Seguridad de la Información

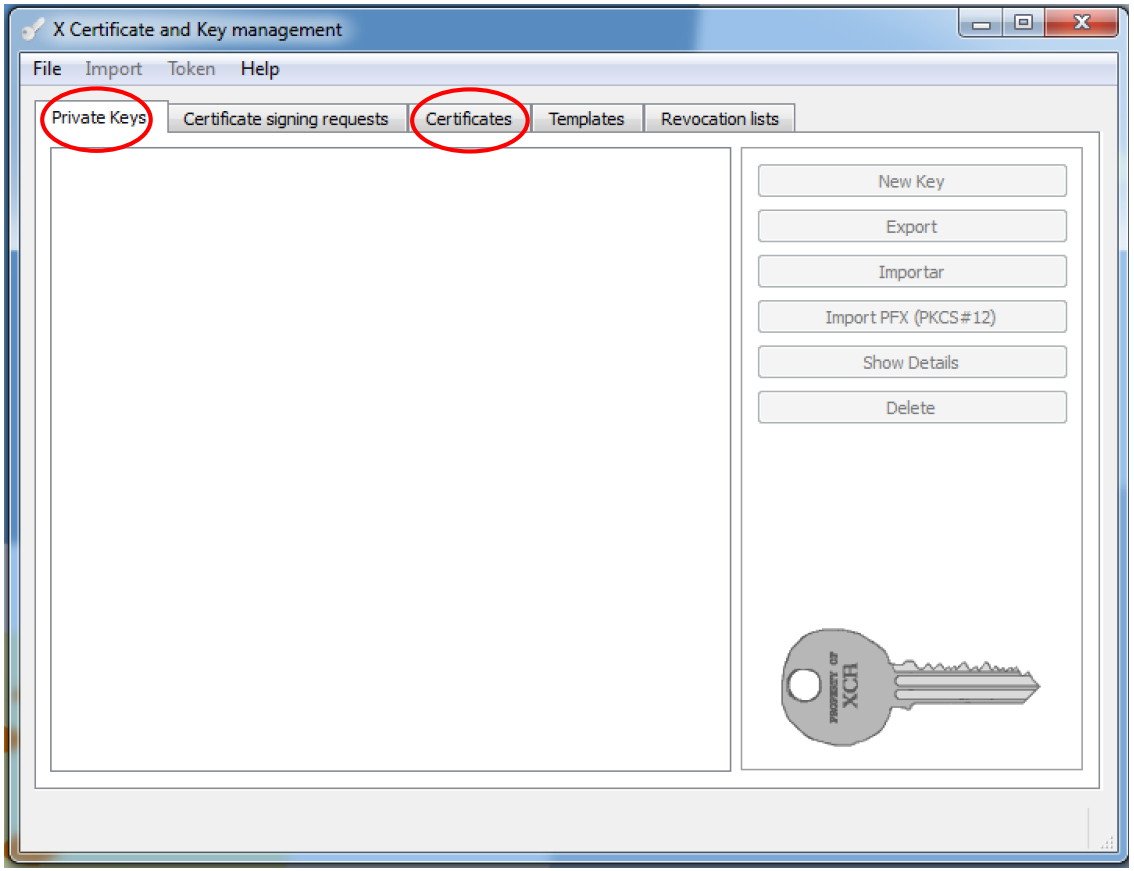
Transparencias de apoyo

XCA

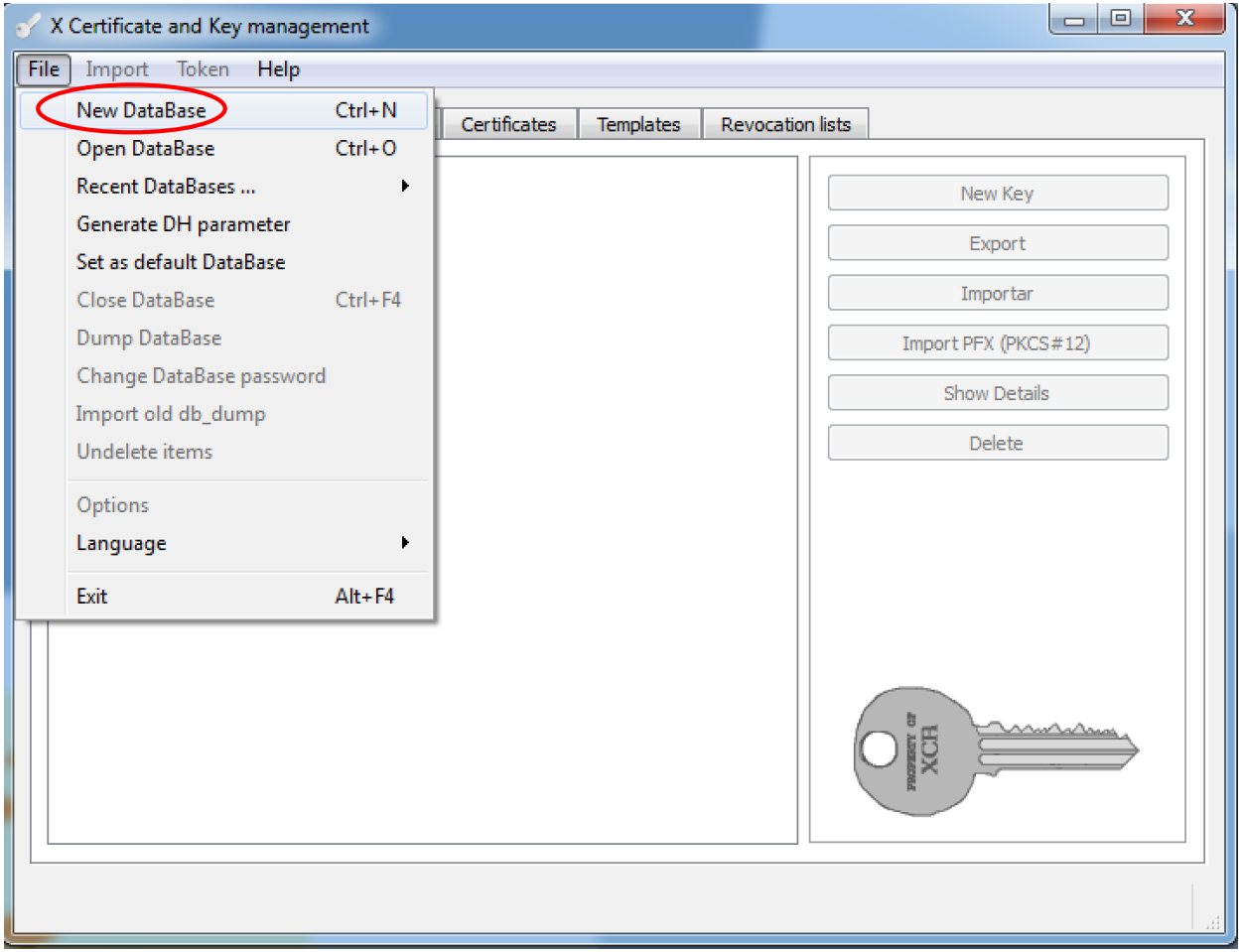
https://hohnstaedt.de/xca/

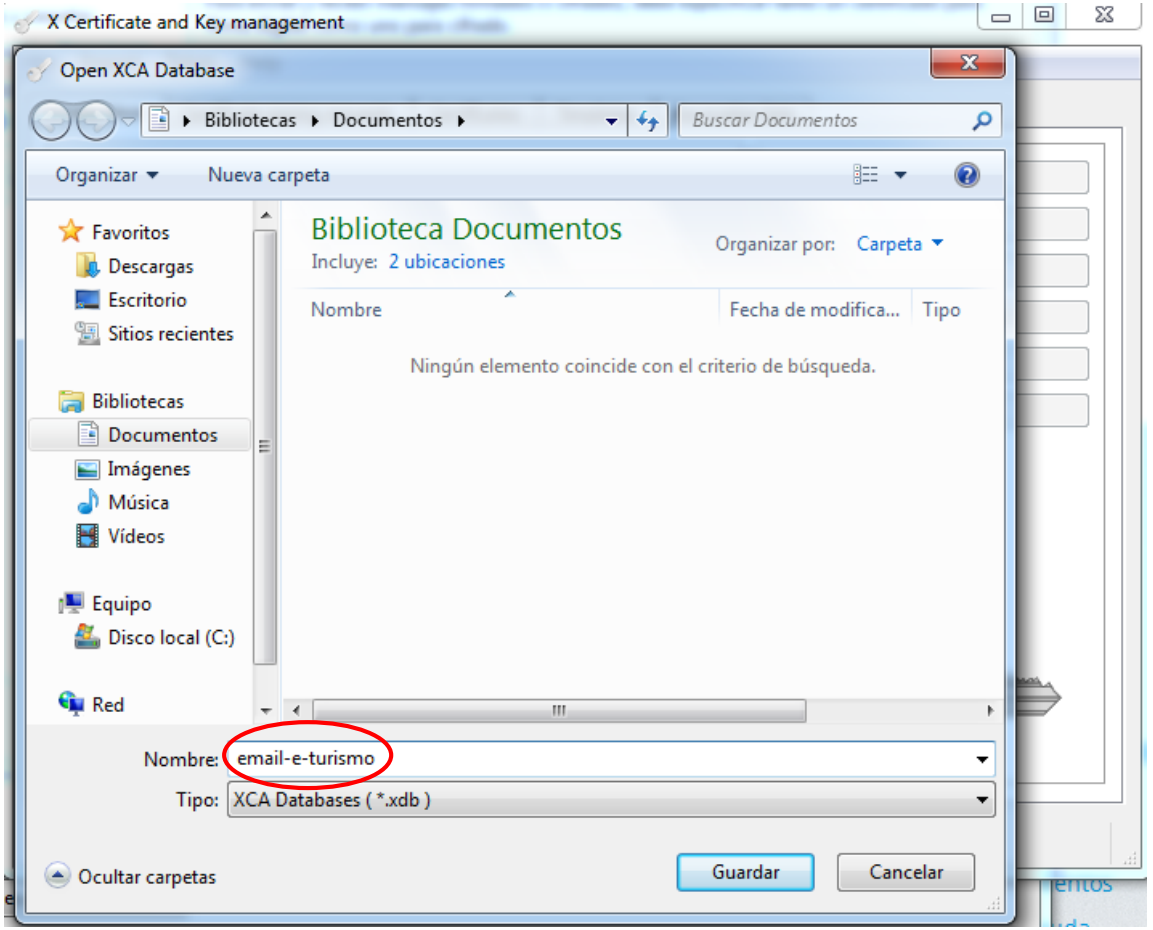
XCA – Inicio del programa

- Para empezar a usar el programa, hay que crear una base de datos donde se guardarán los certificados y las claves privadas

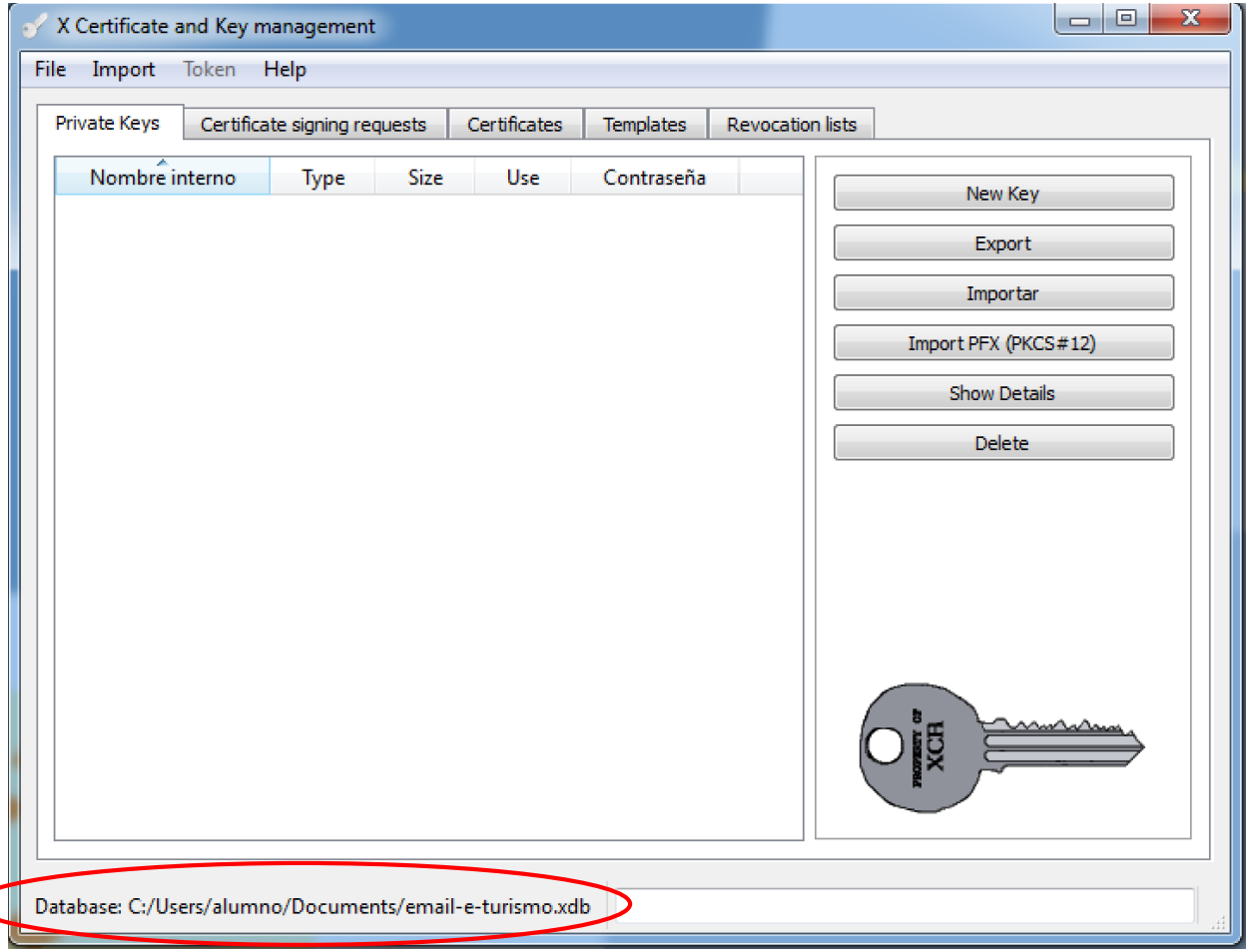


- Comenzamos la generación de la base de datos de XCA



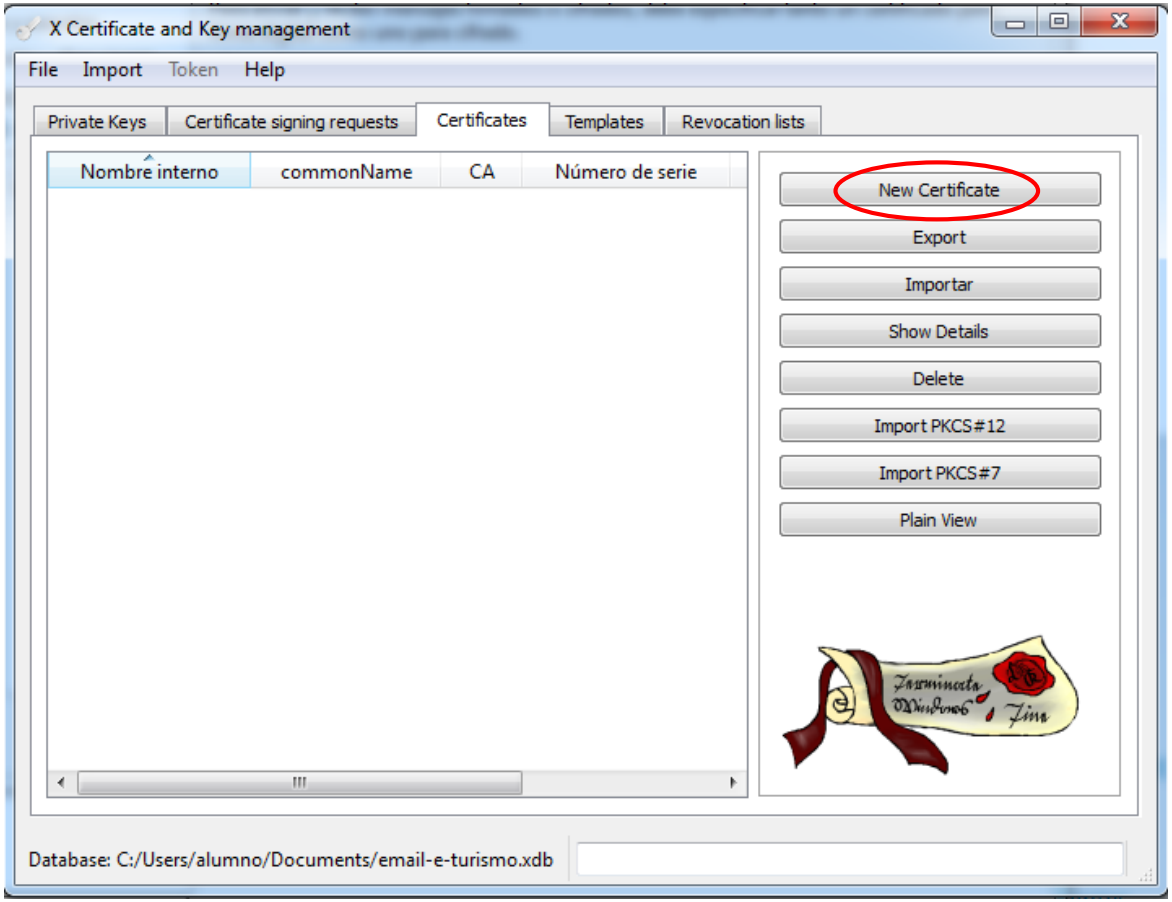

X Certificate and Key management
Open XCA Database
Bibliotecas ▸ Documentos ▸
Buscar Documentos
Organizar
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Documentos
Imágenes
Música
Vídeos
Equipo
Disco local (C:)
Red
Biblioteca Documentos
Incluye: 2 ubicaciones
Organizar por: Carpeta
Nombre
Fecha de modifica...
Tipo
Ningún elemento coincide con el criterio de búsqueda.
Nombre: email-e-turismo
Tipo: XCA Databases (*.xdb)
Ocultar carpetas
Guardar
Cancelar

- Ahora las opciones del menú de la derecha ya se pueden utilizar

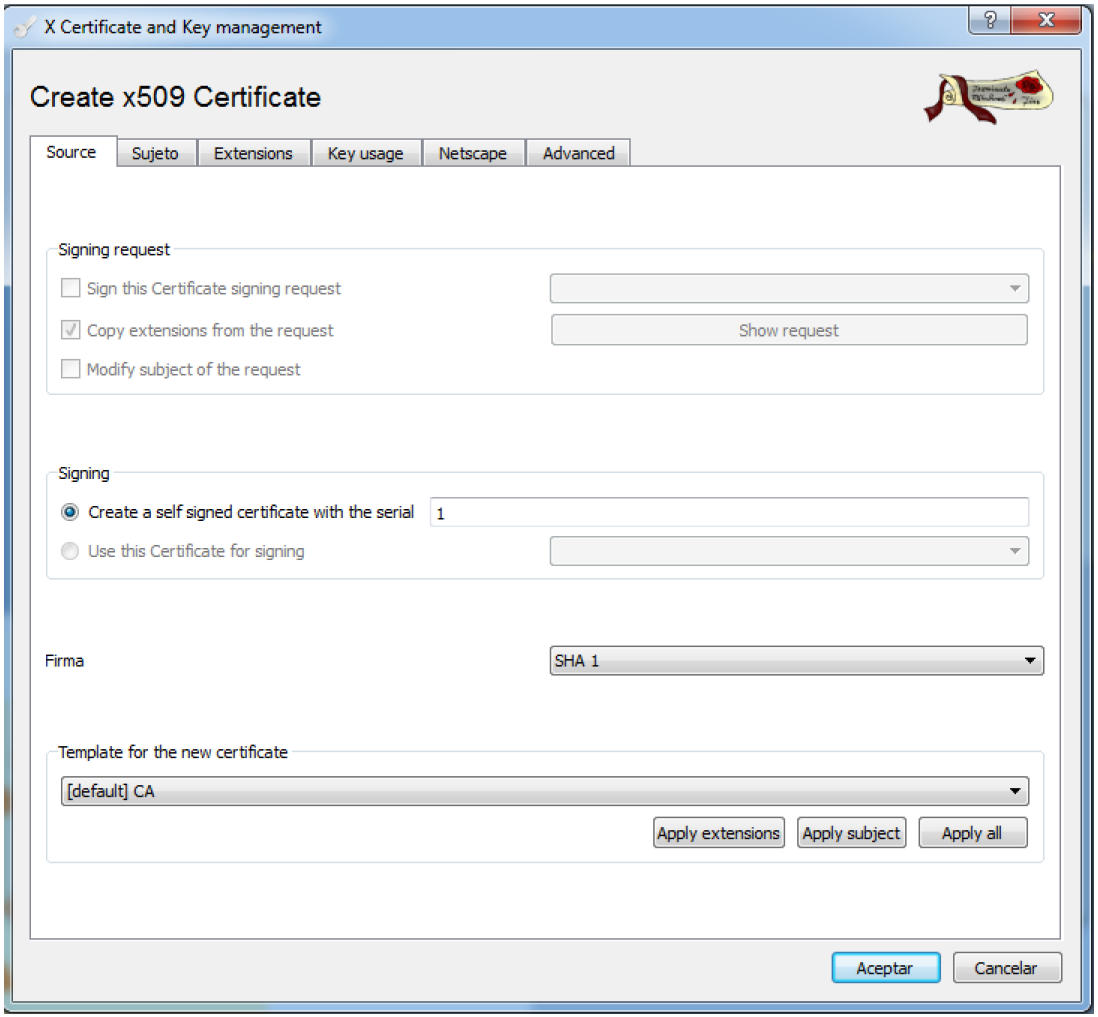


XCA – Generar Certificados

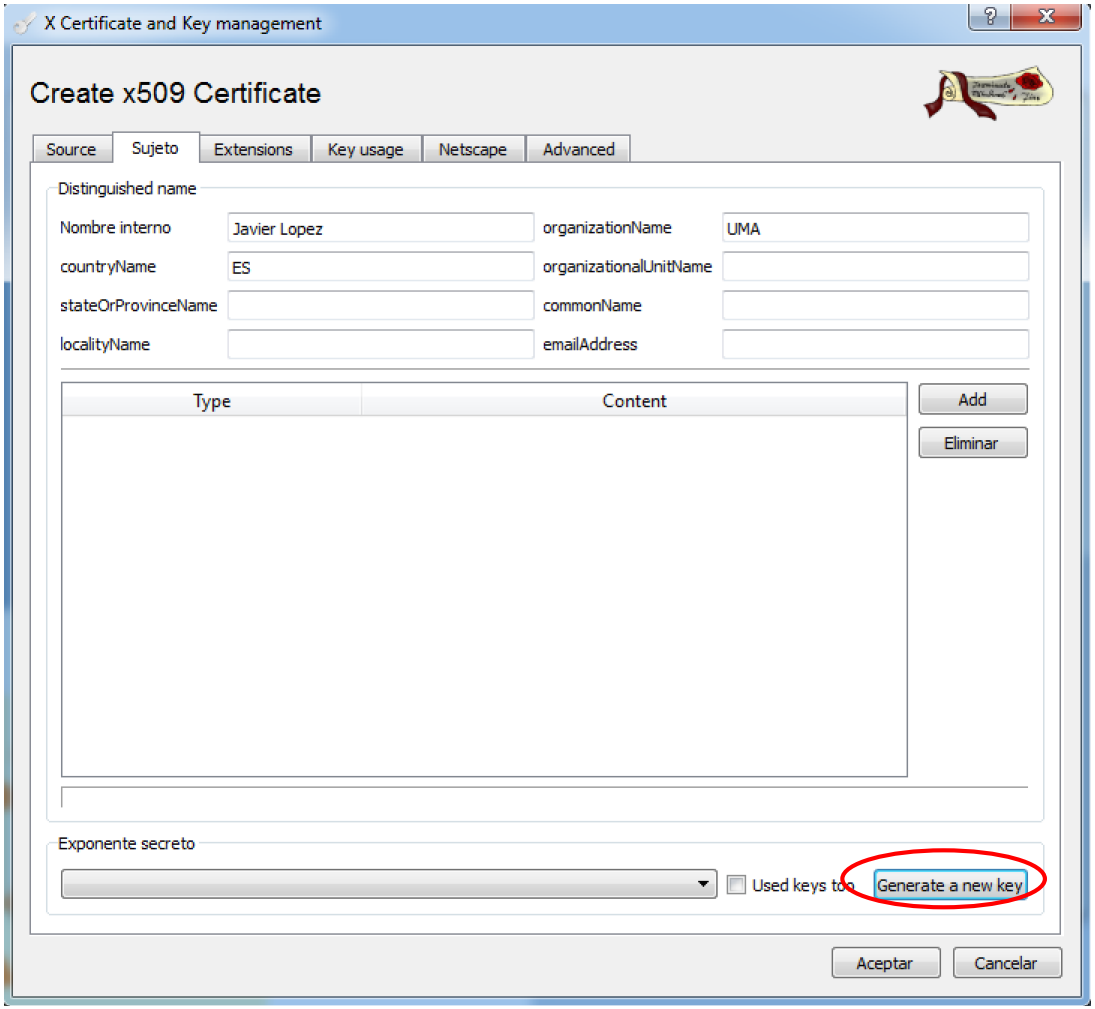
- Pestaña “Certificates” – ‘New Certificate’

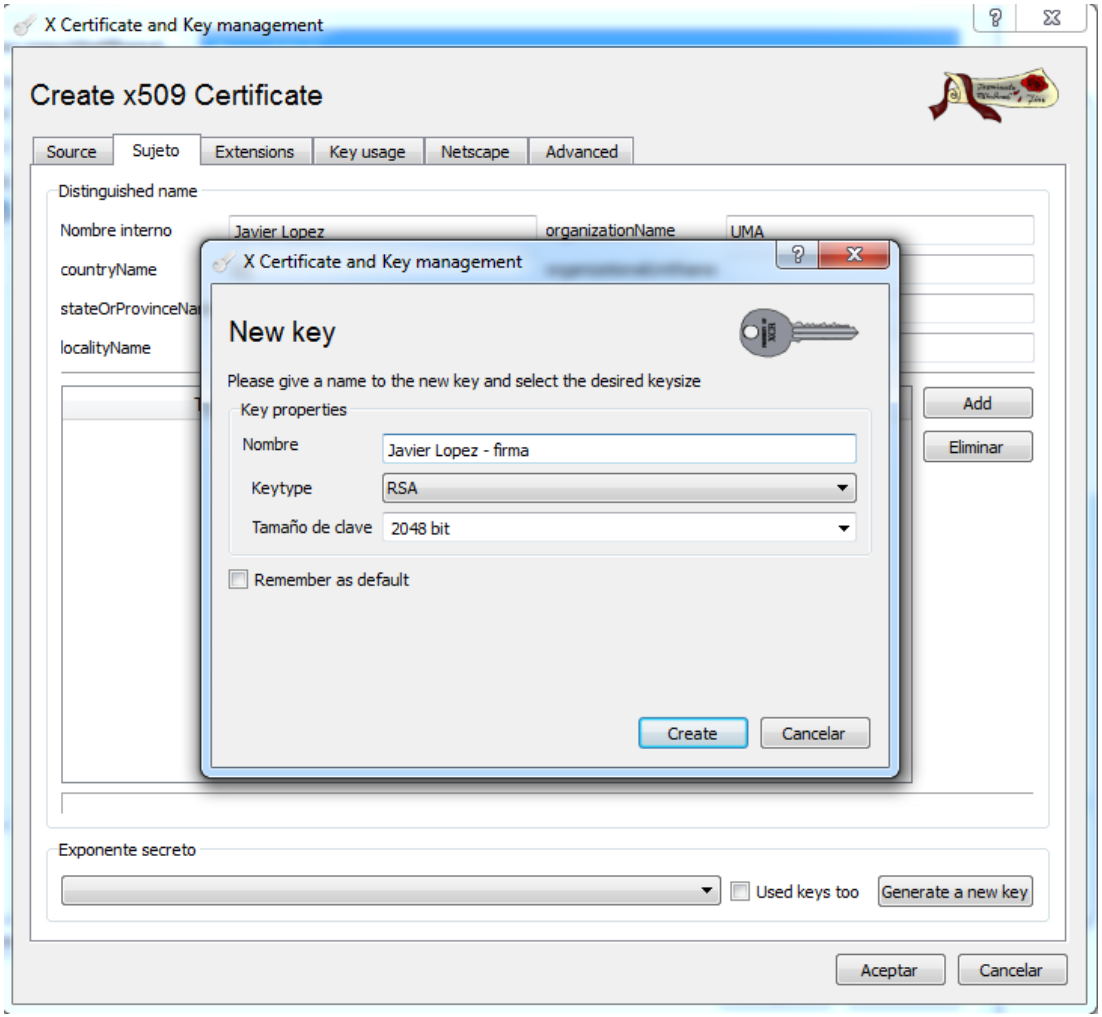


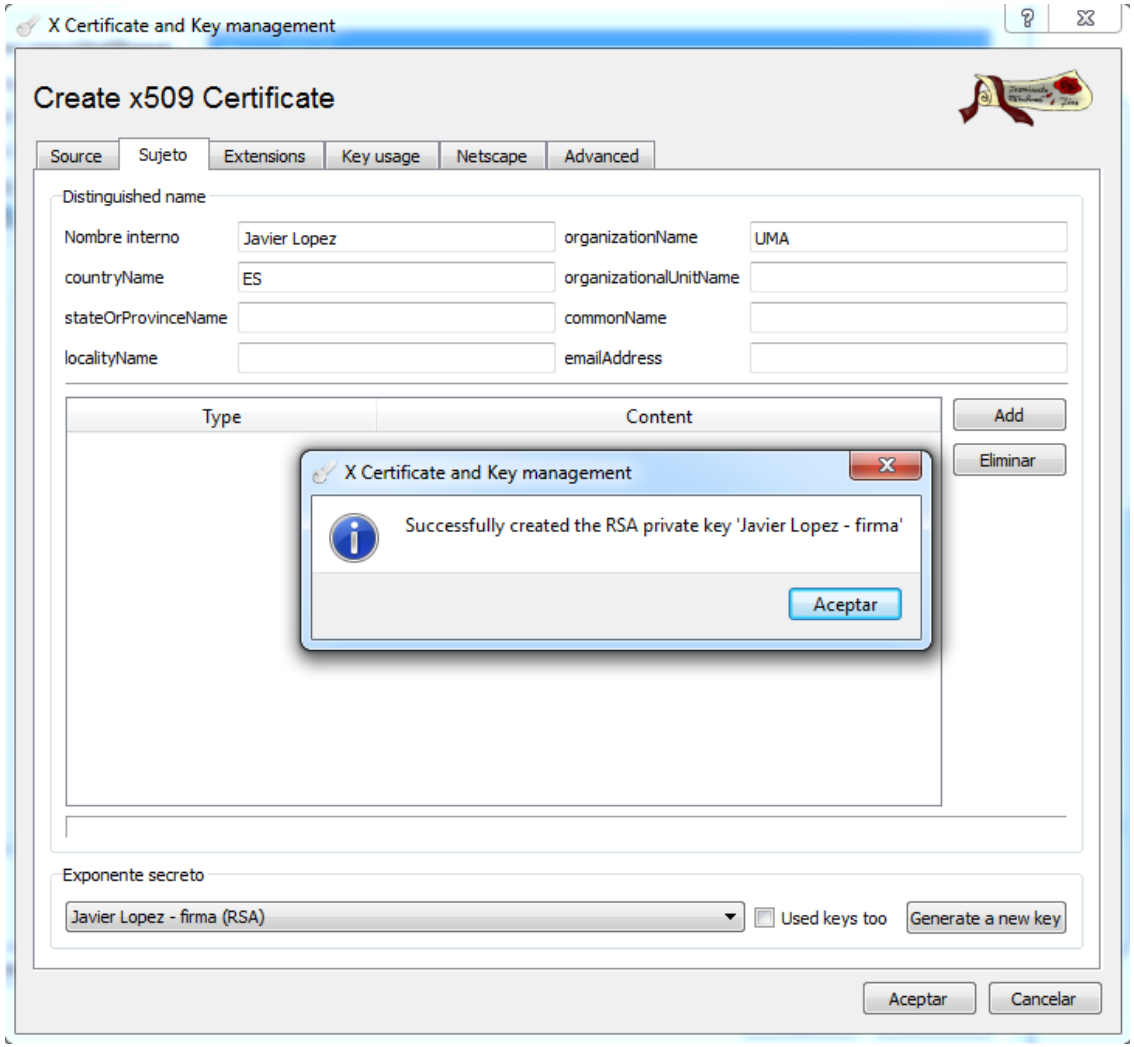
- Pestaña “Source” (quién firma este certificado)



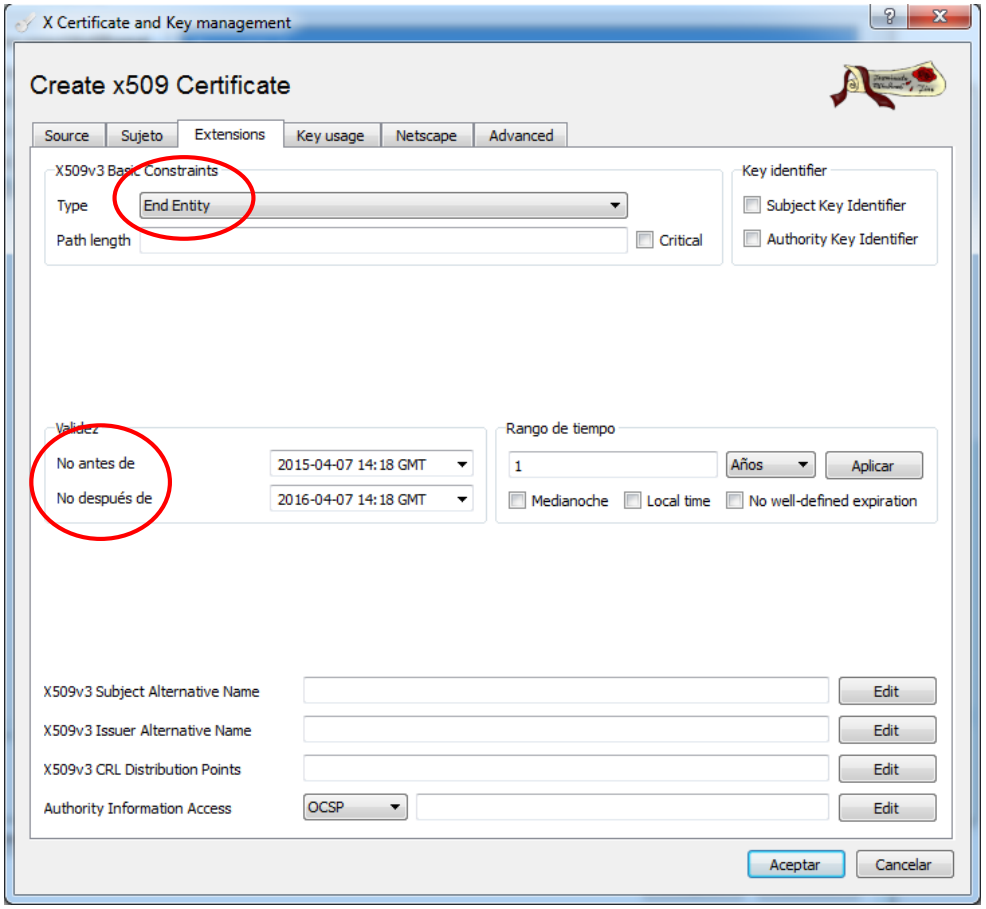
- Pestaña Sujeto/Subject (Info sujeto, clave privada)



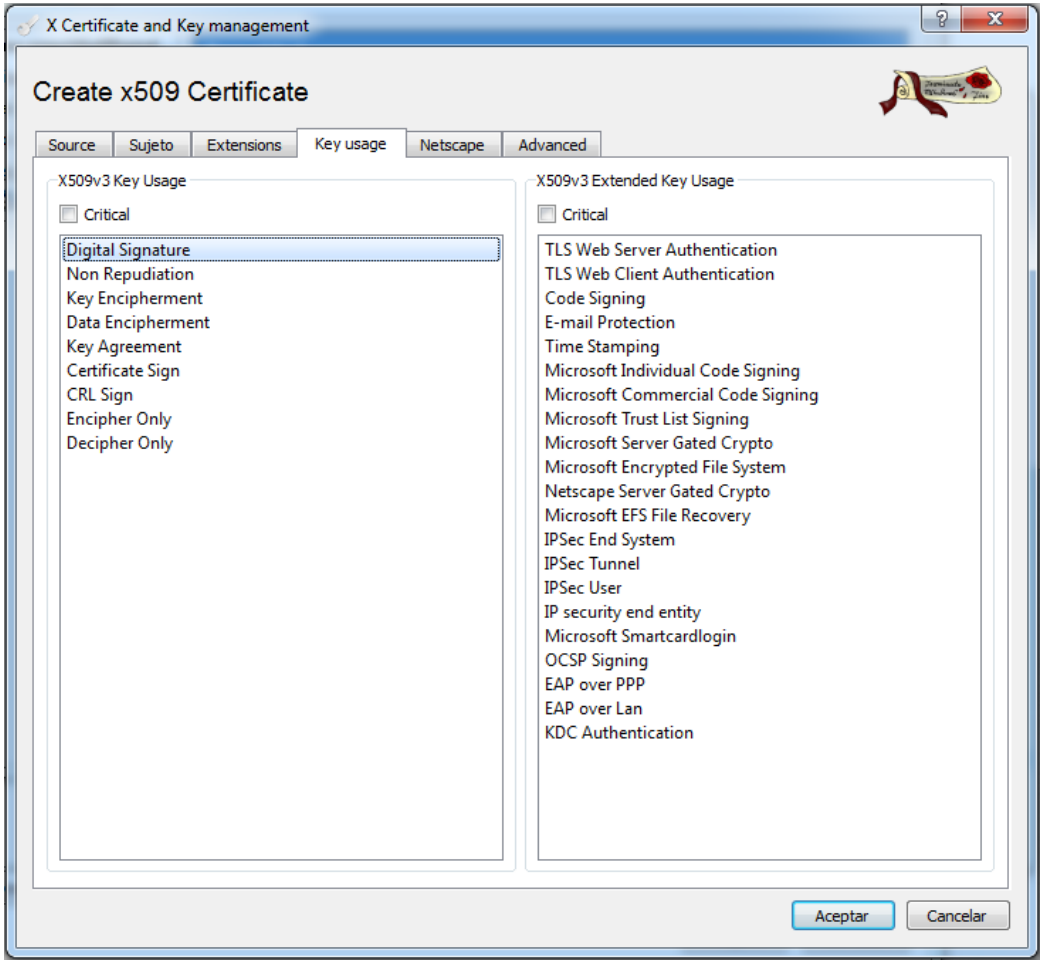

X Certificate and Key management
Create x509 Certificate
Source
Sujeto
Extensions
Key usage
Netscape
Advanced
Distinguished name
Nombre interno
Javier Lopez
organizationName
UMA
countryName
stateOrProvinceNa
localityName
Add
Eliminar
Exponente secreto
Used keys too
Generate a new key
Aceptar
Cancelar
X Certificate and Key management
New key
Please give a name to the new key and select the desired keysize
Key properties
Nombre
Javier Lopez - firma
Keytype
RSA
Tamaño de clave
2048 bit
Remember as default
Create
Cancelar


X Certificate and Key management
Create x509 Certificate
Source
Sujeto
Extensions
Key usage
Netscape
Advanced
Distinguished name
Nombre interno
Javier Lopez
organizationName
UMA
countryName
ES
organizationalUnitName
stateOrProvinceName
commonName
localityName
emailAddress
Type
Content
Add
Eliminar
X Certificate and Key management
Successfully created the RSA private key 'Javier Lopez - firma'
Aceptar
Exponente secreto
Javier Lopez - firma (RSA)
Used keys too
Generate a new key
Aceptar
Cancelar

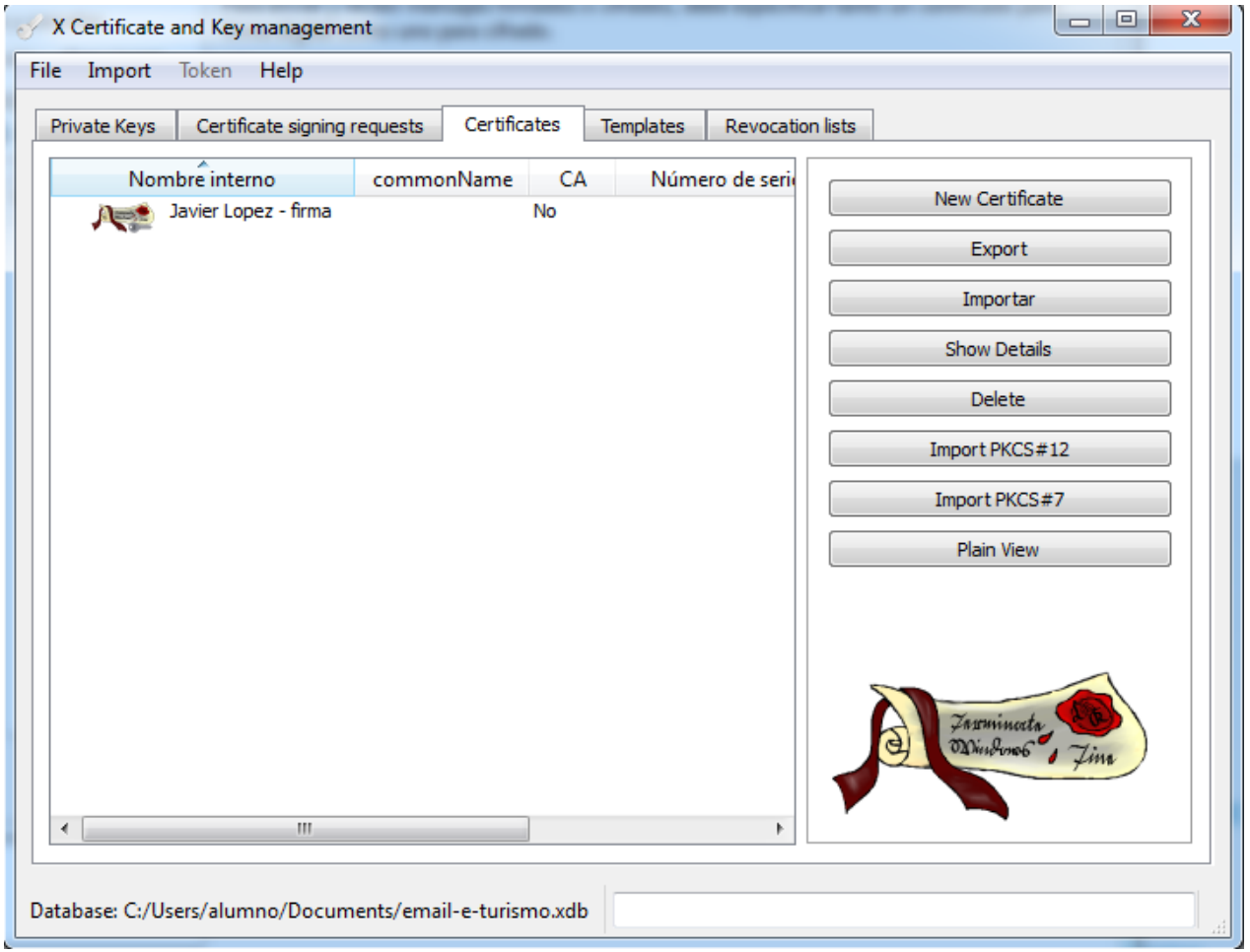
- Pestaña extensions (Tipo de Certificado, Caducidad)



- Pestaña “Key Usage” (extensiones: Uso del certificado)

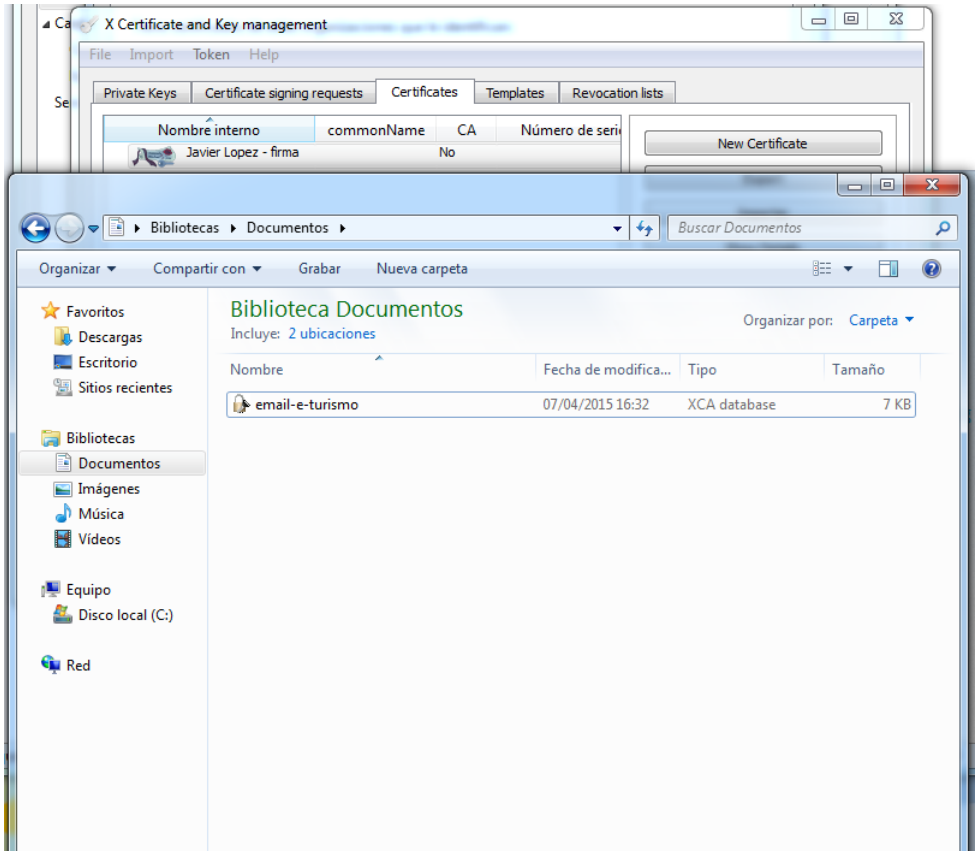


- … y ya hemos creado el certificado para firma digital

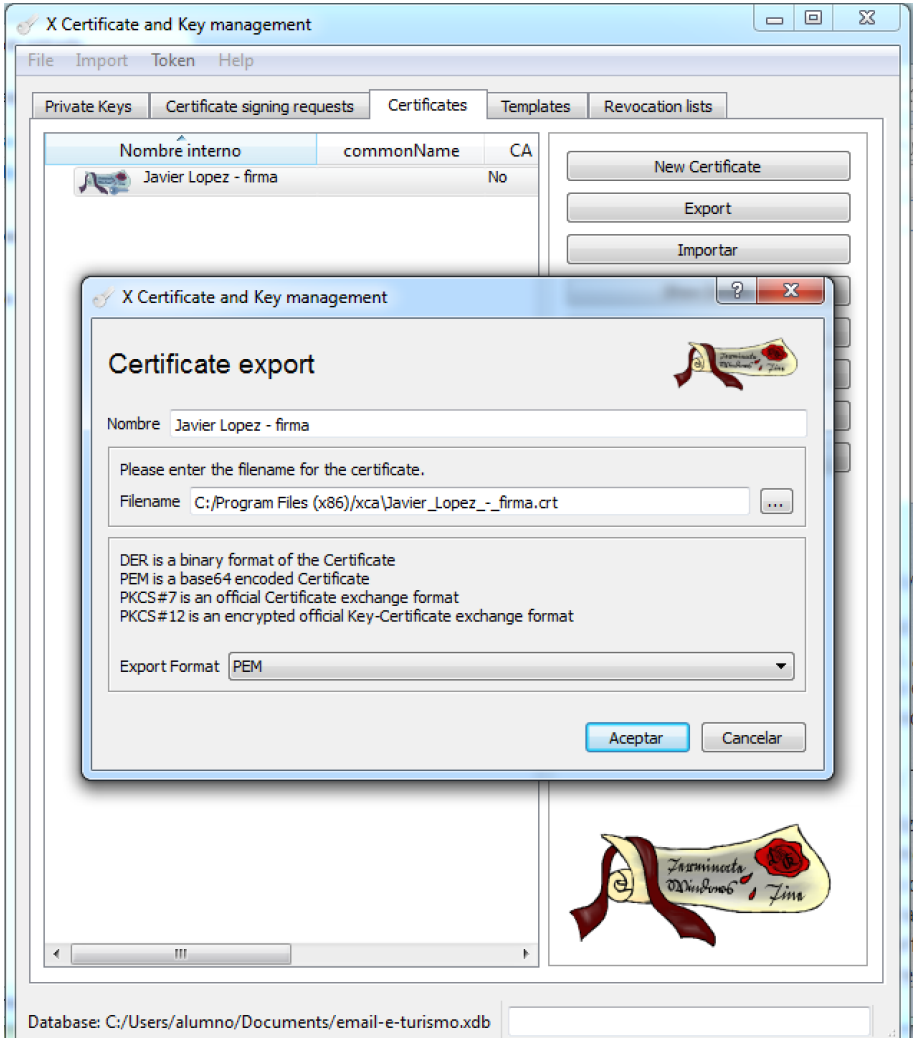


XCA – Exportar certificado

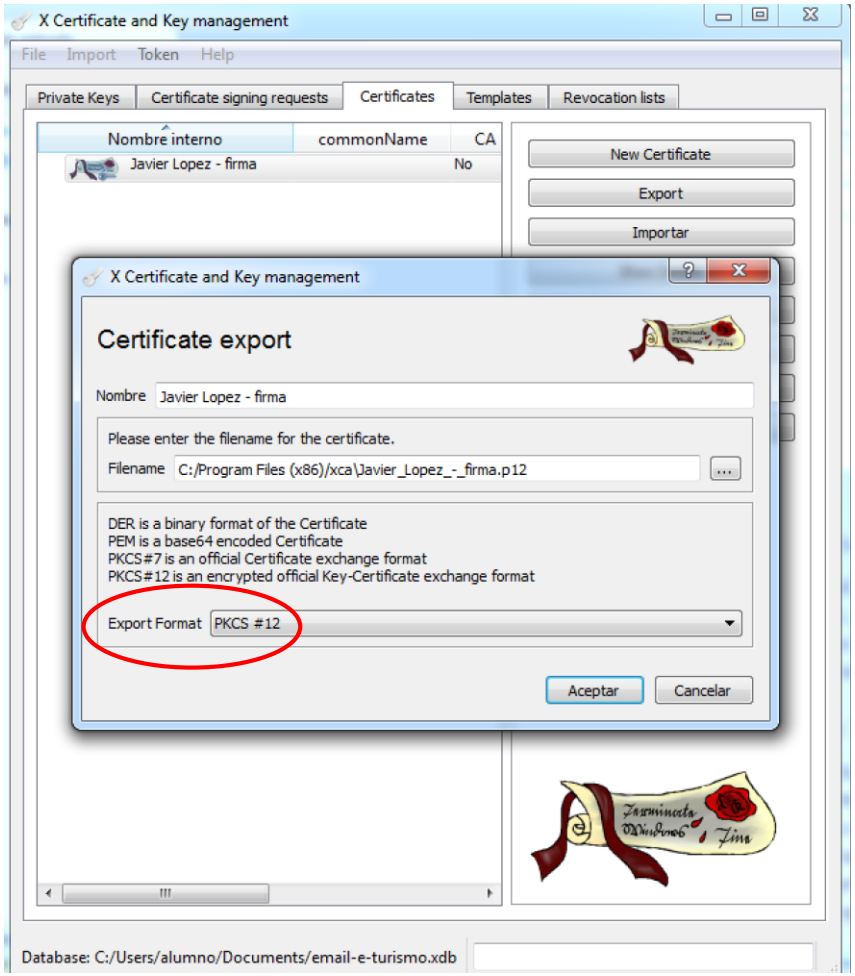
- El certificado está creado sólo en la base de datos de XCA, y es necesario exportarlo



- Botón “Export”



- Formato (visto en las transparencias de las prácticas)



- Contraseña con la que guardar el certificado