CAcert Client Certificate – Step by Step

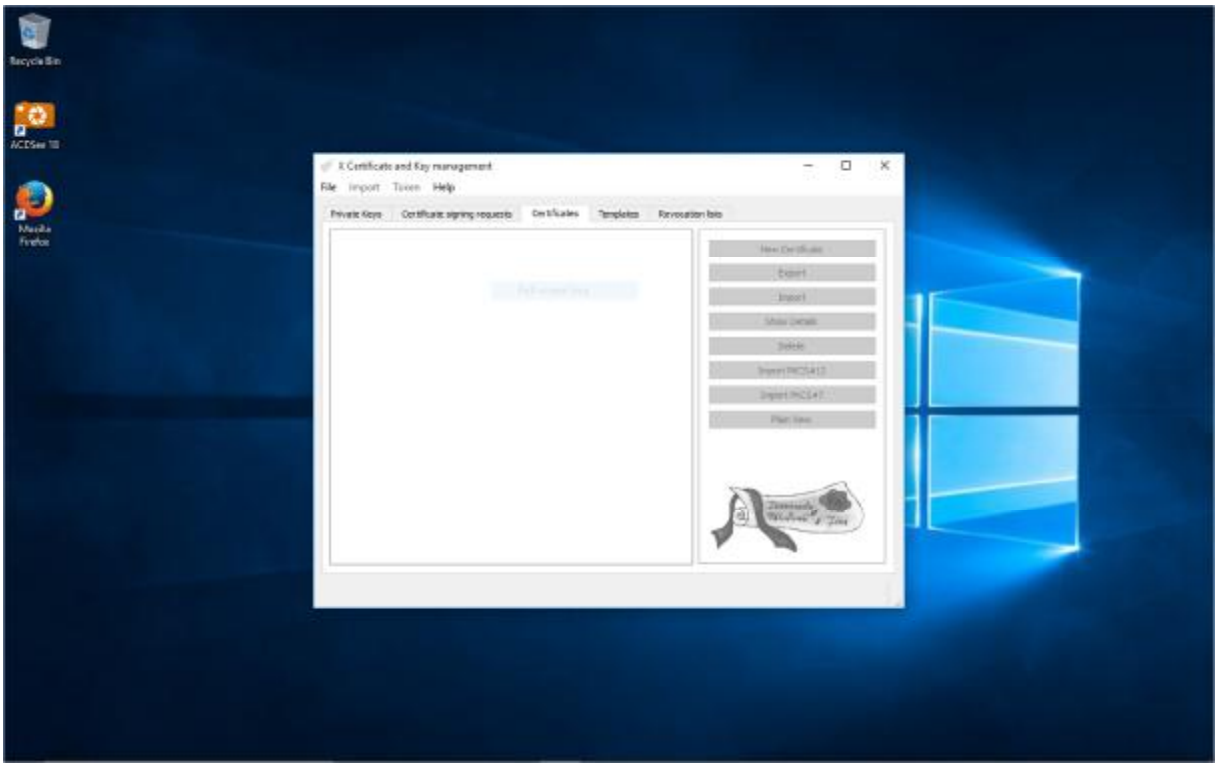
This document instructs to request a certificate and prepare it to get a PKCS#12 file.
In this document I used the CAcert test system. The usage is similar to the production system.

Prerequisites:

Imported and trusted “CAcert Public Root Certificate” in the Web-Browser.
Installed certificate manager XCA http://sourceforge.net/projects/xca/
Activated account at https://secure.cacert.org

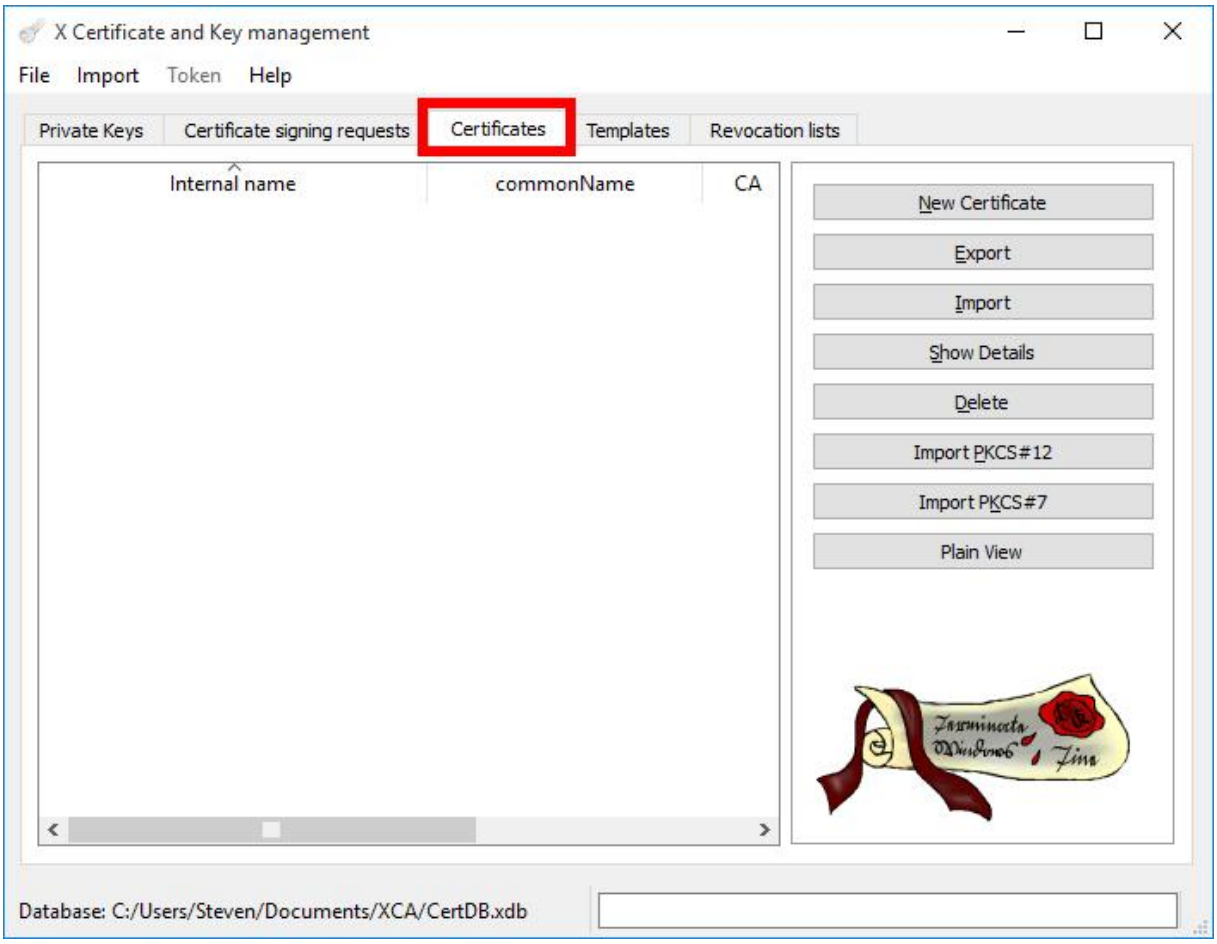
Author: Stefan Thode Creation Date: 2015-10-16 V4

Preparation



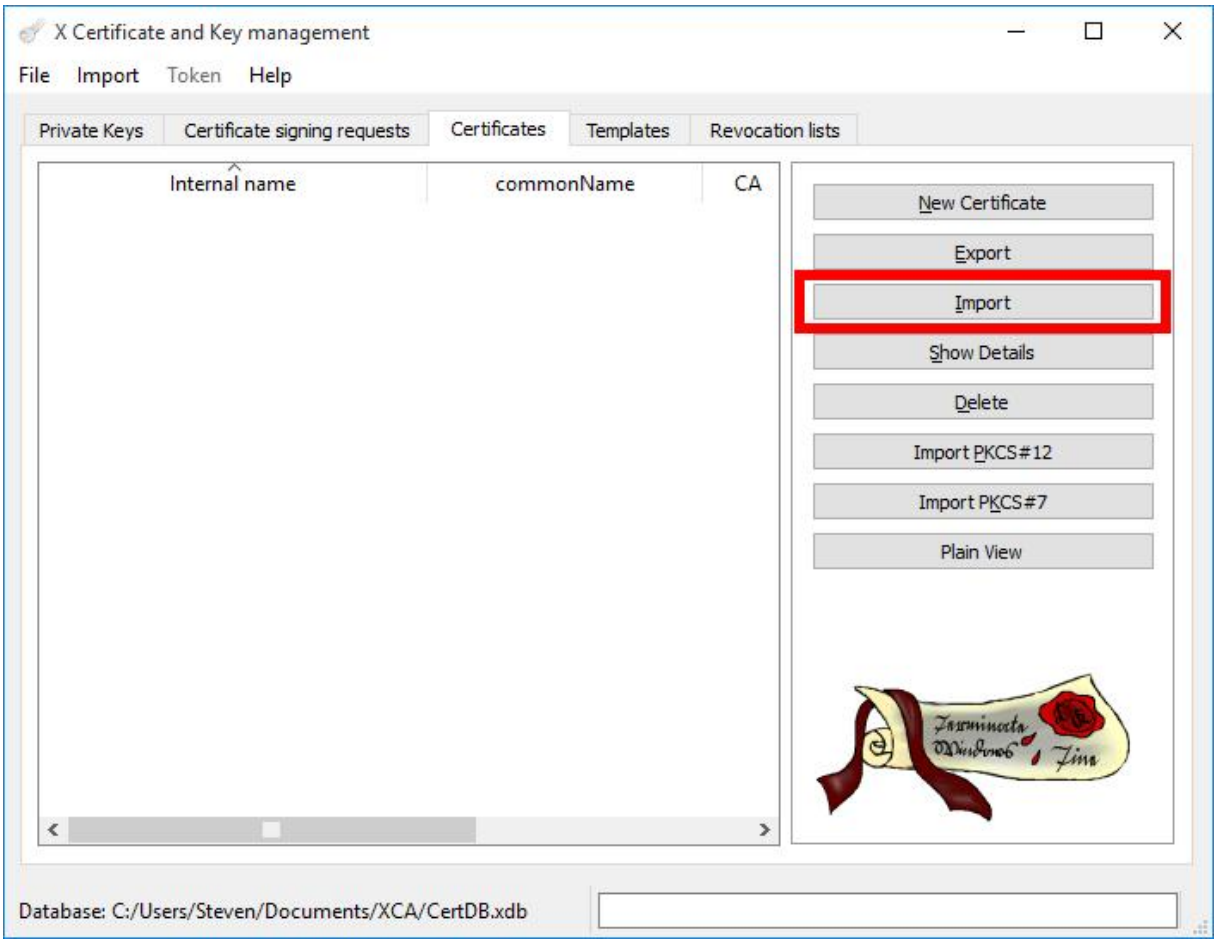
Start XCA

At the “File” menu use “New DataBase” to create a certificate database and save it to a file. Don’t lose your password to the new database! Or open an existing database from your filesystem.

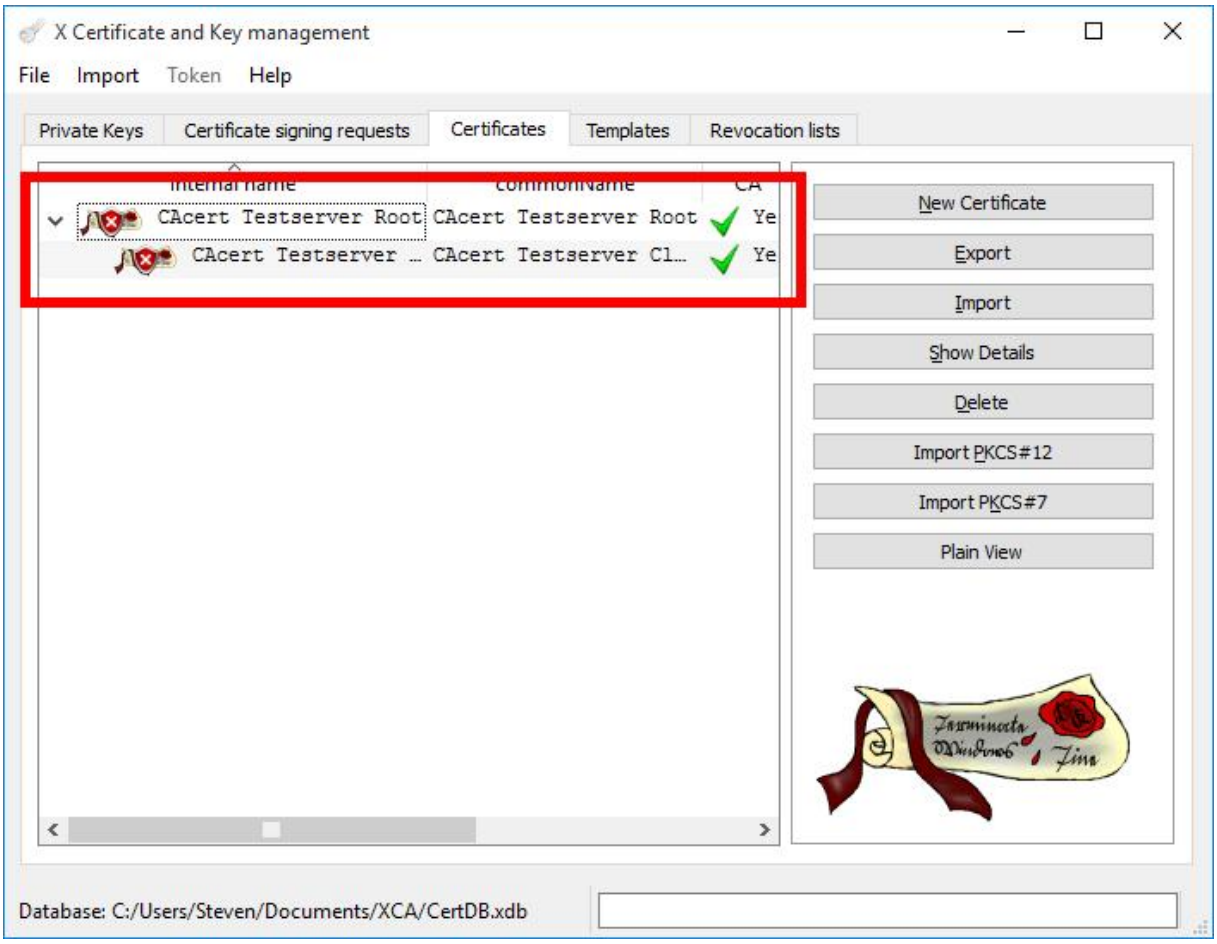


Go into tab “Certificates”.

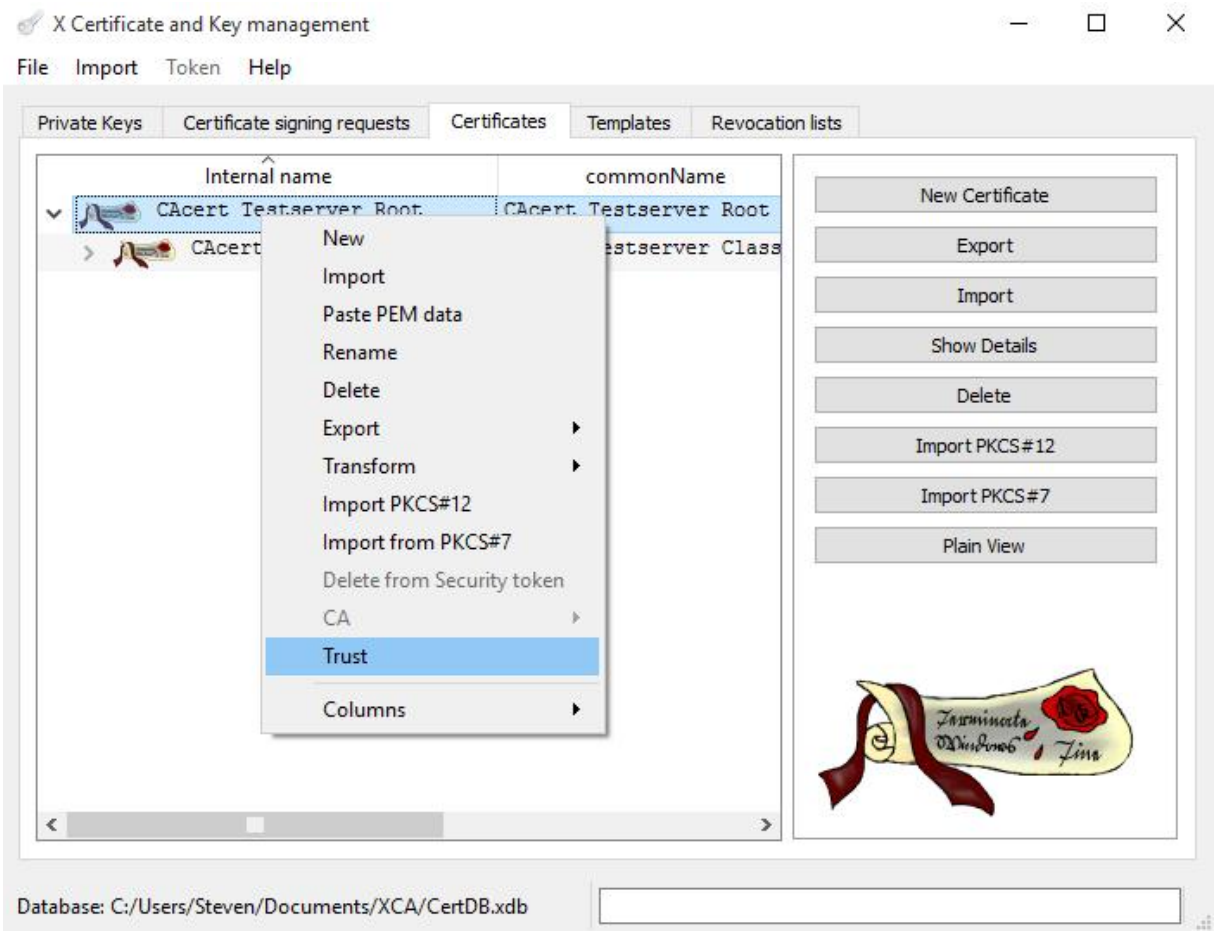
Support



Use “Import” to allow XCA to recognize certificates of CAcert.

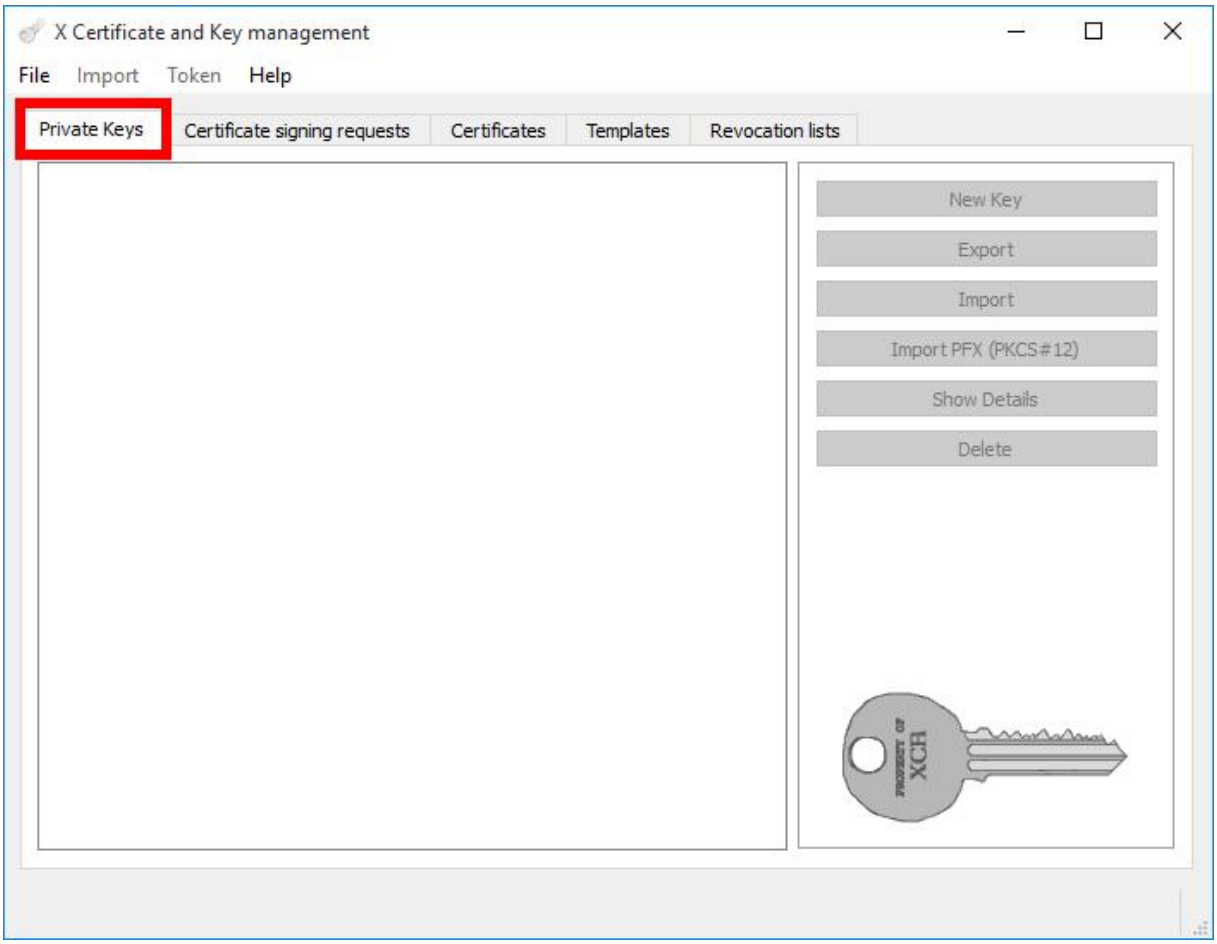


Import the “CAcert Public Root Certificates” “root” and “class3” in this order.

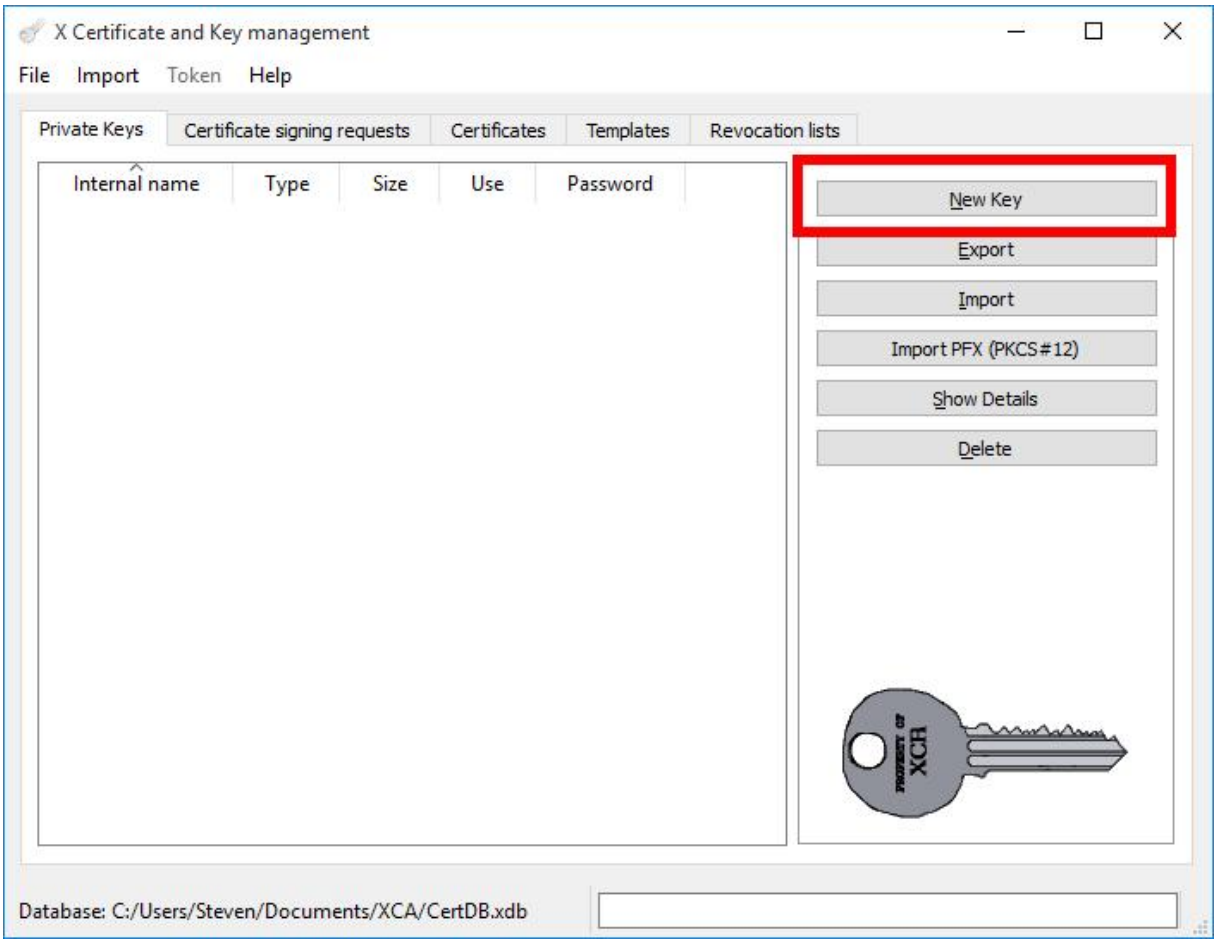


Trust the imported “CAcert Public Root Certificates” in the Context Menu with “Trust”.

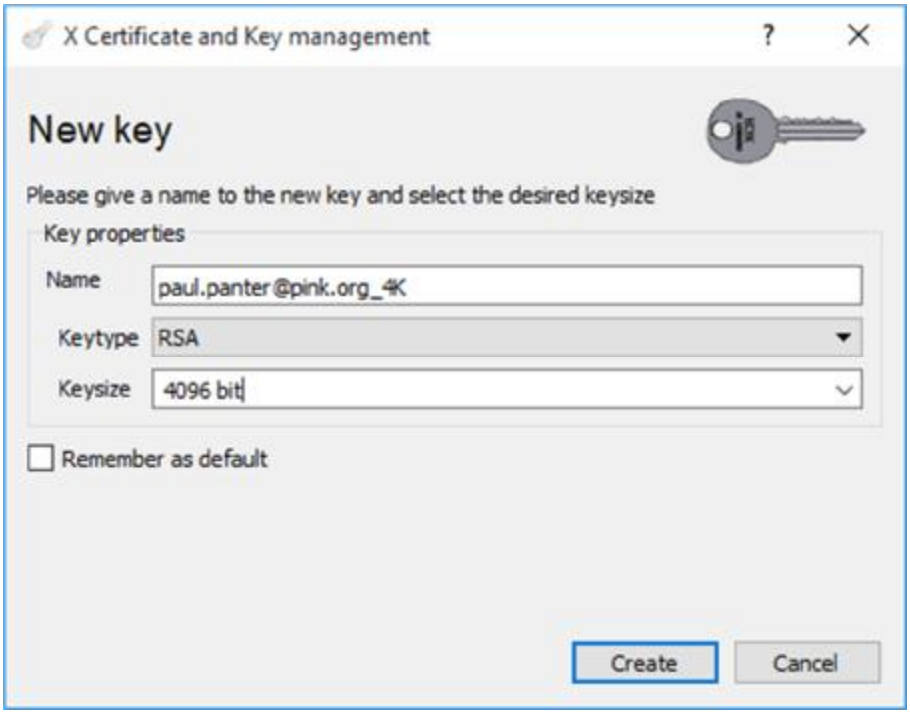
Private Key



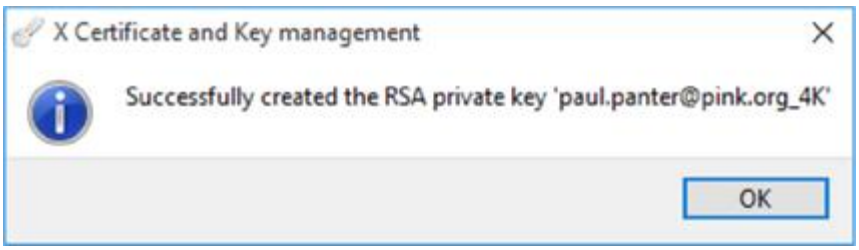
Go into tabs “Private Keys”.



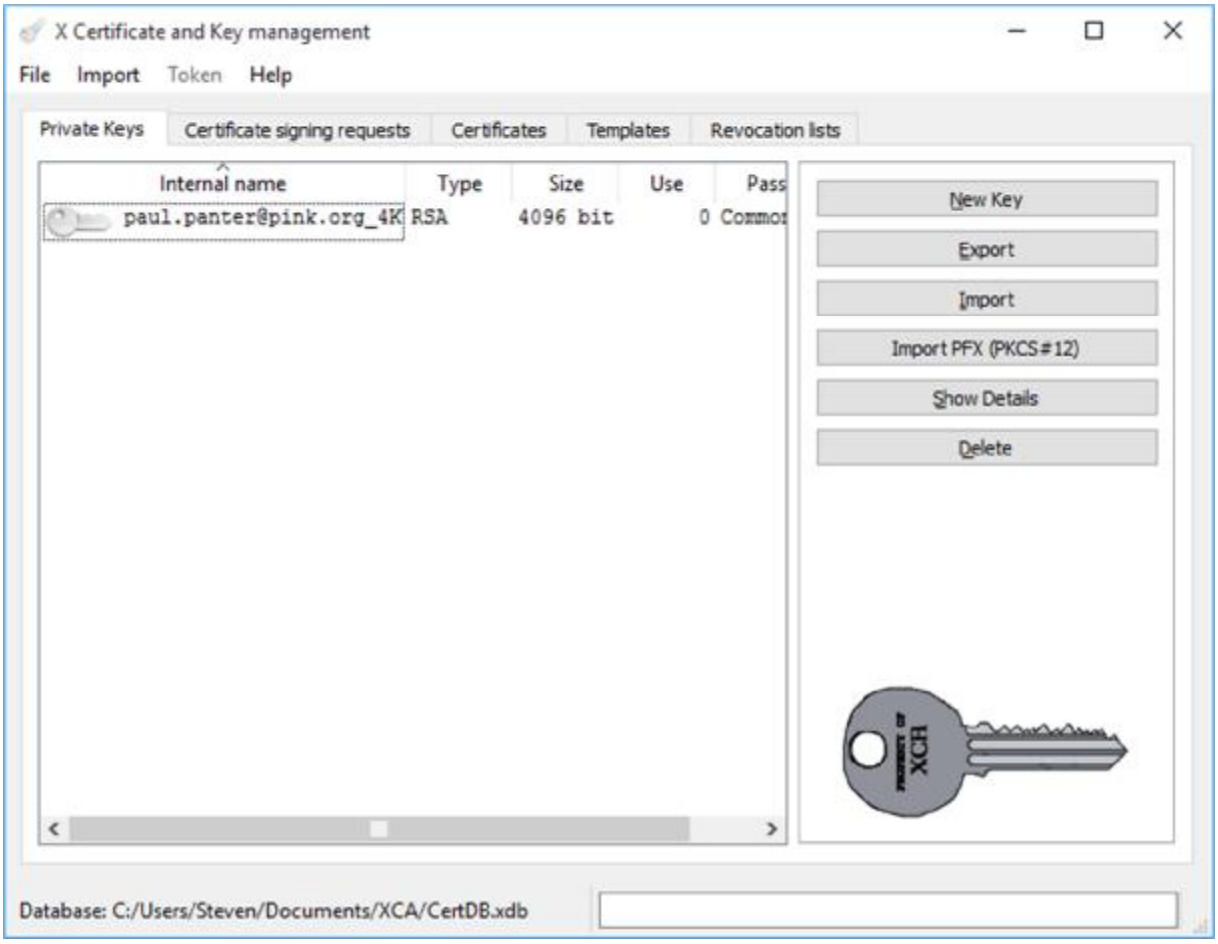
Use “New Key” for a new Private Key.



Choose a name for the new key with e.g. the intended purpose included. This name is for your reference only.
Use a speaking name of the Key with the planned purpose, that you can identify the Key for reuse of this purpose. Furthermore you need to select the type and strength (size) of the key that should be generated. Currently RSA with 4096 bit is fine.

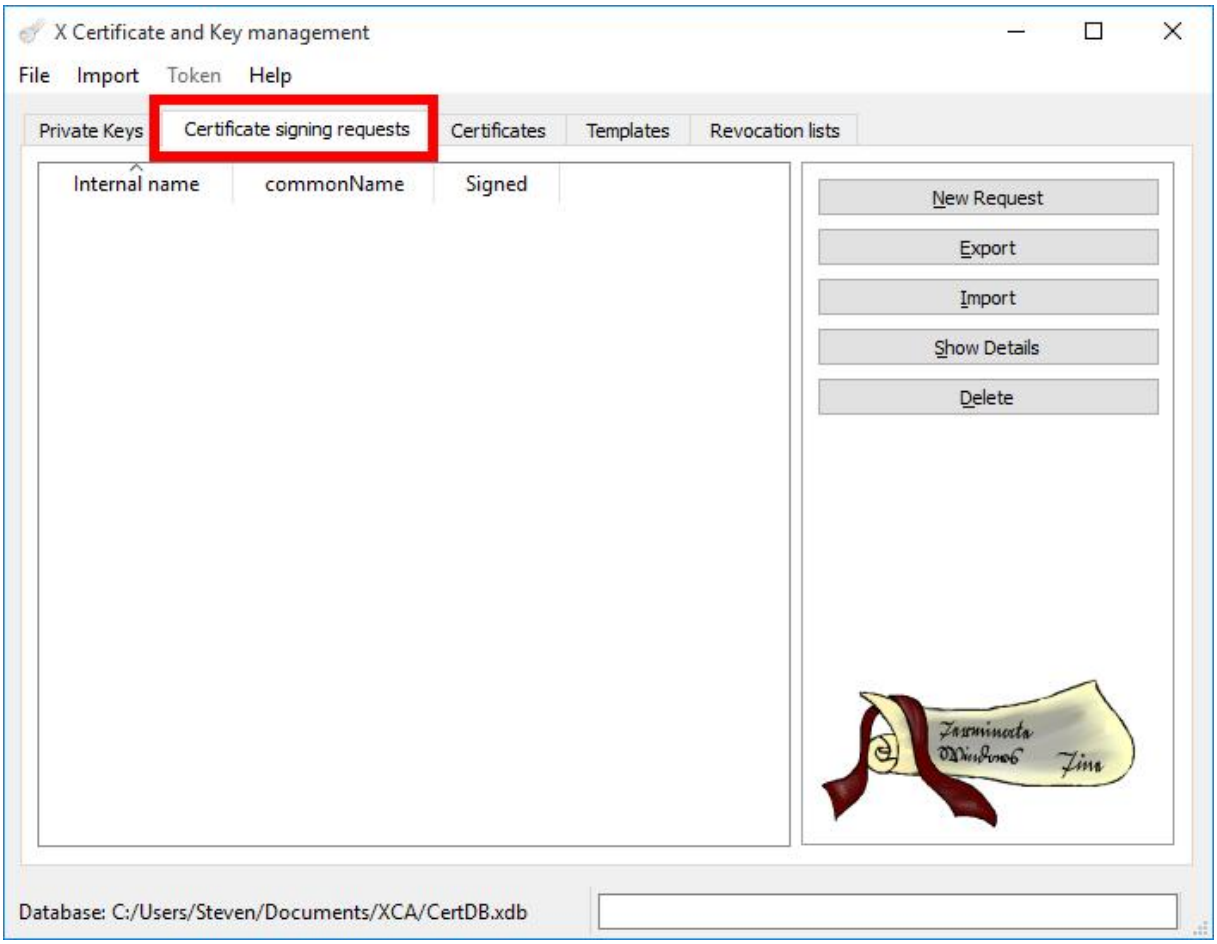


The new Private Key is ready and…

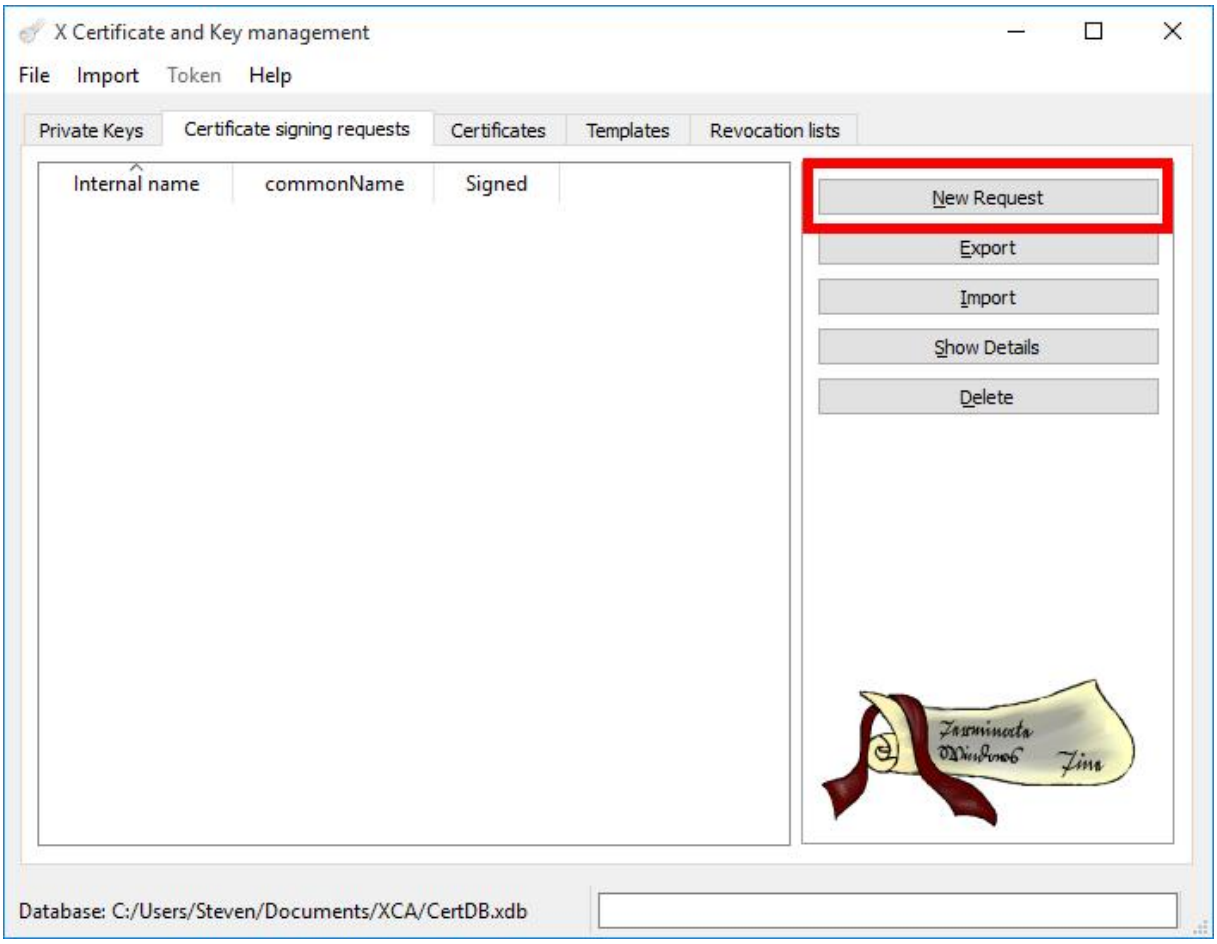


...appears in your list of private Keys.

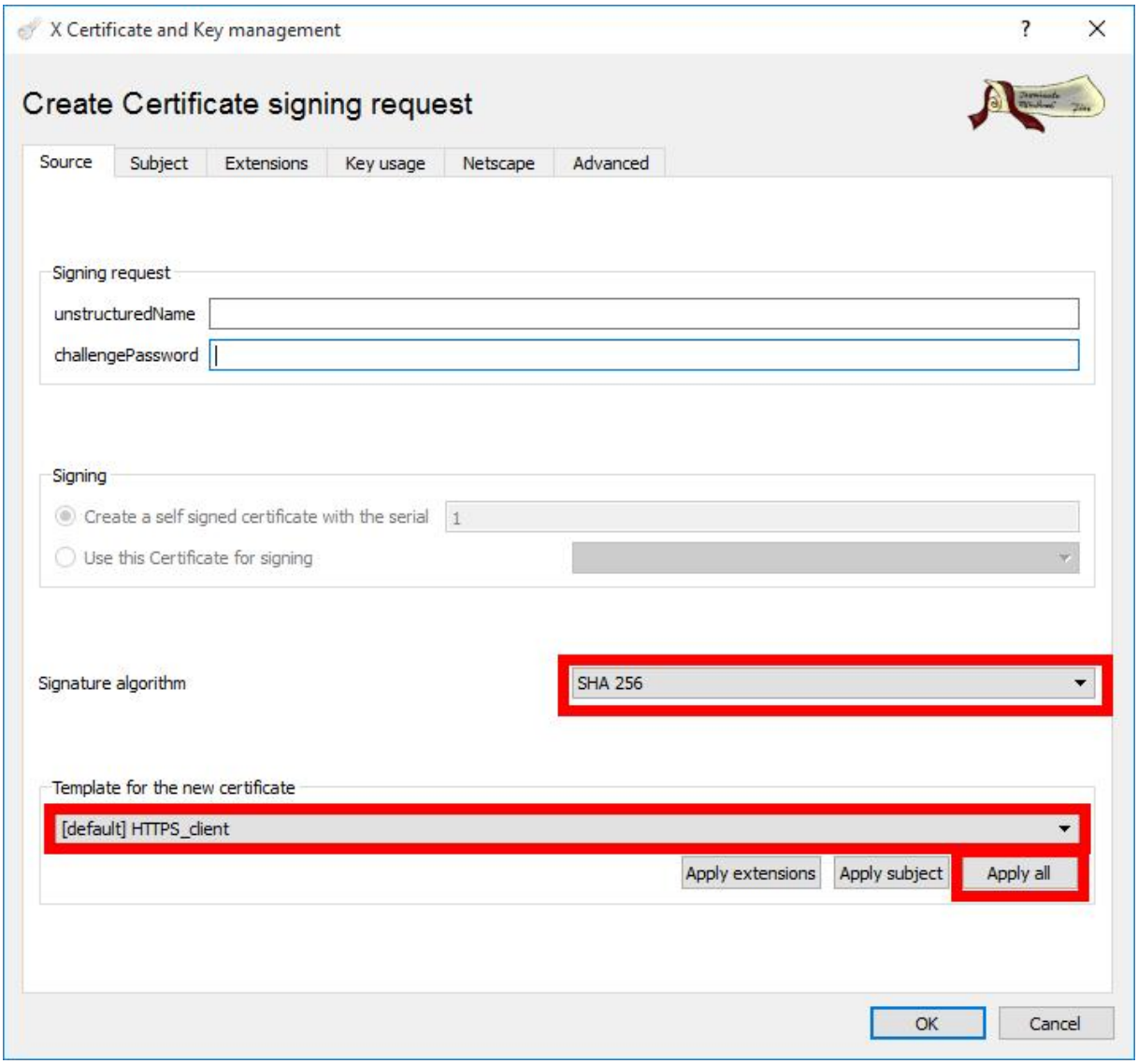
Certificate Signing Request – CSR



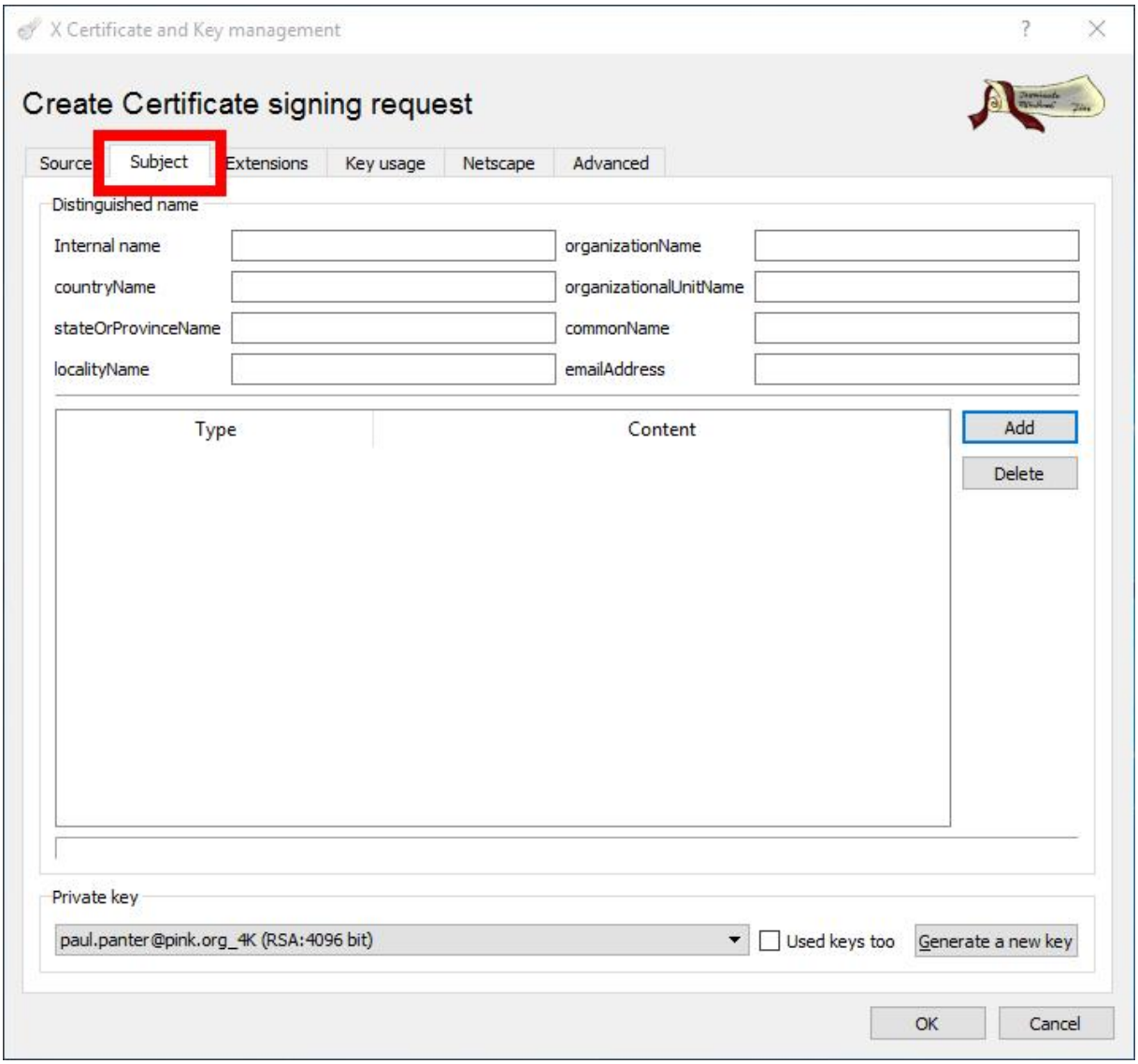
For the next step go into tab “Certificate signing requests”



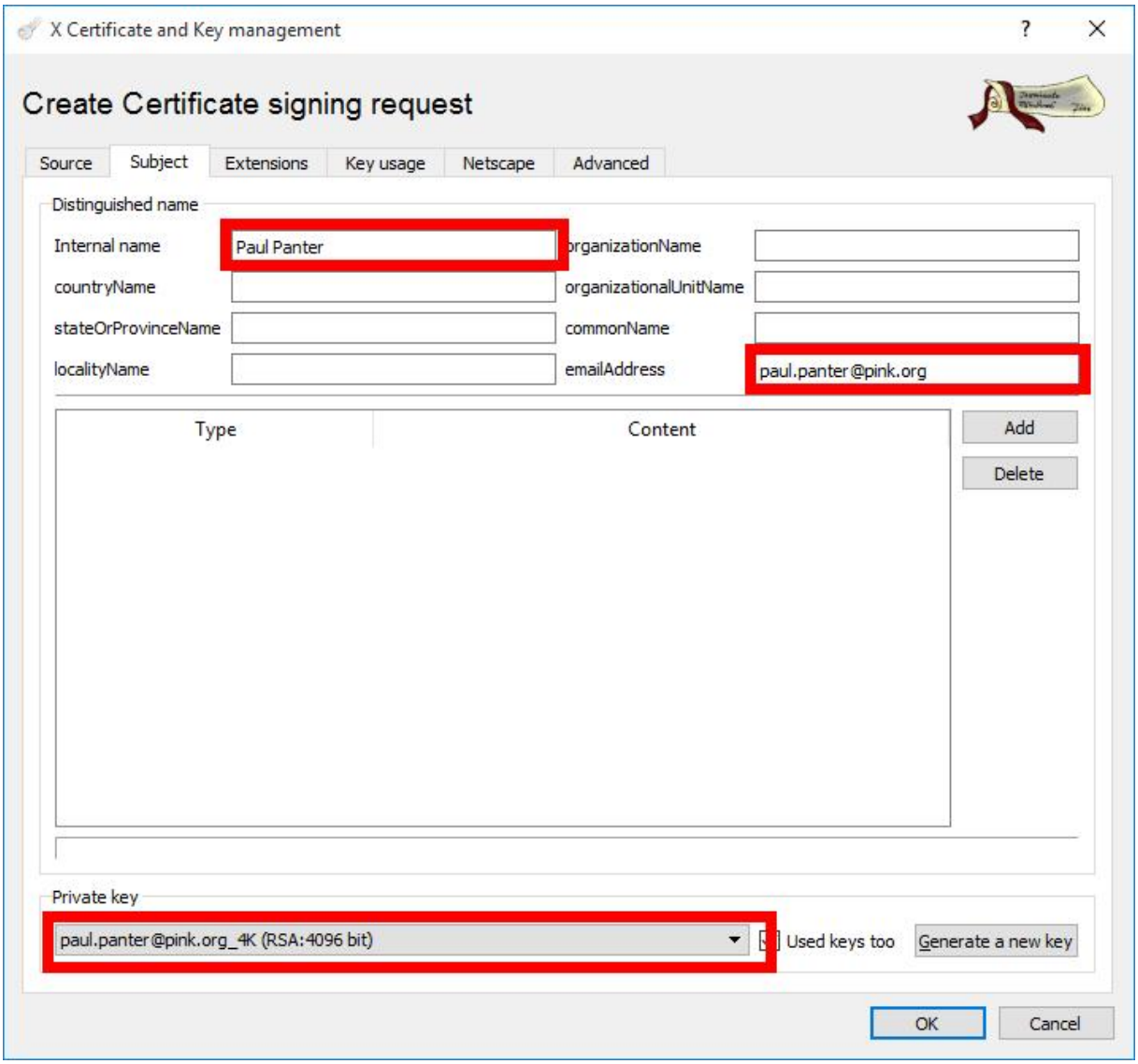
Use “New Request” to create a CSR.



Select a certificate template first and apply it, then choose the signature algorithm.

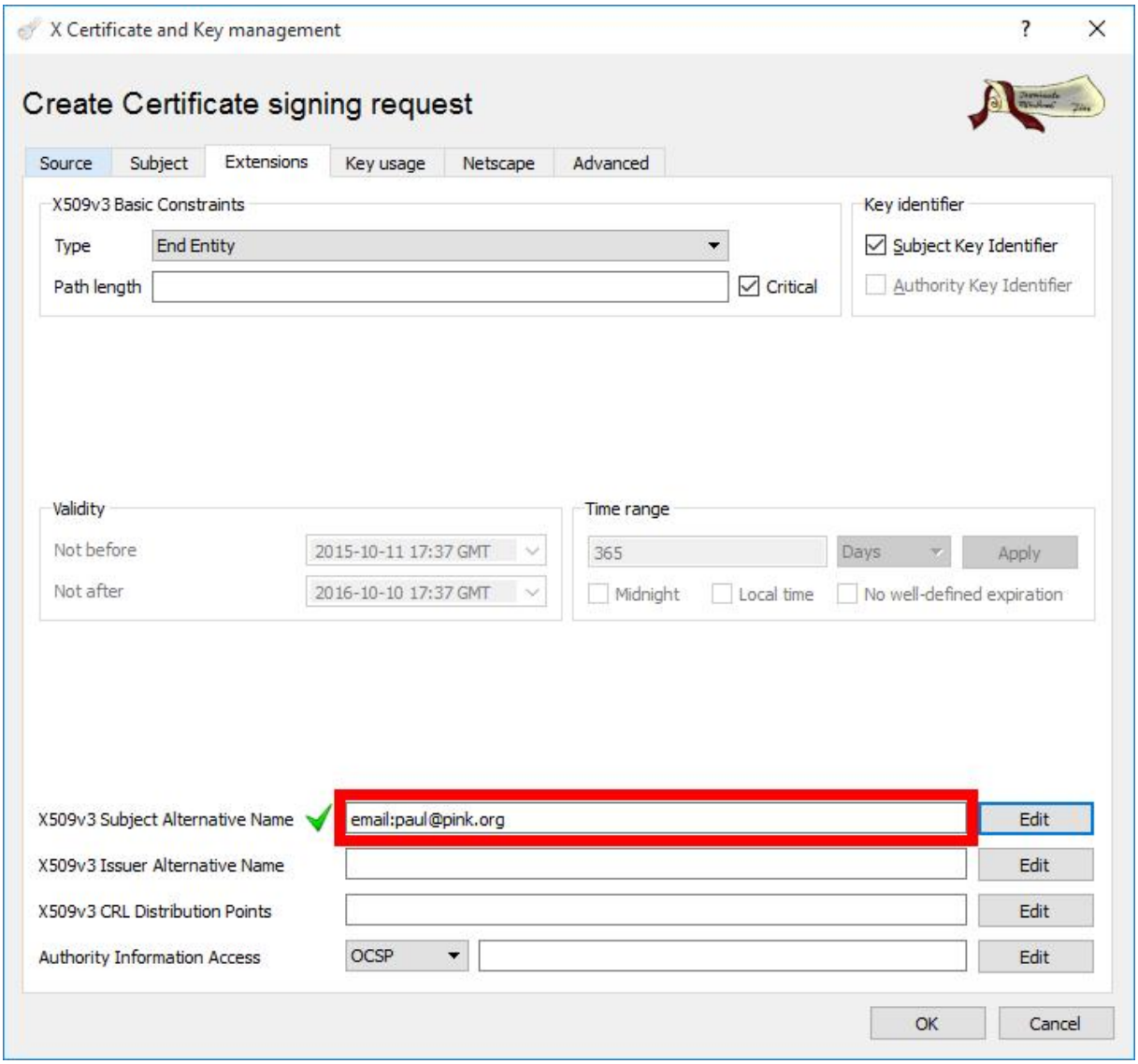


Go into tab “Subject”.

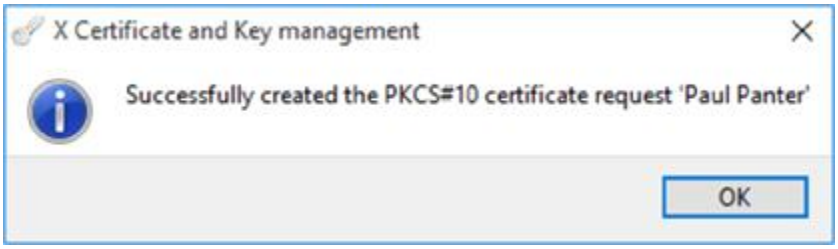


Select the Private Key to use, Insert the „Internal Name“ and the „emailAddress“.

In the bottom of the dialog you can choose to select one of the existing private keys or create a new one in case you forgot to create one before starting the CSR creation.

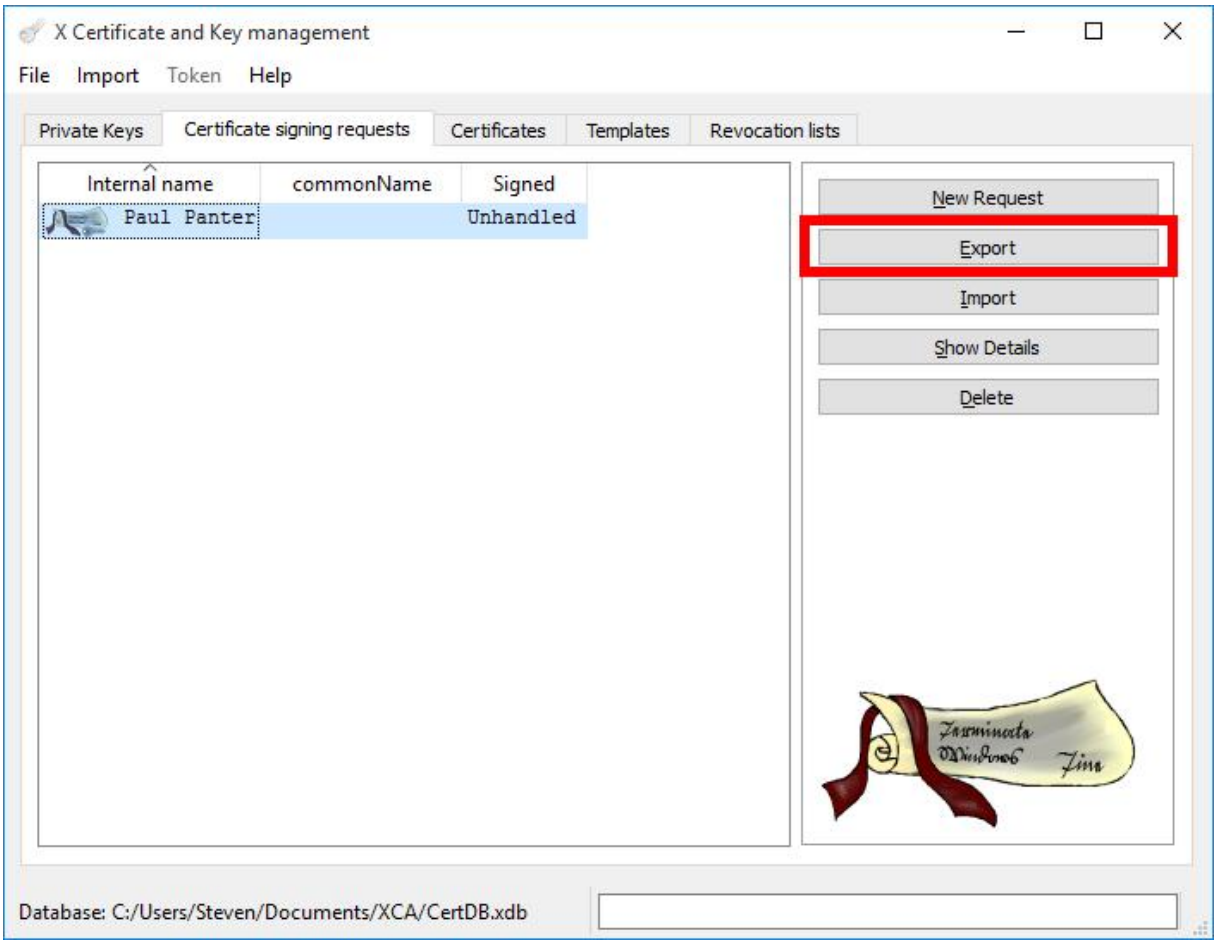


As option, you can include Aliases into the field “X509v3 Subject Alternative Name”. Create the CSR with “OK”.

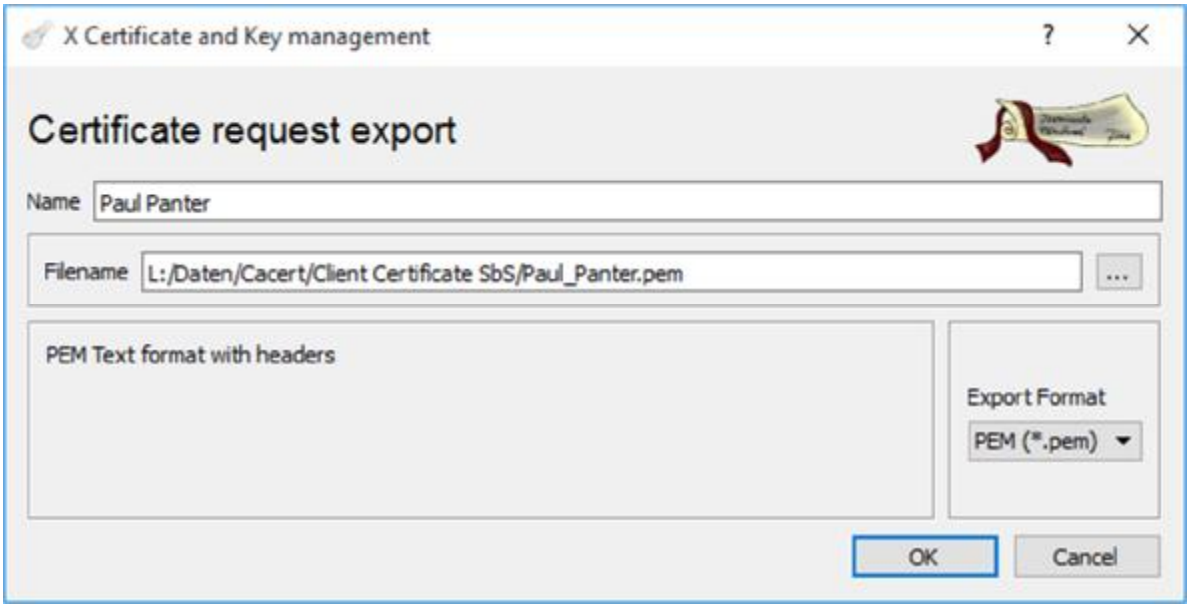


The CSR is ready.

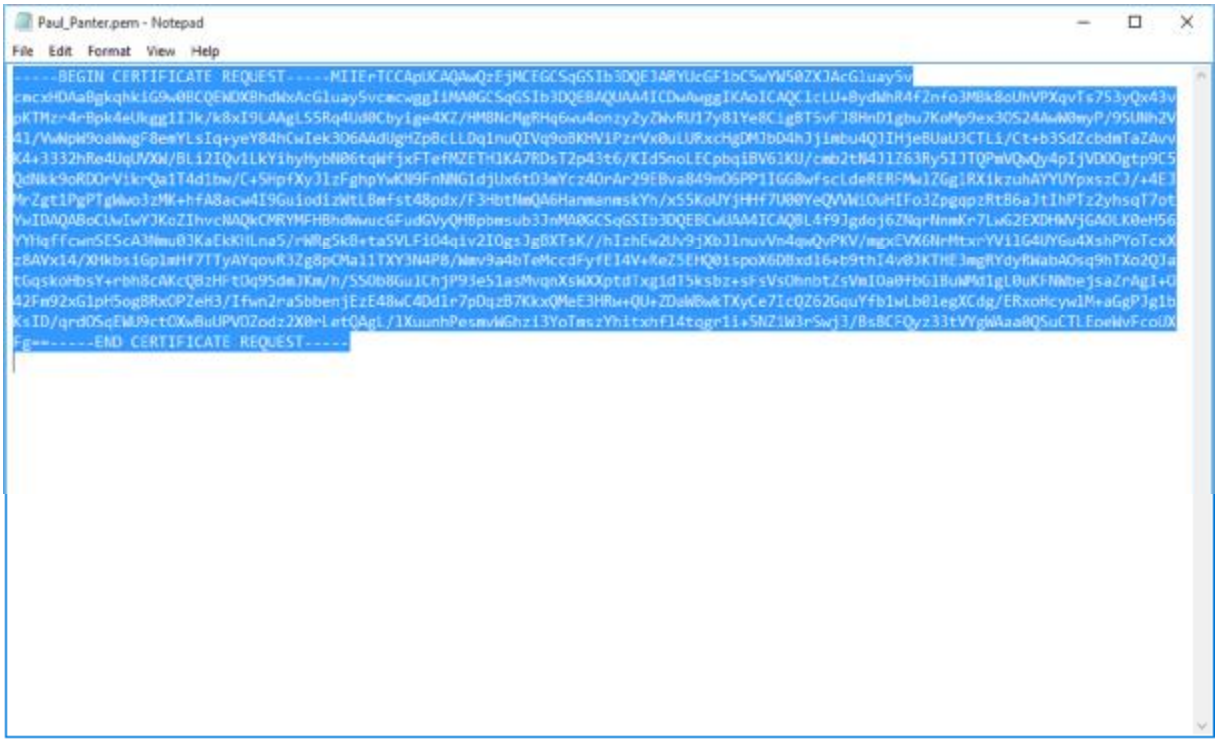
Signing Process



Select the new CSR and “Export”.

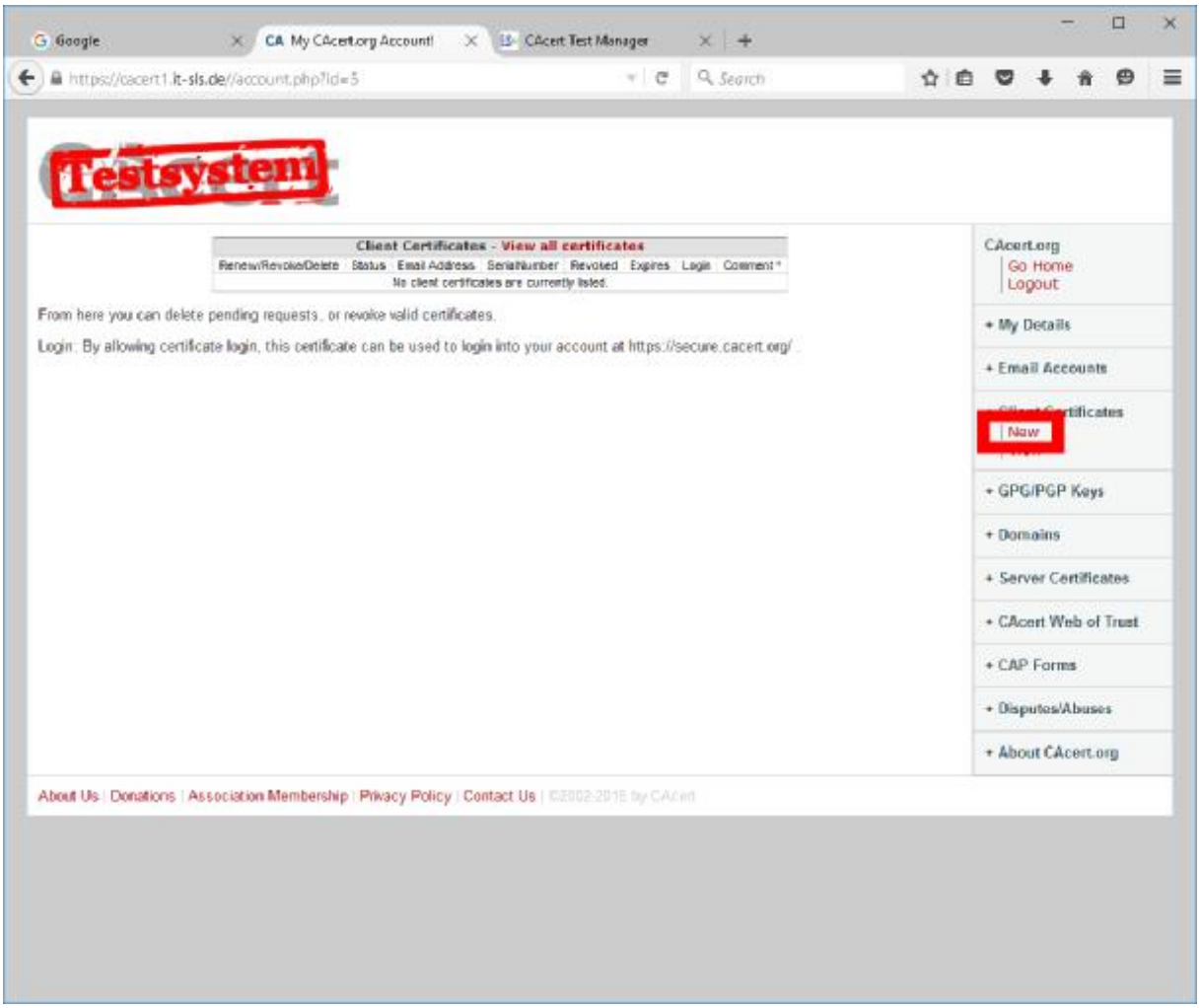


Save the CSR to file in pem Format but with extension .csr

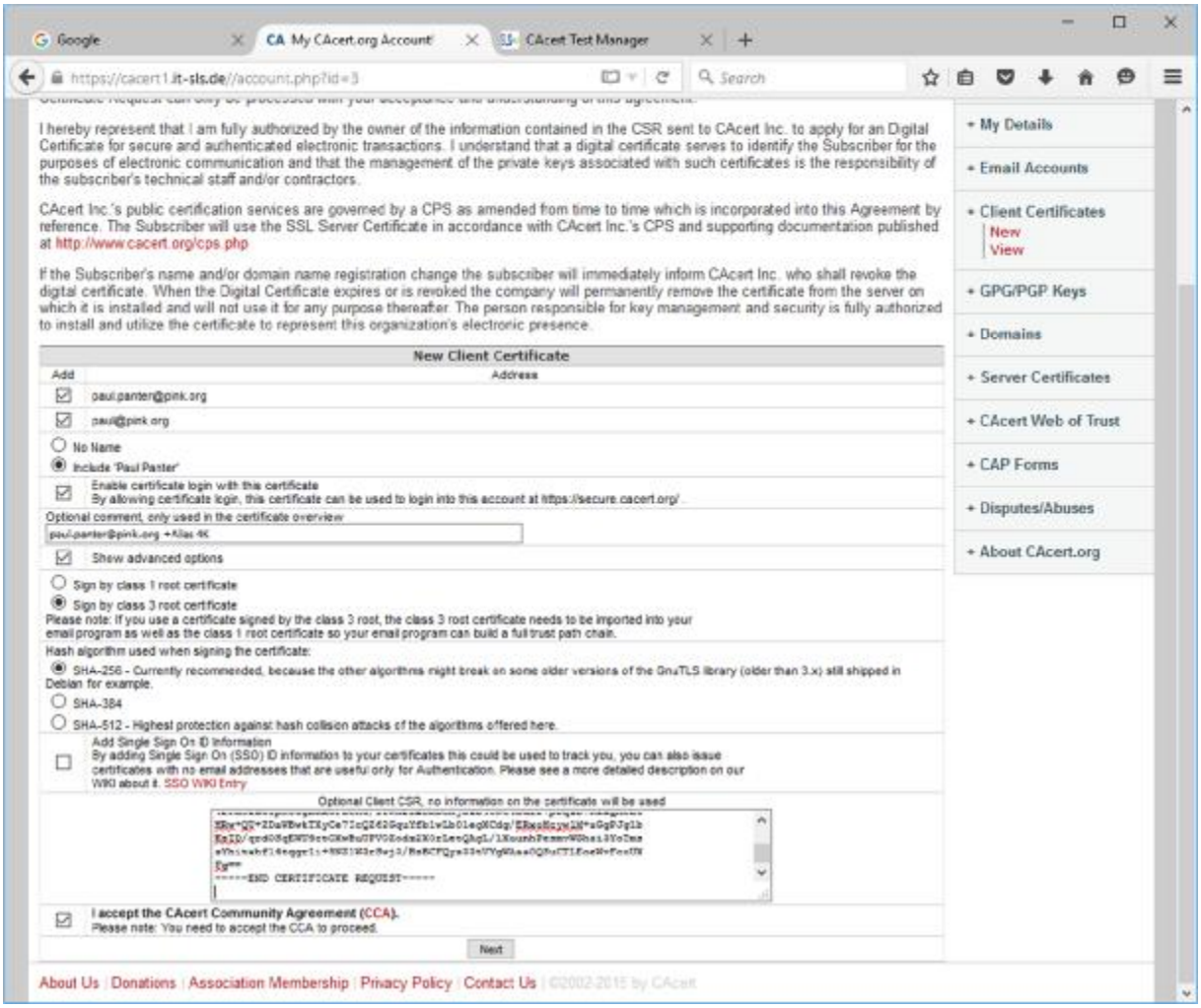


Open the CSR in an editor, select ALL and copy the content.

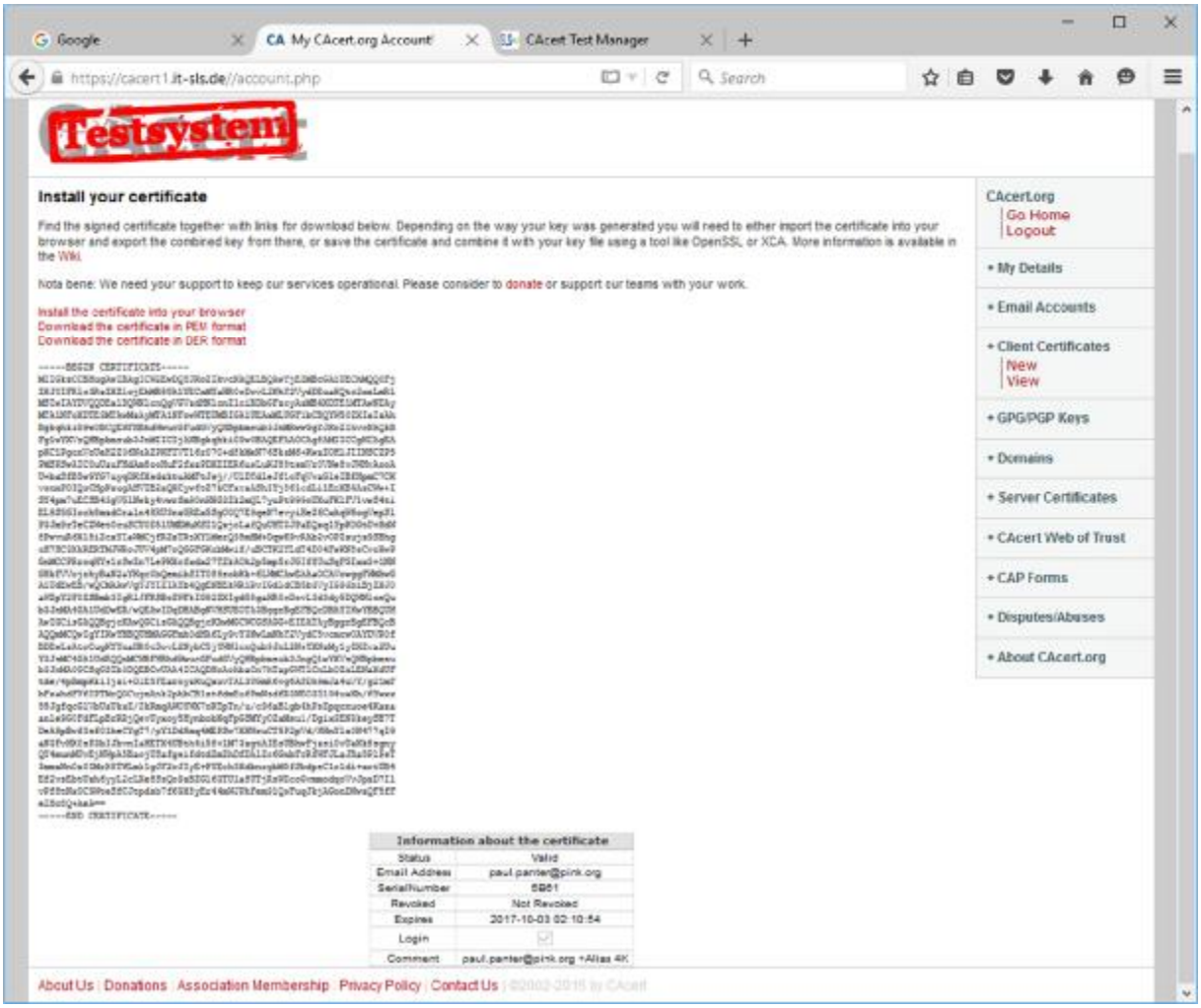
Support



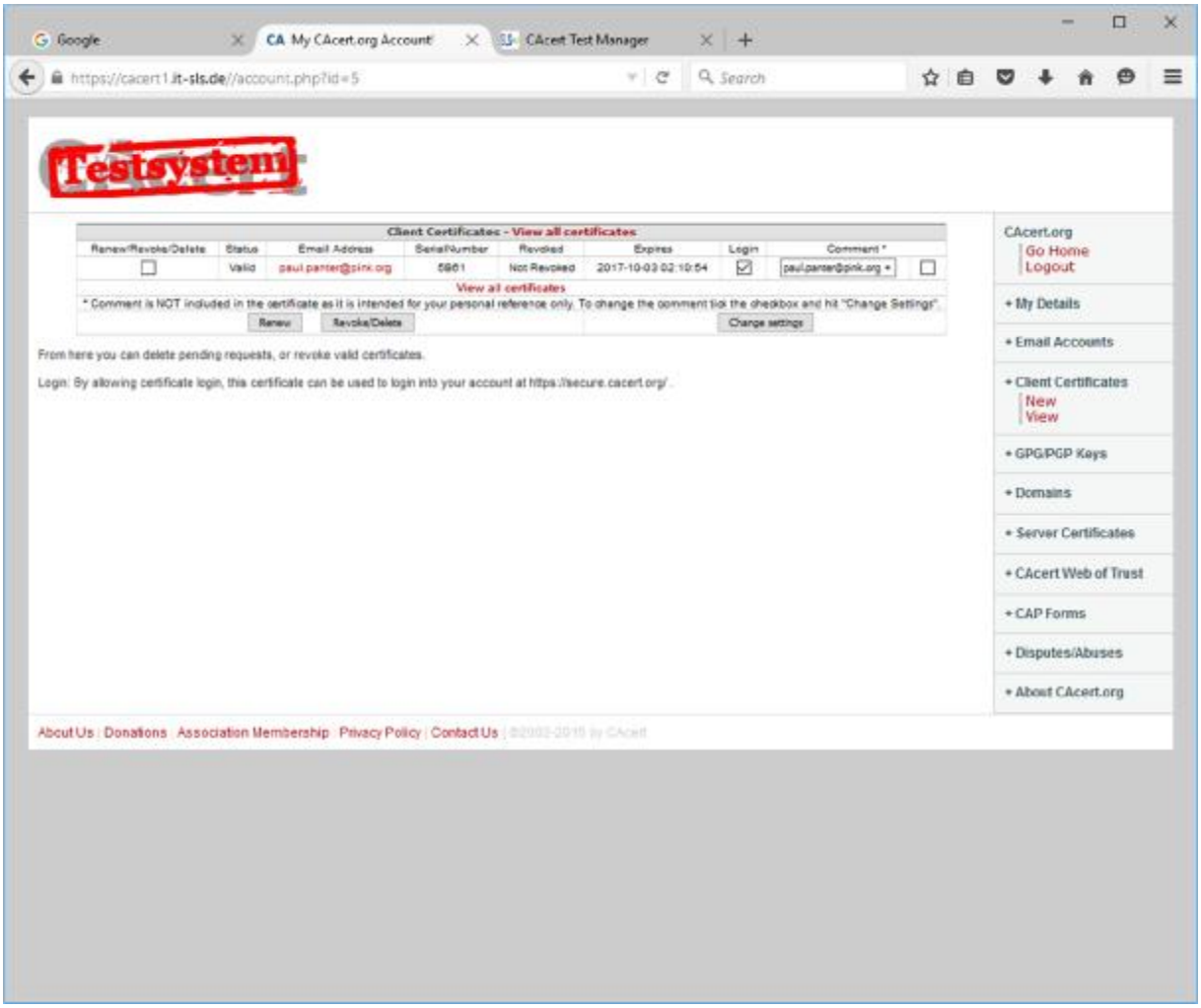
Open Website cacert.org and login into your account. Go into “Client Certificates” and “New”.



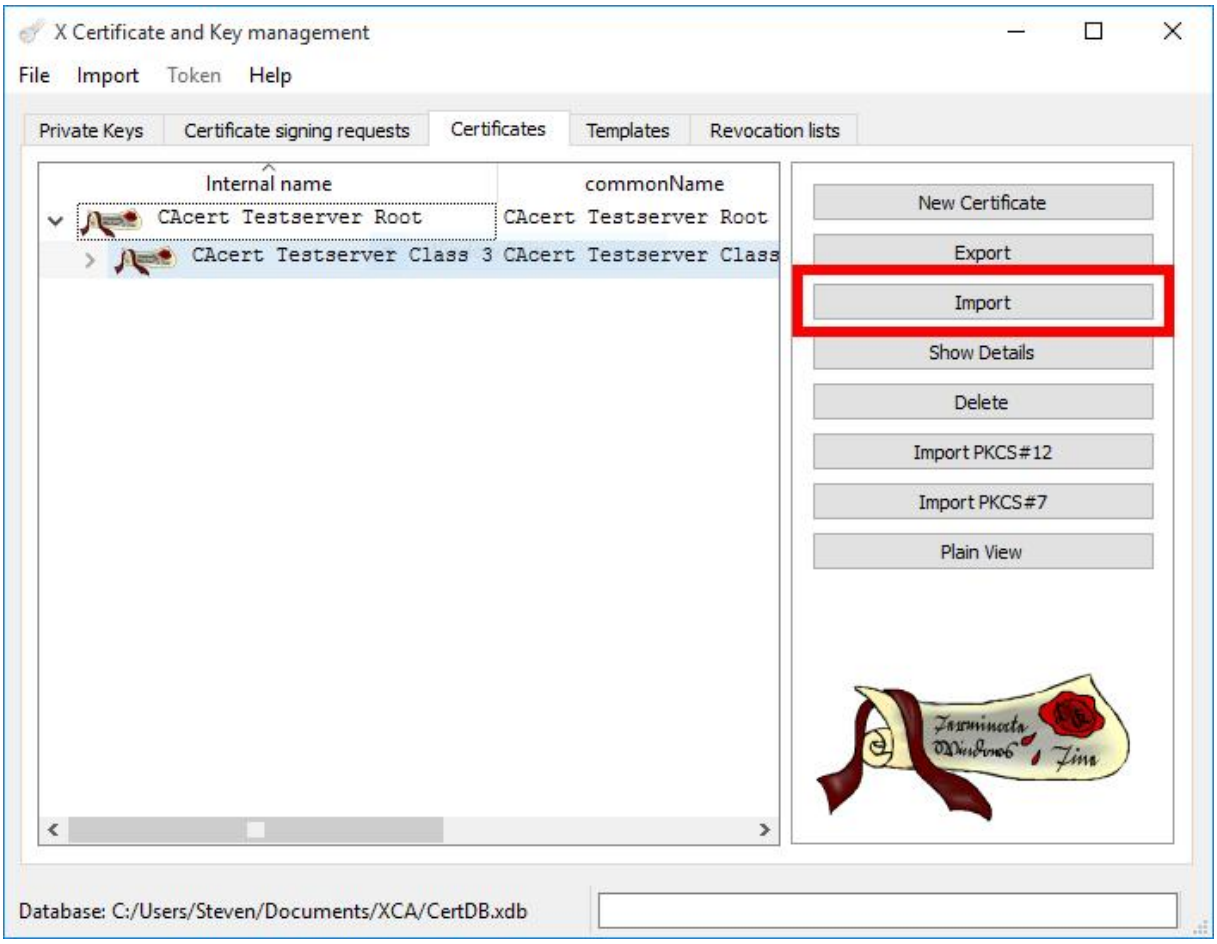
Activate advanced options and insert the CSR into the text area.
Select the email-addresses and your name to include. If presented, choose the signing certificate (only for community members with 50 AP or more) that you want your certificate signed with. Preferably you should use the class 3 certificate option here. Enter a comment for the certificate for future identification. “Next”



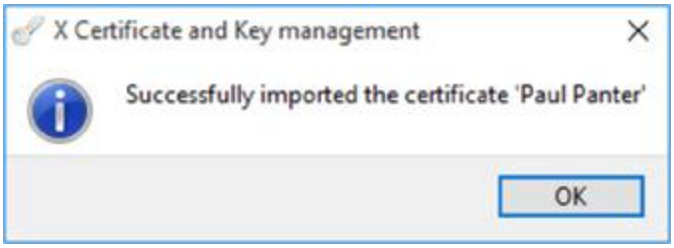
As result the new certificate will be displayed in the browser. Use the link “Download the certificate in PEM format” to save the certificate in the pem Format. As an alternative you can select the cryptic blob of text below including the BEGIN/END CERTIFICATE lines for direct import using "Import (PEM)" in XCA.



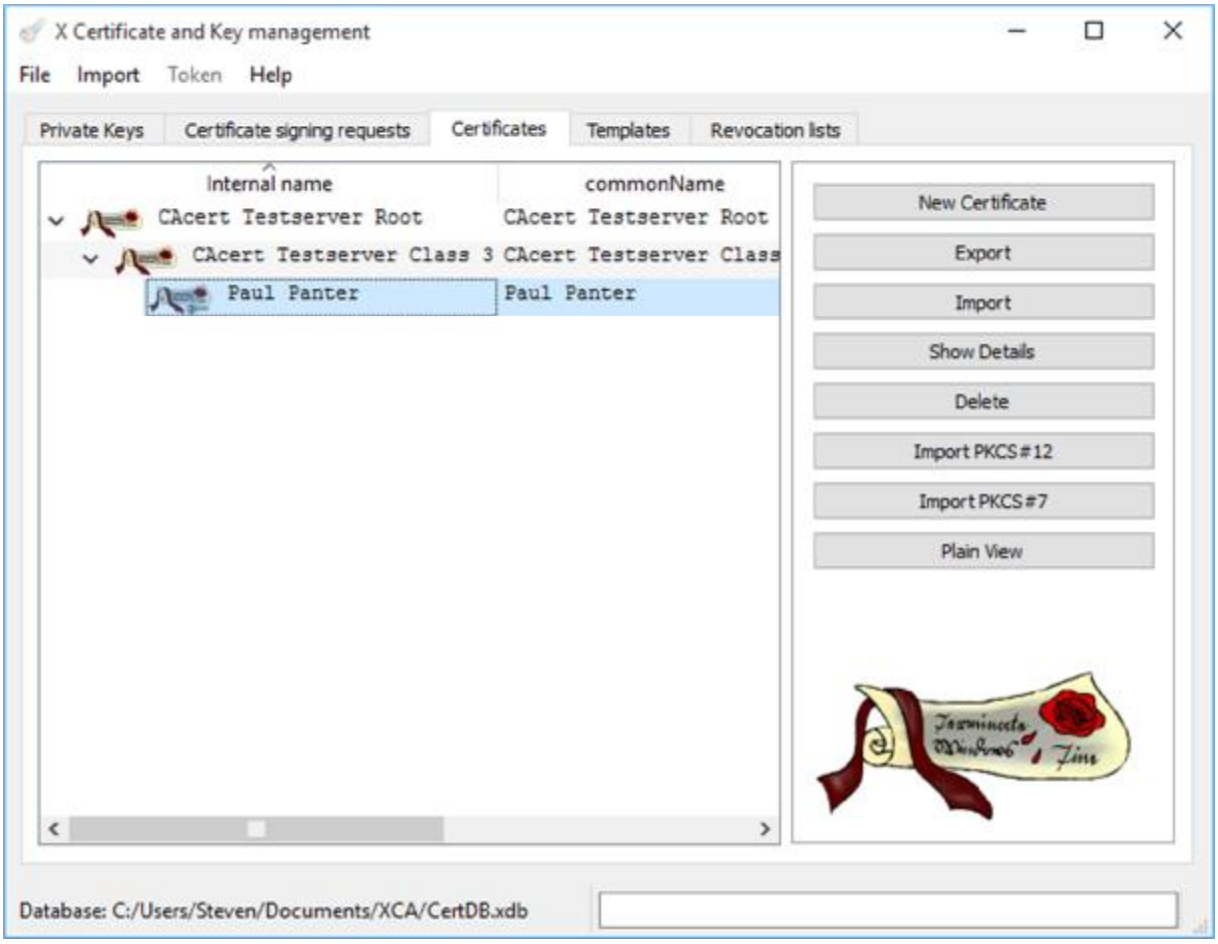
See the certificate in “Client Certificates” and “View”.



Use “Import” in XCA to import the certificate result from the CA.

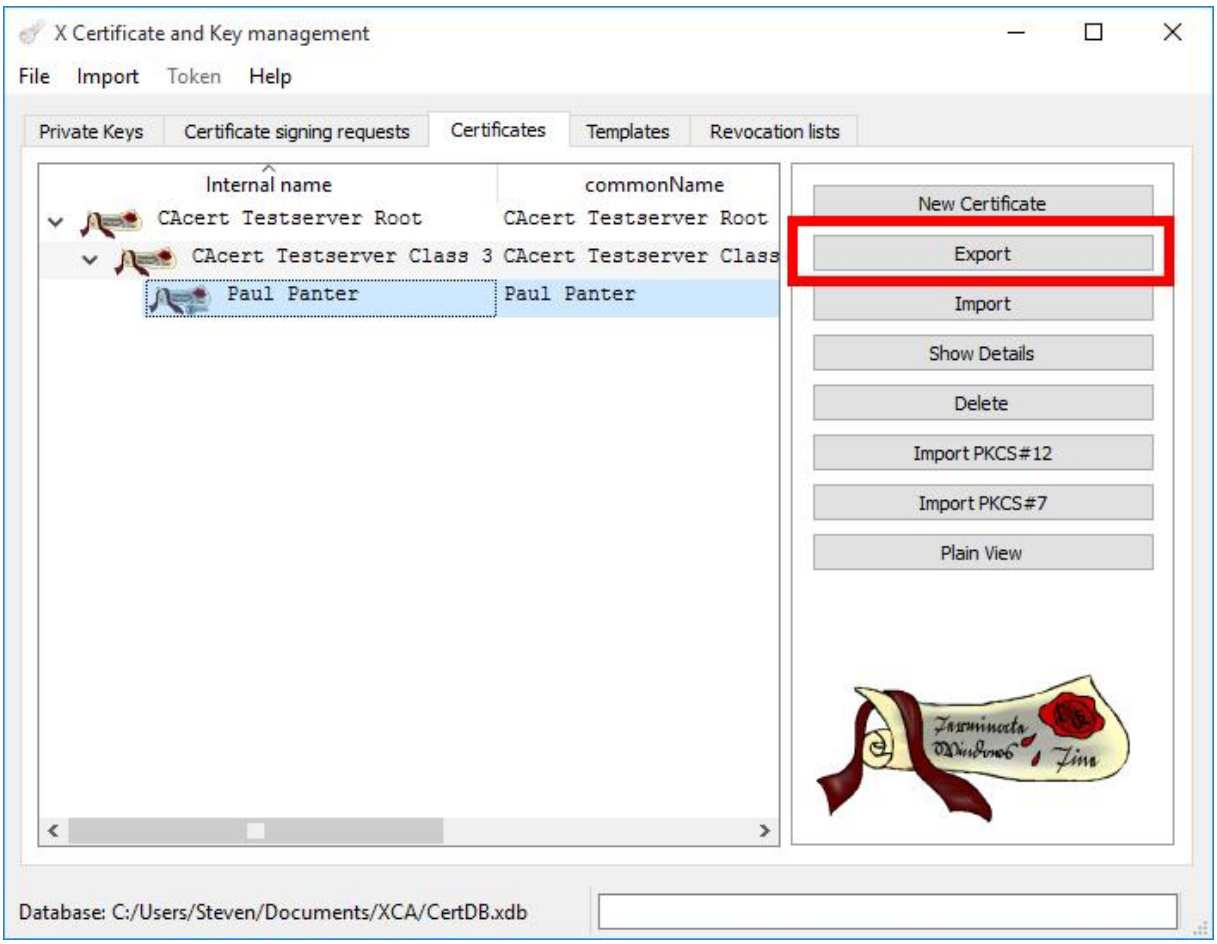


Import was successful.

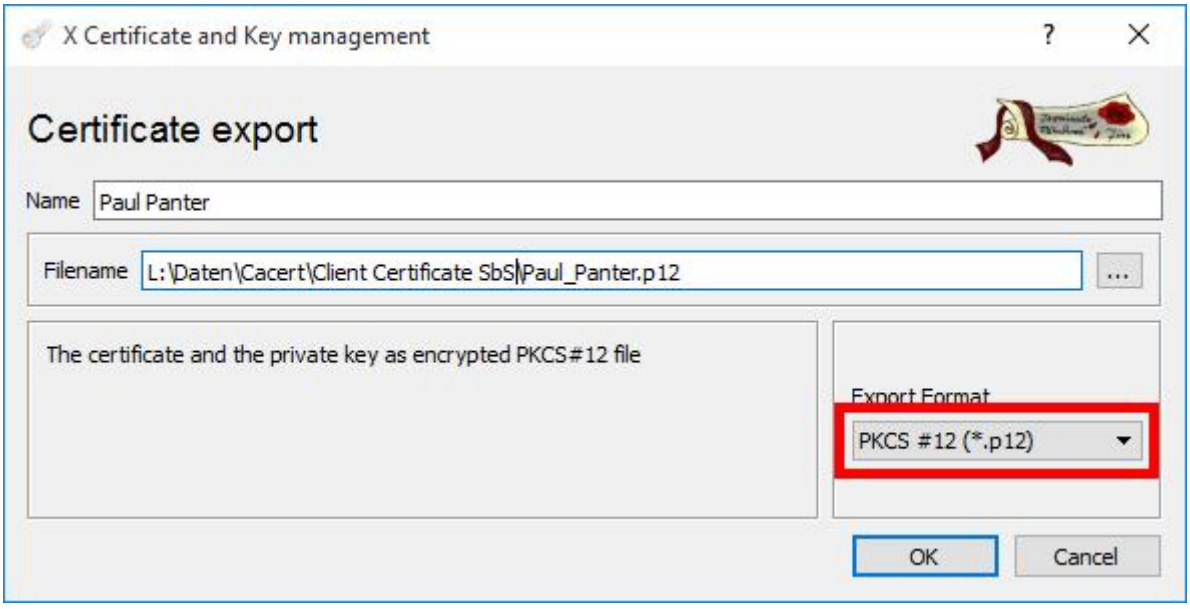


The certificate is listed below the signer certificate you choose earlier.

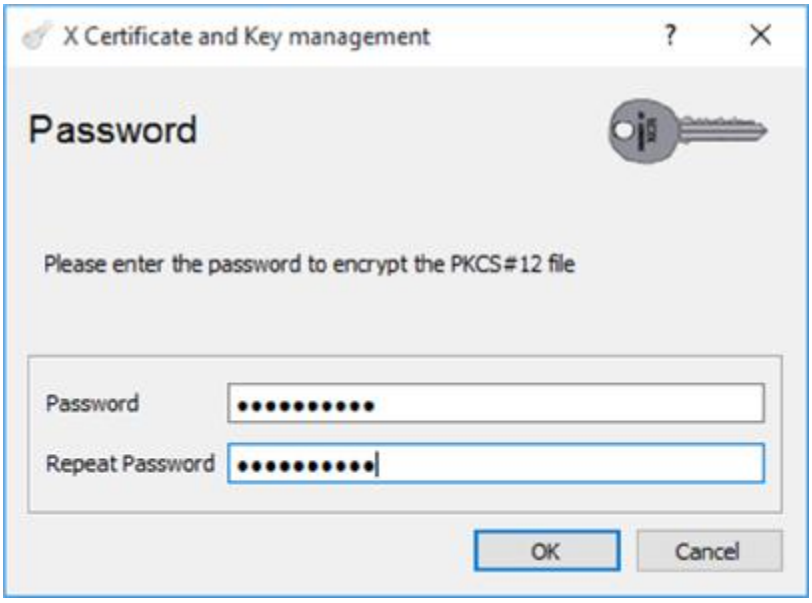
Export PKCS#12 File



Select your new certificate and use “Export”



Save your certificate export as PKCS#12 and



...define a Password to protect your private-key from unauthorized use. This password will be asked from you when importing this file into your browser or mail client.

You have a certificate in the PKCS#12 Format for the import into browser, email client, OS ...

Congratulations!