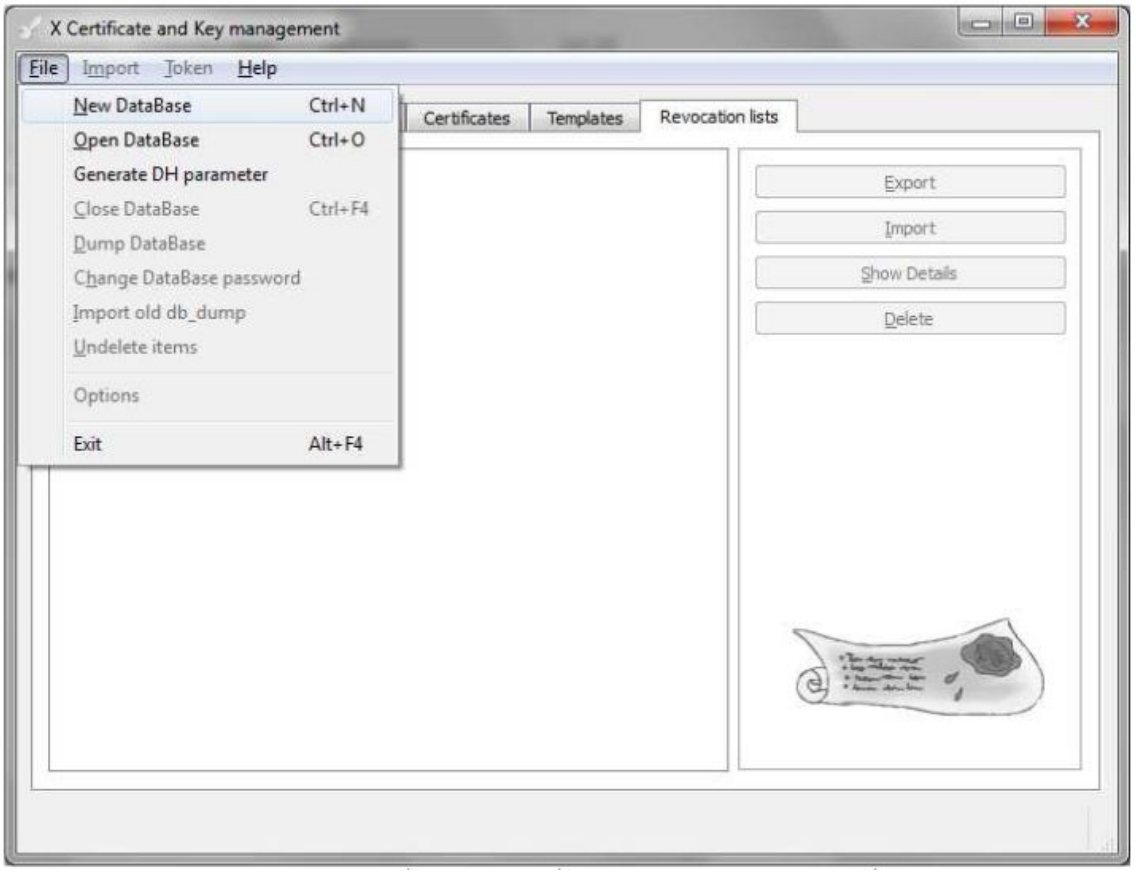
PKI - Creación con XCA

XCA es una herramienta de código abierto que nos permite crear y gestionar certificados X.509, así como gestionar claves asimétricas RSA o DSA. Implementa todo lo que necesita una pequeña Autoridad de Certificación (CA) para crear y firmar certificados.

Para comenzar a utilizarla, debemos descargarnos el instalador desde la web del proyecto http://sourceforge.net/projects/xca

Creación del almacén de datos

El primer paso a realizar después de la instalación de XCA, y tras arrancar éste, es la creación de una base de datos (o almacén) donde se guardarán las claves generadas, las peticiones de firma de certificados, los certificados en sí, las listas de revocación, etc. Para ello, vamos al menú File y seleccionamos la opción New DataBase



Guardamos la base de datos en nuestra carpeta de trabajo con el nombre de Certificados.

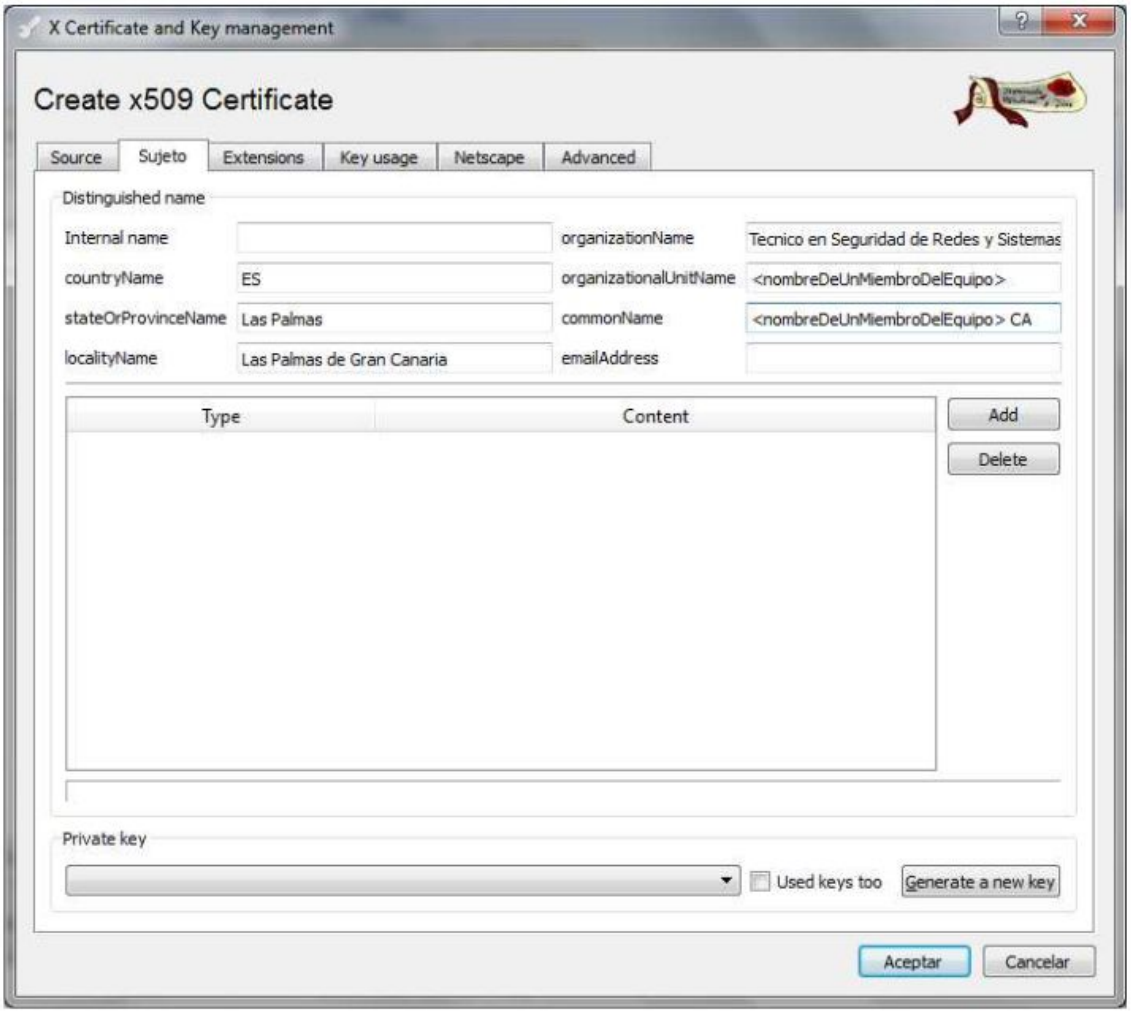
Se nos pedirá una contraseña, utilizada para encriptar (cifrar) las claves privadas que se generen.

Una vez creada la base de datos, ya estamos listos para crear nuestro primer certificado, justamente el de la Autoridad de Certificación (CA).

Creación del certificado de la CA

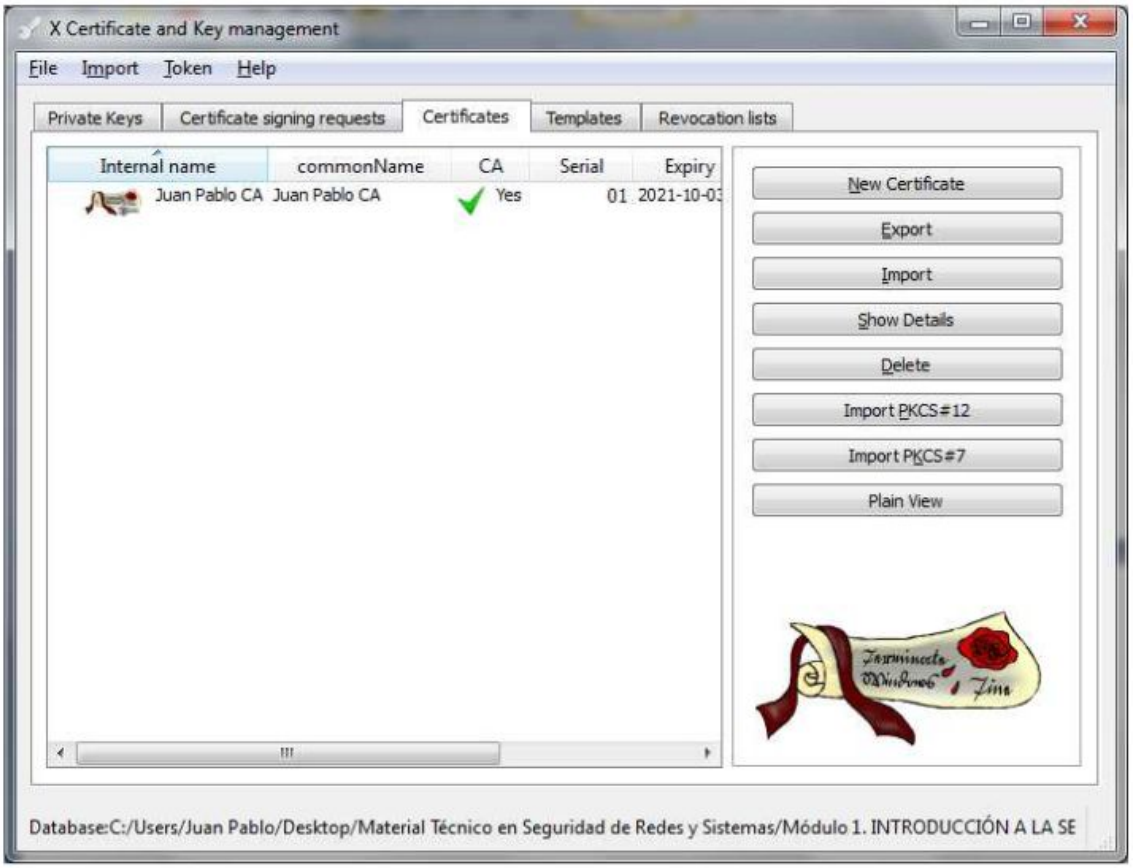
Vamos a crear el certificado para la Autoridad de Certificación. Para ello:

- ❏ Hacemos clic en la pestaña Certificates
- ❏ Pulsamos el botón New Certificate
- ❏ Verificamos que en la pestaña Source está seleccionada la opción [default] CA en la sección Template for the new certificate. Si no lo está, la seleccionamos del desplegable
- ❏ Pulsamos el botón Apply all para que se actualice el resto de pestañas con la configuración indicada en Source
- ❏ Nos situamos en la pestaña Sujeto y rellenamos los datos acorde a la siguiente imagen (hemos de sustituir <nombreDeUnMiembroDelEquipo> por el nombre de uno de los intregrantes del equipo, nombre que escribiremos sin espacios y sin tildes, y que consideraremos donde se nos solicite en todos los apartados siguientes de la práctica)



Pulsamos el botón “Generate a new key”

- Pulsamos Create, lo que hará que se nos cree la clave privada del certificado de la CA
- Pulsamos la pestaña Extensions y observamos que el tiempo de validez del certificado que queremos generar será de 10 años
- Por último, pulsamos el botón Aceptar y esto hará que se nos cree el certificado para nuestra Autoridad Certificadora

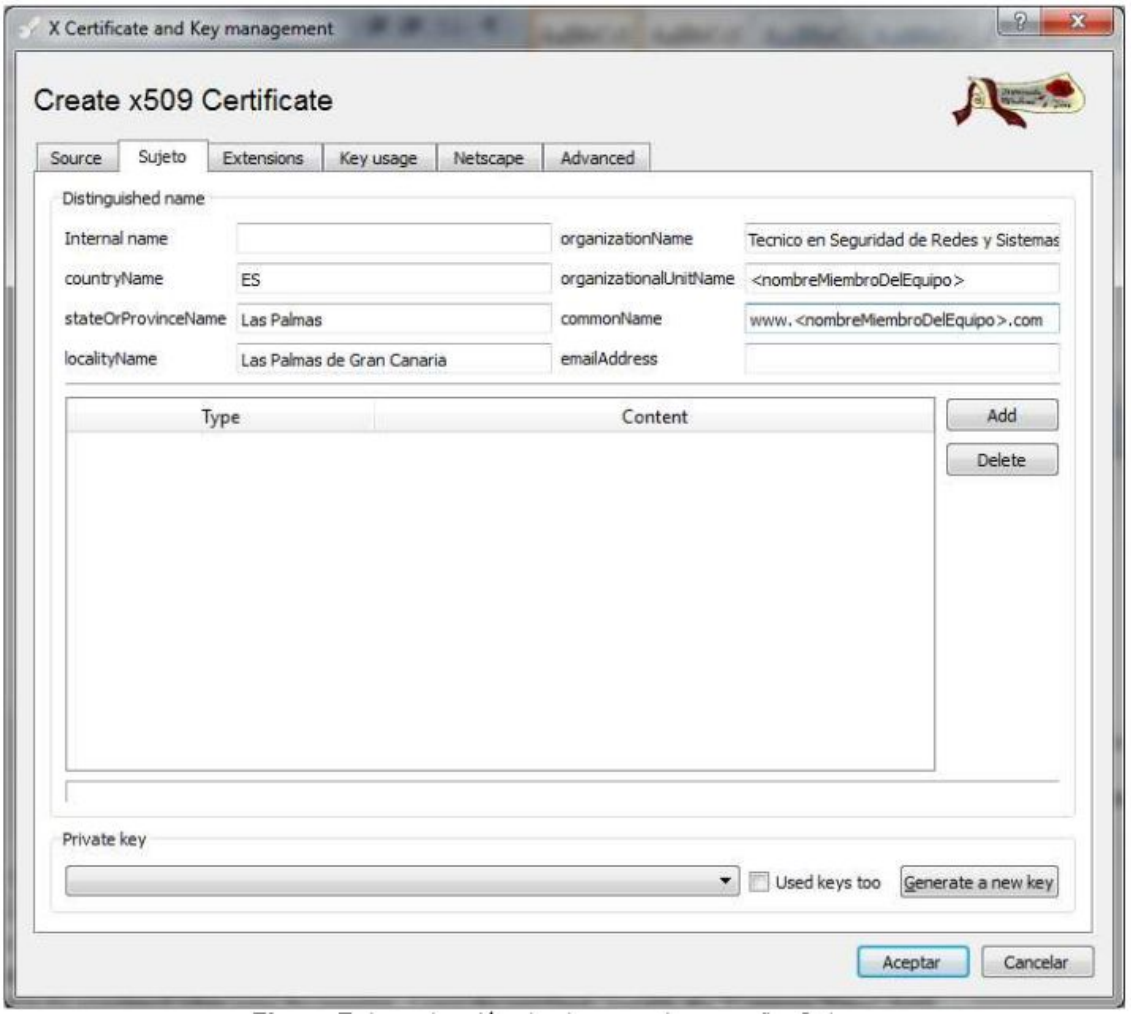


Creación de un certificado de servidor

Vamos a crear un certificado para dar autenticidad (confianza) a nuestro servidor web y confidencialidad a los datos que se envíen desde/hacia él. Para ello:

- ❏ Hacemos clic en la pestaña Certificates
- ❏ Pulsamos el botón New Certificate
- ❏ En la pestaña Source marcamos la opción "Use this Certificate for signing" de la sección Signing
- ❏ En el desplegable asociado a la opción debe aparecer el certificado de la CA que nos creamos anteriormente
- ❏ Seleccionamos la opción [default] HTTPS_server en la sección Template for the new certificate
- ❏ Pulsamos el botón Apply all para que se actualice el resto de pestañas con la configuración indicada en Source
- ❏ Nos situamos en la pestaña Sujeto y rellenamos los datos acorde a la siguiente imagen (recordemos que hemos de sustituir <nombreMiembroDelEquipo> por el nombre de uno de los integrantes del equipo, nombre que escribiremos sin espacios y sin tildes)

commonName será el nombre por el que se conectarán a nuestro servidor. Eso significa que si, por ejemplo, en commonName escribimos www.juanpablo.com, cualquiera que desee acceder al servidor deberá teclear esa URL.



- Pulsamos el botón Generate a new key
- Pulsamos Create en la siguiente pantalla, lo que hará que se nos cree la clave privada del certificado de servidor
- Pulsamos la pestaña Extensions y observamos que el tiempo de validez del certificado que queremos generar será de 365 días
- Por último, pulsamos el botón Aceptar y esto hará que se nos cree el certificado que utilizaremos en nuestro servidor web

---

Autor: Fabian Martinez Portantier

Fuentes:

- www.wikipedia.org