Sitio web seguro con HTTPS

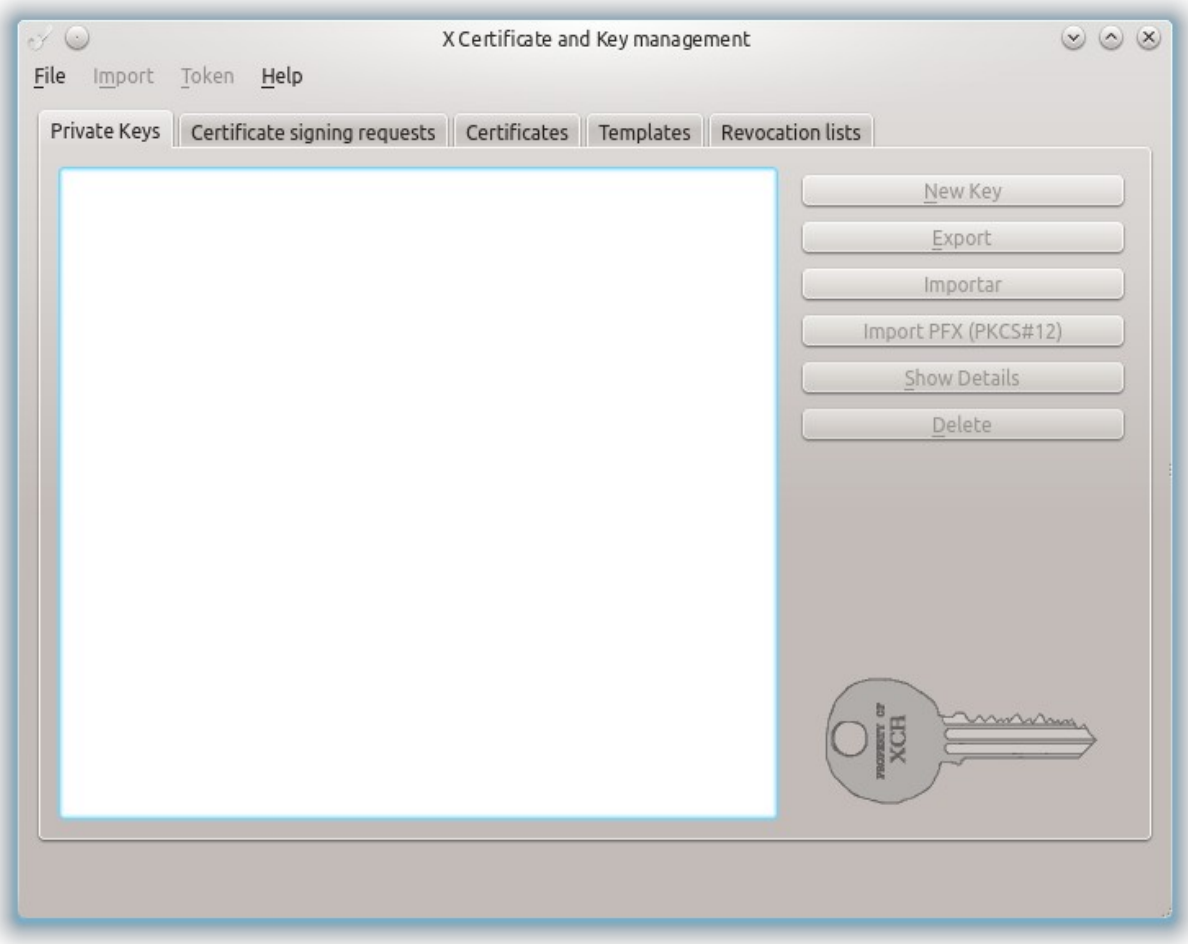
Índice de contenido

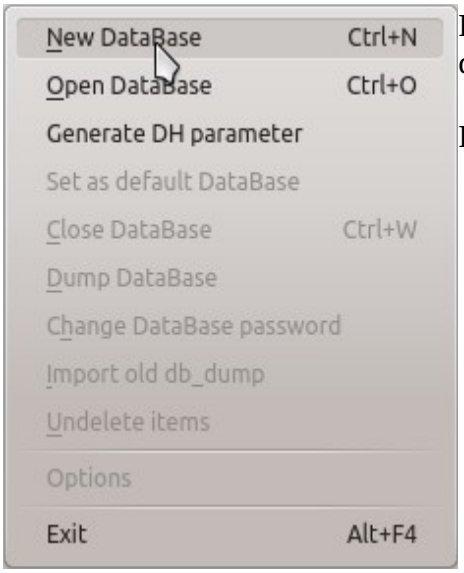
Vamos a crear de una forma sencilla un certificado autofirmado que utilizaremos en nuestro servidor web Apache para habilitar las comunicaciones seguras HTTPS.
Este resumido tutorial ha sido realizado con el siguiente software:

- Linux (escritorio KDE) como equipo de cliente y servidor.
- Apache2 como servidor web
- Aplicación XCA para generación de certificados.

Tanto Apache como XCA son multiplataforma y gratuitos, por lo que este tutorial puede aplicarse también a Windows con algunos cambios.

Creación de un certificado autofirmado con XCA

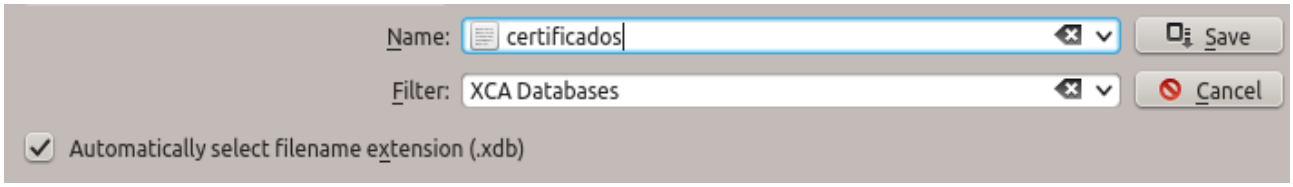




Para empezar a trabajar con XCA debemos de crear una base de datos donde se guardará toda la información.

Pulsamos en File y después en “New Database”.

Le damos un nombre a la base de datos.

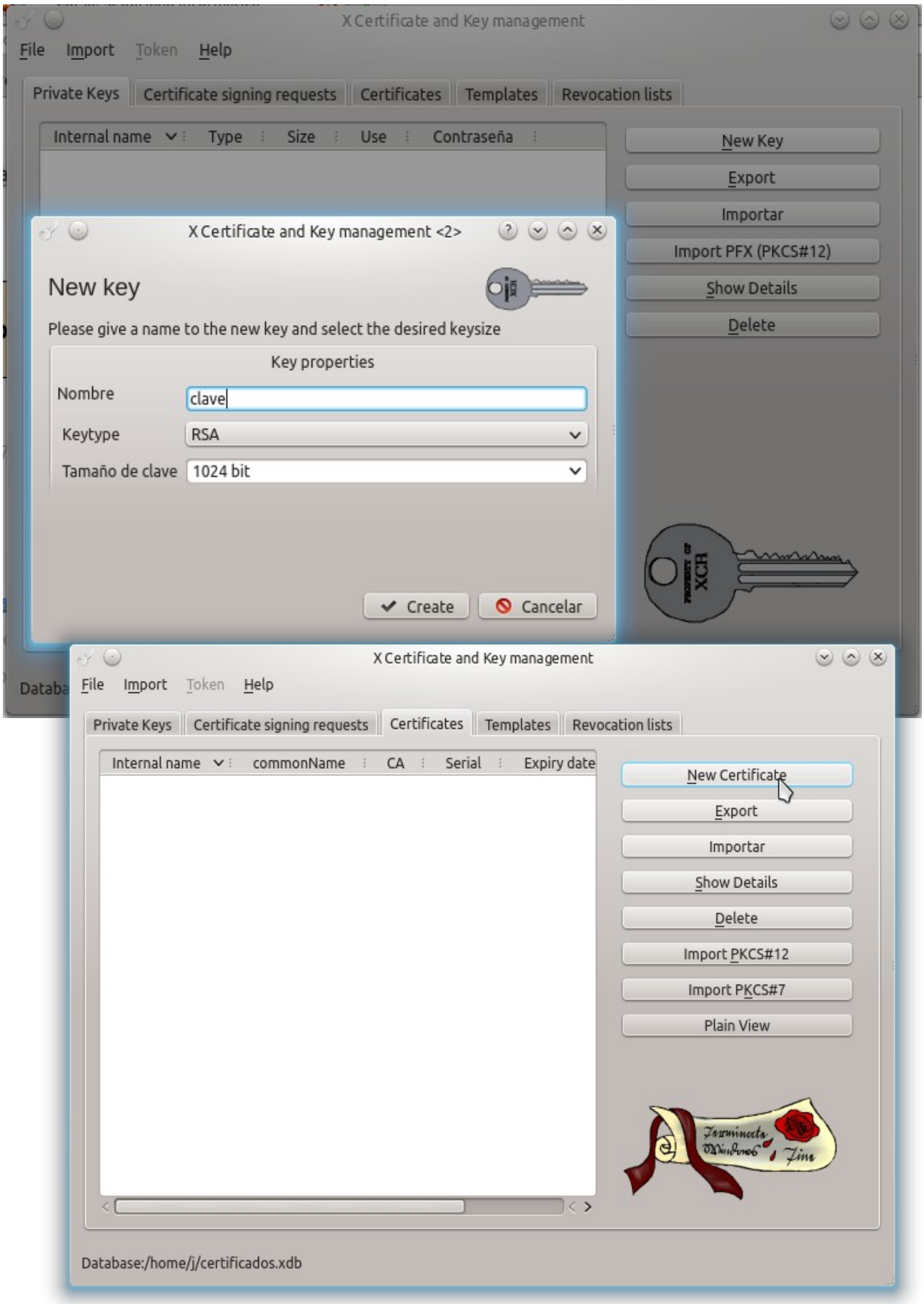


Nos pide una contraseña para proteger la base de datos.

A continuación crearemos la clave asimétrica.

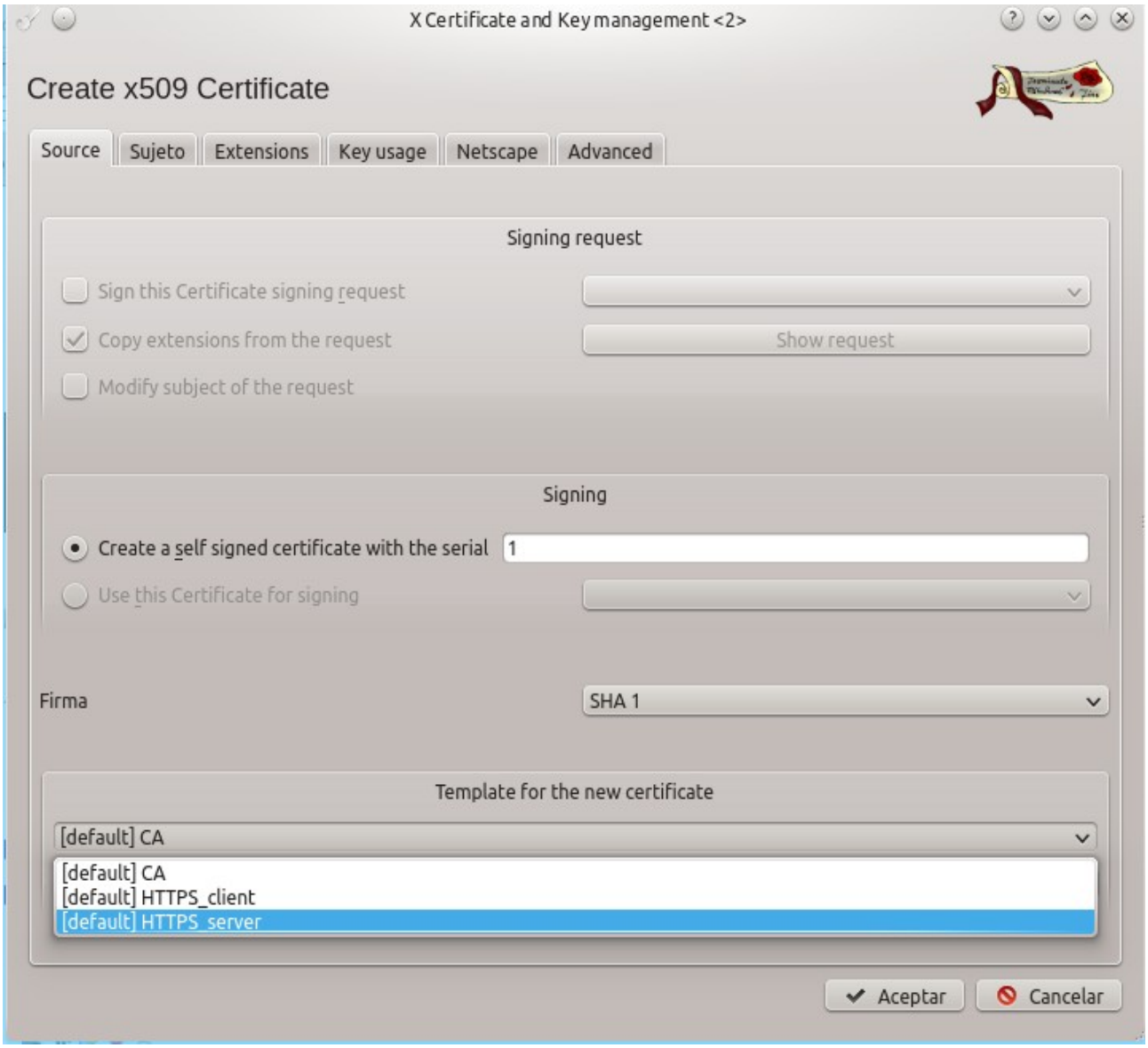
Para ello pulsamos en el botón “New key”.

Ponemos un nombre y pulsamos en el botón “Create”.


X Certificate and Key management
File Import Token Help
Private Keys Certificate signing requests Certificates Templates Revocation lists
Internal name Type Size Use Contraseña
New Key
Export
Importar
Import PFX (PKCS#12)
Show Details
Delete
X Certificate and Key management <2>
New key
Please give a name to the new key and select the desired keysize
Key properties
Nombre clave
Keytype RSA
Tamaño de clave 1024 bit
Create
Cancelar
X Certificate and Key management
File Import Token Help
Private Keys Certificate signing requests Certificates Templates Revocation lists
Internal name commonName CA Serial Expiry date
New Certificate
Export
Importar
Show Details
Delete
Import PKCS#12
Import PKCS#7
Plain View
Database:/home/j/certificados.xdb

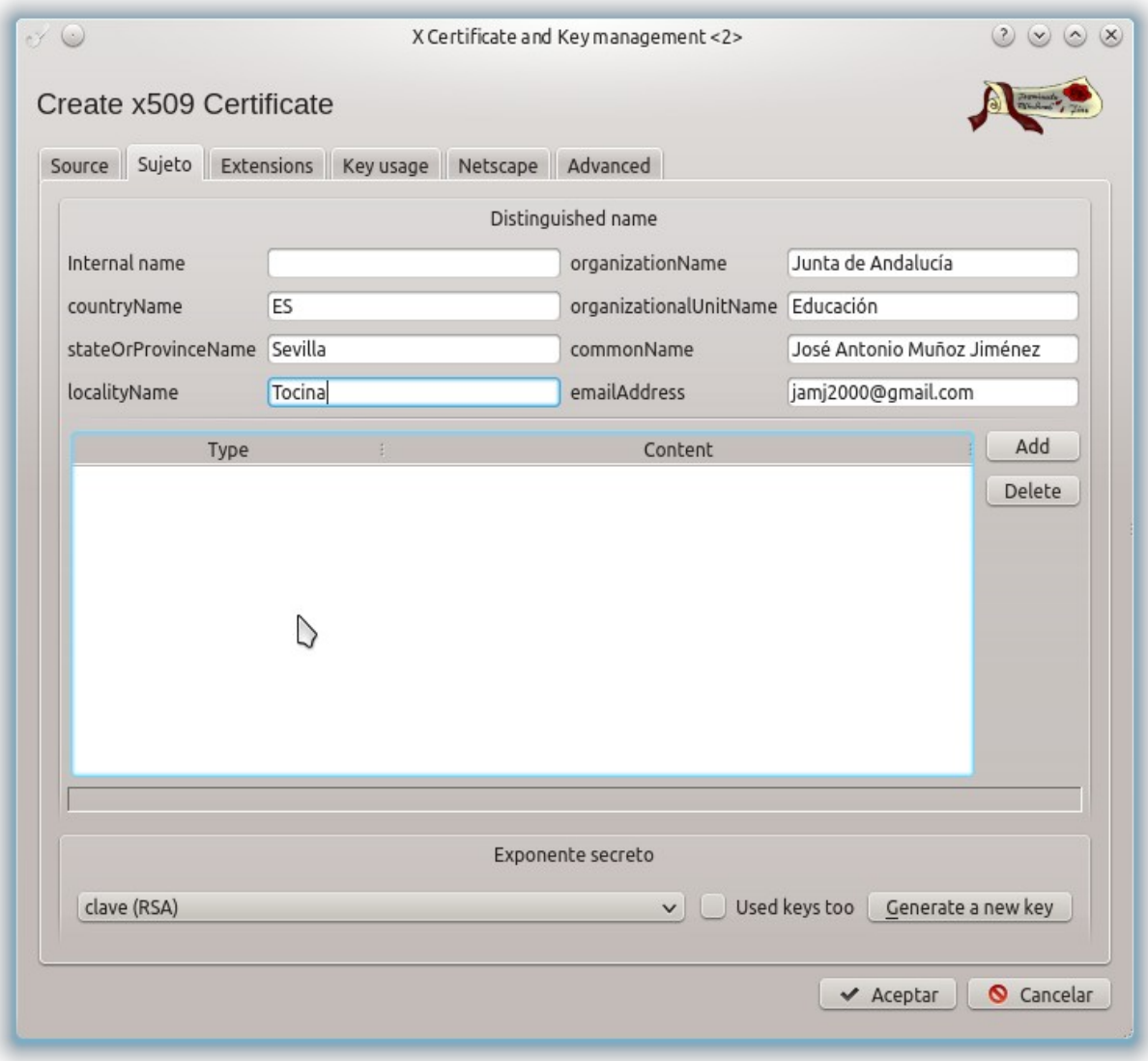
Para crear un certificado autofirmado procederemos de la siguiente forma:

Pulsamos en la pestaña “Certificates” y luego en el botón “New Certificate”.



En la pestaña “Source”, elegimos como plantilla “[default] HTTPS_server”.

A continuación en la pestaña “Sujeto” introducimos los datos del certificado y marcamos la clave que creamos anteriormente:

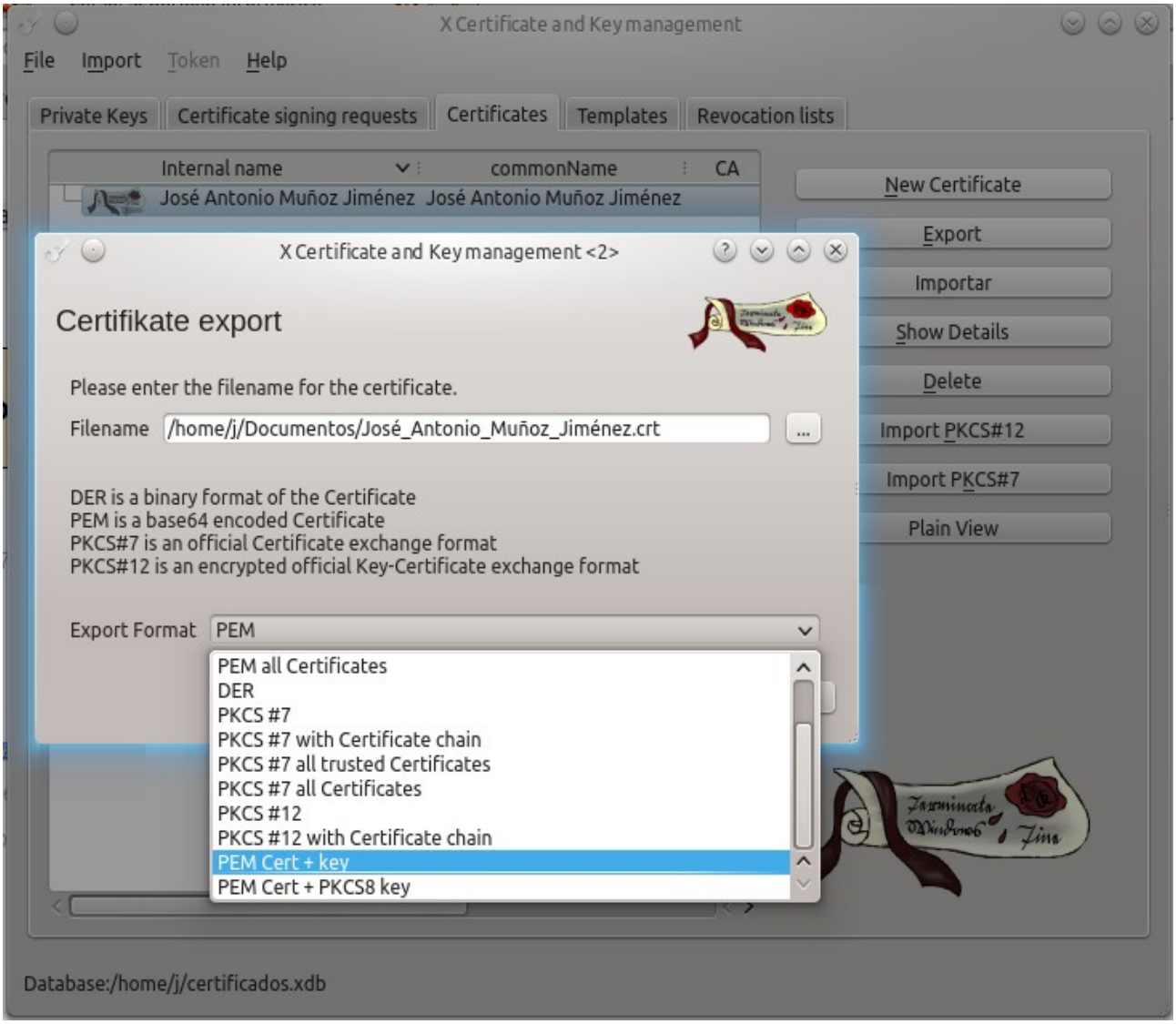


Por último, para que el servidor Apache pueda hacer uso de dicho certificado que tenemos guardado en nuestra base de datos vamos a exportarlo a un archivo.

Para ello nos vamos a la pestaña “Certificates” de la ventana principal y luego pulsamos en el botón “Export”.

En el formato elegimos “PEM Cert + key”.

Esto nos permitirá tener el certificado y la clave privada en un sólo archivo y la configuración del servidor será más sencilla.



Configuración de Apache 2

Seguimos los siguientes pasos:

1. Movemos el certificado creado anteriormente al directorio **/etc/ssl/certs**

2. Editamos el archivo /etc/apache2/sites-available/default-ssl

```
#   /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile    /etc/ssl/certs/José_Antonio_Muñoz_Jiménez.crt
# SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

3. Desde un terminal de texto, con permisos de administrador (root), habilitamos el módulo SSL de apache:

a2enmod ssl

4. A continuación, habilitamos el sitio seguro:

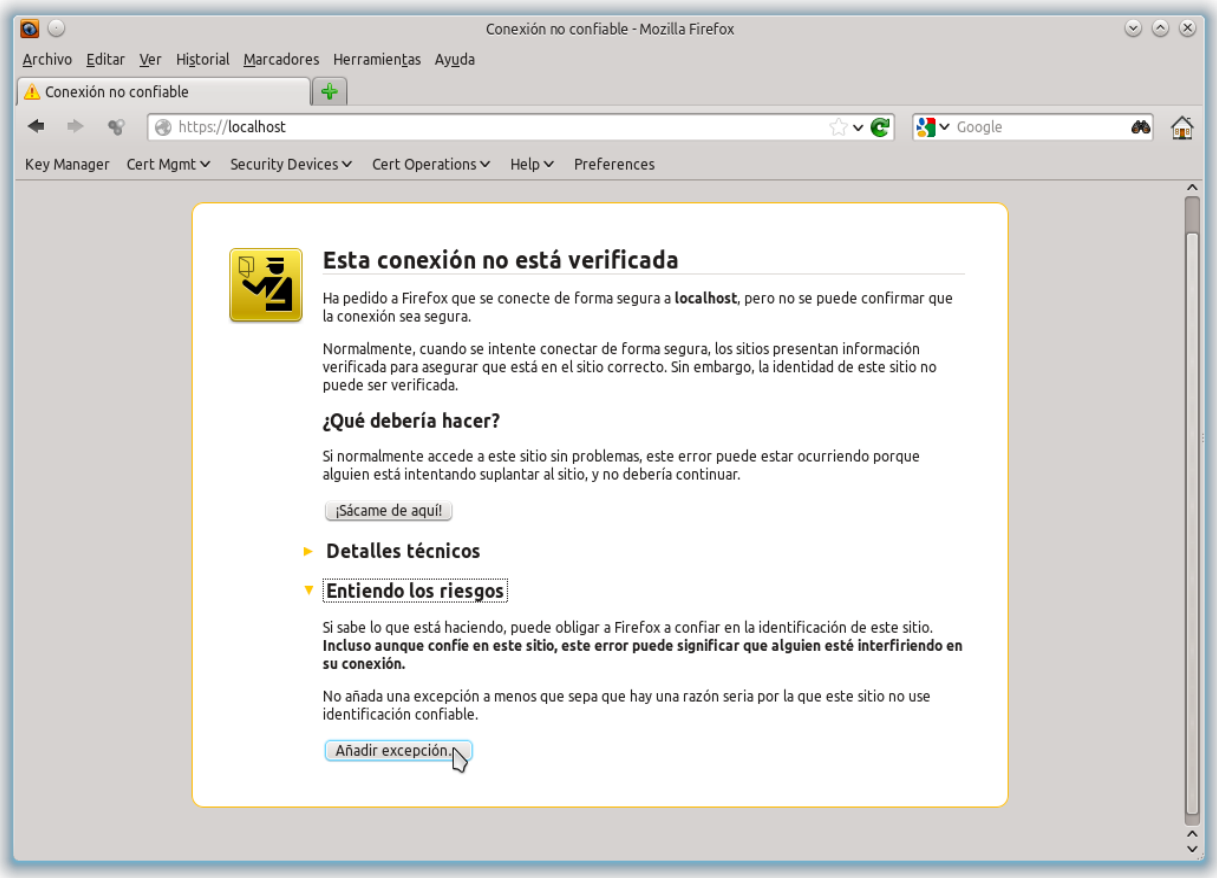
a2ensite default-ssl

5. Y finalmente reiniciamos el servidor web apache:

/etc/init.d/apache2 restart

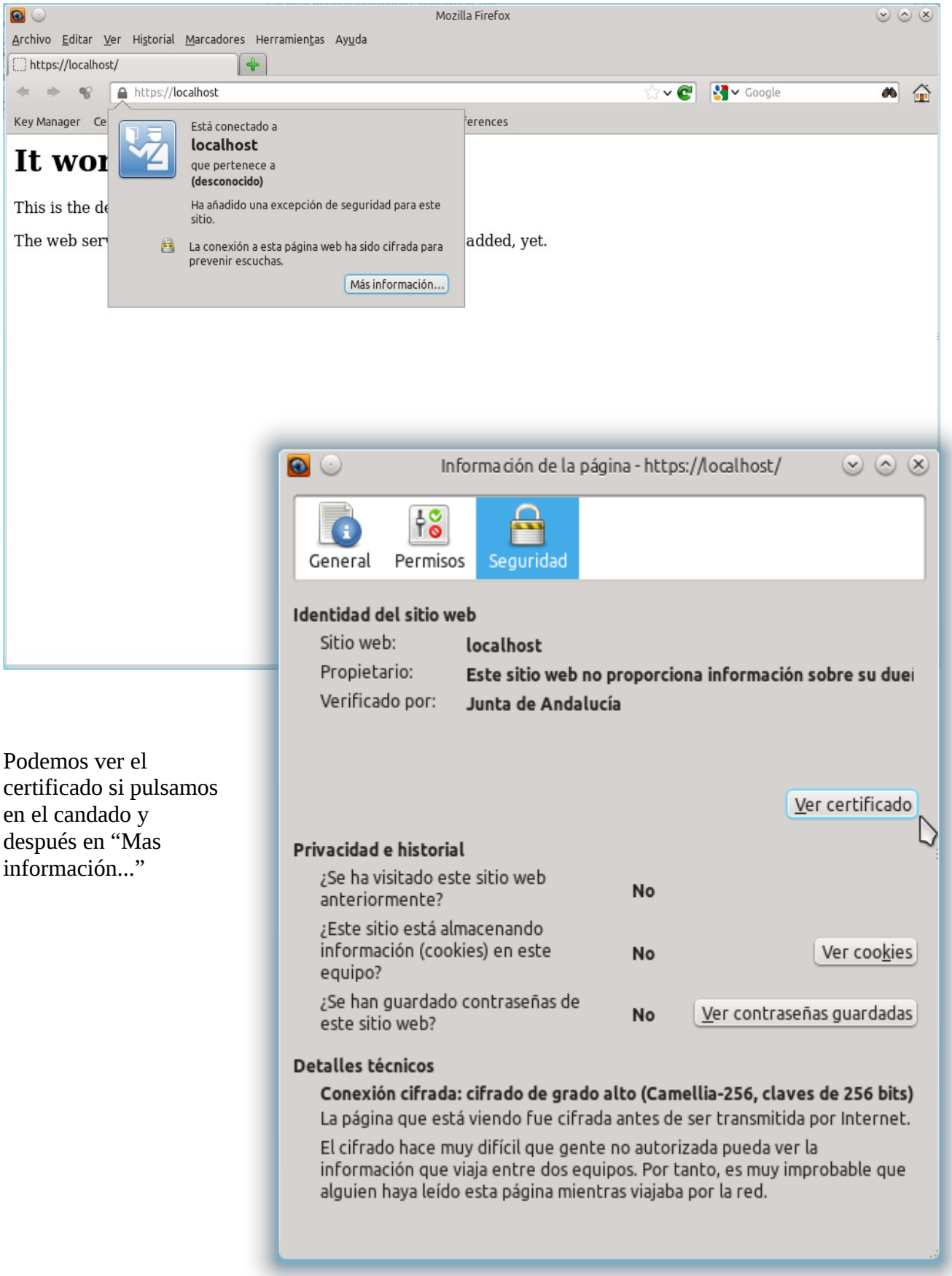
Comprobamos el correcto funcionamiento

Abrimos el navegador y vamos a la URL **https://localhost**

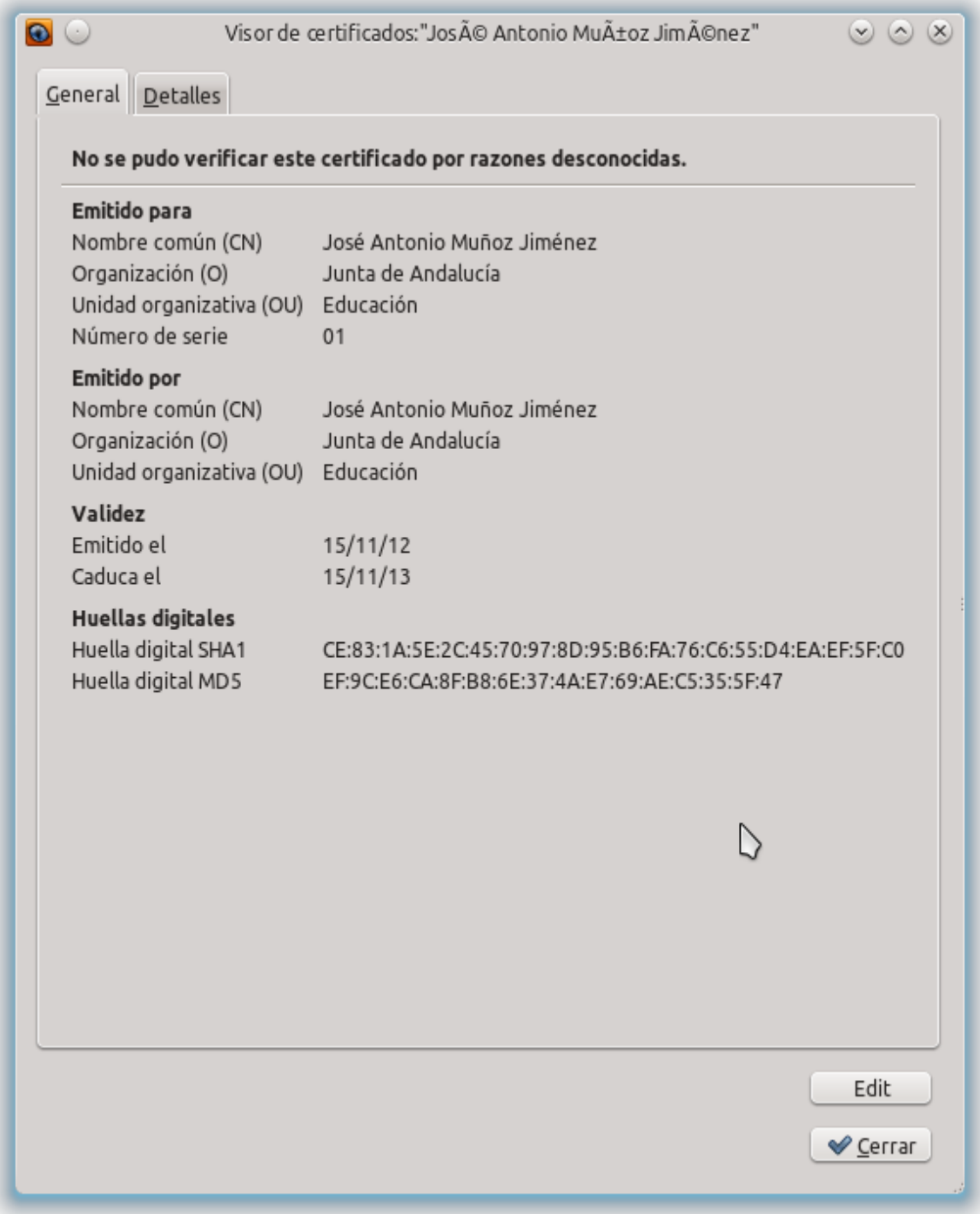


Pulsamos en “Entiendo los riesgos” y después en “Añadir excepción”.

A continuación pulsamos en “Confirmar excepción de seguridad”.



Podemos ver el certificado si pulsamos en el candado y después en “Mas información...”


Visor de certificados:"JosÃ© Antonio MuÃ±oz JimÃ©nez"
General
Detalles
No se pudo verificar este certificado por razones desconocidas.
Emitido para
Nombre común (CN) José Antonio Muñoz Jiménez
Organización (O) Junta de Andalucía
Unidad organizativa (OU) Educación
Número de serie 01
Emitido por
Nombre común (CN) José Antonio Muñoz Jiménez
Organización (O) Junta de Andalucía
Unidad organizativa (OU) Educación
Validez
Emitido el 15/11/12
Caduca el 15/11/13
Huellas digitales
Huella digital SHA1 CE:83:1A:5E:2C:45:70:97:8D:95:B6:FA:76:C6:55:D4:EA:EF:5F:C0
Huella digital MD5 EF:9C:E6:CA:8F:B8:6E:37:4A:E7:69:AE:C5:35:5F:47
Edit
Cerrar