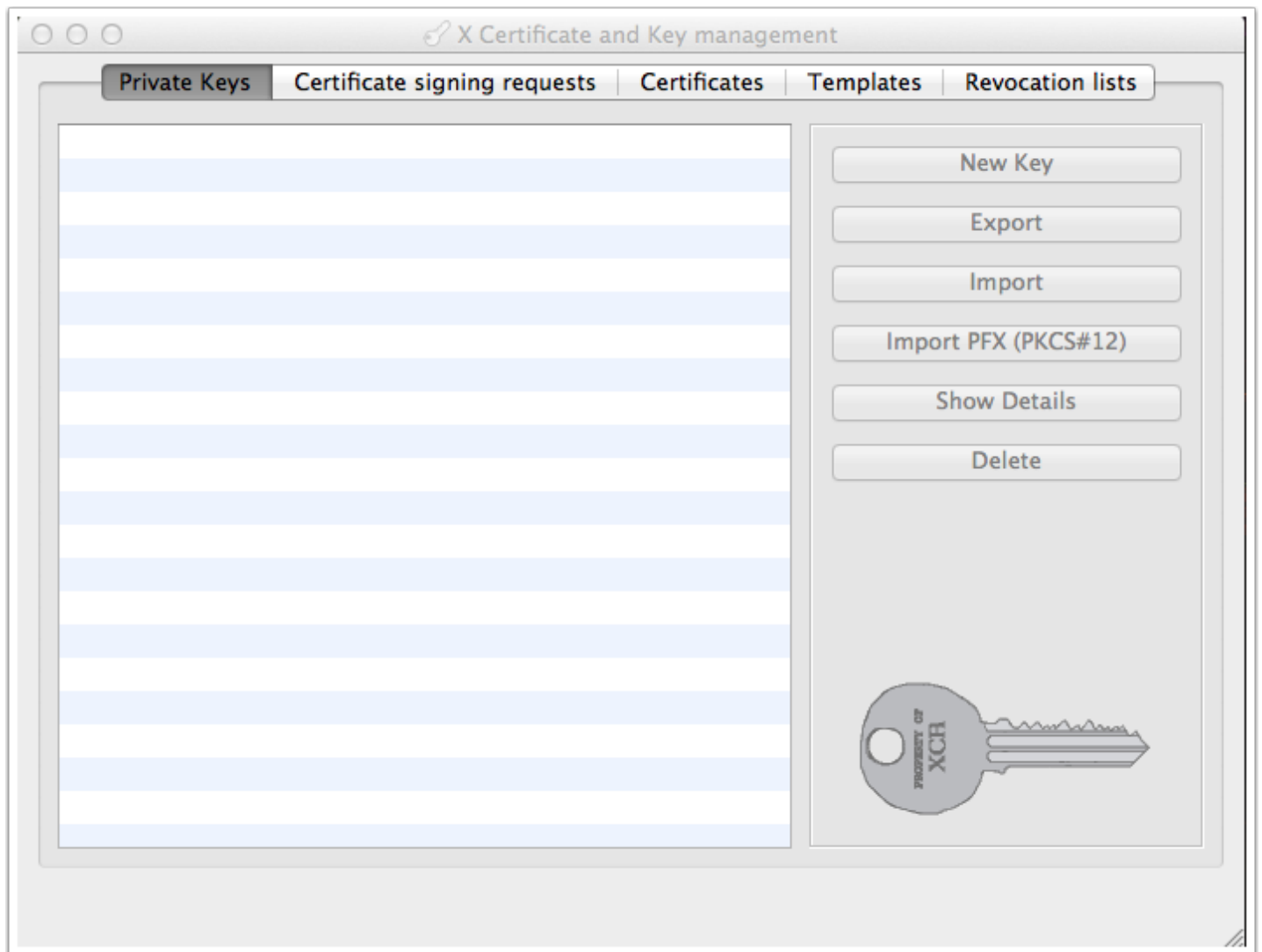
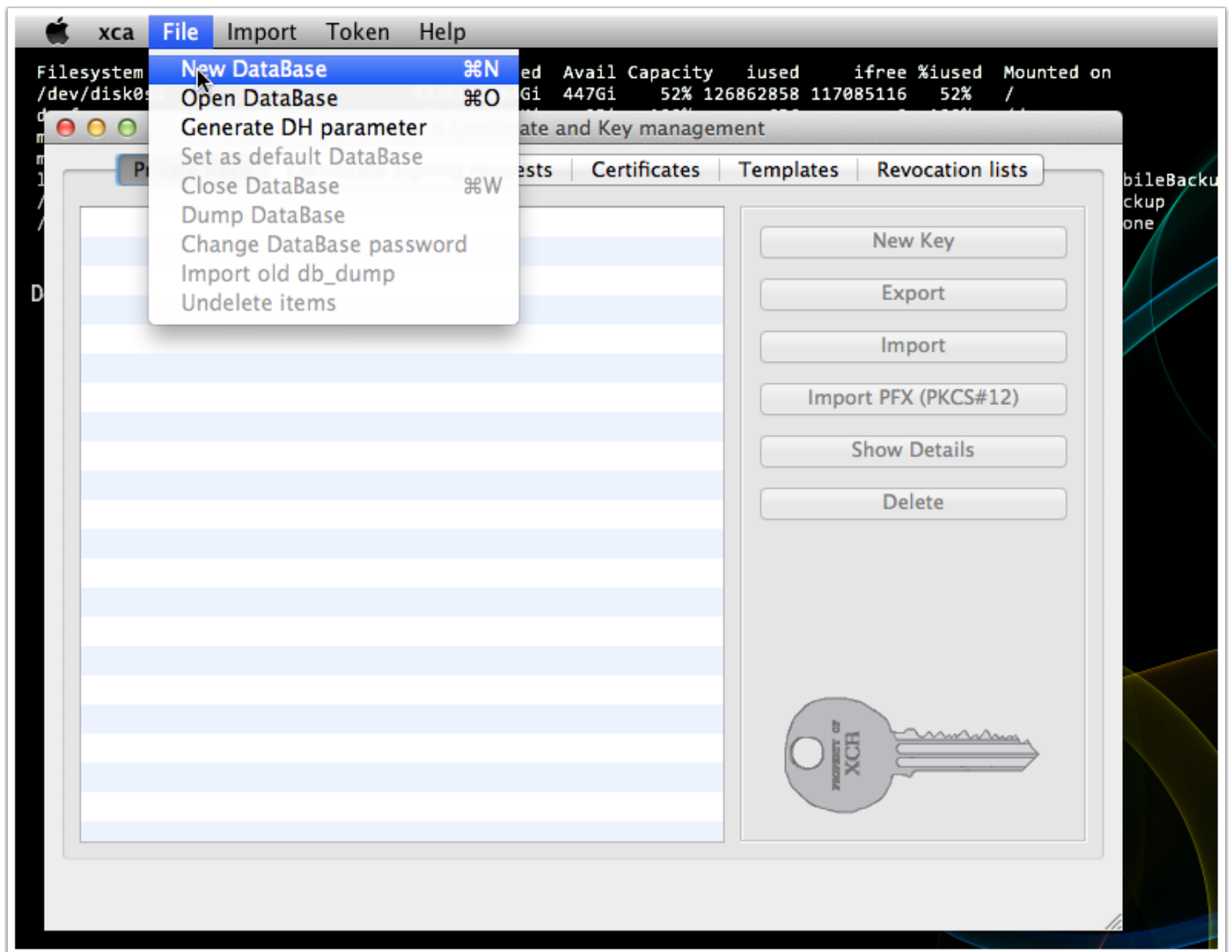


Generating, signing and exporting keys and certificates with XCA

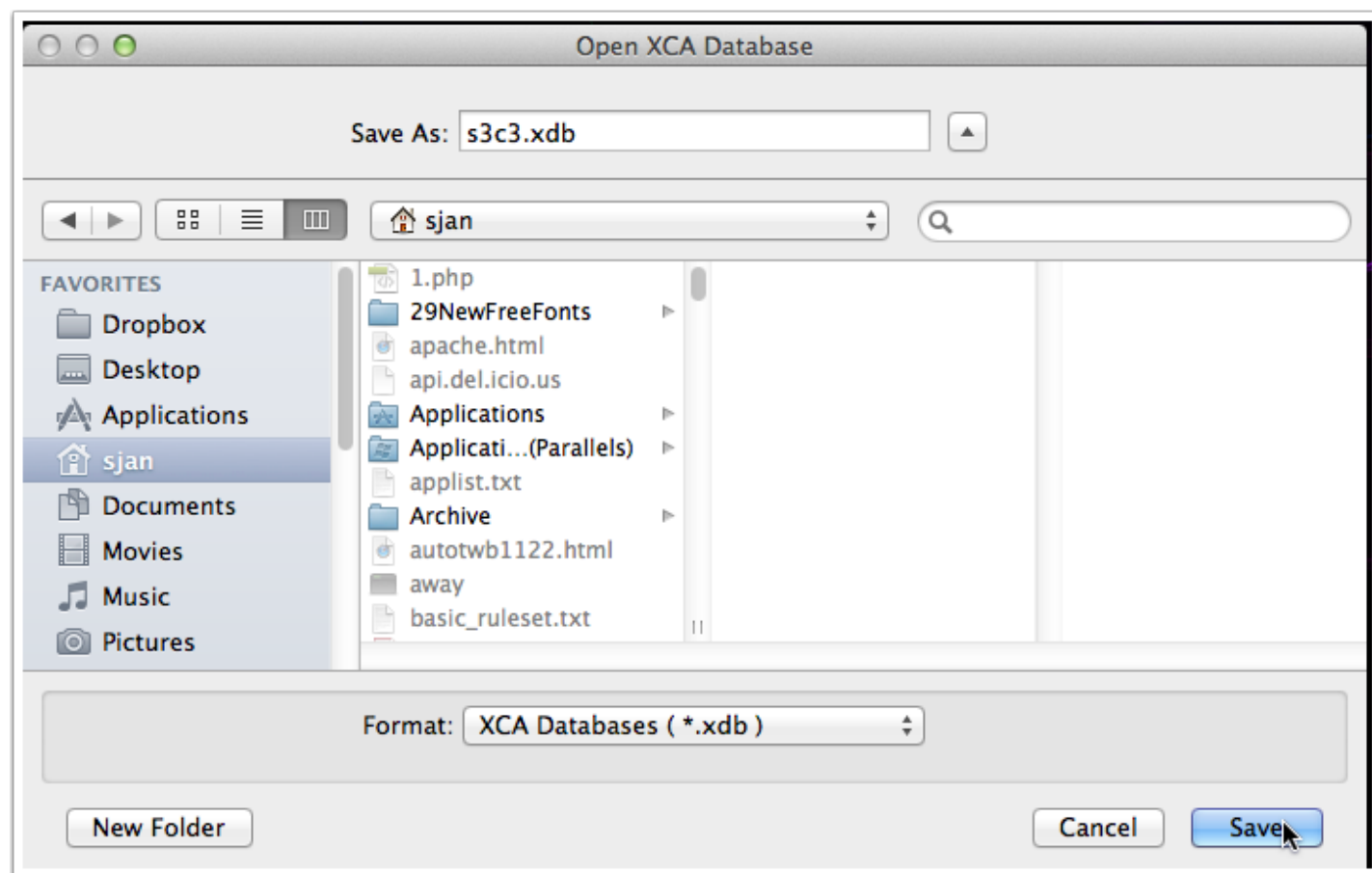
Start XCA



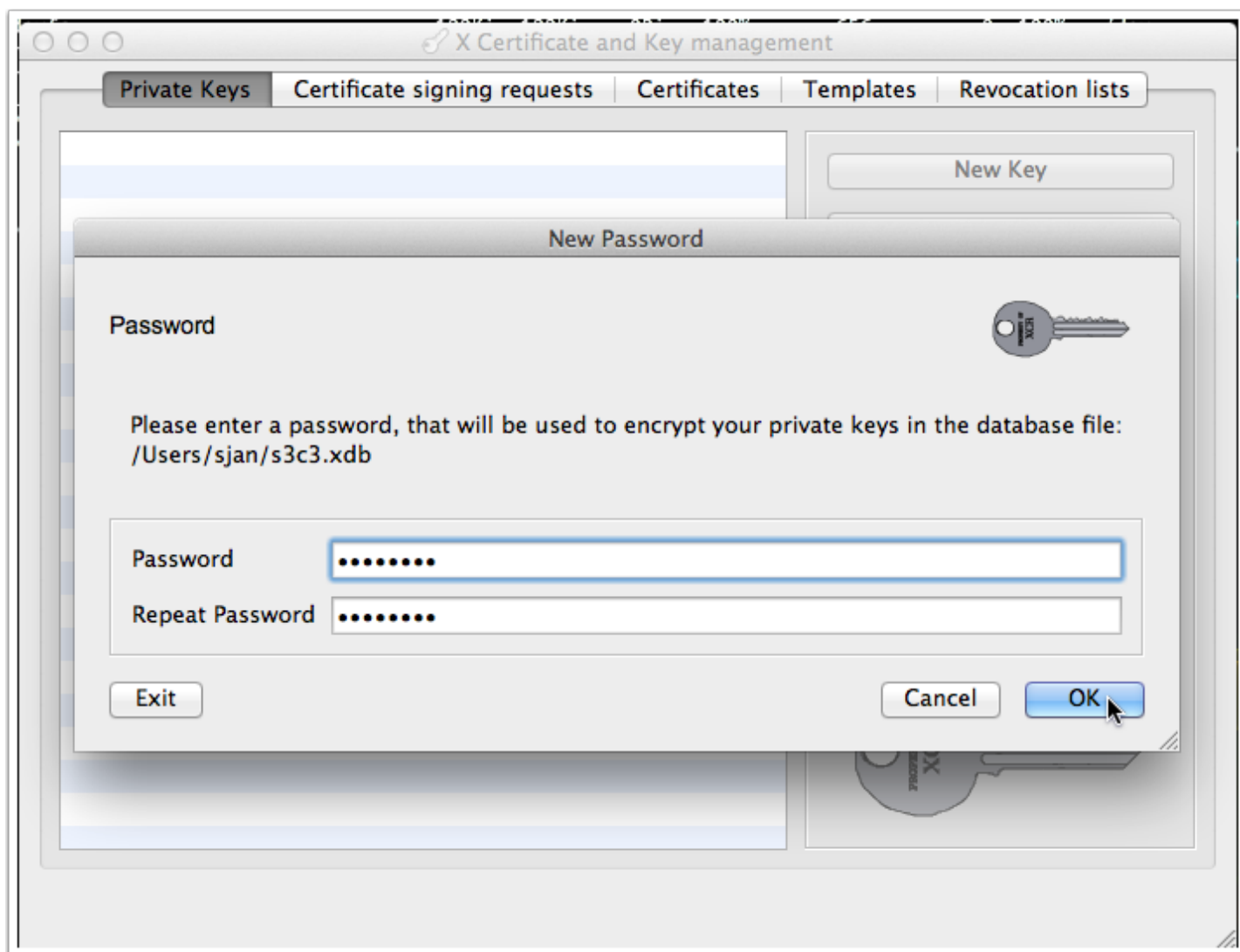
Create a new database



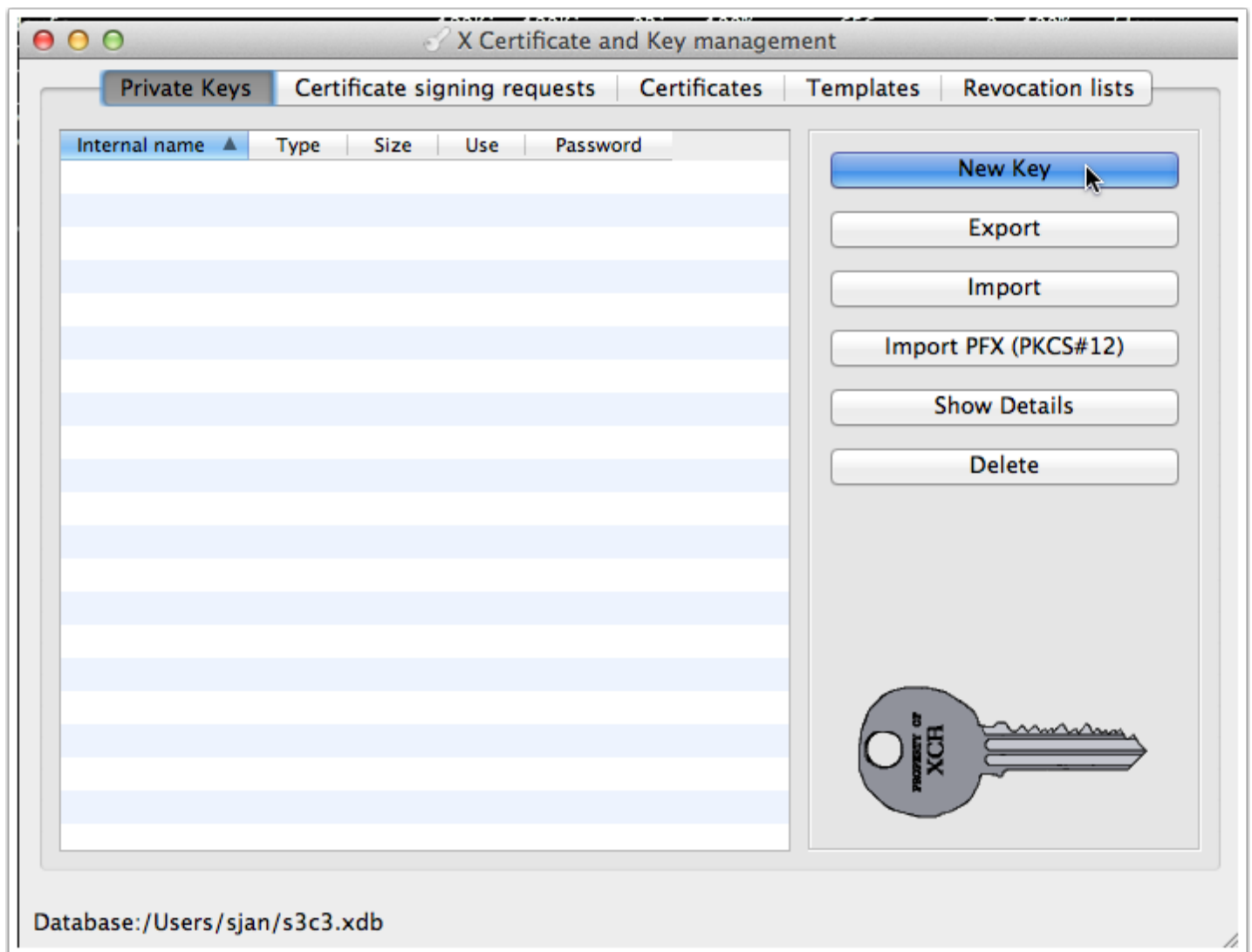
Name and save your database



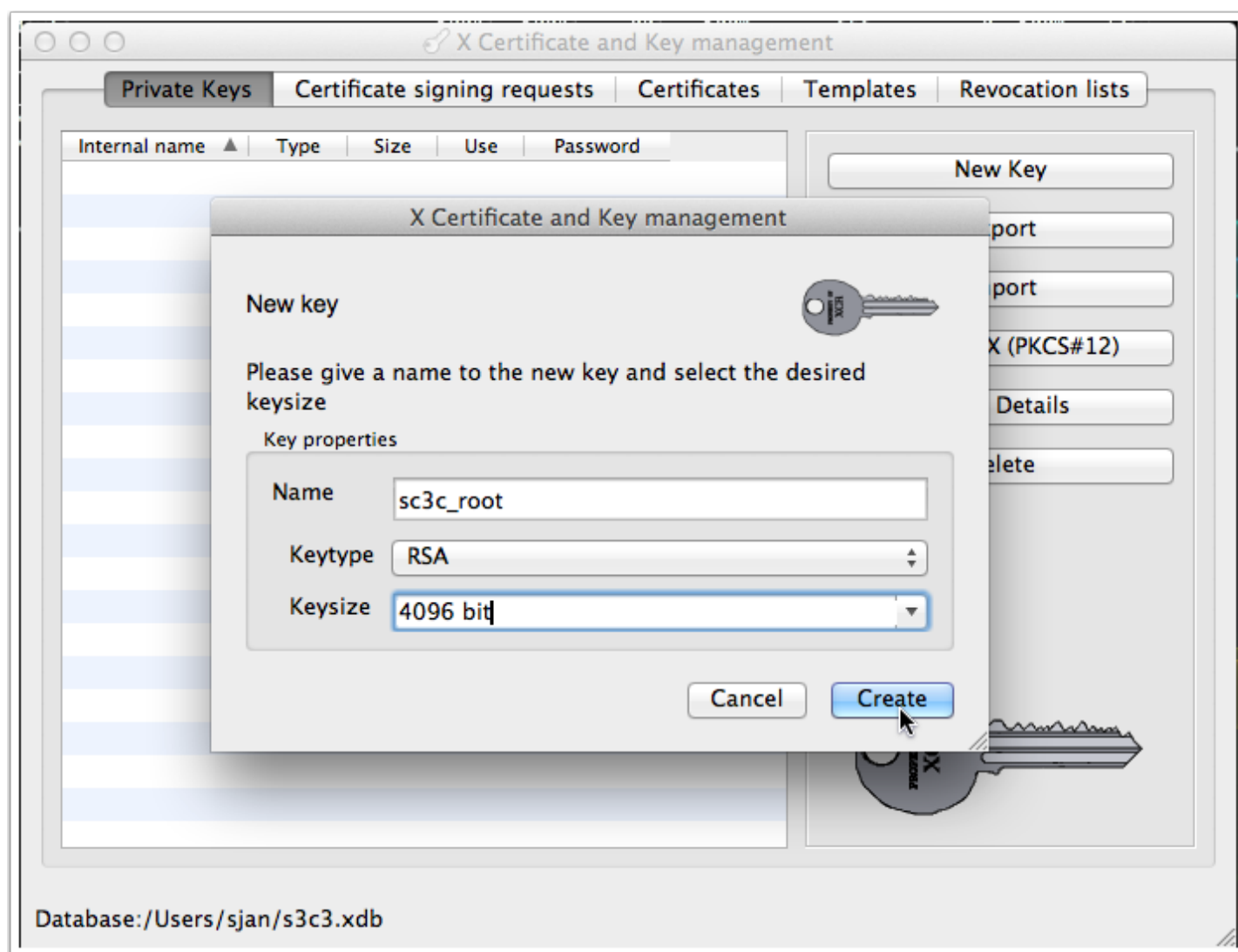
Select a password - you will need this every time you reopen this database



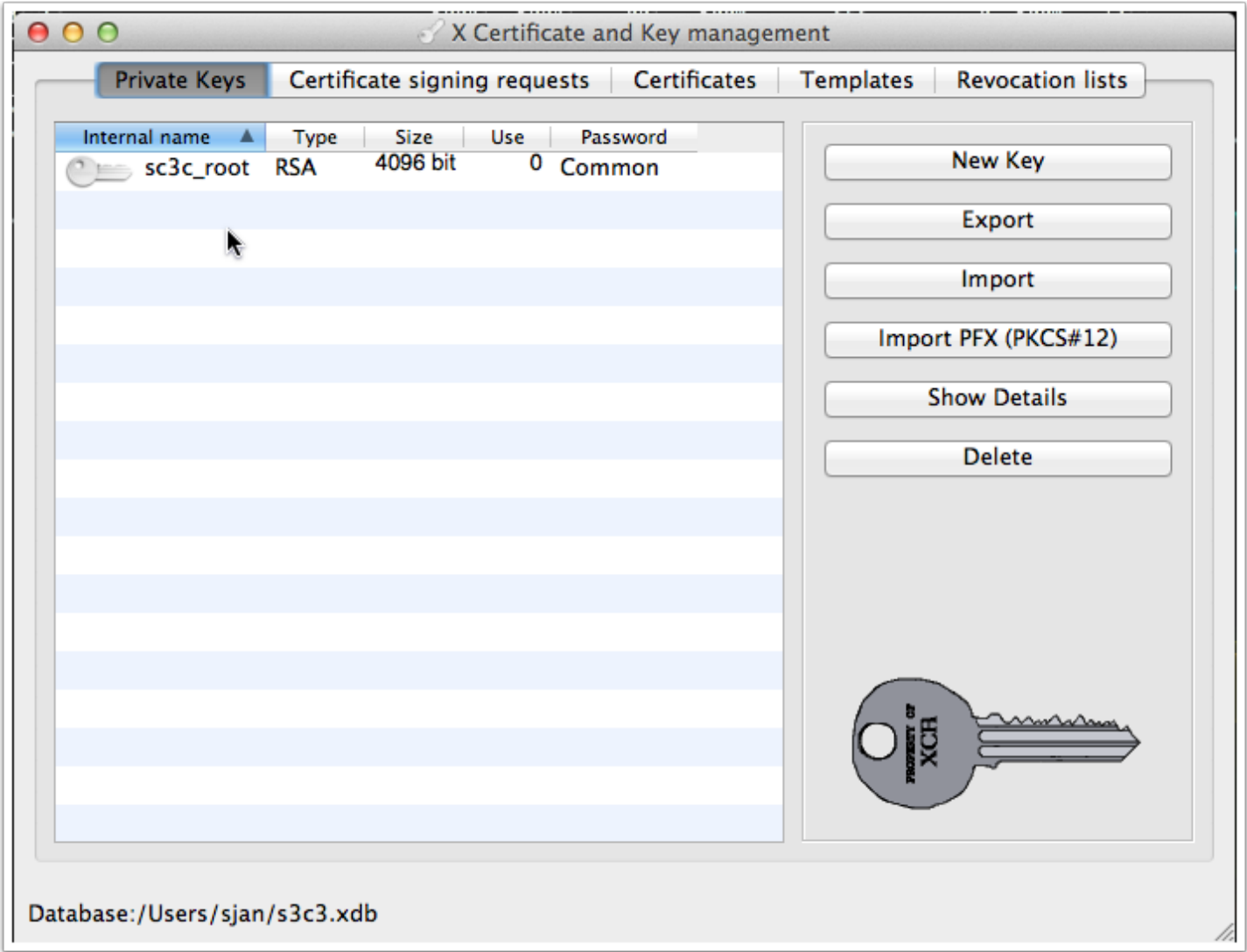
Generate a new private key for the root CA



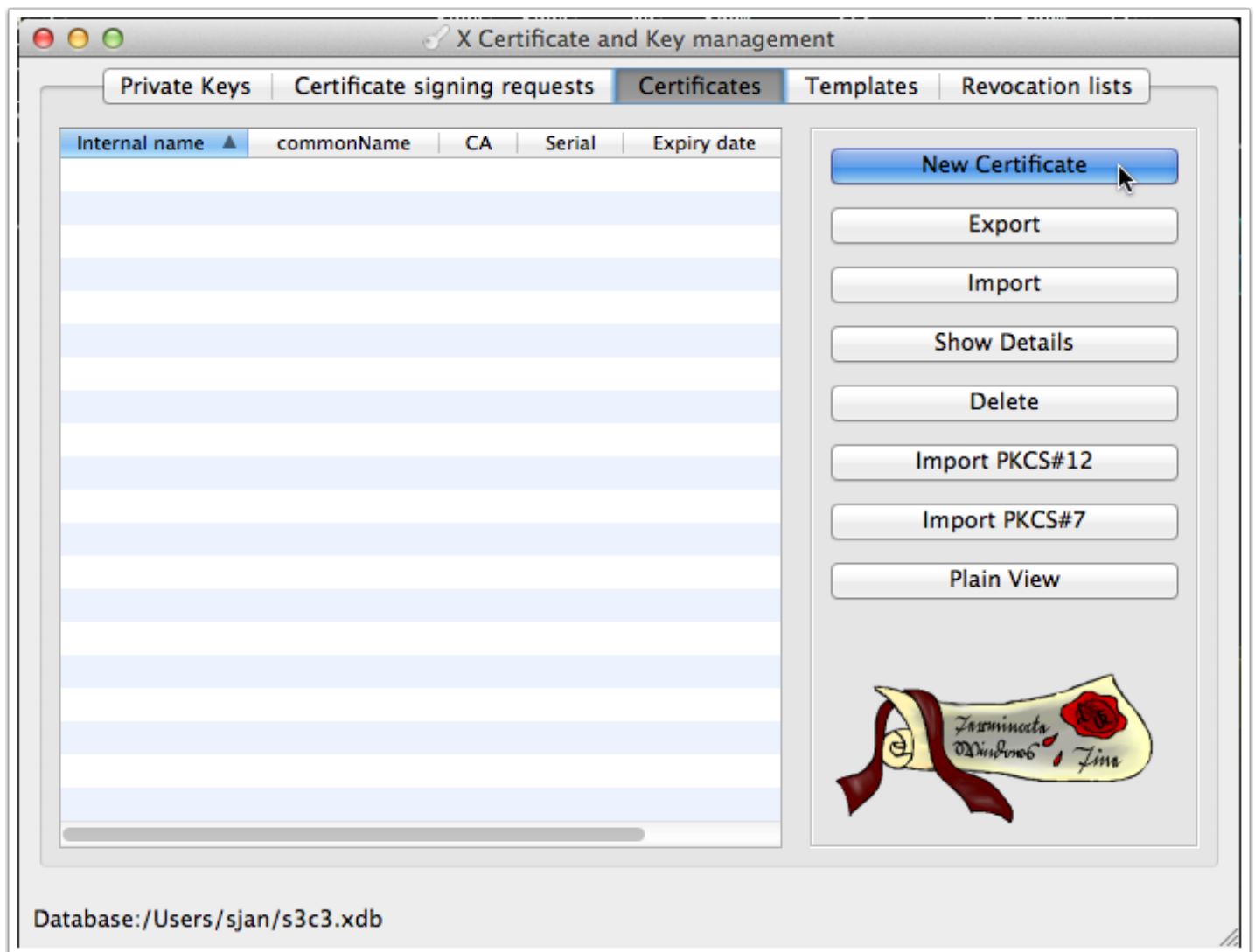
Name it something like **s3c3_root** - we are using 4098 bits for the example



Your shiny new key



Create a new self-signed certificate



Make sure the selected template is CA and click on Apply extensions

The screenshot shows the 'Create x509 Certificate' dialog box in XCA, with the 'Source' tab selected. The dialog has a title bar 'X Certificate and Key management' and a small icon in the top right corner. The 'Source' tab is active, showing options for signing requests and signing. The 'Signing request' section has three checkboxes: 'Sign this Certificate signing request' (unchecked), 'Copy extensions from the request' (checked), and 'Modify subject of the request' (unchecked). There is a 'Show request' button. The 'Signing' section has two radio buttons: 'Create a self signed certificate with the serial' (selected) and 'Use this Certificate for signing' (unchecked). The 'Create a self signed certificate with the serial' option has a text field containing '1'. The 'Signature algorithm' is set to 'SHA 1'. The 'Template for the new certificate' is set to '[default] CA'. At the bottom right of the dialog are 'Cancel' and 'OK' buttons. There are also 'Apply extensions', 'Apply subject', and 'Apply all' buttons at the bottom of the main content area.

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

Signing request

☐ Sign this Certificate signing request

☒ Copy extensions from the request

☐ Modify subject of the request

Show request

Signing

☒ Create a self signed certificate with the serial 1

☐ Use this Certificate for signing

Signature algorithm SHA 1

Template for the new certificate [default] CA

Apply extensions Apply subject Apply all

Cancel OK

Fill out the subject fields

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name	s3c3_root	organizationName	S3C3 Demo
countryName	US	organizationalUnitName	
stateOrProvinceName	Washington	commonName	S3C3 Master
localityName	Lacey	emailAddress	s3c3@example.com

Type	Content

Add
Delete

Private key

sc3c_root (RSA) ☐ Used keys too

Cancel OK

In extensions, make sure it is marked as type "Certification Authority" and "Critical" and "Subject Key Identifier" checked - set lifetime to 10 years

X Certificate and Key management

Create x509 Certificate

Source Subject **Extensions** Key usage Netscape Advanced

Basic constraints

Type: Certification Authority

Path length: ☒ Critical

Key identifier

☒ Subject Key Identifier
☐ Authority Key Identifier

Validity

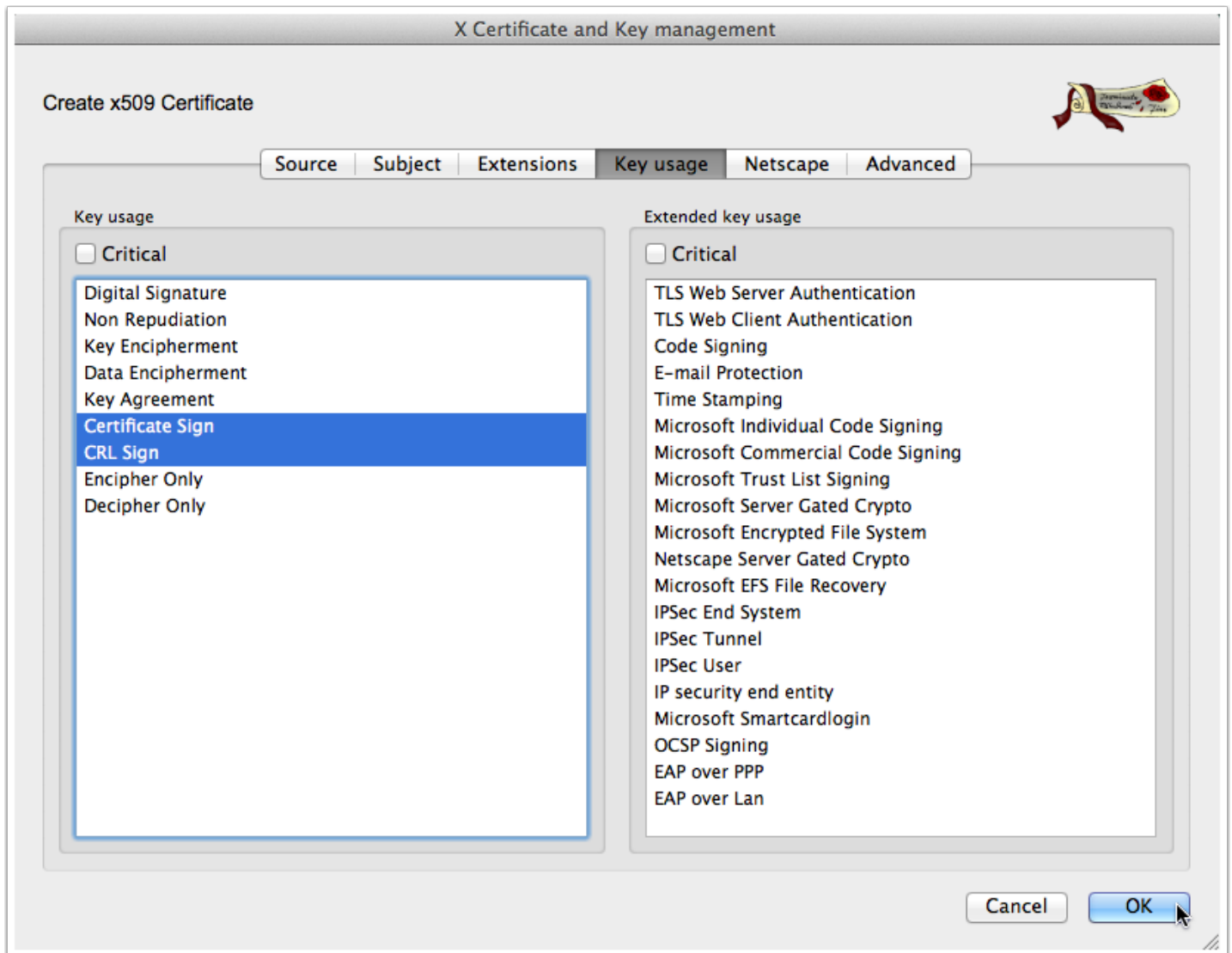
Not before: 2013-07-09 01:26 GMT
 Not after: 2023-07-09 01:26 GMT

Time range

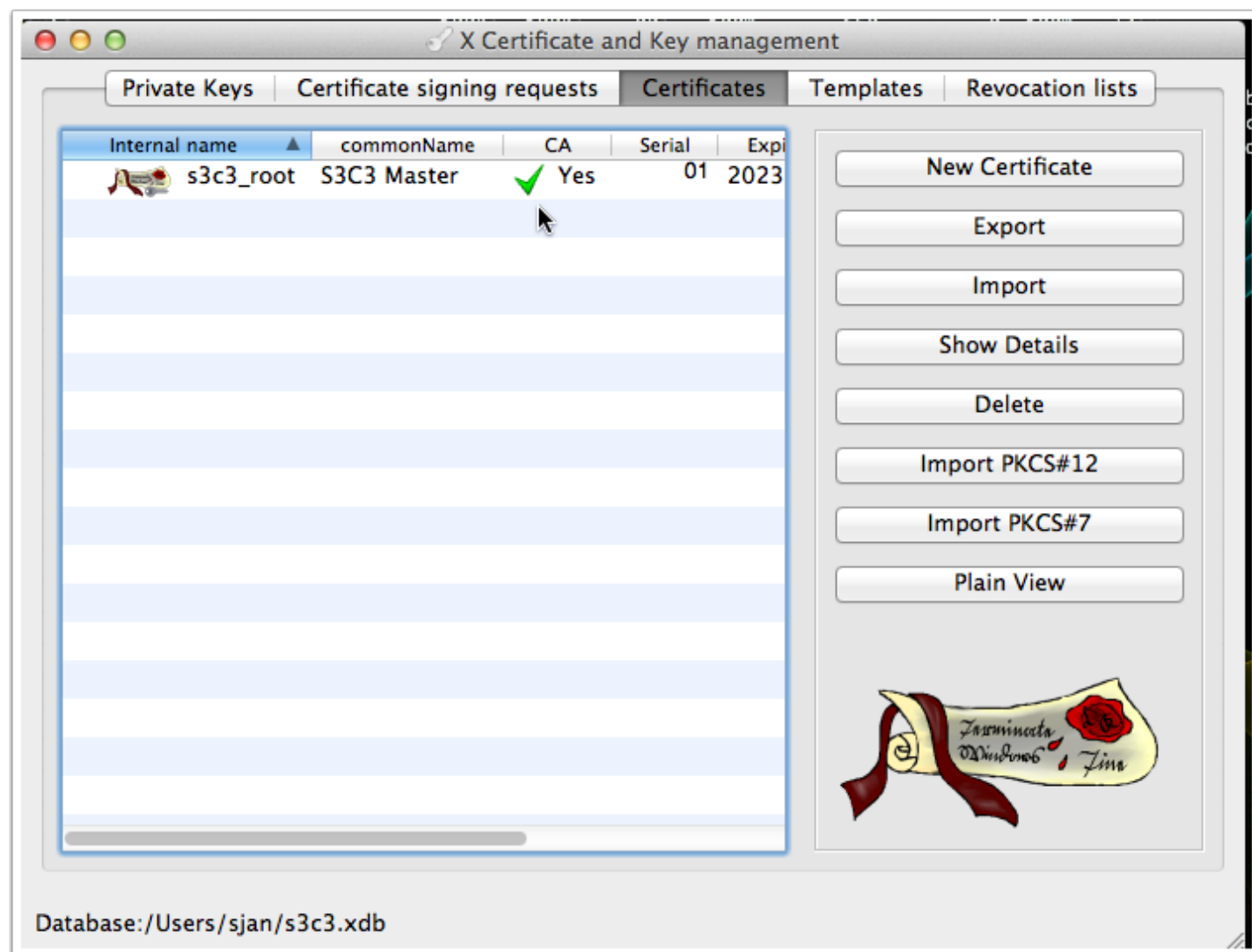
10 Years
☐ Midnight ☐ Local time ☐ No well-defined expiration

subject alternative name
 issuer alternative name
 CRL distribution point
 Authority Info Access: CA Issuers

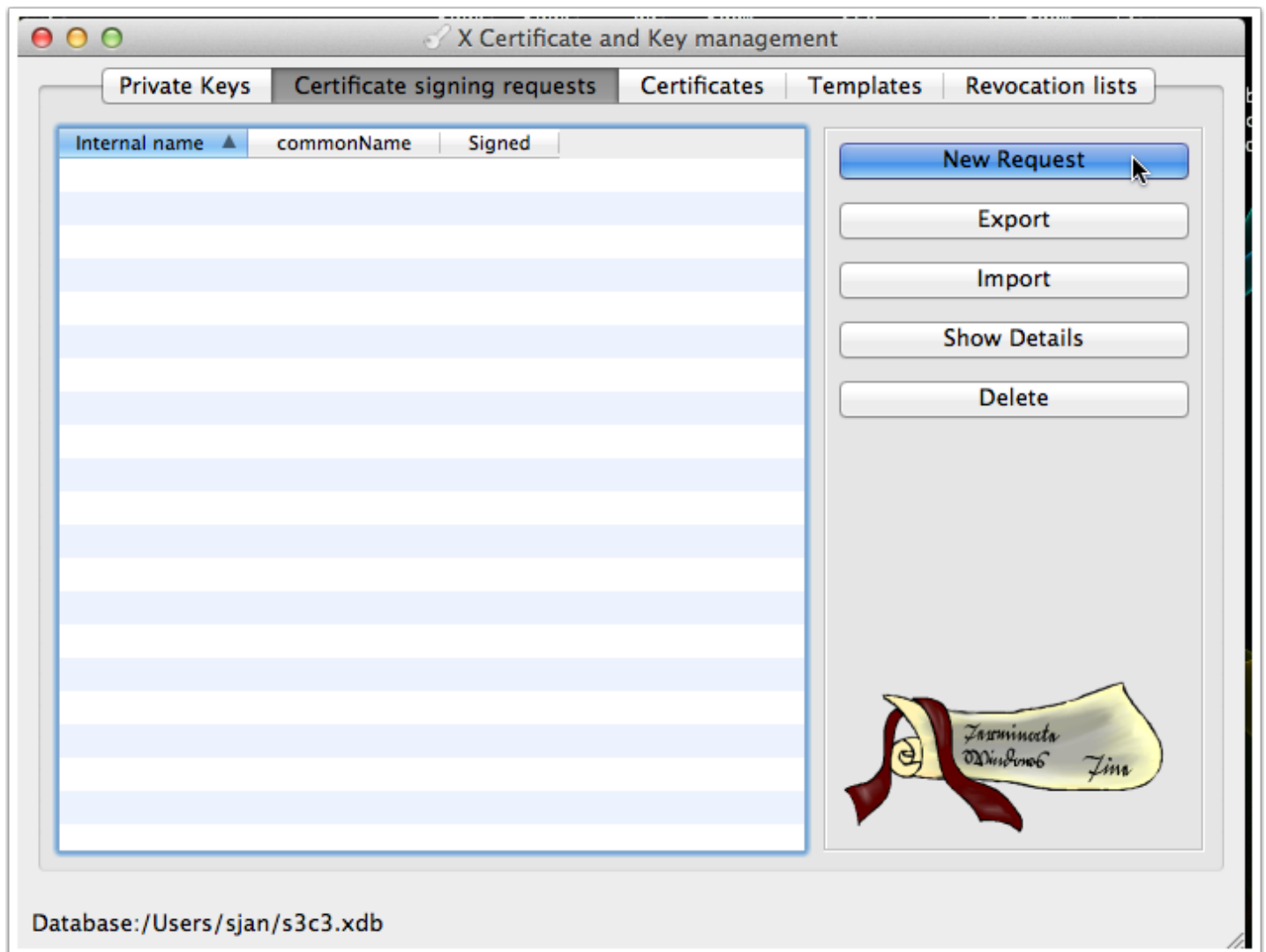
Make sure Certificate Sign and CRL Sign are selected under Key usage and click OK



You should have a new CA Certificate now



Create a new client certificate - start with a new Certificate signing request



Set the template to HTTPS_client and click Apply extensions

X Certificate and Key management

Create Certificate signing request

Source Subject Extensions Key usage Netscape Advanced

Signing request

unstructuredName server1_client

challengePassword

Signing

☒ Create a self signed certificate with the serial 1

☐ Use this Certificate for signing s3c3_root

Signature algorithm SHA 1

Template for the new certificate

[default] HTTPS_client

Apply extensions Apply subject Apply all

Cancel OK

Fill out the subject and click on Generate a new key

X Certificate and Key management

Create Certificate signing request

Source Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name	server1_client	organizationName	S3C3 Demo
countryName	US	organizationalUnitName	
stateOrProvinceName	Washington	commonName	Server 1
localityName	Lacey	emailAddress	s3c3@example.com

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

Add

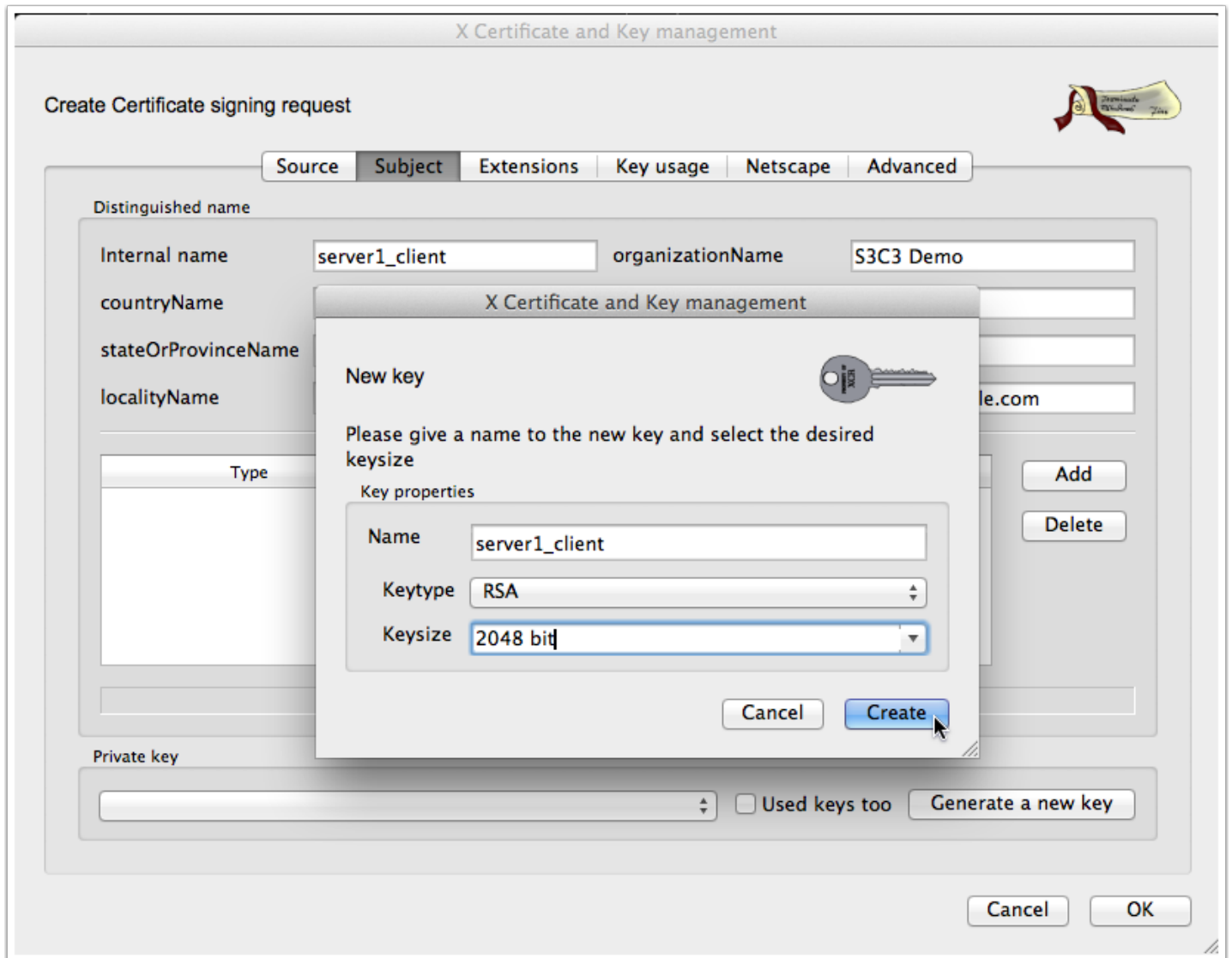
Delete

Private key

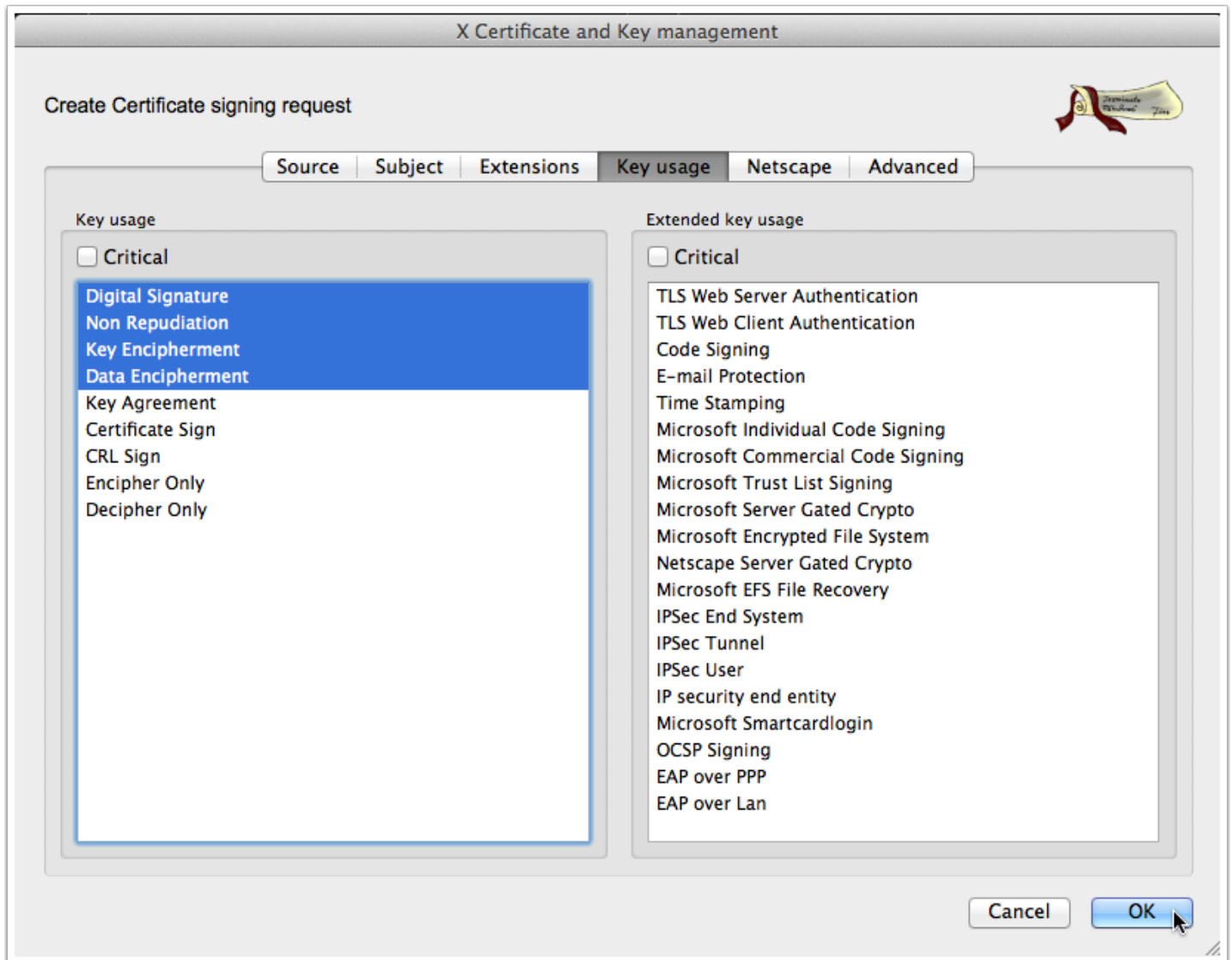
☐ Used keys too **Generate a new key**

Cancel OK

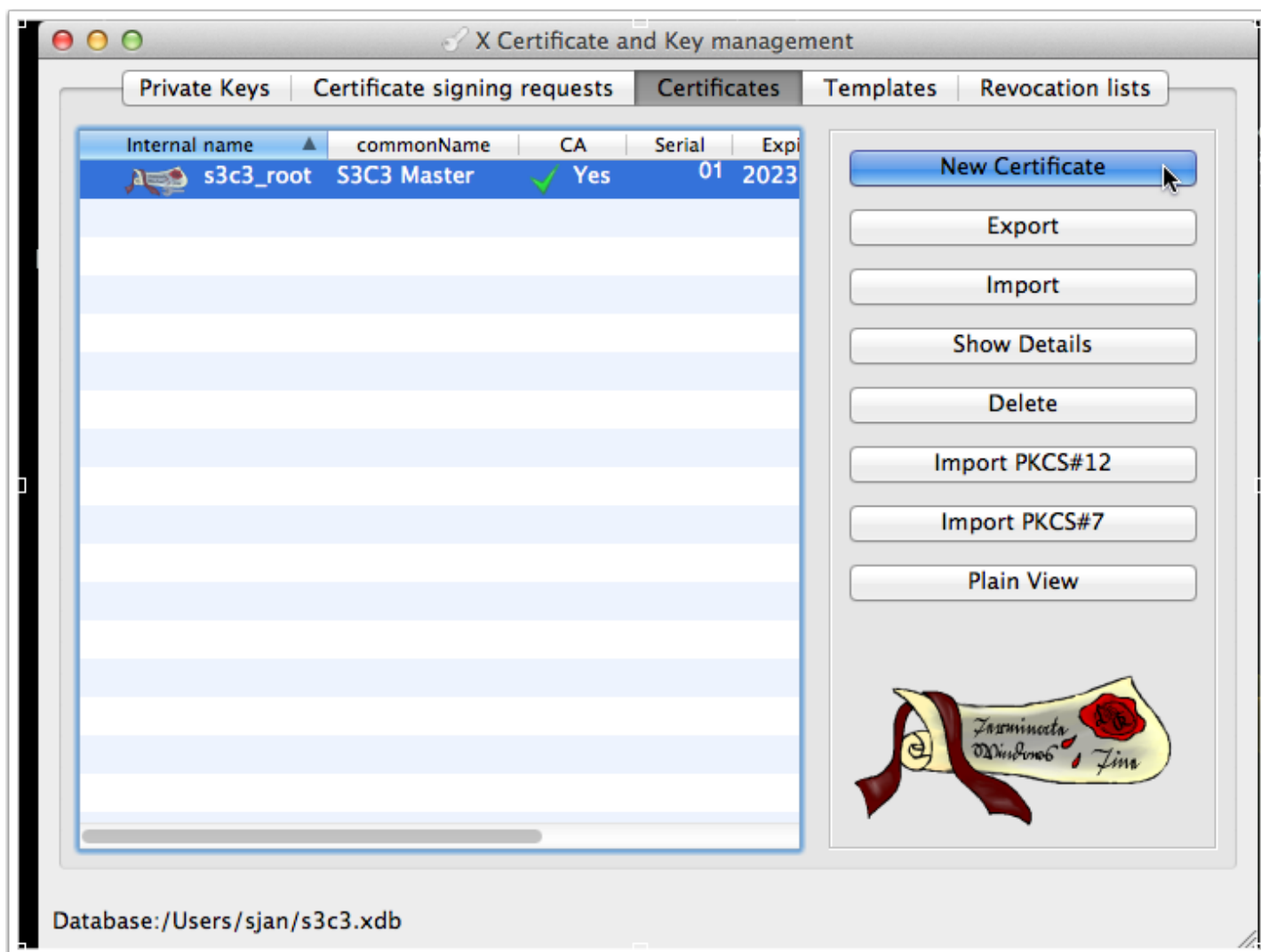
Set the name of the server (server1 in this example) and add _client to the name - use a 2048 bit key or larger



Make sure to also select Non Repudiation in the Key usage pane and click OK



In the Certificates pane, click on New Certificate



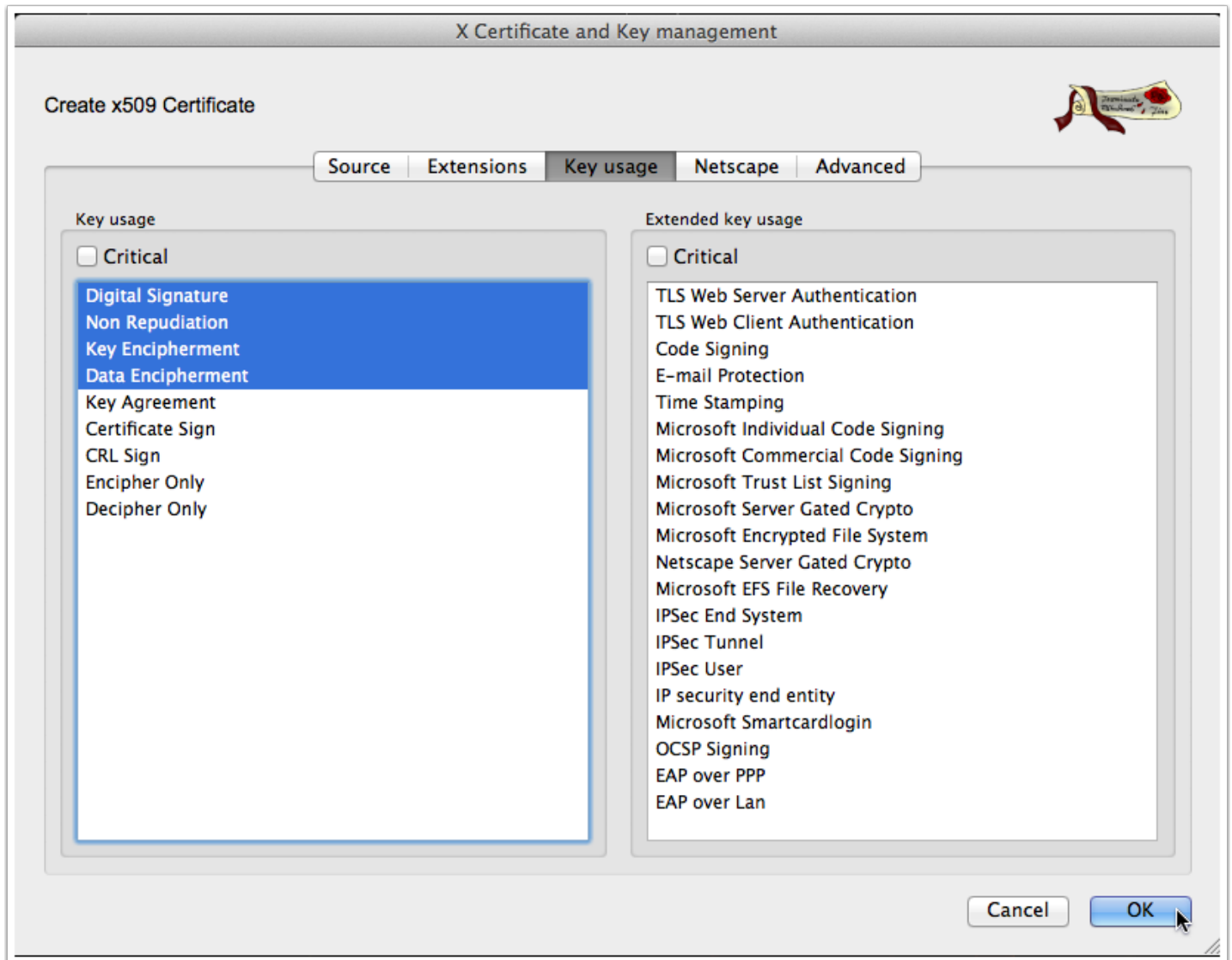
Check Sign this request, uncheck copy extensions, make sure to check "Use this Certificate for signing" and use your root, select HTTPS_client in templates and click Apply all

The screenshot shows the 'Create x509 Certificate' dialog box in XCA, with the 'Extensions' tab selected. The dialog has a title bar 'X Certificate and Key management' and a small icon in the top right corner. The main area is divided into several sections:

- Signing request:** Contains three checkboxes: 'Sign this Certificate signing request' (checked), 'Copy extensions from the request' (unchecked), and 'Modify subject of the request' (unchecked). To the right of these checkboxes is a dropdown menu showing 'server1_client' and a 'Show request' button.
- Signing:** Contains two radio buttons: 'Create a self signed certificate with the serial' (unchecked) and 'Use this Certificate for signing' (checked). To the right of the second radio button is a dropdown menu showing 's3c3_root'.
- Signature algorithm:** A dropdown menu showing 'SHA 1'.
- Template for the new certificate:** A dropdown menu showing '[default] HTTPS_client'.

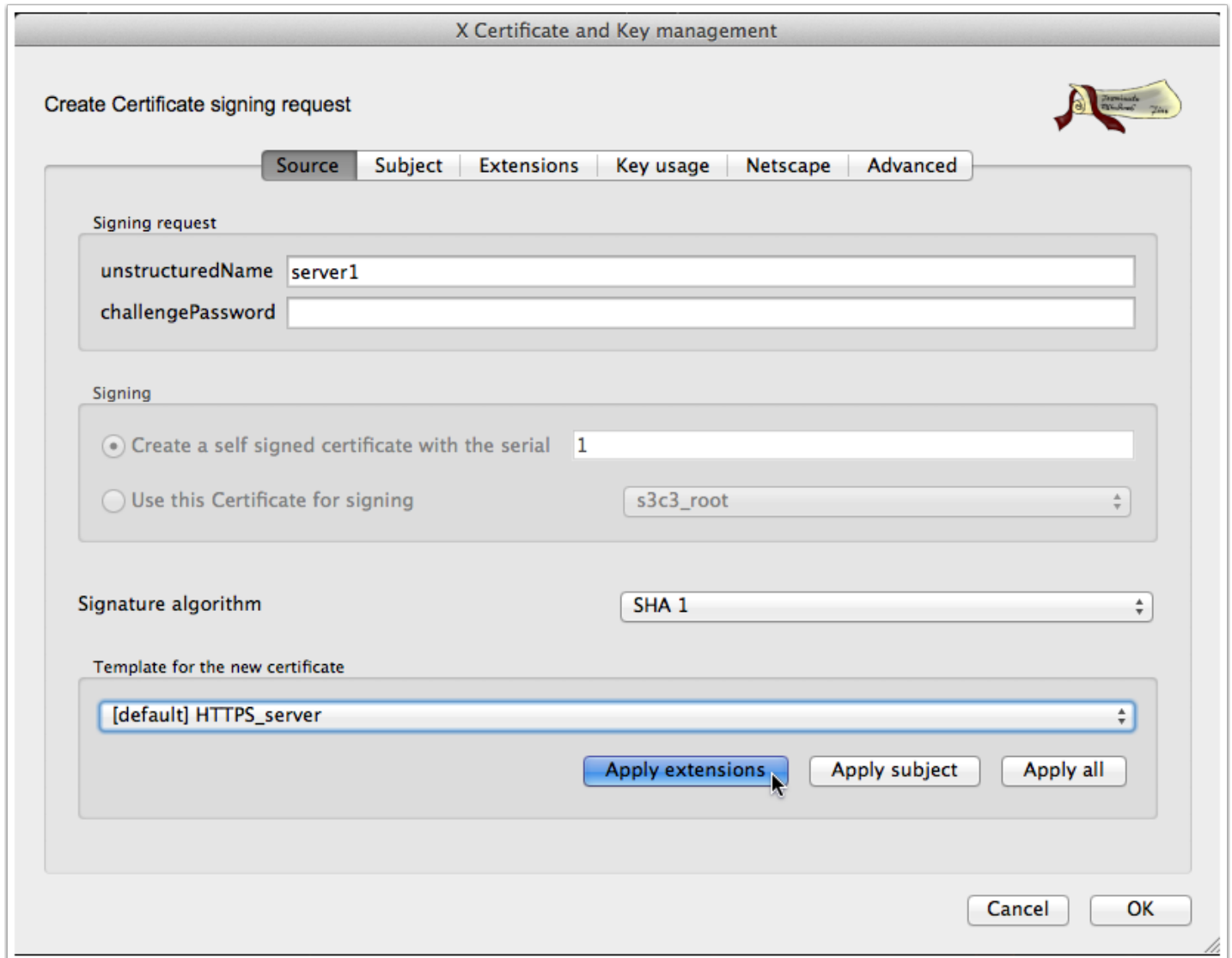
At the bottom of the dialog, there are three buttons: 'Apply extensions', 'Apply subject', and 'Apply all' (highlighted with a mouse cursor). At the very bottom right, there are 'Cancel' and 'OK' buttons.

Make sure Non Repudiation is also selected and click on OK



Generating a server certificate is the same as a client, except you will use the HTTPS_server template

Note that you WILL need to choose "Use this Certificate for signing" and select your root key. I forgot to while building the screenshots and had to rebuild this certificate.



The screenshot shows the 'X Certificate and Key management' window with the 'Create Certificate signing request' dialog open. The 'Source' tab is selected. The 'Signing request' section has 'unstructuredName' set to 'server1' and an empty 'challengePassword' field. The 'Signing' section has the radio button 'Create a self signed certificate with the serial' selected, with '1' in the serial field. The 'Use this Certificate for signing' option is unselected, and 's3c3_root' is selected in the dropdown. The 'Signature algorithm' is set to 'SHA 1'. The 'Template for the new certificate' dropdown shows '[default] HTTPS_server'. At the bottom right are 'Cancel' and 'OK' buttons. A mouse cursor is pointing at the 'Apply extensions' button.

X Certificate and Key management

Create Certificate signing request

Source Subject Extensions Key usage Netscape Advanced

Signing request

unstructuredName server1

challengePassword

Signing

☒ Create a self signed certificate with the serial 1

☐ Use this Certificate for signing s3c3_root

Signature algorithm SHA 1

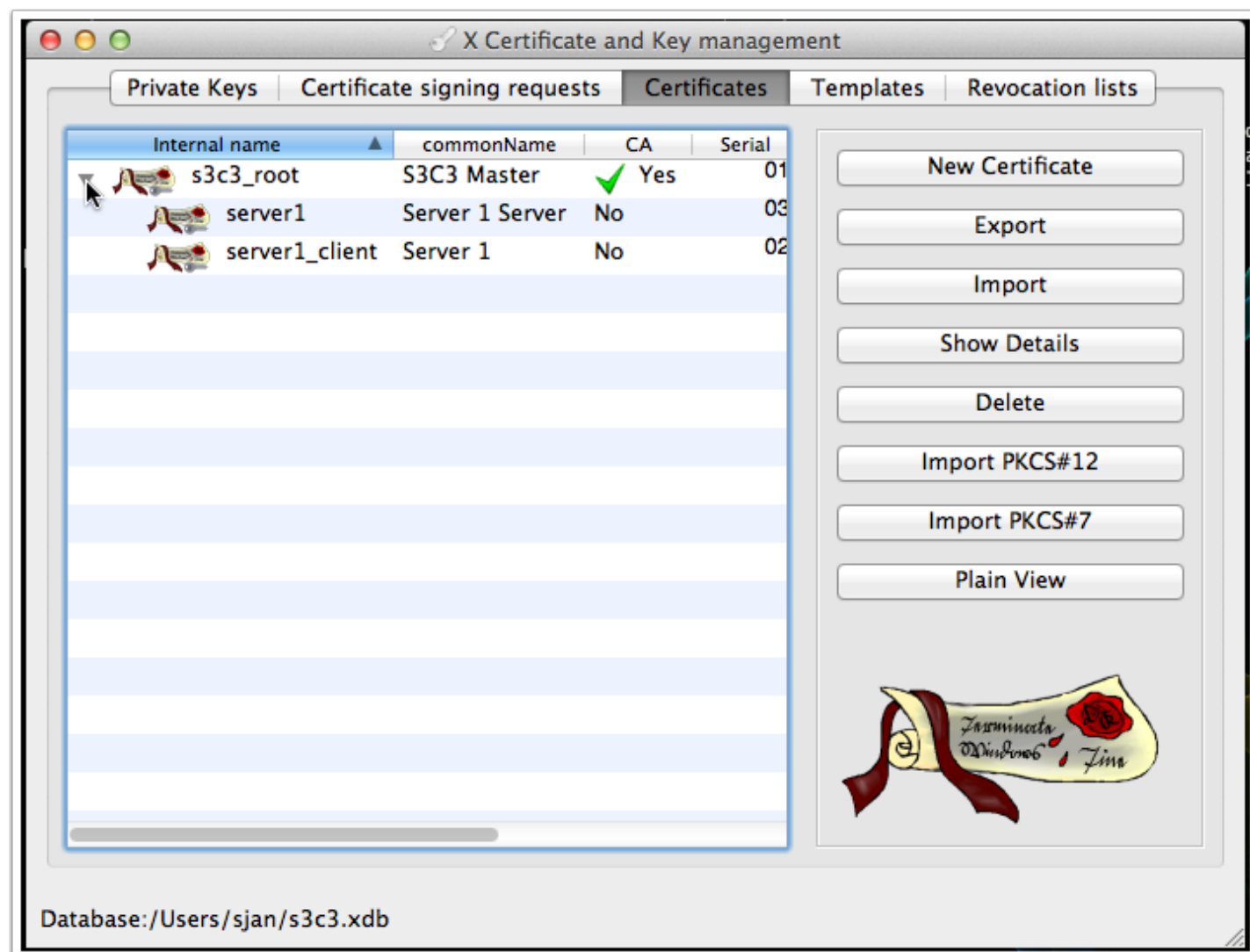
Template for the new certificate

[default] HTTPS_server

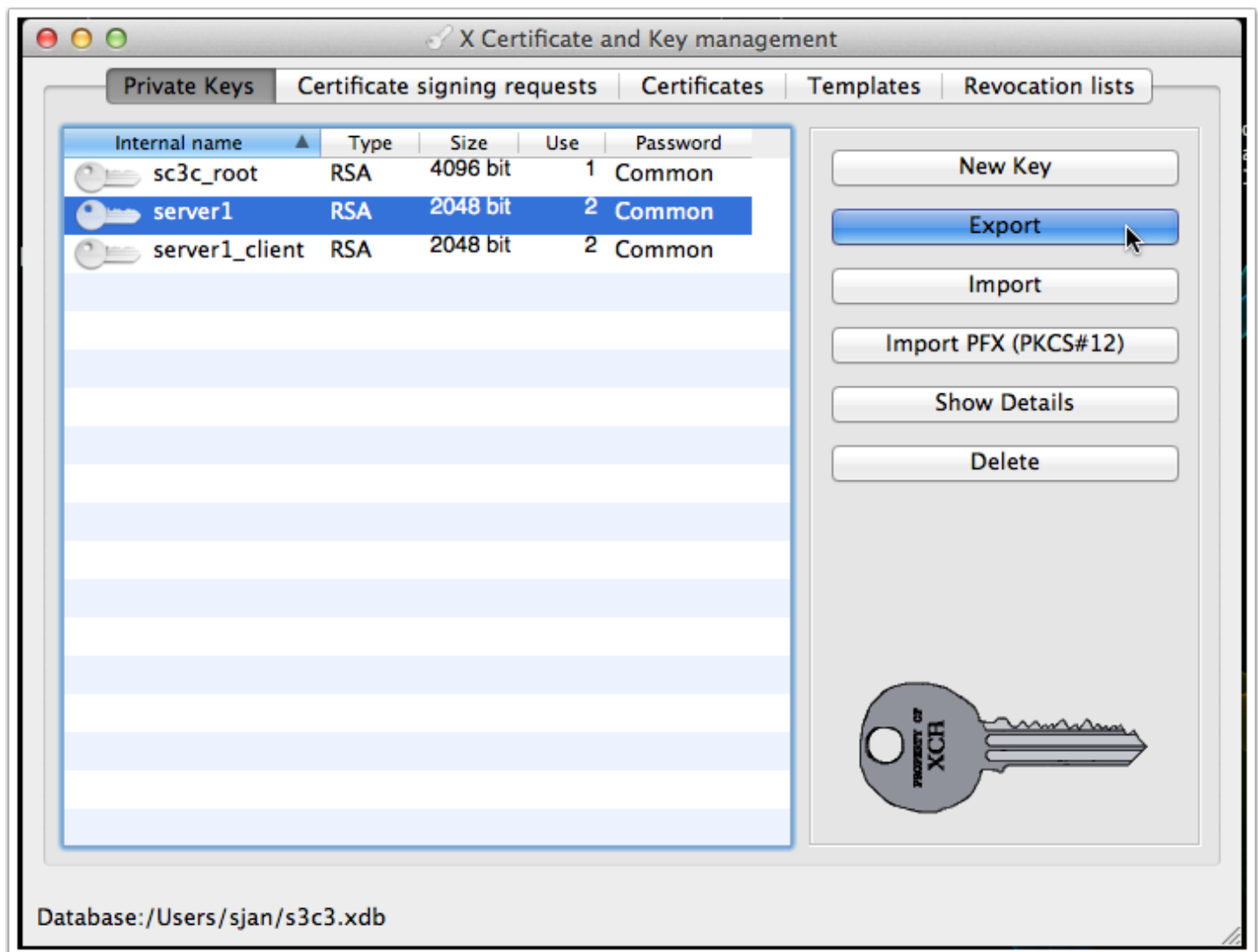
Apply extensions Apply subject Apply all

Cancel OK

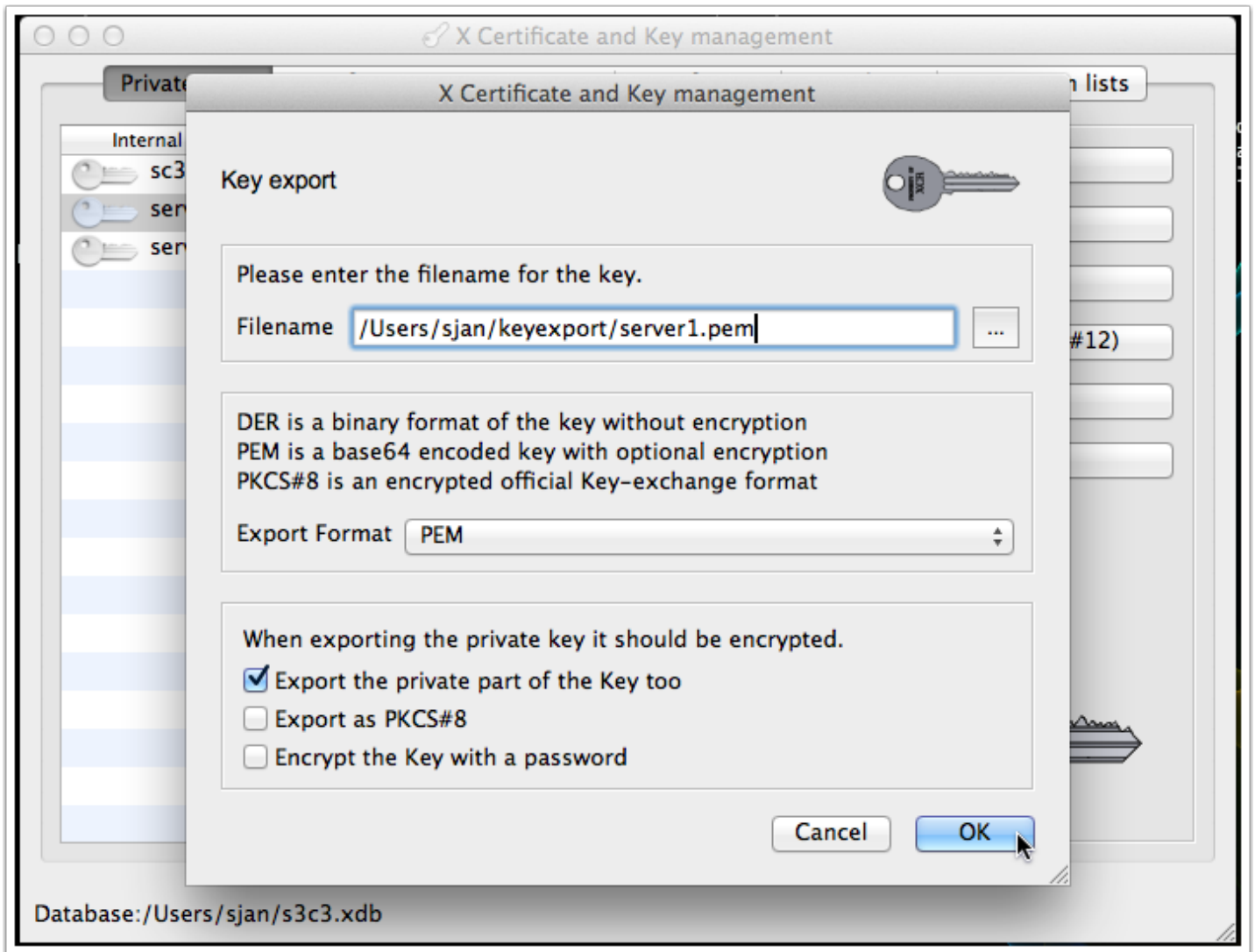
X Certificate and Key management



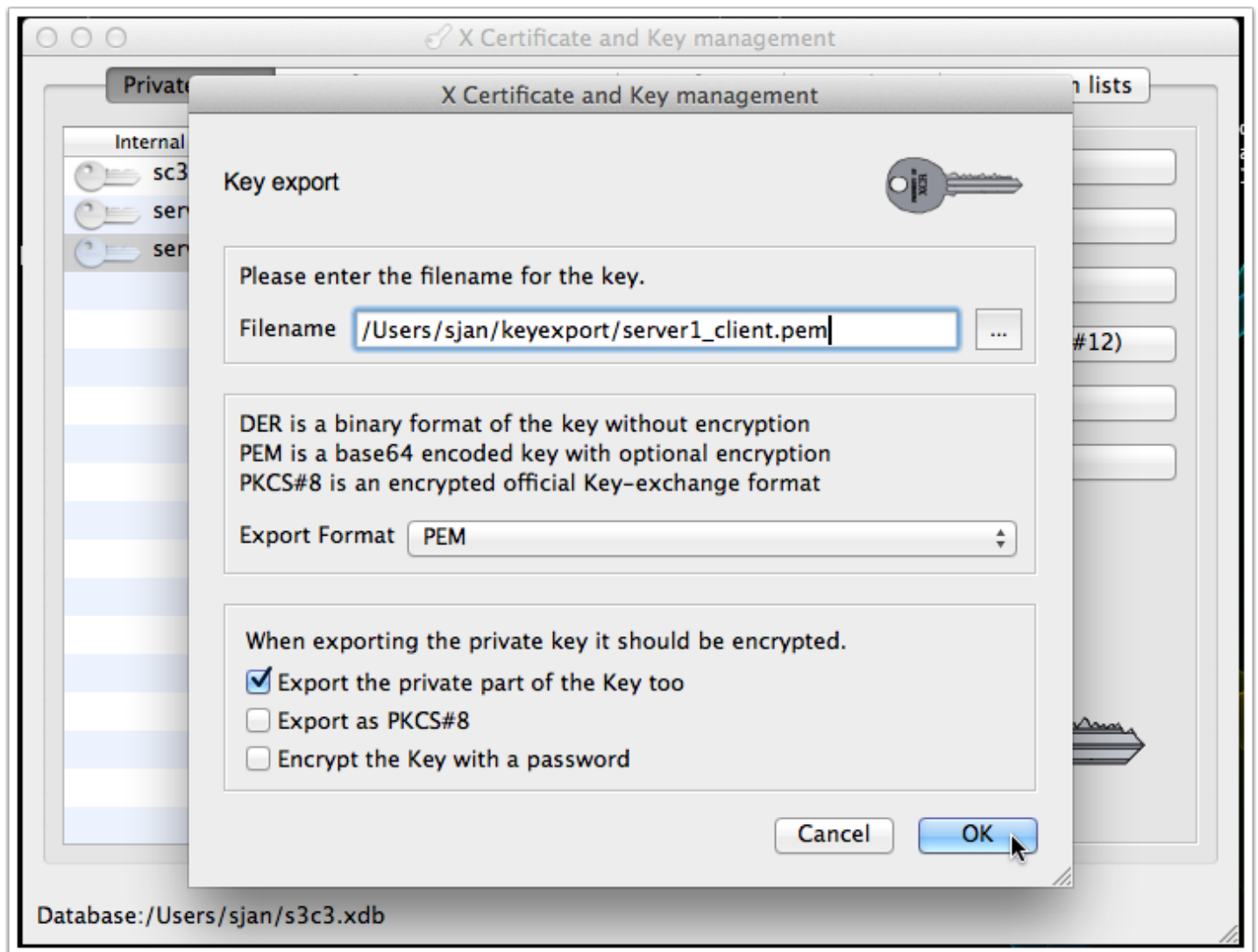
Export the keys for server 1, the private server key ...



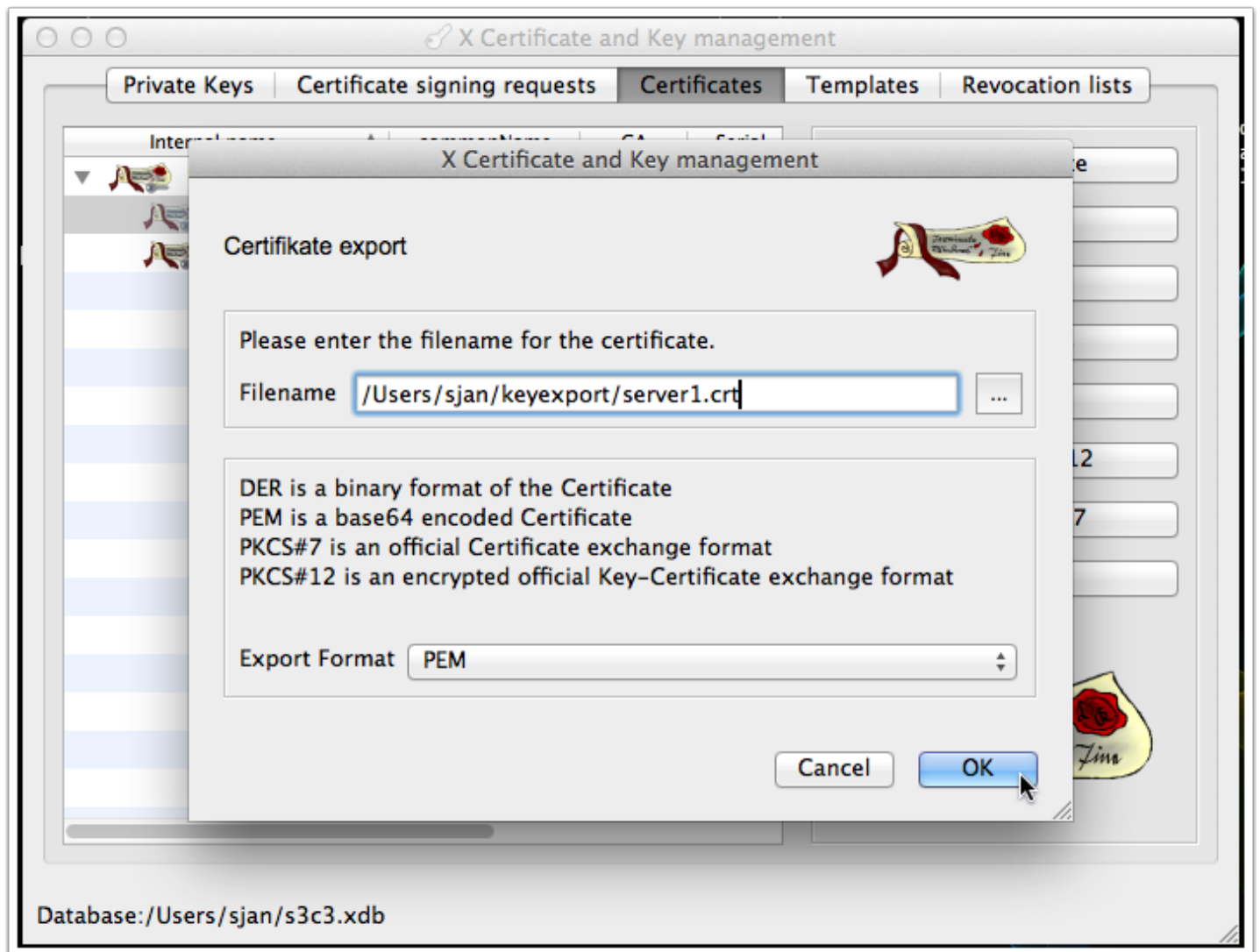
... which should be named **servername.pem** (server1.pem for our example server1)



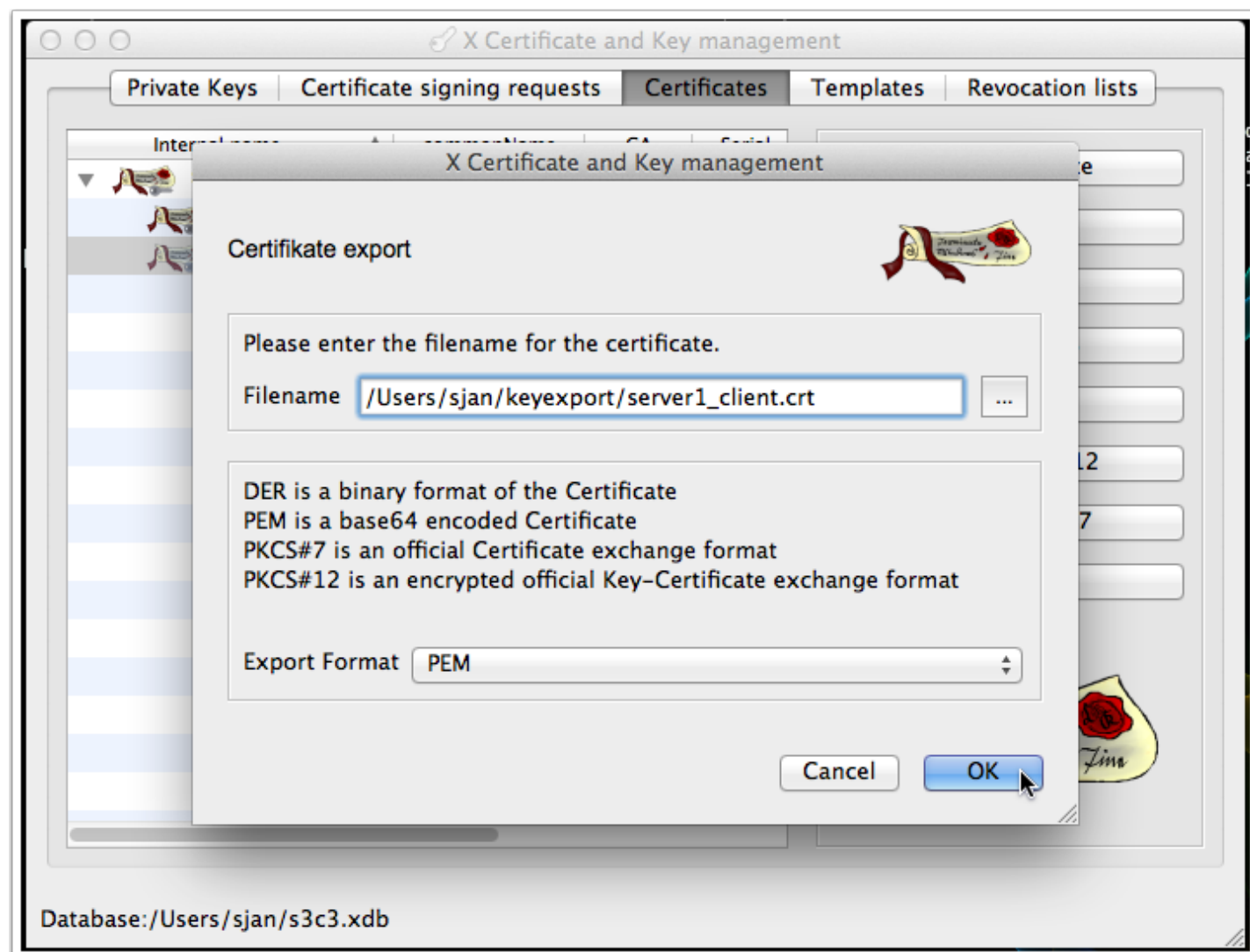
Export the client private key (servername_client.pem - or server1_client.pem for our example server1)



Export the certificates - same naming scheme as the keys, but with the crt extension



... client certificate the same



And don't forget the root CA certificate

