 2016 GMT
  Reason: keyCompromise
  Revocation Time: Mar  7 17:40:01 2016 GMT
root@srdsi:~/pki#
```

Se observa que indica el estado del certificado, es decir, que ha sido revocado y la razón que ha dado la CA, que es que la clave ha sido comprometida.

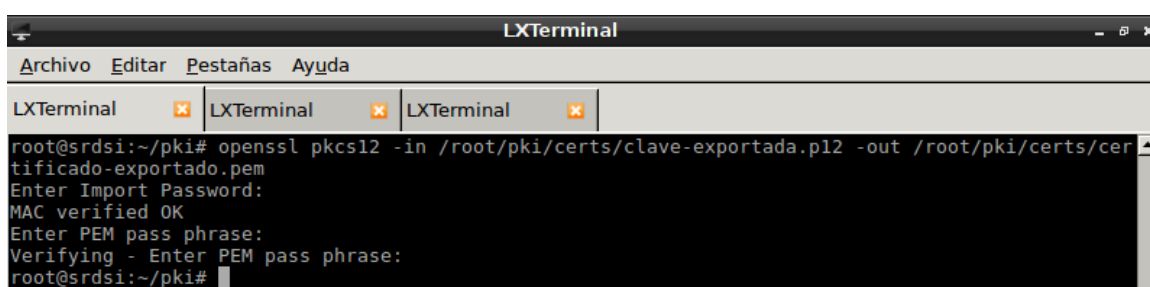
F.- Exportar certificado y clave privada

Es probable que en algunos casos se desee exportar un certificado con su clave privada para almacenarlo en dispositivos extraíbles o para usarlo en un ordenador distinto.

Hay que tener presente que el poseedor de un certificado es responsable de la conservación y custodia de la clave privada asociada al certificado. Debe evitar el conocimiento de la misma por terceros. En las siguientes imágenes de detalla cómo llevar a cabo este proceso.

```
root@srdsi:~/pki# openssl pkcs12 -export -out /root/pki/certs/clave-exportada.p12 -in /root/pki/certs/certificado-usuario3.crt -inkey /root/pki/private/clave-privada-usuario3.key
Enter Export Password:
Verifying - Enter Export Password:
root@srdsi:~/pki#
```

En este paso se ha exportado el certificado y la clave.



```
LXTerminal
Archivo Editar Pestañas Ayuda
LXTerminal LXTerminal LXTerminal
root@srdsi:~/pki# openssl pkcs12 -in /root/pki/certs/clave-exportada.p12 -out /root/pki/certs/certificado-exportado.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
root@srdsi:~/pki#
```

En este paso se ha extraído a un fichero con extensión “.pem”.

G.- Dedicación

	Ejecución	Documentación	Total
Tiempo	4h.	6h.	10h.

Durante la elaboración de éste laboratorio hubo algunos problemas resultaron en un incremento en el tiempo de ejecución de las tareas. Especialmente el cuarto punto, el de la generación y firmado del certificado de la CA fue el que más problemas dio. Algunos errores en el fichero de configuración y en las rutas de los directorios ocasionaron también algún que otro inconveniente.