

Laboratorio PKI

Indice

Descripción.....	2
XCA.....	2
Prerequisitos.....	2
Instalación de XCA.....	2
Uso de XCA.....	2
Laboratorio.....	4
Creación Root CA.....	4
Creación Sub CA.....	7
Apache sobre Linux.....	10
Generar CSR.....	10
Enviar CSR a la CA.....	10
XCA.....	11
Importar CSR.....	11
Firmar CSR.....	11
Exportar Certificado.....	13
Apache.....	15
Configurar el módulo TLS.....	15
Crear VirtualHost.....	15
Reiniciar el apache.....	15
Probar servicio por HTTPS.....	15

Descripción

En el laboratorio se llevará a cabo la instalación de la aplicación XCA, la cual permite la puesta en marcha de una PKI simple. Una vez instalado dicho software se generará los certificados digitales tanto de la RootCA como de la SubCA.

Posteriormente se generará un certificado digital para ser utilizado en un servidor Web Apache.

XCA

Esta aplicación está diseñada para crear y administrar certificados X.509, solicitudes de certificados, claves privadas RSA, DSA y EC, tarjetas inteligentes y CRL.

Para un uso fácil, posee plantillas personalizables que se pueden usar para la generación de certificados o solicitudes.

Todos los datos criptográficos se almacenan en una base de datos SQL. Se admiten bases de datos SQLite, MySQL (MariaDB) y PostgreSQL.

Prerequisitos

Se instalará sobre el SO Kali, previamente instalado.

Actualización de paquetes del SO:

apt update

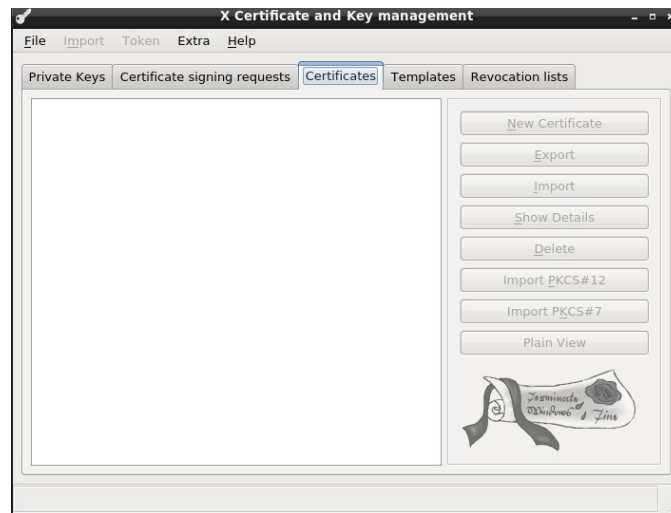
Instalación de XCA

apt install xca -y

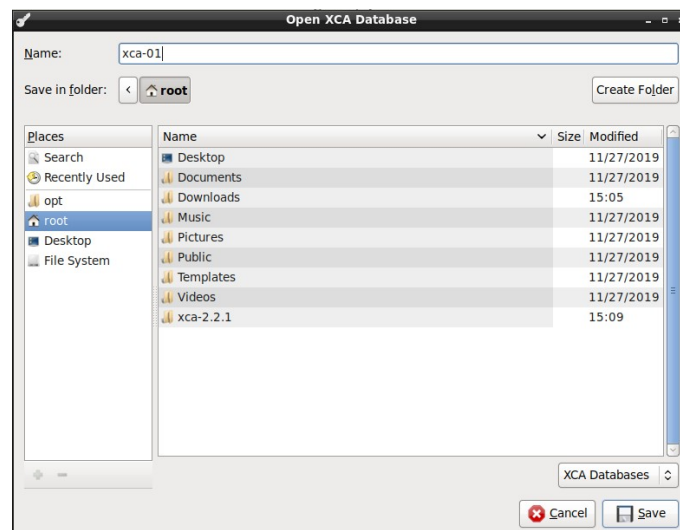
Uso de XCA

Una vez instalada la aplicación deberá generarse la base de datos donde se almacenarán las claves, csr y certificados digitales.

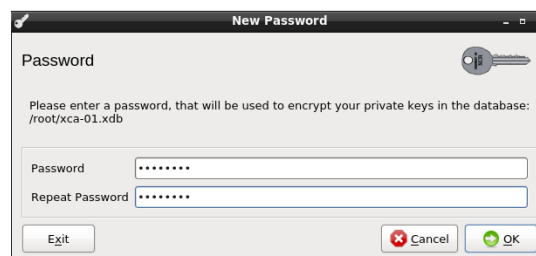
Para ello se abrirá la aplicación y se deberá ir al *Menú File – New Database*



Elegir el nombre y la ubicación de la base de datos.



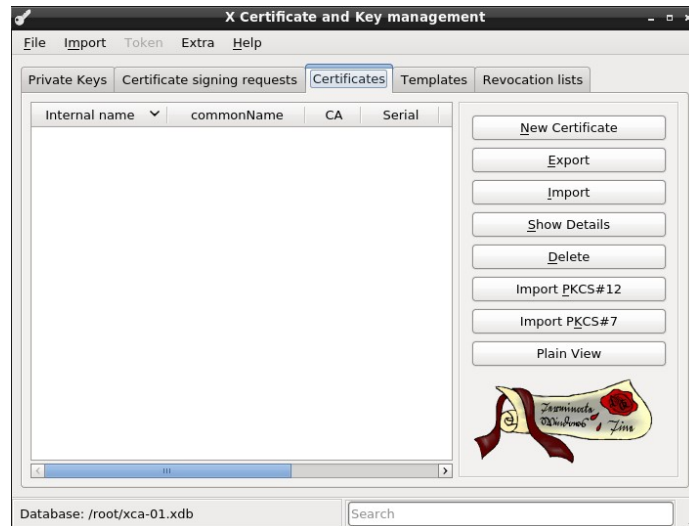
Se deberá elegir una contraseña para resguardar los datos contenidos en la base.



Laboratorio

Creación Root CA

Una vez generada la base de datos, en la solapa *Certificates* presionar sobre el botón “*New Certificate*” para generar el certificado de nuestra **Root CA**.



Con la finalidad de seguir buenas prácticas de seguridad, seleccionaremos el algoritmo SHA256 como HASH, corroborar que el template a utilizar sea CA y presionar “*Apply all*”



Ir a la pestaña Sujeto identificar los datos de la Root CA, tal como se muestra en la siguiente imagen y presionar el botón “*Generate a new key*”.

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced Comment

Internal Name: Root CA

Distinguished name

countryName: AR organizationalUnitName: Seguridad Informatica

stateOrProvinceName: CABA commonName: RootCA

localityName: CABA emailAddress:

organizationName: Autoridad Certificante

Type	Content

Private key: ☐ Used keys too

Poner el nombre “Root CA”, elegir el algoritmo “RSA” y seleccionar el tamaño de la clave en “8192 bits”

New Key

Please give a name to the new key and select the desired keysize

Key properties

Name: Root CA

Keytype: RSA

Keysize: 8192 bit

☐ Remember as default

X Certificate and Key management

Successfully created the RSA private key 'Root CA'

Una vez generada la clave, presionar en la solapa *Extensions*, corroborar que en Type se encuentre seleccionado “*Certificate Authority*” y que el Rango de Tiempo sea 10 años.

X Certificate and Key management

Create x509 Certificate

Source Subject **Extensions** Key usage Netscape Advanced Comment

X509v3 Basic Constraints

Type: Certification Authority

Path length:

☒ Critical

Key identifier

☒ Subject Key Identifier

☐ Authority Key Identifier

Validity

Not before: 2020-04-13 18:23 GMT

Not after: 2030-04-13 18:23 GMT

Time range

10 Years

☐ Midnight ☐ Local time ☐ No well-defined expiration

Apply

X509v3 Subject Alternative Name: Edit

X509v3 Issuer Alternative Name: Edit

X509v3 CRL Distribution Points: Edit

Authority Information Access: OCSP Edit

Cancel OK

Presionar “Aceptar”. Tal como puede evidenciarse, hemos generado el certificado para nuestra Root CA.

X Certificate and Key management

File Import Token Extra Help

Private Keys Certificate signing requests **Certificates** Templates Revocation lists

Internal name	commonName	CA	Serial
Root CA RootCA	Root CA RootCA	Yes	6A25AD0E2

New Certificate

Export

Import

Show Details

Delete

Import PKCS#12

Import PKCS#7

Plain View

Successfully created the certificate 'Root CA'

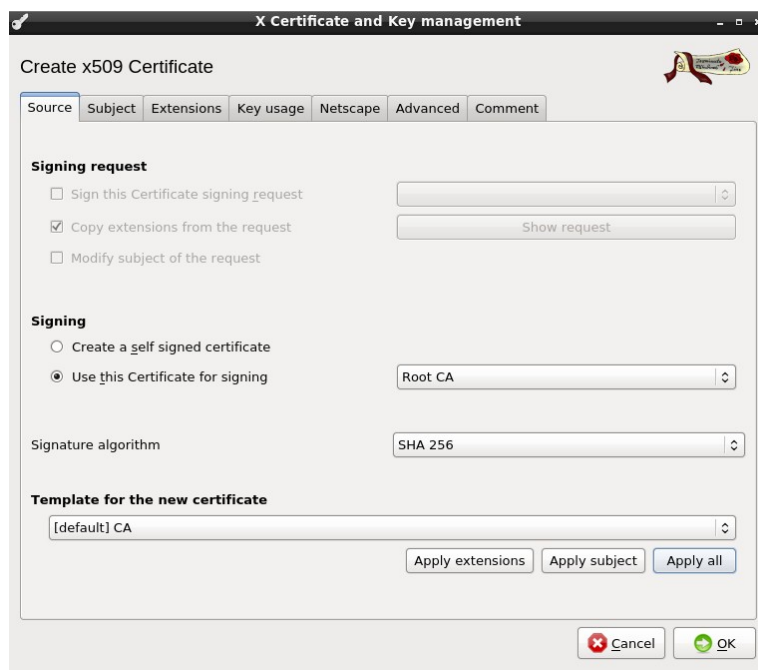
OK

Database: /root/xca-01.xdb

Search

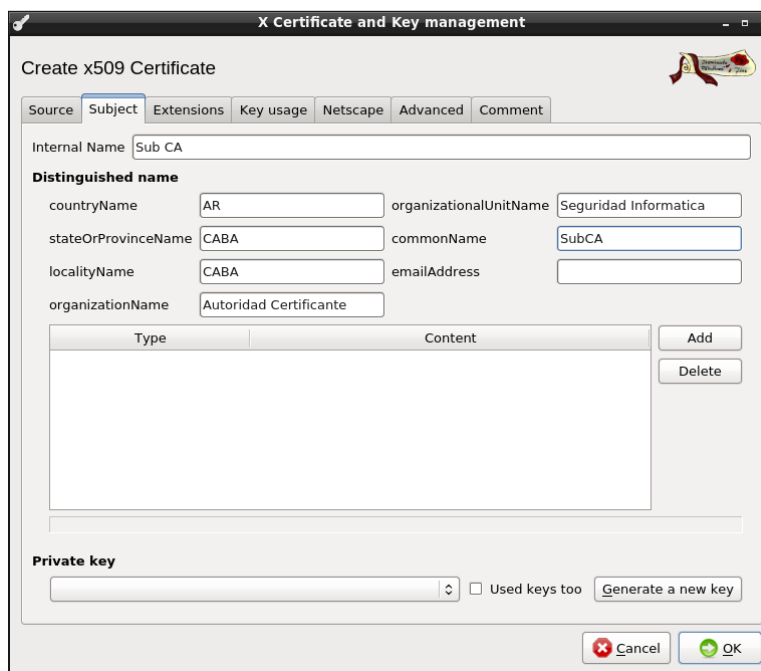
Creación Sub CA

Ahora es el momento de generar el certificado de la **SubCA**. En este caso debemos asegurarnos que se encuentre seleccionada la opción “*Use this Certificate for signing*” y seleccionar Root CA. Cambiar el HASH a SHA256, corroborar que se encuentre seleccionado el template CA y presionar el botón “Apply All”



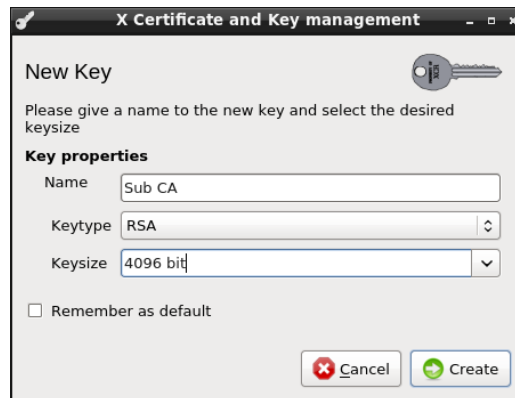
The screenshot shows the 'Create x509 Certificate' dialog box with the 'Advanced' tab selected. The 'Signing request' section has 'Copy extensions from the request' checked. The 'Signing' section has 'Use this Certificate for signing' selected, with 'Root CA' chosen from the dropdown. The 'Signature algorithm' is set to 'SHA 256'. The 'Template for the new certificate' is '[default] CA'. At the bottom right are 'Apply extensions', 'Apply subject', 'Apply all', 'Cancel', and 'OK' buttons.

En la solapa Sujeto cargar los datos que figuran en la siguiente imagen y presionar el botón “*Generate a new key*”

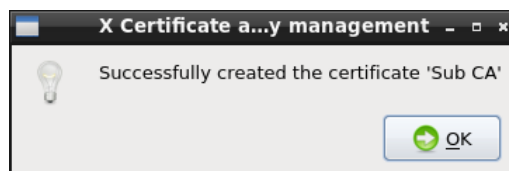
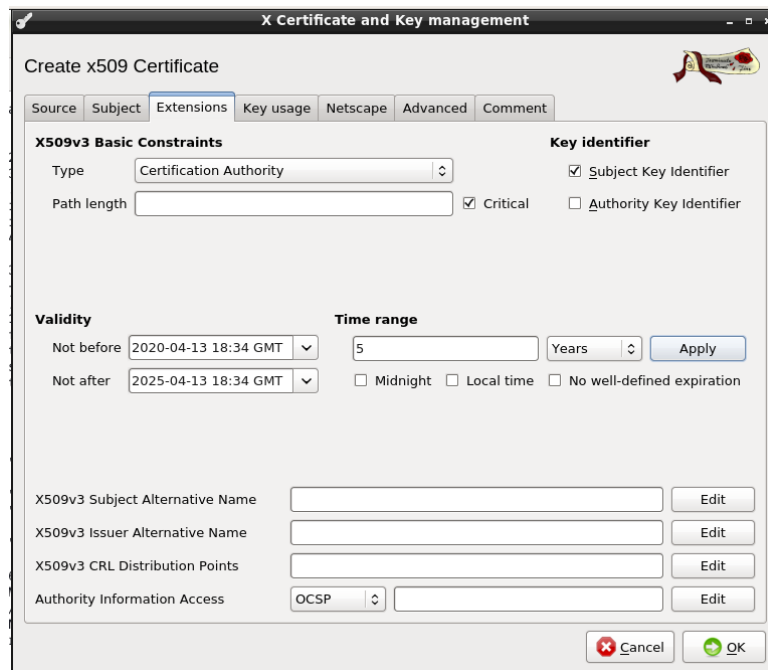


The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Internal Name' is 'Sub CA'. The 'Distinguished name' section contains the following fields: 'countryName' (AR), 'organizationalUnitName' (Seguridad Informatica), 'stateOrProvinceName' (CABA), 'commonName' (SubCA), 'localityName' (CABA), 'emailAddress' (empty), and 'organizationName' (Autoridad Certificante). Below these is a table with columns 'Type' and 'Content'. At the bottom are 'Add' and 'Delete' buttons. The 'Private key' section has a dropdown menu, a checkbox for 'Used keys too', and a 'Generate a new key' button. At the bottom right are 'Cancel' and 'OK' buttons.

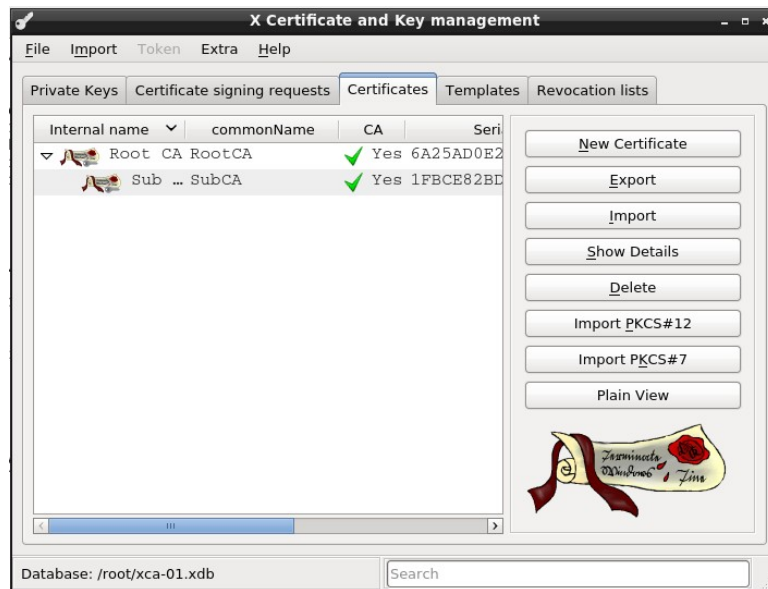
Los datos de la clave deben ser los que figuran en la siguiente imagen.



Una vez generada la clave presionaremos en la solapa extensiones y nos aseguraremos que se encuentre seleccionada en Type la opción “*Certificate Authority*”. En este caso deberemos modificar el rango de tiempo, dejarlo en 5 años y presionar el botón “Aplicar”.



Con esto habremos generado el certificado de la SubCA, la cual utilizaremos para firmar los certificados digitales para los servidores Web.



Apache sobre Linux

Generar CSR

Generamos la clave y el request con openssl ejecutando el siguiente comando:

openssl req -out apache.csr -new -newkey rsa:2048 -nodes -keyout apache.key

```
root@kali:~# openssl req -out apache.csr -new -newkey rsa:2048 -nodes -keyo
ut apache.key
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'apache.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]:AR
State or Province Name (full name) [Some-State]:CABA
Locality Name (eg, city) []:CABA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Empresa
Organizational Unit Name (eg, section) []:Seguridad Informatica
Common Name (e.g. server FQDN or YOUR name) []:apache.empresa.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@kali:~# █
```

Enviar CSR a la CA

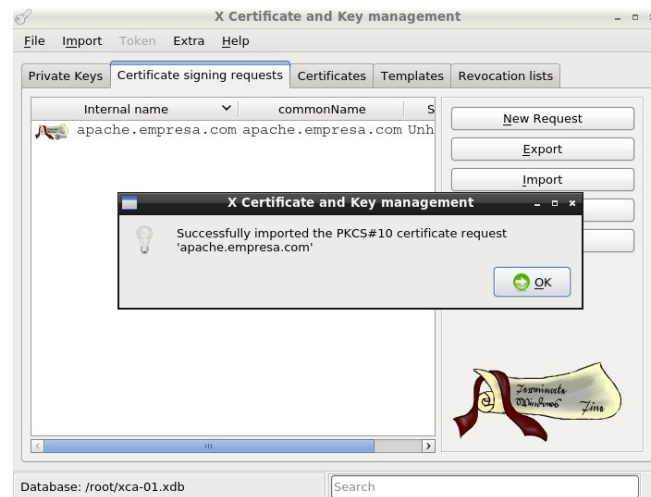
Luego realizar la acción anterior deberán hacer llegar el CSR a la CA para que genere el certificado. Y almacenar de forma segura la clave privada ubicada en el archivo apache.key.

```
root@kali:~# ls -l
total 260
-rw-r--r--  1 root root  1029 Apr 13 16:06 apache.csr
-rw-----  1 root root  1704 Apr 13 16:05 apache.key
```

XCA

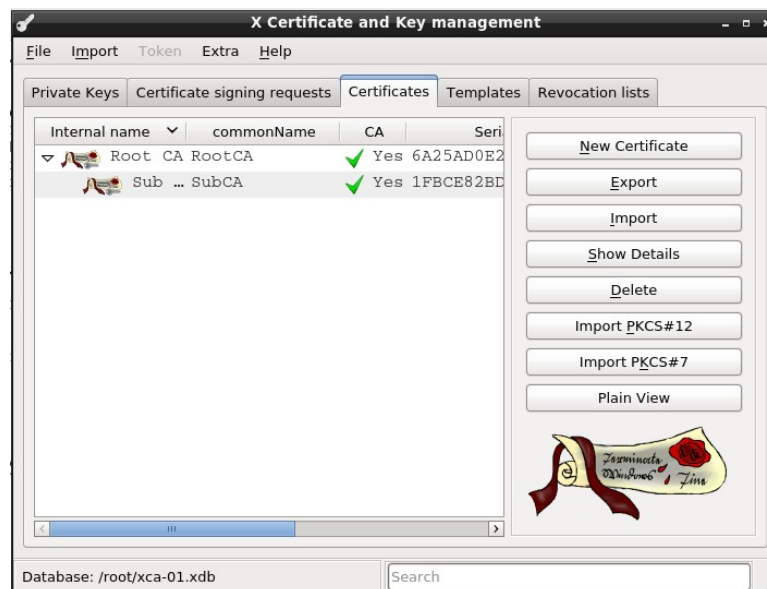
Importar CSR

Volviendo a XCA, en la solapa *Certificate signing request* presionaremos el botón “*Import*” y buscaremos el CSR generado recientemente.



Firmar CSR

Una vez importado, procederemos a firmarlo. Para ello iremos a la pestaña *Certificates* y presionaremos el botón “*New Certificate*”



Seleccionaremos el check “*Sign this Certificate signing request*” indicando el CSR a firmar, tal como muestra la siguiente imagen. Asimismo debemos seleccionar la opción “*Use this Certificate for signing*” y deberemos elegir “*Sub CA*”. Como en el resto de los certificados creados elegiremos SHA256 como algoritmo de HASH pero en este caso seleccionaremos el template *TLS_server* y presionaremos el botón “*Apply all*”.

Create x509 Certificate

Source Extensions Key usage Netscape Advanced Comment

Signing request

☒ Sign this Certificate signing request apache.empresa.com

☒ Copy extensions from the request Show request

☐ Modify subject of the request

Signing

☐ Create a self signed certificate

☒ Use this Certificate for signing Sub CA

Signature algorithm SHA 256

Template for the new certificate

[default] TLS_server

Apply extensions Apply subject Apply all

Cancel OK

En la solapa *Extensions* deberá figurar que es “*End Entity*” y el rango de tiempo es de 365 días. Finalizada esta comprobación presionaremos Aceptar. Configurar también el campo X509v3 Subject Alternative name de la siguiente manera incorporando el DNS prueba.empresa.com

X509v3 Subject Alternative Name ✓ DNS:copycn, DNS:prueba.empresa.com

Edit

Create x509 Certificate

Source Extensions Key usage Netscape Advanced Comment

X509v3 Basic Constraints

Type End Entity

Path length

☒ Critical

Key identifier

☒ Subject Key Identifier

☐ Authority Key Identifier

Validity

Not before 2020-04-13 19:19 GMT

Not after 2021-04-13 19:19 GMT

Time range

365 Days Apply

☐ Midnight ☐ Local time ☐ No well-defined expiration

X509v3 Subject Alternative Name Edit

X509v3 Issuer Alternative Name Edit

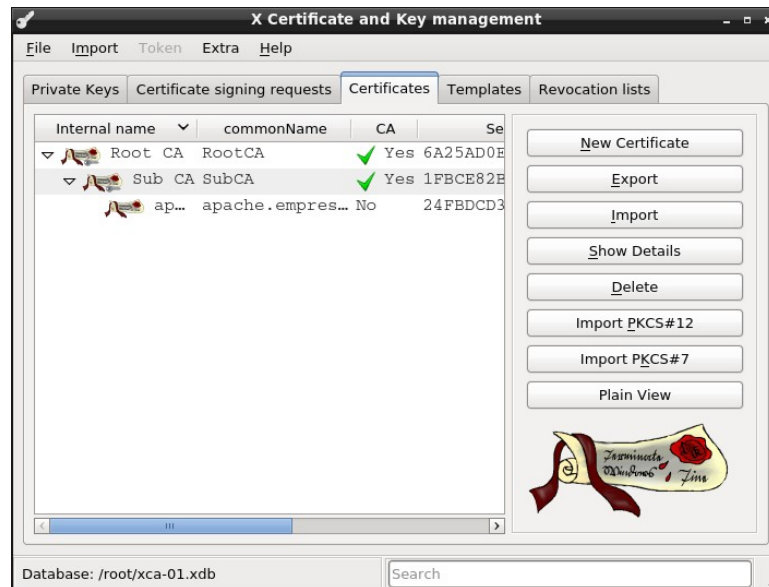
X509v3 CRL Distribution Points Edit

Authority Information Access OCSP Edit

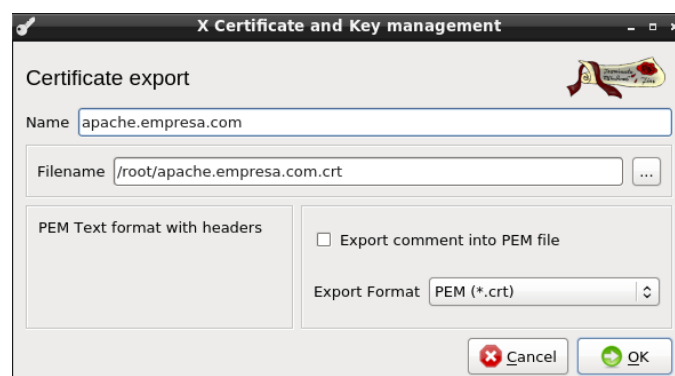
Cancel OK

Una vez hecho esto, habremos firmado el CSR con nuestra Sub CA, obteniendo el Certificado Digital para ser utilizado por el servidor web Apache.

Procedemos a exportar el certificado identificando la ruta donde queremos almacenarlo.



Exportar Certificado



Una vez generado el certificado deberán enviar el mismo hasta el servidor web con Apache.

Apache

Configurar el módulo TLS

Para habilitar el módulo en el servidor deberá ejecutarse el siguiente comando:

```
a2enmod ssl
```

Crear VirtualHost

Luego, editar el archivo /etc/apache2/sites-enabled/000-default.conf y agregar el siguiente contenido al final:

```
<VirtualHost *:443>
    ServerName apache.empresa.com
    SSLEngine on
    SSLCertificateFile "/ruta/del/certificado.crt"
    SSLCertificateKeyFile "/ruta/de/la/clave.key"
</VirtualHost>
```

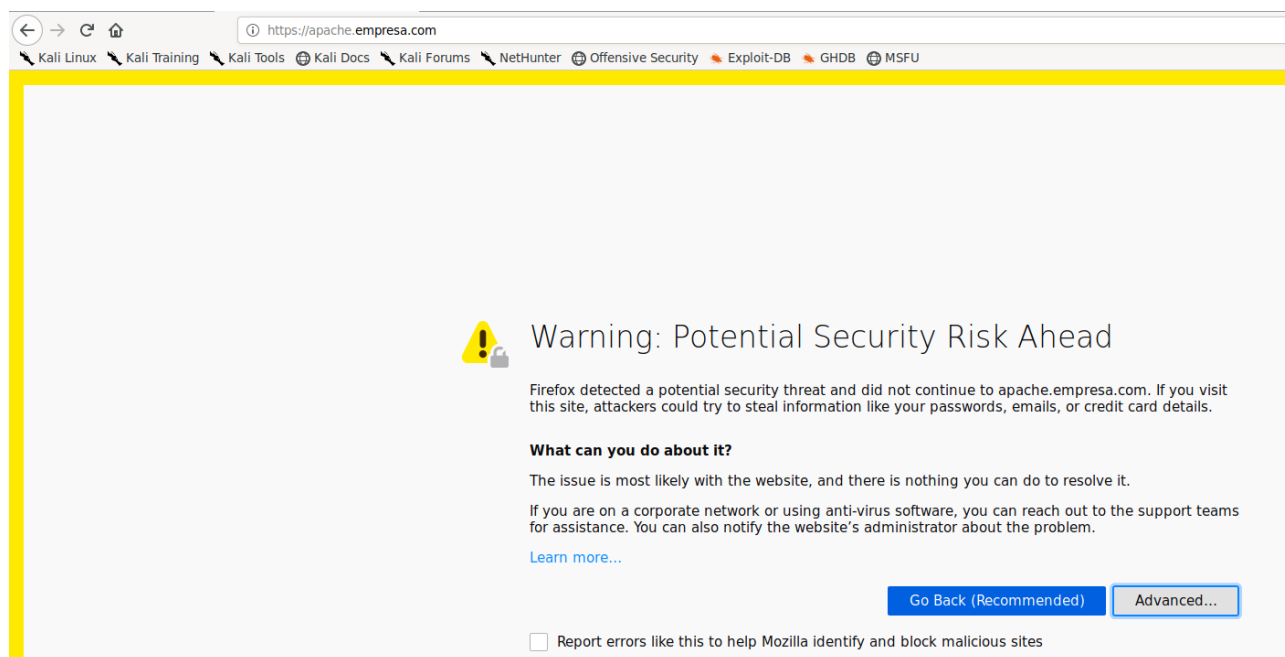
Reiniciar el apache

```
service apache2 restart
```

Probar servicio por HTTPS

Una vez hecho esto probar, desde otro equipo, acceder mediante el navegador a <https://apache.empresa.com>¹

Si accedemos por medio de nuestro navegador, el mismo nos dará la siguiente advertencia



¹ Recordar que desde la máquina con Windows tiene que resolver el nombre apache.empresa.com

Esto es debido a que nuestro browser no confía en nuestra CA, por lo tanto el siguiente paso será instalar los certificados digitales de la CA, tanto el certificado de la RootCA como de la SubCA.

Para probar el Subject Alternative Name, navegue al servidor por las URL

<https://apache.empresa.com>

<https://prueba.empresa.com>

<https://prueba2.empresa.com>

(Recordar que desde la máquina con Windows tiene que resolver los nombres correspondientes al IP de kali)

Opcional: Suponga que se vio comprometida la clave privada en el servidor apache.empresa.com.

Realice con XCA y apache las acciones que considere necesarias para que los clientes que confían en su PKI no accedan a un certificado donde su clave privada se haya visto comprometida.