

vpn,, ipsec,, certificados

VPN ipsec con certificados

Vamos a realizar todo el proceso necesario para realizar conexiones a nuestro fortigate mediante certificados. Para ello necesitamos un crear una entidad certificadora, ya sea con un servidor Windows con el rol de AD CS(mirar las páginas de referencia), mediante openssl, o como en nuestro caso usando una aplicación para windows llamada XCA <http://xca.sourceforge.net/>.

Los pasos que vamos a seguir son:

1. Crear una entidad certificadora
2. Generar un certificado raíz
3. Generar certificados para los clientes de la vpn
 1. Generar un petición para los clienes desde el XCA
 2. Firmar la petición
 3. exportar el certificado firmado de cliente
 4. exportar desde el fortigate el certificado raíz CA_Cert
 5. importar los certificados clientes y raíz al Forticlient
4. Crear vpn, políticas y usuarios en el fortigate

Una VPN con certificados nos garantiza una mayor seguridad, ya que por un lado usamos una clave de encriptación de mayor tamaño y por otro lado implica un segundo factor de autenticación ya que además del usuario/contraseña es necesario tener instalado un segundo elemento como es el certificado

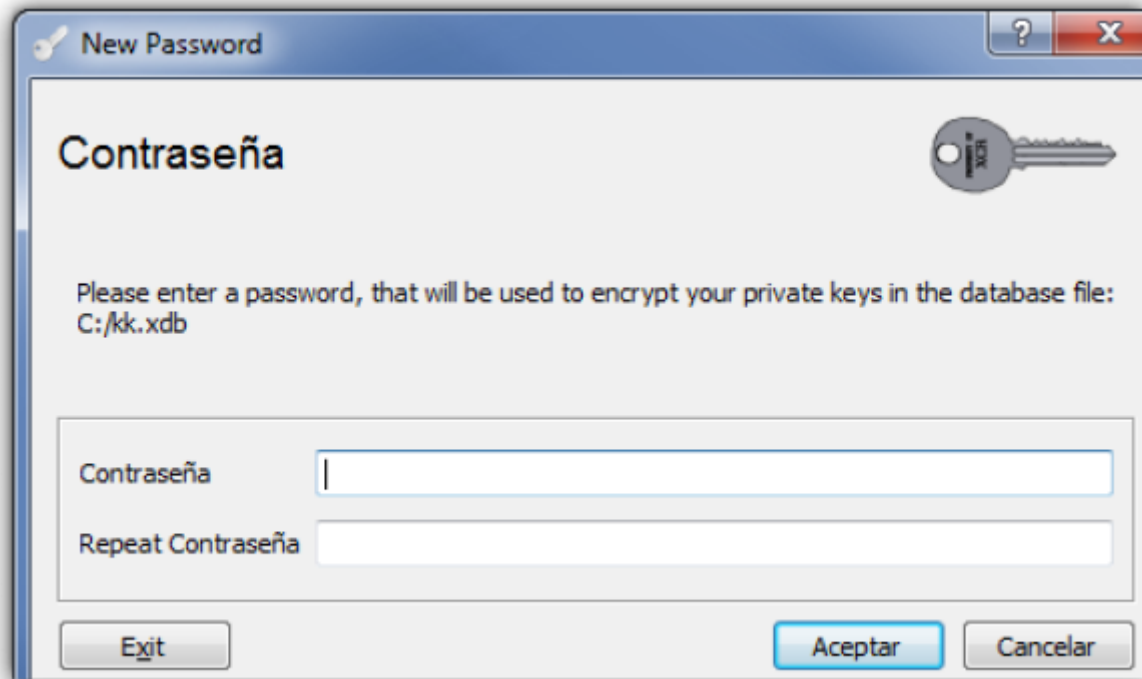
Crear una entidad certificadora

Nos bajamos el XCA y lo instalamos en nuestro equipo con permisos de administrador

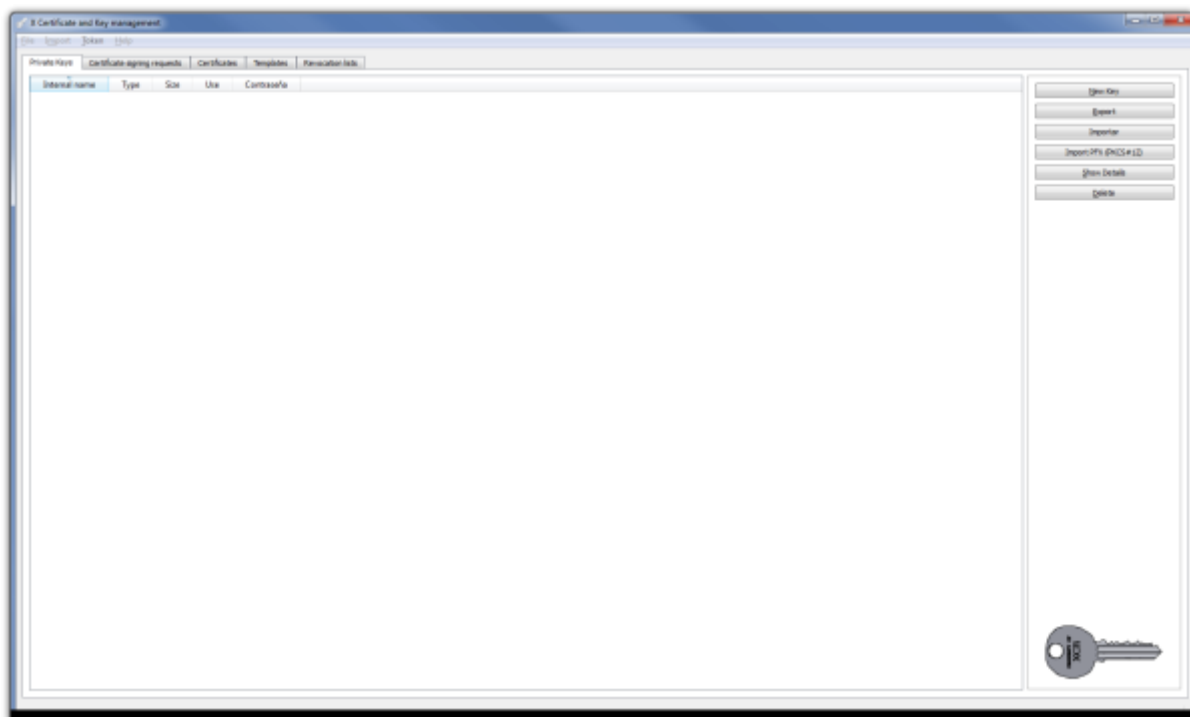
En XCA cada CA (Autoridad Certificadora)se almacena en un fichero con extensión *.xdb. Se recomienda usar distintas bases de datos para cada PKI (Infraestructura de clave pública) que creemos.

Ejecutamos el programa Click File > New Database.

- En la ventana que se abre especificar el nombre y la ubicación donde se almacena el fichero con la base de datos XCA y pulsar guardar.
- Nos aparece una ventana donde debemos poner una contraseña para encriptar el fichero de la base de datos. Esa contraseña es necesaria para cada vez que vayamos a abrir esa base de datos.

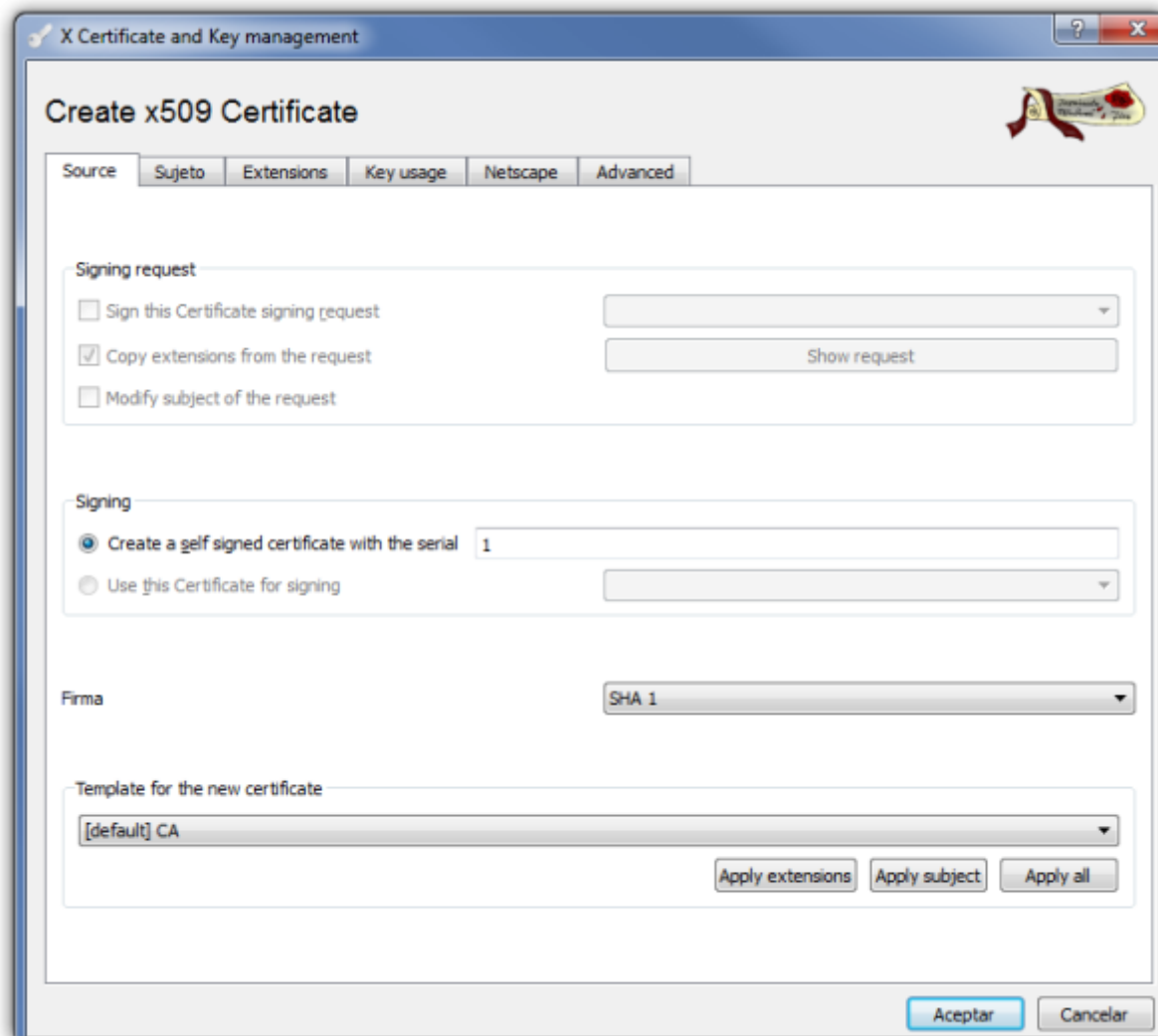


Nos aparece la siguiente ventana



Generar el certificado Raíz

Pulsamos sobre la pestaña **Certificates** y entonces pulsamos en el botón **New Certificate**.



Configuramos los parámetros del certificado.

Pestaña Sujeto

Configuramos la información de identificación.

Rellenamos los campos de Distinguished name y pulsamos sobre el botón inferior **Generate a new key**

The screenshot shows the 'Create x509 Certificate' window with the 'Sujeto' tab selected. The 'Distinguished name' section contains the following fields:

Field	Value
Internal name	Certificado Raiz
countryName	es
stateOrProvinceName	Gran Canaria
localityName	Gran Canaria
organizationName	nombre empresa
organizationalUnitName	mi organización
commonName	empresa
emailAddress	tic@miempresa.es

Below the distinguished name fields is a table for extensions with columns 'Type' and 'Content'. To the right of this table are 'Add' and 'Delete' buttons. At the bottom, there is a section for 'Exponente secreto' with a dropdown menu, a checkbox for 'Used keys too', and a 'Generate a new key' button. The window has 'Aceptar' and 'Cancelar' buttons at the bottom right.

Seleccionamos el tamaño de la clave y pulsamos el botón **Create**

The screenshot shows the 'New key' window. It prompts the user to 'Please give a name to the new key and select the desired keysize'. The 'Key properties' section contains the following fields:

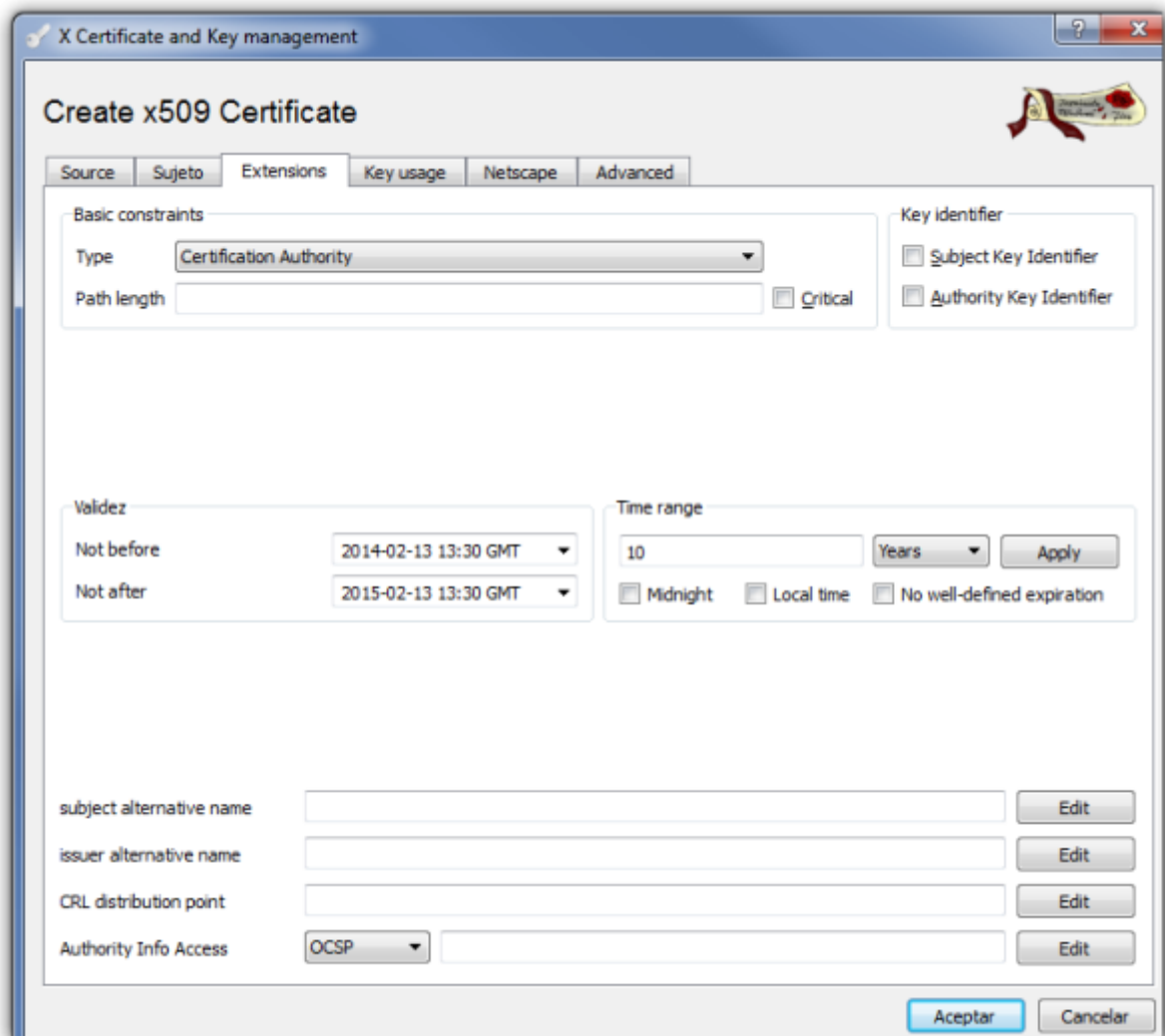
Field	Value
Nombre	Certificado Raiz
Keytype	RSA
Tamaño de clave	2048 bit

At the bottom right, there are 'Create' and 'Cancelar' buttons.

Pestaña Extensions

modificamos los siguientes parámetros:

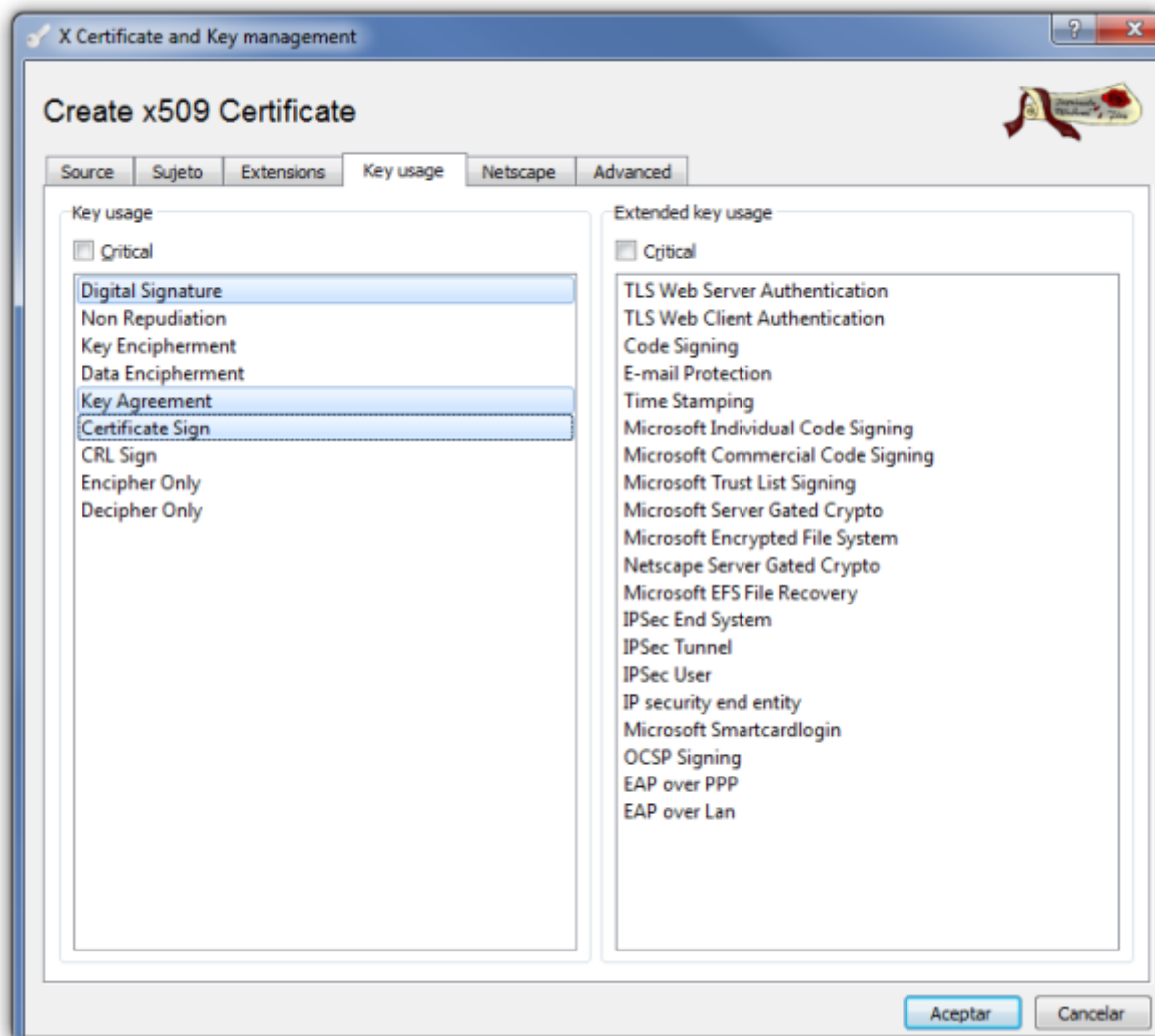
- en la lista desplegable **Type** elegimos **Certification Authority**
- En la casilla **Time range** ponemos 10 para que el certificado raíz tenga una validez de 10 años



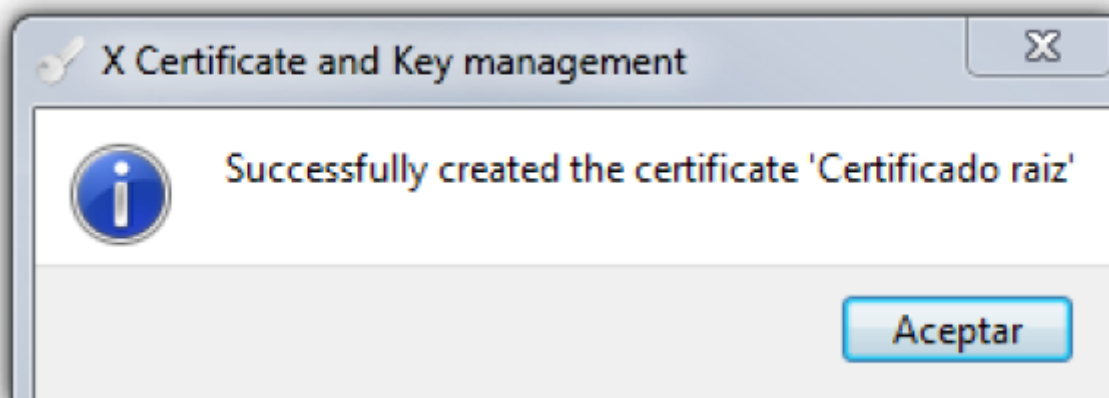
Pestaña Key usage

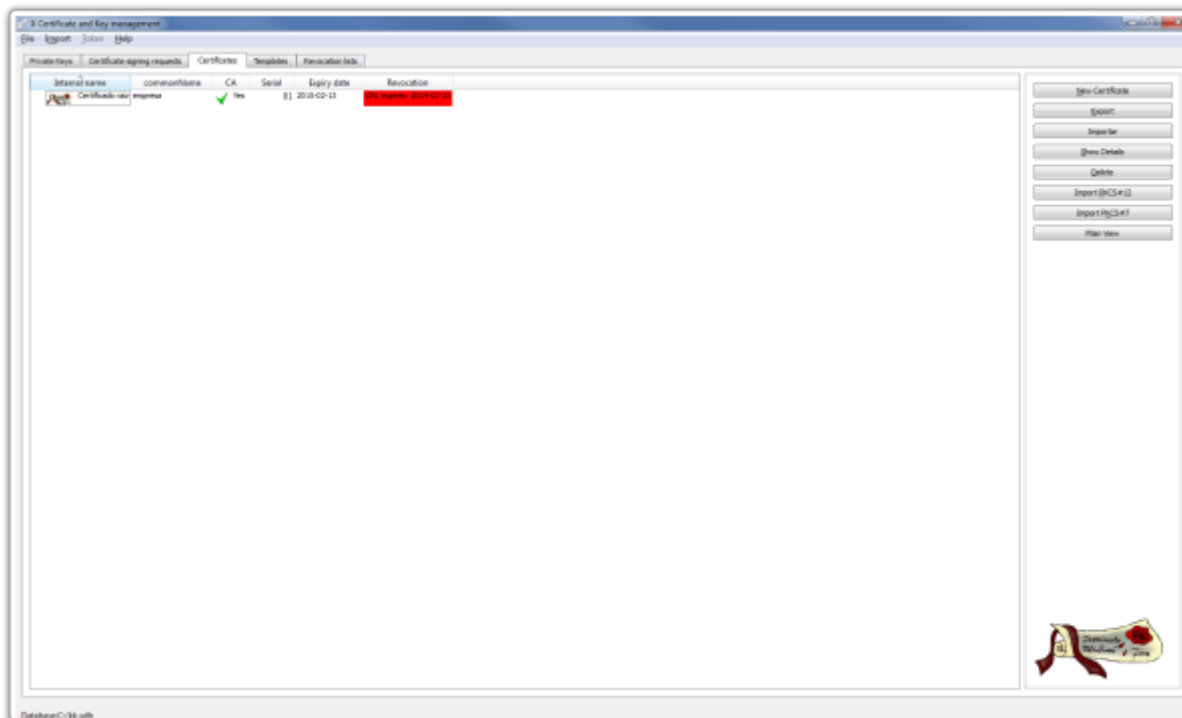
En el panel de la izquierda comprobamos que tenemos las opciones:

- Digital Signature
- Key Agreement
- Certificate Sign



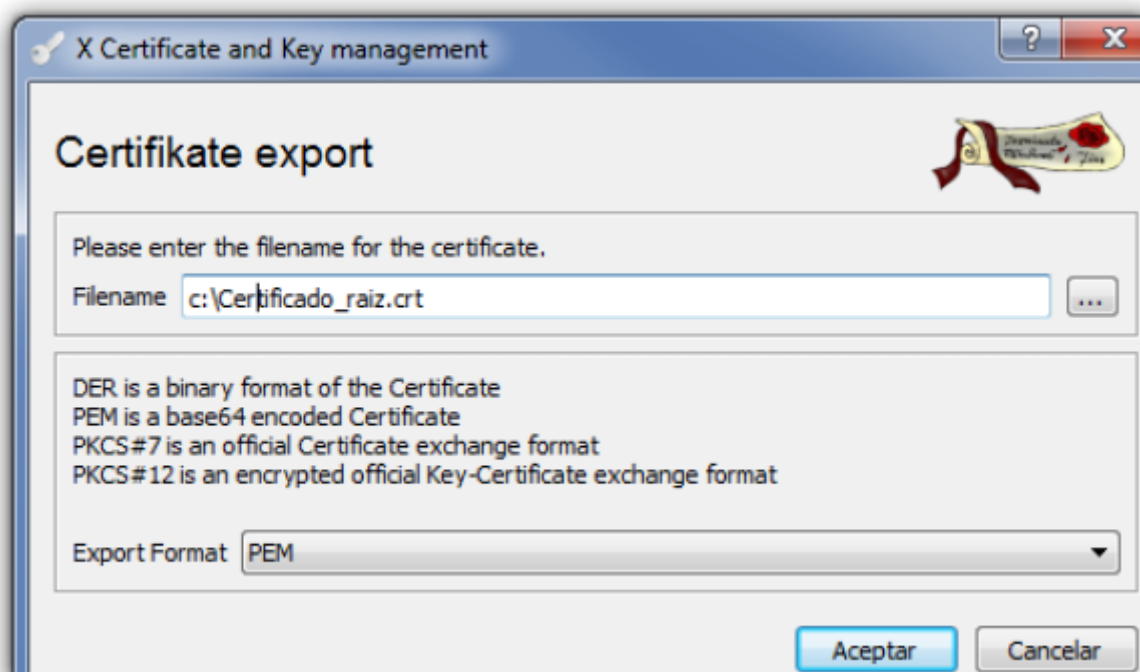
Pulsamos Aceptar y nos debe aparecer una ventana indicandonos que el certificado ha sido creado





Lo siguiente es exportar el certificado raíz para tener una copia de seguridad. Para ello hacemos lo siguiente:

- Pestaña certificados → Seleccionamos el certificado de la CZ → Botón exportar → ponemos la ubicación y el nombre de donde guardamos el certificado y pulsamos sobre el botón Aceptar



Crear certificados para los clientes

Abrimos el XCA → Pestaña Solicitudes de Certificado (Certificate signing requests) → Nueva solicitud (New Request)

X Certificate and Key management

Create Certificate signing request

Source | **Sujeto** | Extensions | Key usage | Netscape | Advanced

Signing request

unstructuredName

challengePassword

Signing

☒ Create a self signed certificate with the serial

☐ Use this Certificate for signing Certificado Raiz

Firma SHA 1

Template for the new certificate

[default] CA

Apply extensions Apply subject Apply all

Aceptar Cancelar

Seleccionamos nuestra plantilla de CA para generar el nuevo certificado

En la ventana que se abre → Pestaña Subject → Rellenamos los campos y pulsamos sobre el botón generar una nueva clave (generate a new key)

X Certificate and Key management

Create Certificate signing request

Source | **Sujeto** | Extensions | Key usage | Netscape | Advanced

Distinguished name

Internal name	usuario1	organizationName	mi empresa
countryName	es	organizationalUnitName	mi organizacion
stateOrProvinceName	Gran Canaria	commonName	empresa
localityName	Gran Canaria	emailAddress	tic@empresa.es

Type	Content
------	---------

Add
Delete

Exponente secreto

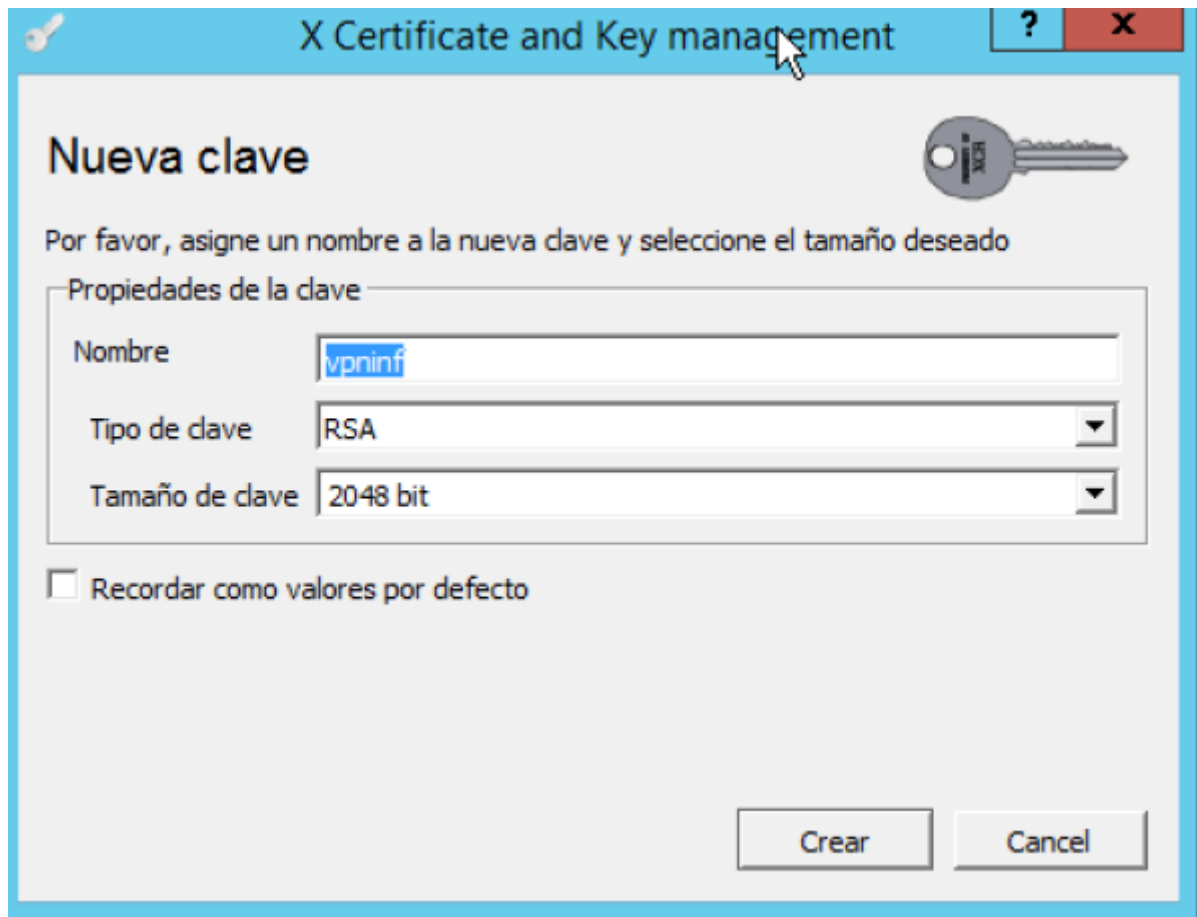
usuario1 (RSA) ☐ Used keys too [Generate a new key](#)

Aceptar Cancelar



el commonname tiene que coincidir con el del usuario pki que creamos en el fortinet

Seleccionamos el tamaño de la clave y pulsamos sobre create.



X Certificate and Key management

Nueva clave

Por favor, asigne un nombre a la nueva clave y seleccione el tamaño deseado

Propiedades de la clave

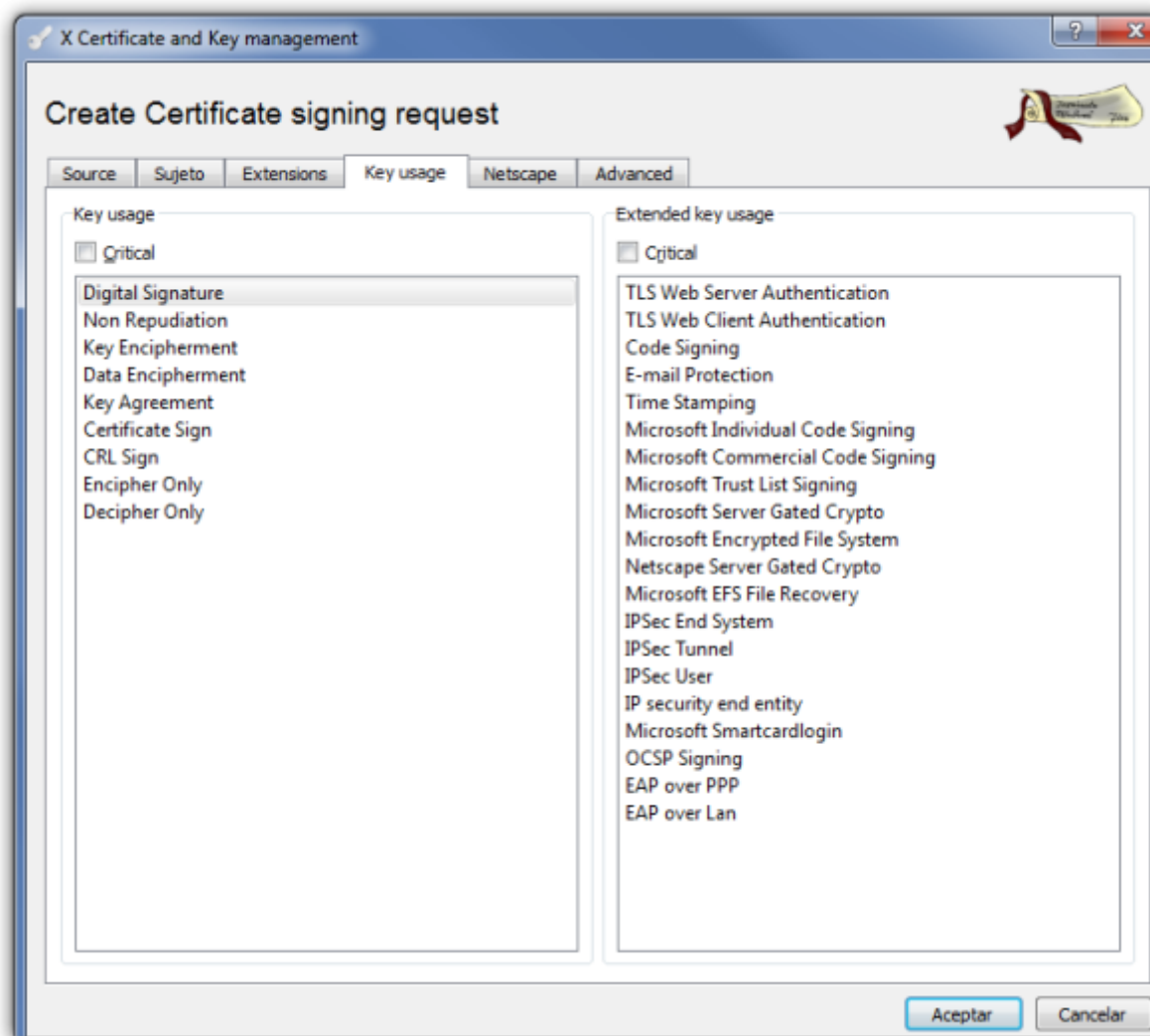
Nombre:

Tipo de clave:

Tamaño de clave:

☐ Recordar como valores por defecto

Una vez creada la clave vamos a la pestaña **key usage** y seleccionamos del panel de la izquierda → Digital signature

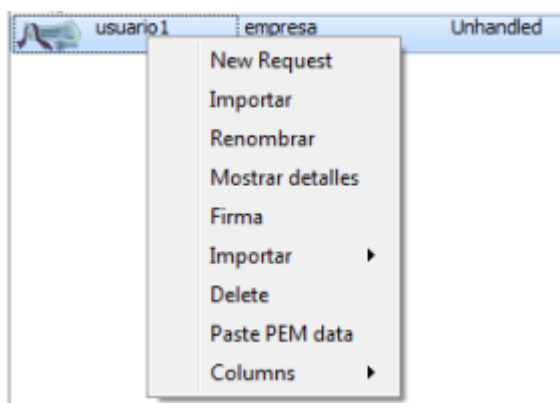


Pulsamos el botón de aceptar

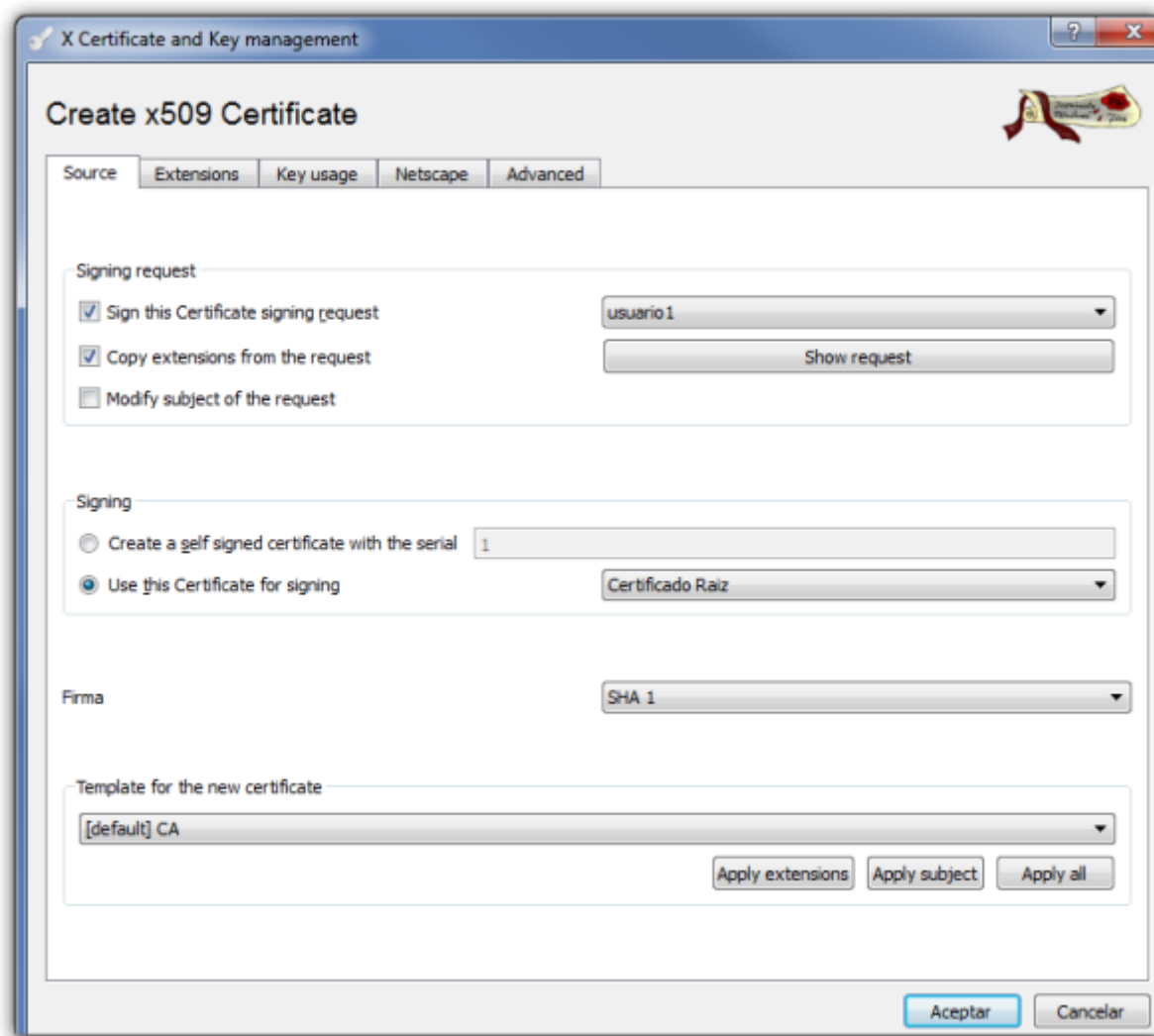
Firma del certificado cliente

El siguiente paso sería firmar la petición de certificado que hemos generado. Vamos a la pestaña **Solicitudes de Certificado (Certificate signing requests)** aparece la petición que acabamos de crear con el estado de la columna firma como No Manejado (Unhandled).

Pulsamos con el botón derecho del ratón y en el menu contextual que aparece seleccionamos Firma



En la ventana que se abre en la parte de signing elegimos la opción **use this Certificate for signing** y seleccionamos el certificado raíz



Verificamos que en la pestaña **Extensions** la validez que queremos darle al certificado y pulsamos sobre aceptar

Ahora nos aparecerá el certificado firmado. Ya sólo falta exportar este certificado y el certificado raíz e importarlos al fortigate XCA→ Pestaña Certificate→ elegimos el certificado y le damos a exportar →PKCS#12

Importar Certificados al Fortigate

Después debemos de exportar los certificados de la CA y del cliente hay que importarlos al Fortigate.

Importar Certificado Raiz

System →Certificates →CA Certificates →Import →Marcamos la casilla Local Pc y seleccionamos el fichero CA Raiz que previamente hemos exportado de nuestra entidad Certificadora

Importar certificado cliente

Vamos al interfaz web del cortafuegos → System →Certificates →Local Certificate → Import → Seleccionamos el certificado cliente del paso anterior

Forticlient

Importar certificados al Forticlient

A su vez desde el XCA → pestaña Certificates →exportamos el certificado cliente en formato pkcs#12 e importamos ambos certificados al forticlient→Menu File→opciones→Gestión de Certificados→botón importar



Es necesario importar los dos certificados CA_Cert1 y el del cliente

Crear la conexión

Añadimos una nueva conexión con los siguientes parámetros

FortiClient

File Help

Create new VPN Connection

Nombre de Conexión: mi vpn

Tipo: ☐ VPN SSL ☒ VPN IPsec

Descripción: conexión a mi vpn

Gateway Remoto: ip del gateway remoto

Método de Autenticación: Certificado X.509

Certificado X.509: [Prompt on connect]

Autenticación (XAuth): ☐ Preguntar en el login ☐ Guardar login ☒ Deshabilitar

Aceptar Cancelar



La autenticación XAuth la he deshabilitado para simplificar, pero sería recomendable activarla tanto el fortigate como en el cliente

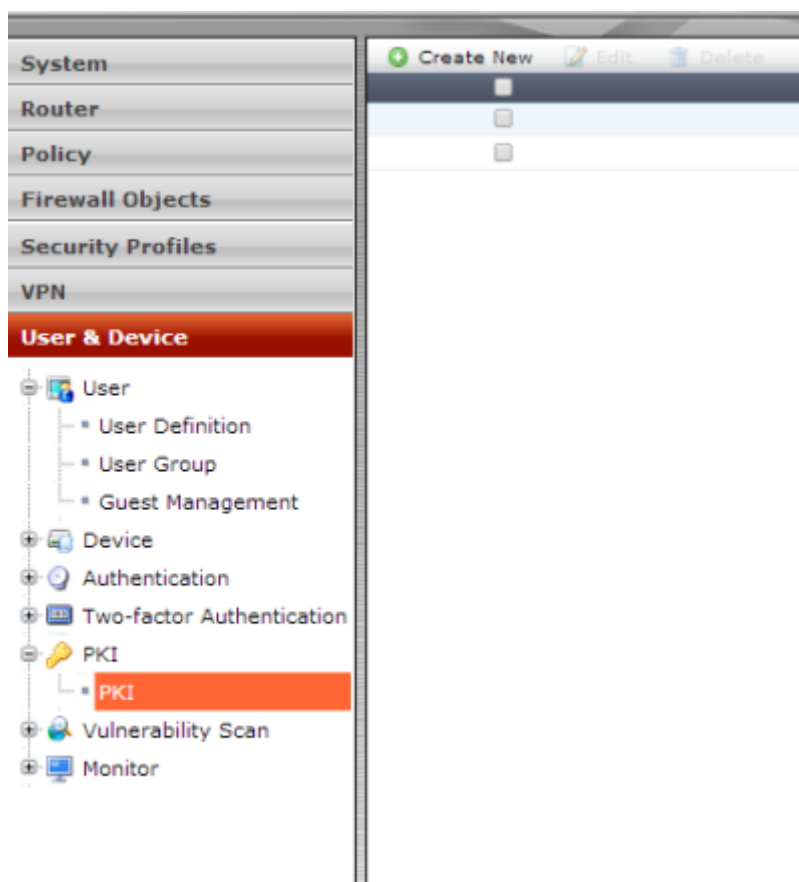
Crear conexión y usuarios en el Fortigate

Aparte de los pasos anteriores se supone que en el fortigate hemos creado las políticas y los usuarios necesarios. En caso contrario los pasos a seguir son:

1. Nos validamos en el Fortigate y vamos a la pestaña VPN
2. Creamos los usuarios de validación
3. Pinchamos sobre el icono **Create FortiClient VPN**
4. Ponemos los siguientes parámetros

Creamos los usuarios de validación

para PKI



Creamos uno nuevo teniendo en cuenta que el Subject tiene que ser el mismo que el del certificado y en CA el certificado de nuestra CA normalmente CA_Cert1

From:
<https://intrusos.info/> - **LCWIKI**

Permanent link:
<https://intrusos.info/doku.php?id=hardware:fortigate:vpn:ipseccertificados&rev=1587726614>

Last update: **2023/01/18 14:38**

