

# SEGURIDAD DE LA INFORMACIÓN

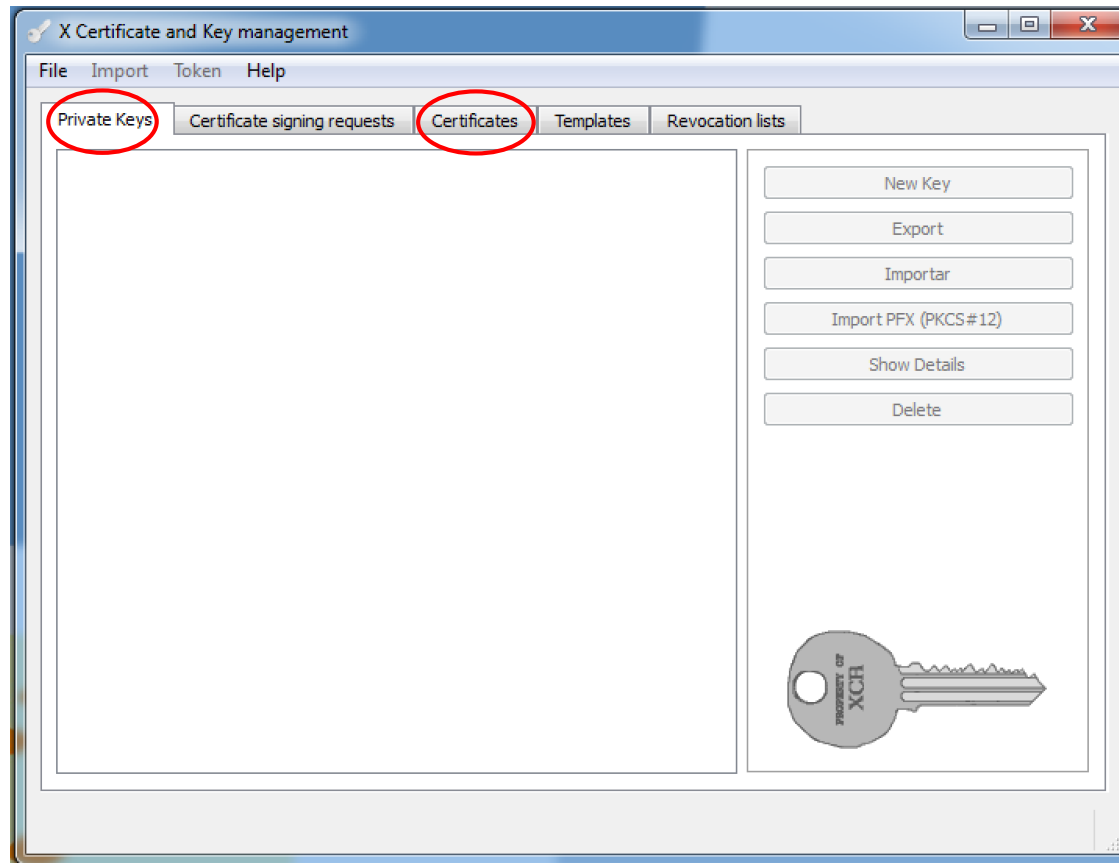
Transparencias de apoyo

**XCA**

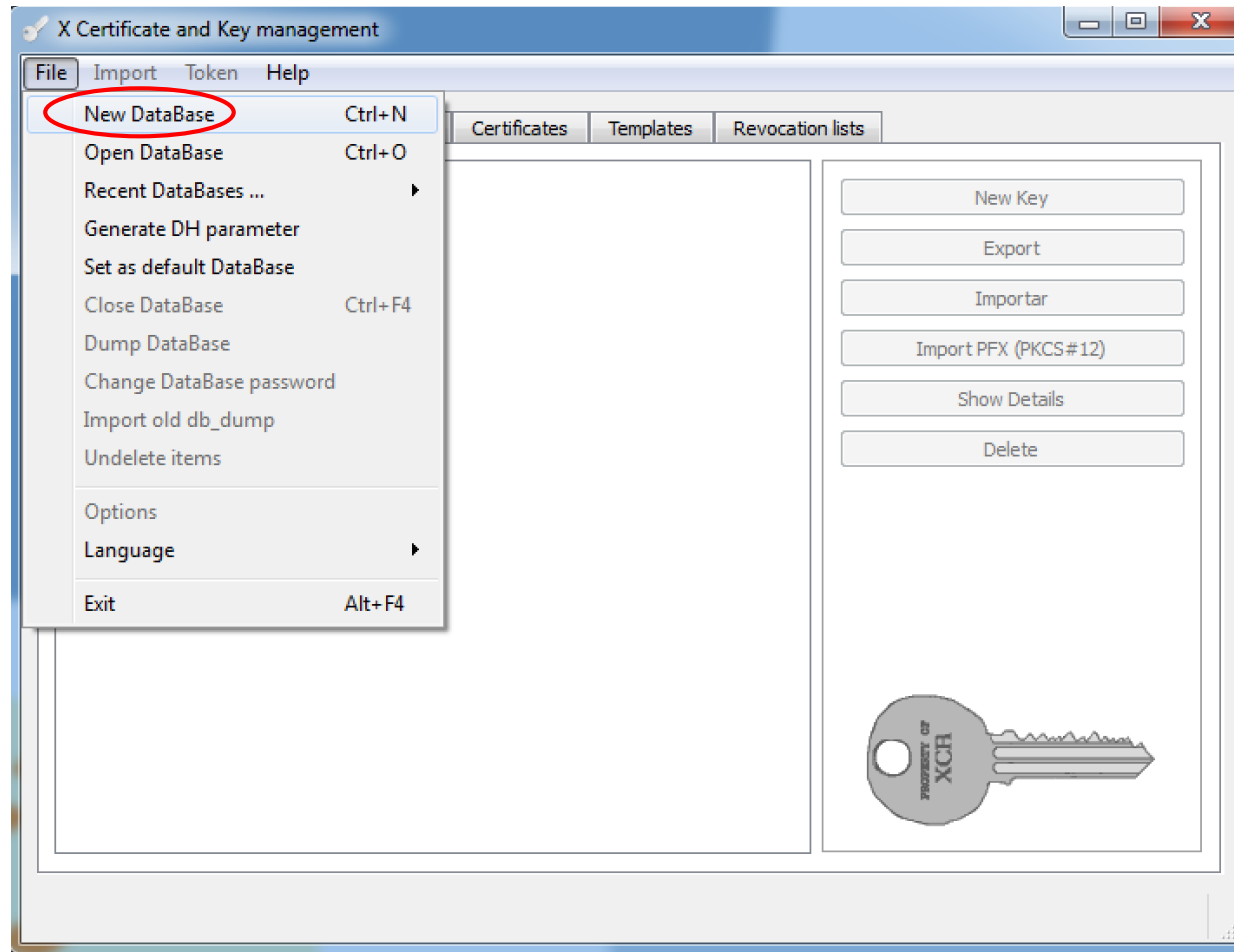
<https://hohnstaedt.de/xca/>

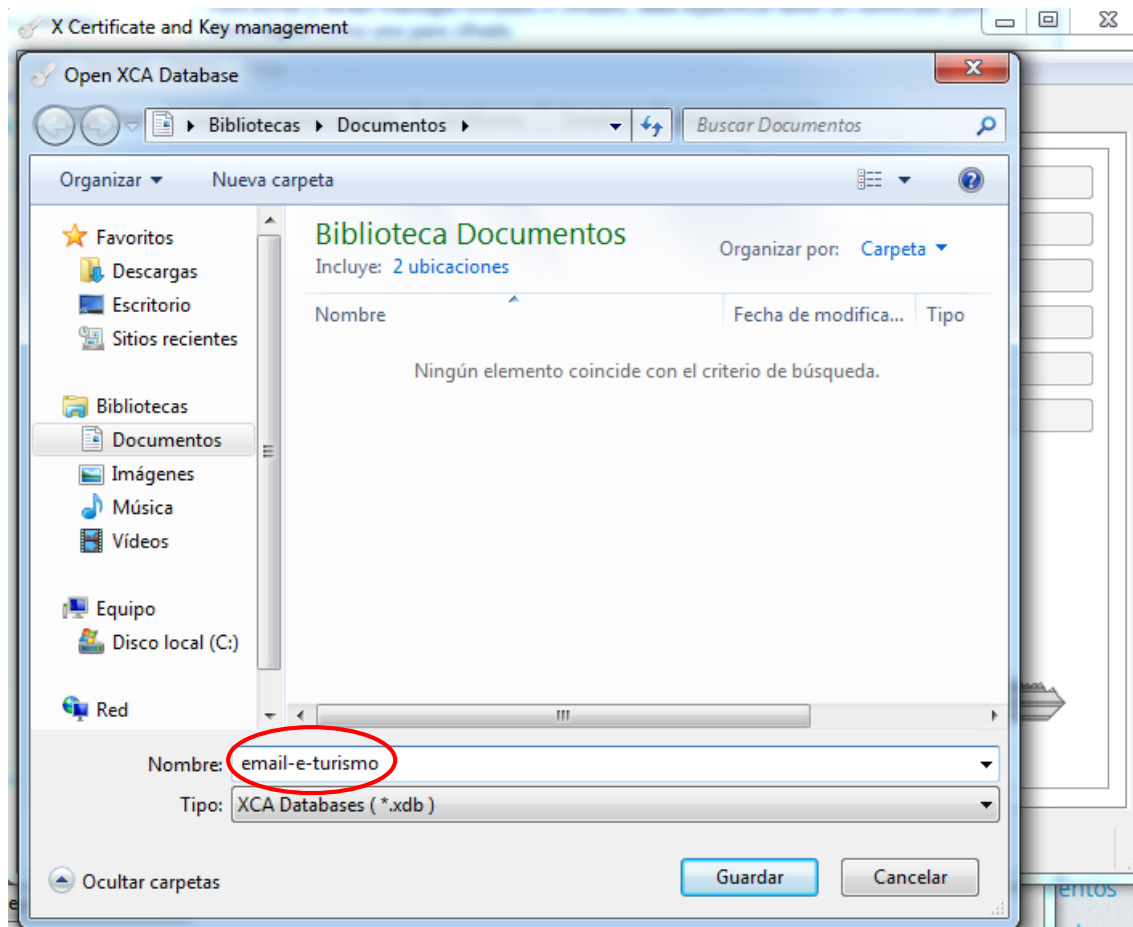
# XCA – Inicio del programa

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

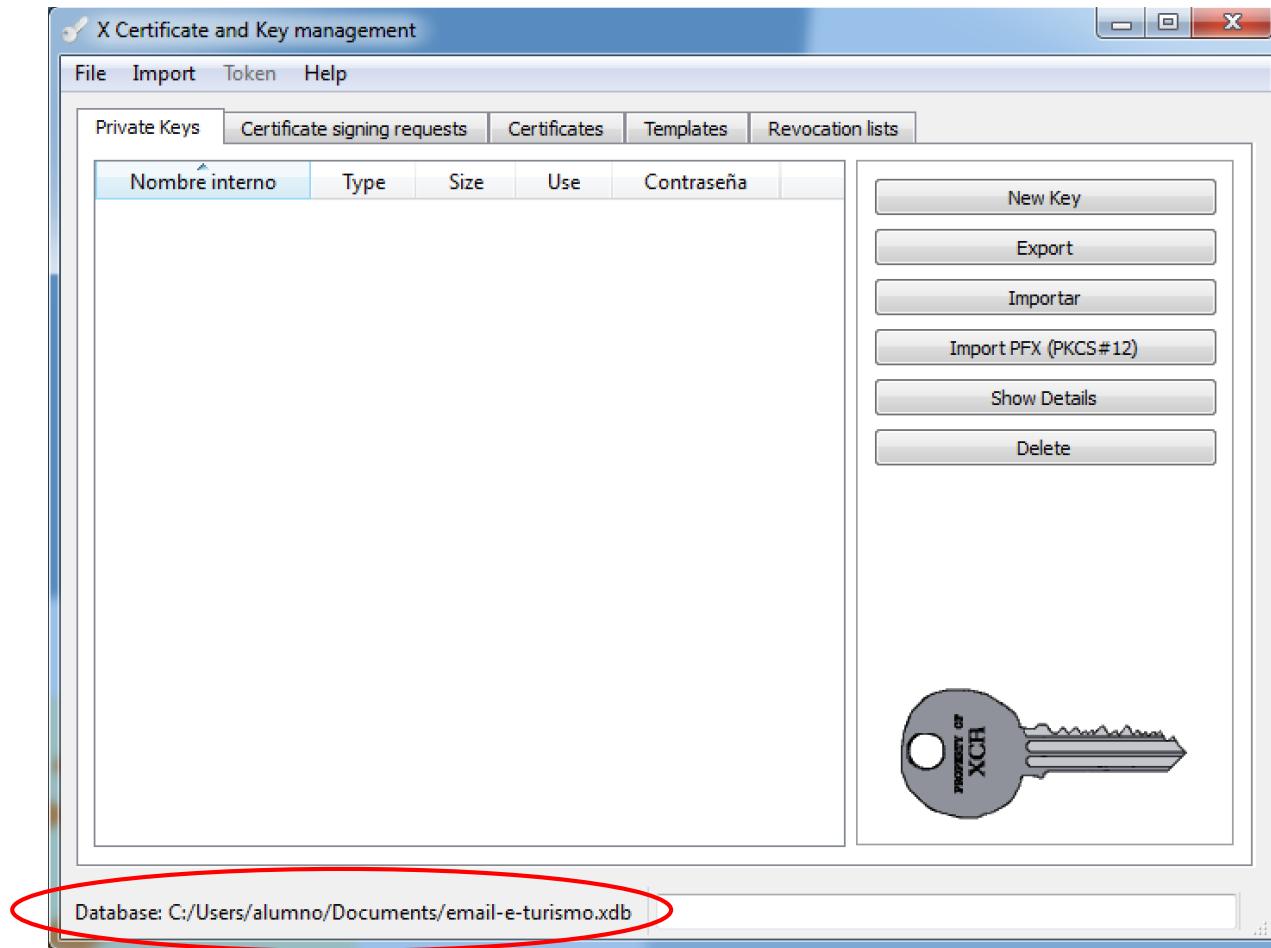


- Comenzamos la generación de la base de datos de XCA



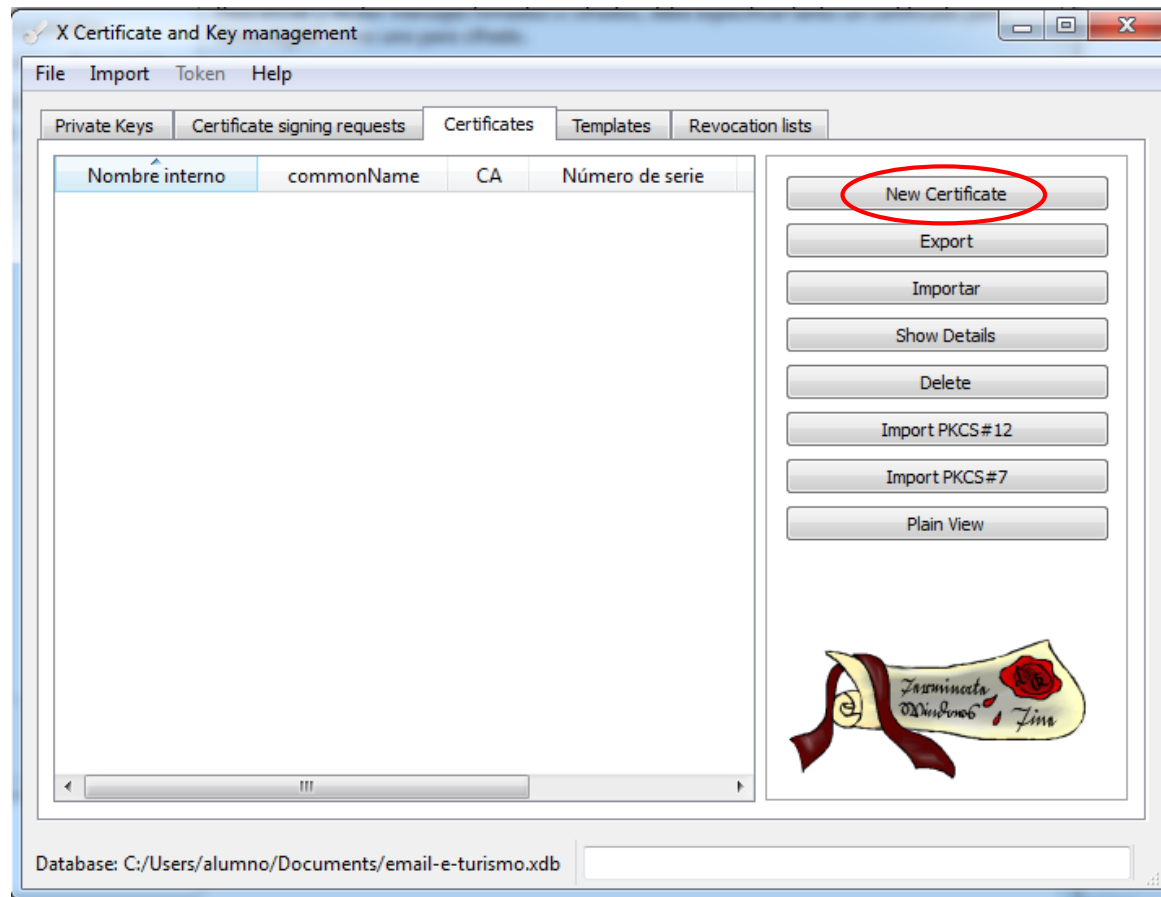


- Ahora las opciones del menú de la derecha ya se pueden utilizar



# XCA – Generar Certificados

- Pestaña “Certificates” – ‘New Certificate’



- Pestaña “Source” (quién firma este certificado)

The screenshot shows a window titled "X Certificate and Key management" with a sub-header "Create x509 Certificate". The window has a ribbon-style tab bar with the following tabs: "Source", "Sujeto", "Extensions", "Key usage", "Netscape", and "Advanced". The "Source" tab is currently selected. Inside the "Source" tab, there are three main sections:

- Signing request:** Contains three checkboxes: "Sign this Certificate signing request" (unchecked), "Copy extensions from the request" (checked), and "Modify subject of the request" (unchecked). To the right of these checkboxes is a dropdown menu and a "Show request" button.
- Signing:** Contains two radio buttons: "Create a self signed certificate with the serial" (selected) and "Use this Certificate for signing" (unselected). The first radio button is followed by a text field containing the number "1". The second radio button is followed by a dropdown menu.
- Firma:** Contains a dropdown menu currently set to "SHA 1".

At the bottom of the "Source" tab, there is a section titled "Template for the new certificate" with a dropdown menu set to "[default] CA". Below this dropdown are three buttons: "Apply extensions", "Apply subject", and "Apply all". At the very bottom of the window are two buttons: "Aceptar" (highlighted in blue) and "Cancelar".

- 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	ES	organizationalUnitName	
stateOrProvinceName		commonName	
localityName		emailAddress	

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

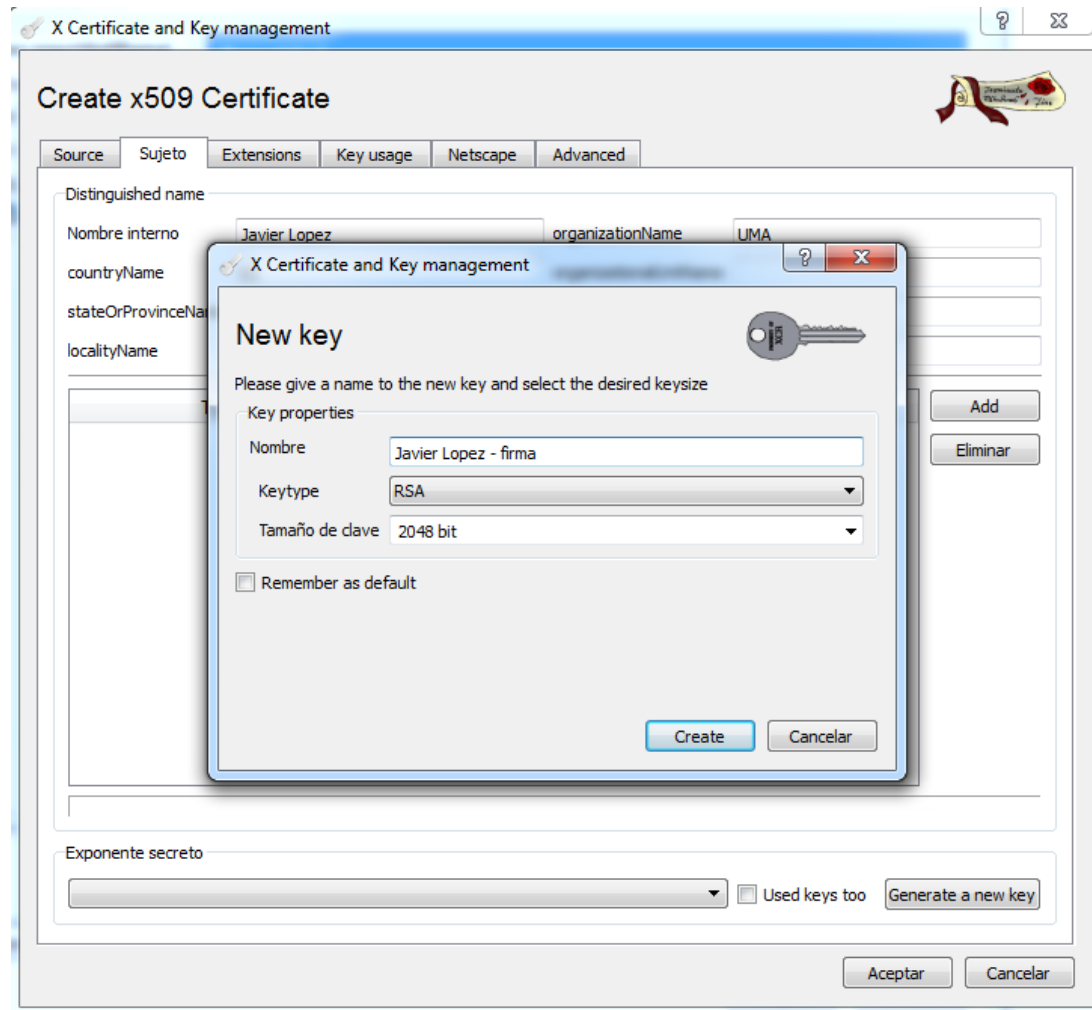
Add  
Eliminar

Exponente secreto

☐ Used keys to **Generate a new key**

Aceptar   Cancelar





X Certificate and Key management

?

Σ

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

i

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)

X Certificate and Key management

### Create x509 Certificate

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

**X509v3 Basic Constraints**

Type: **End Entity** (circled in red)

Path length:  ☐ Critical

**Key identifier**

☐ Subject Key Identifier  
☐ Authority Key Identifier

**Validz** (circled in red)

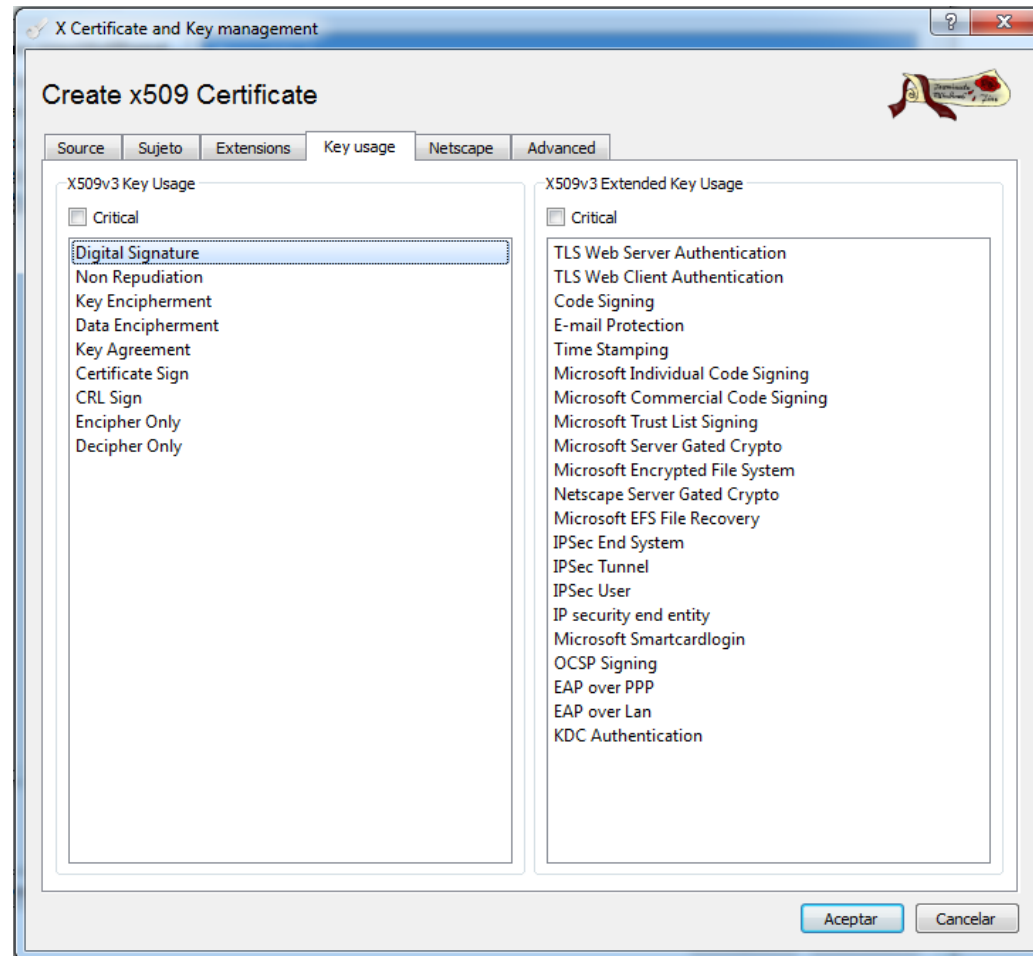
No antes de: 2015-04-07 14:18 GMT  
No después de: 2016-04-07 14:18 GMT

**Rango de tiempo**

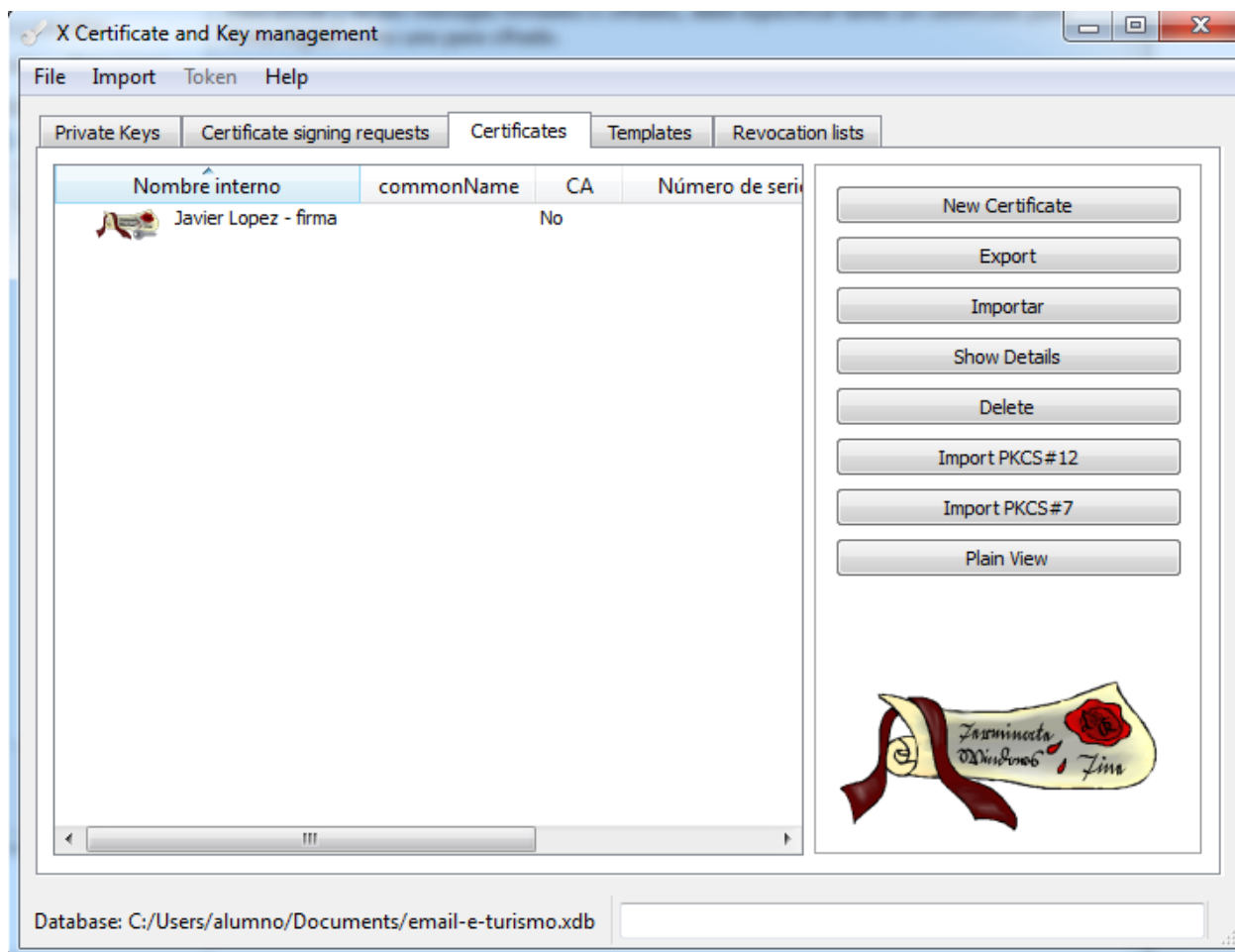
1  Años   
☐ Medianoche ☐ Local time ☐ No well-defined expiration

X509v3 Subject Alternative Name:    
X509v3 Issuer Alternative Name:    
X509v3 CRL Distribution Points:    
Authority Information Access: OCSP

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

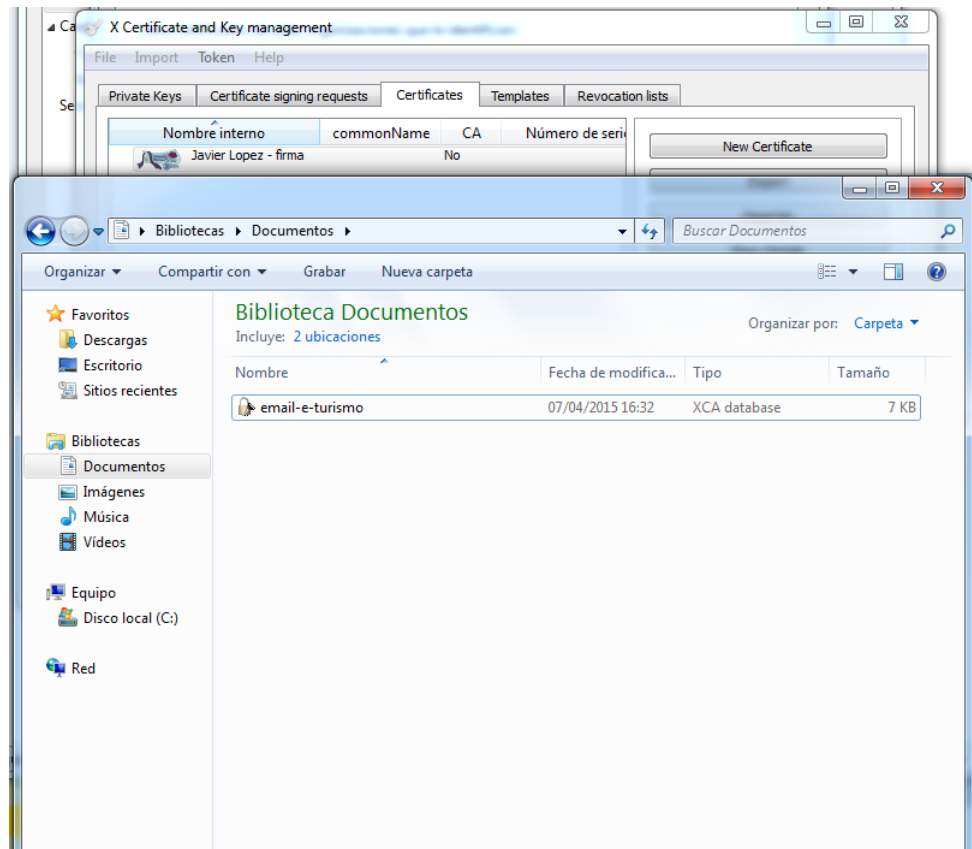


- ... y ya hemos creado el certificado para firma digital

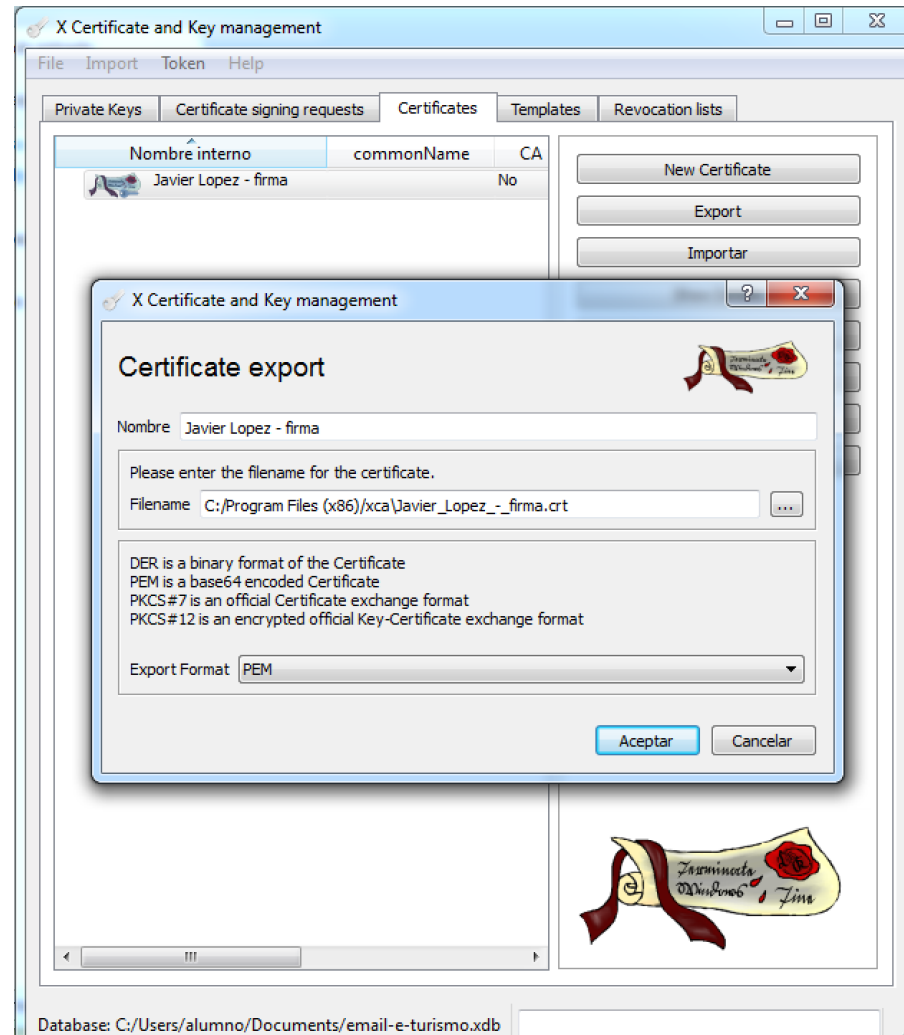


# XCA – Exportar certificado

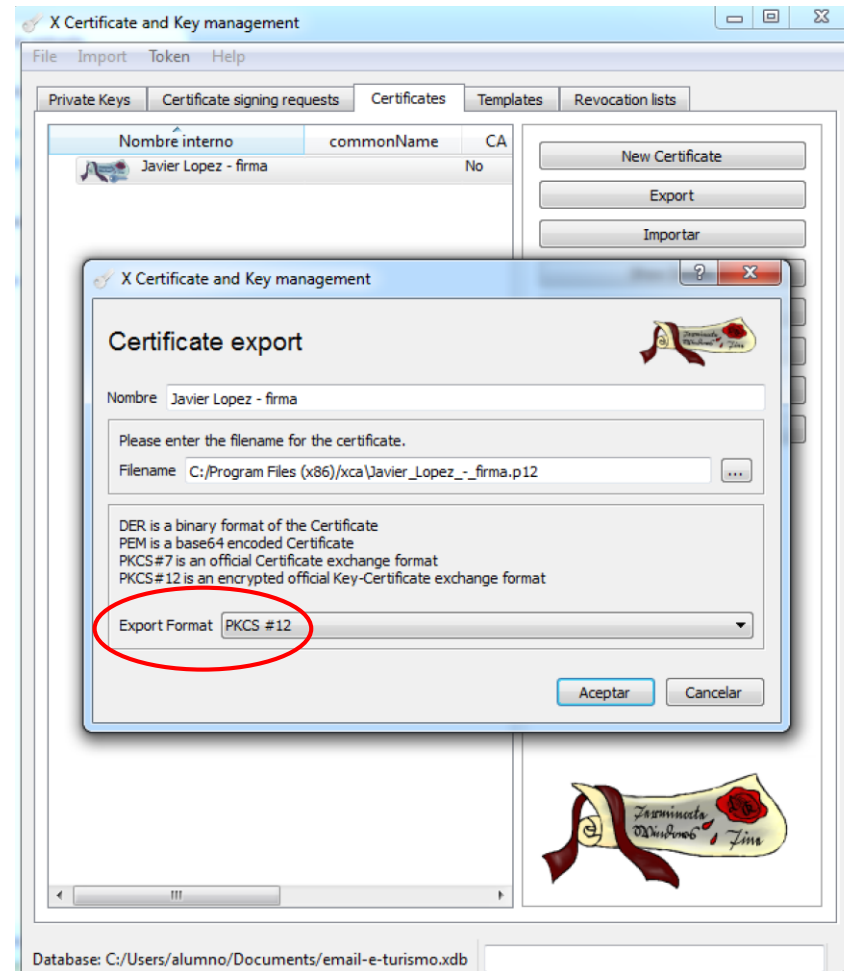
- El certificado está creado sólo en la base de datos de XCA, y es necesario exportarlo



- Botón “Export”



- Formato (visto en las transparencias de las prácticas)





- Contraseña con la que guardar el certificado

