

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.

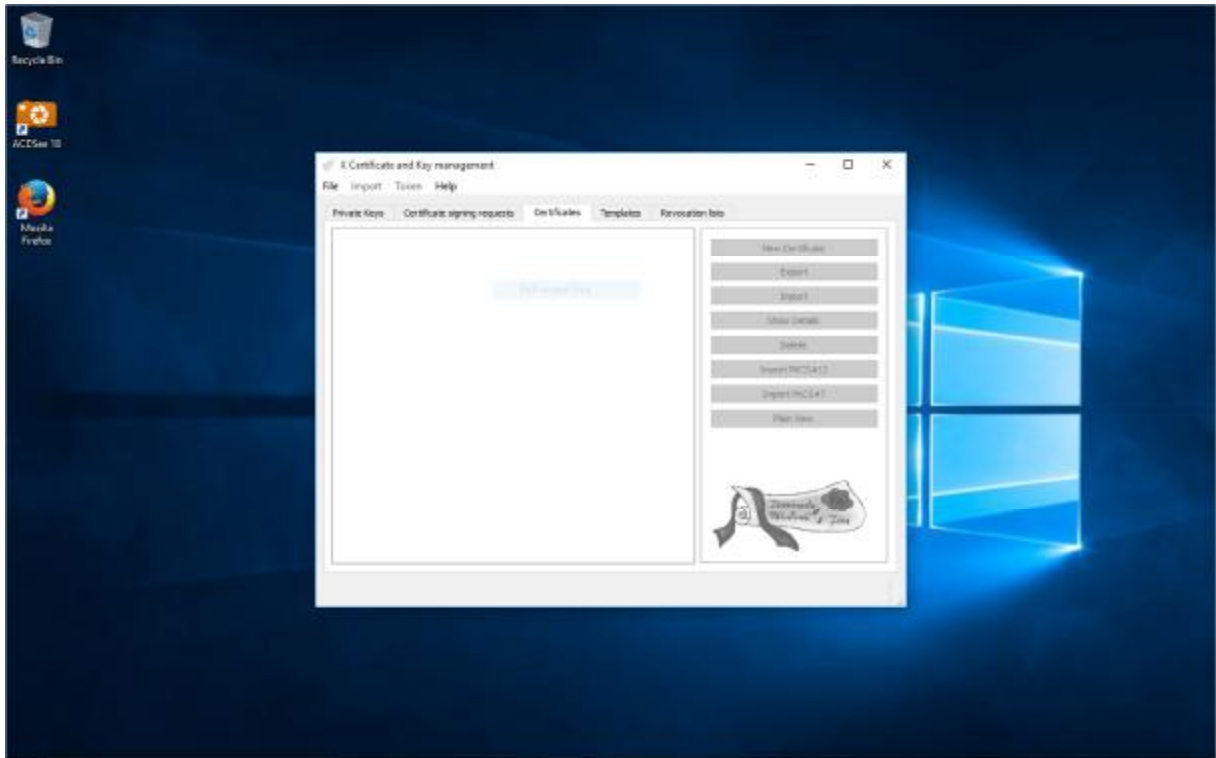
Prerequisites:

Imported and trusted "CAcert Public Root Certificate" in the Web-Browser.

Installed certificate manager XCA <http://sourceforge.net/projects/xca/>

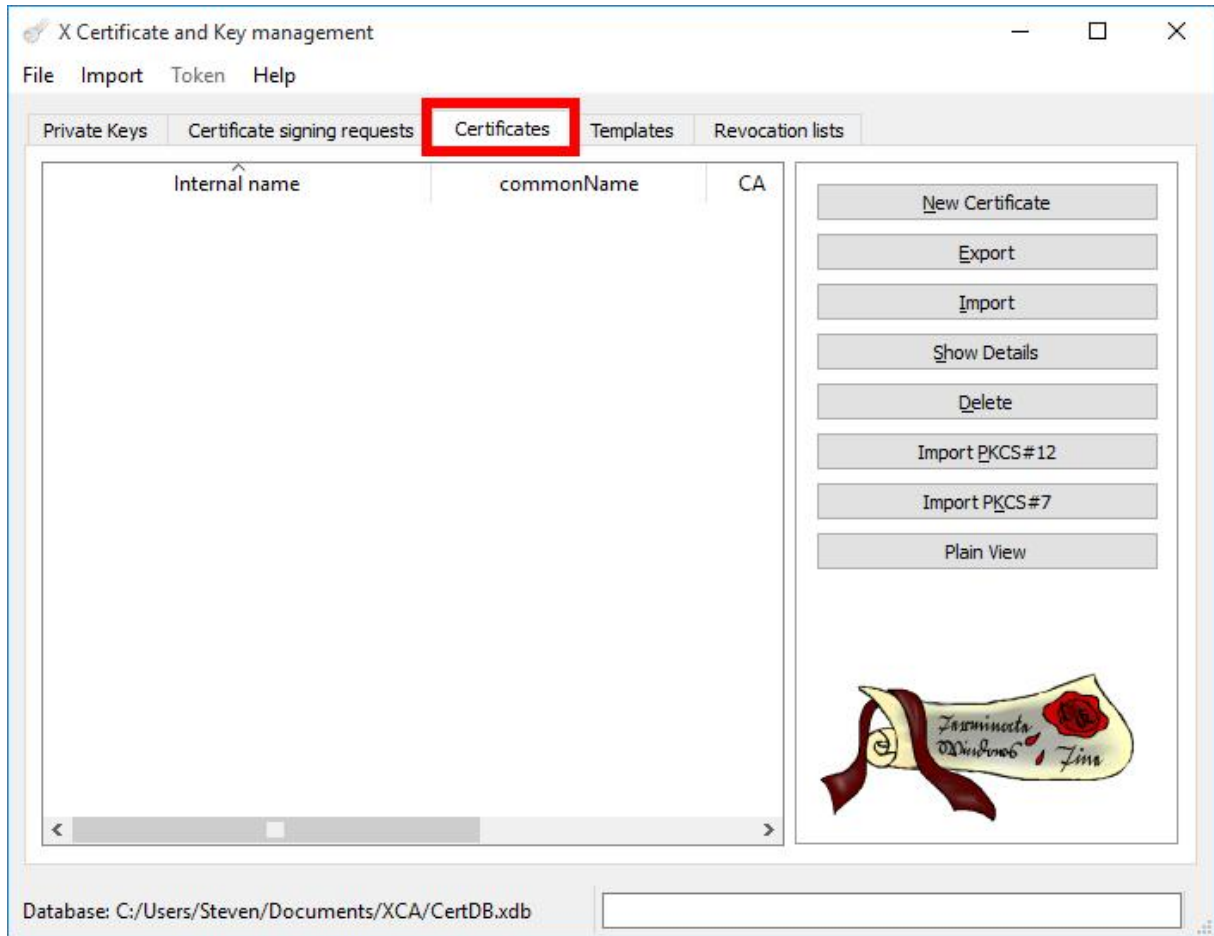
Activated account at <https://secure.cacert.org>

Preparation

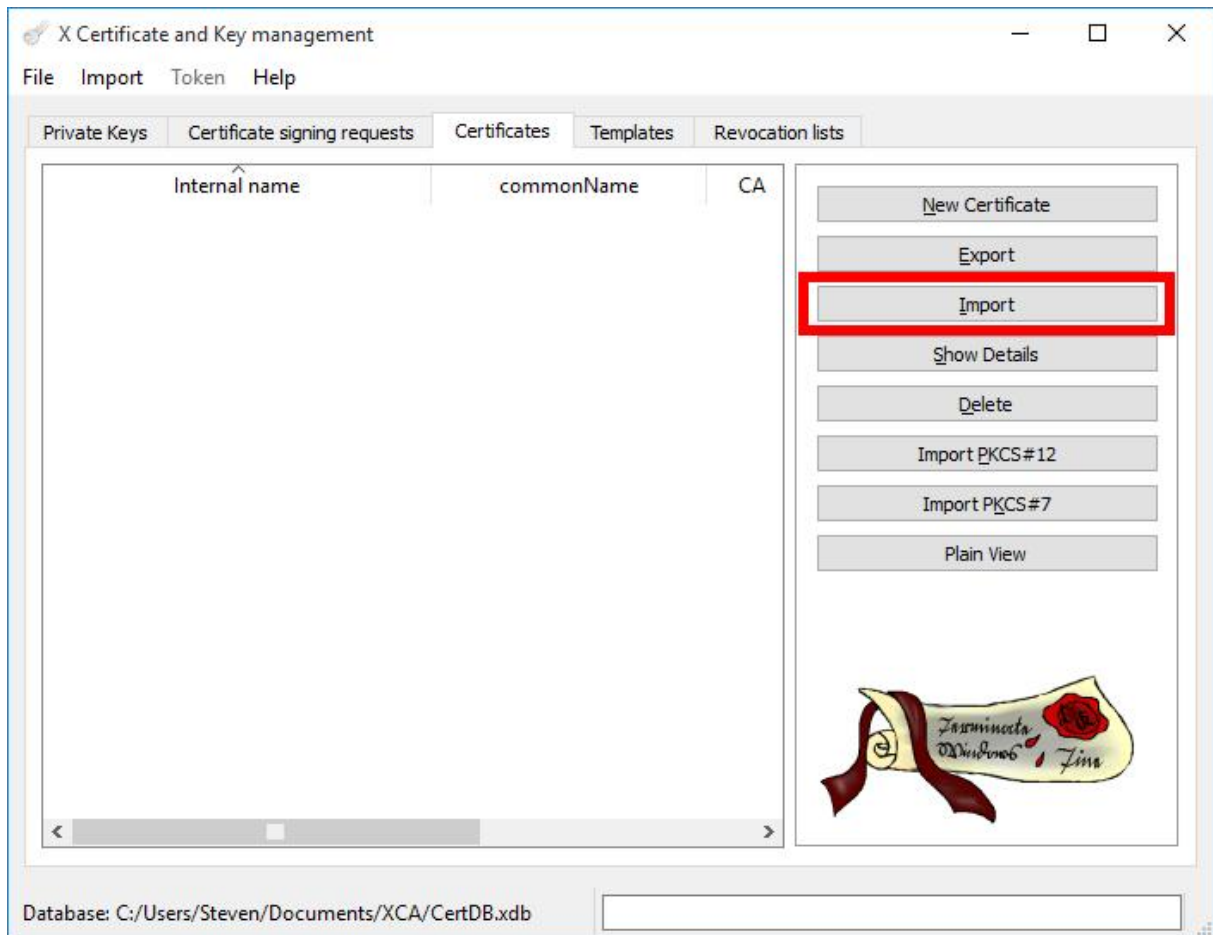


Start XCA

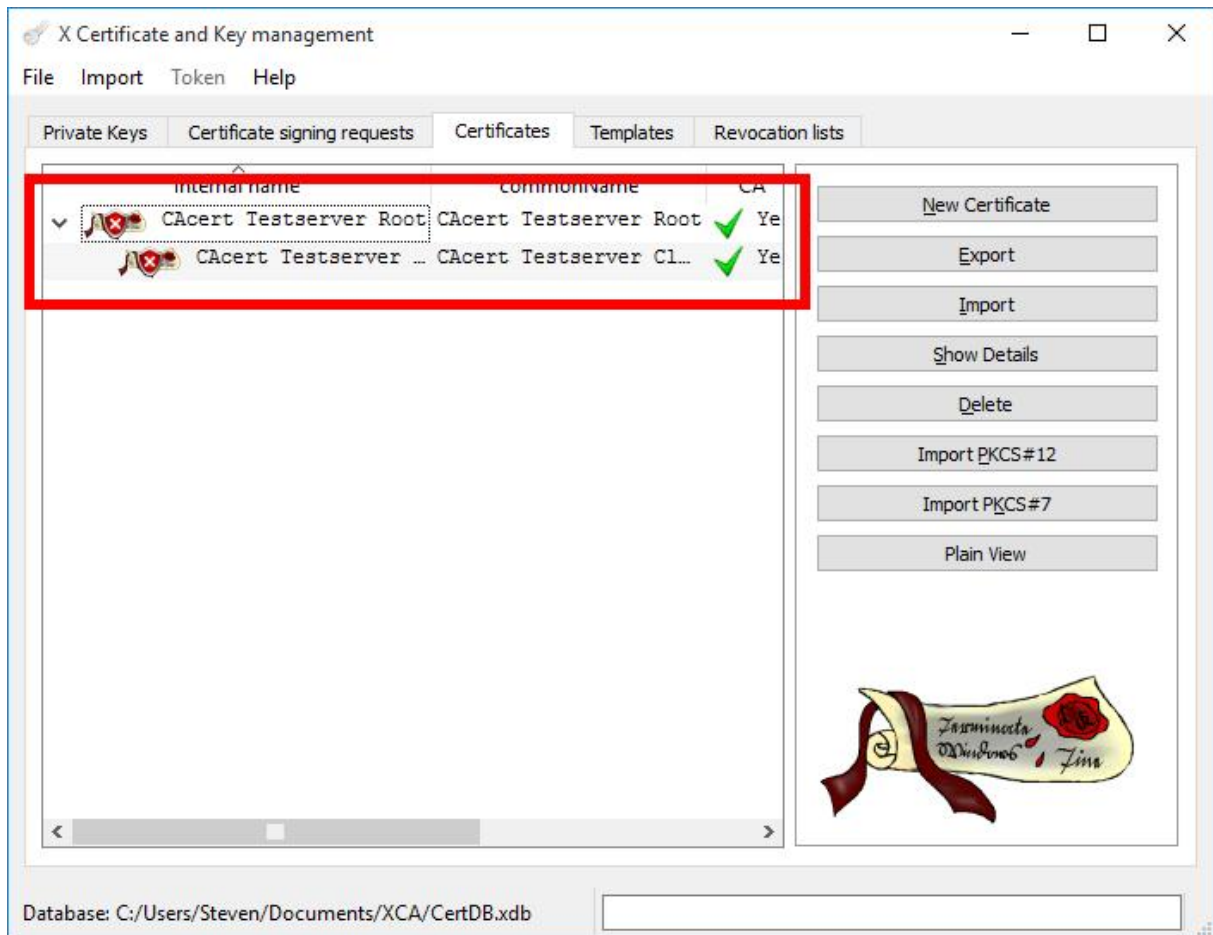
At the "File" menu use "New DataBase" to create a certificate database and save it to a file. Don't lose your password to the new database! Or open an existing database from your filesystem.



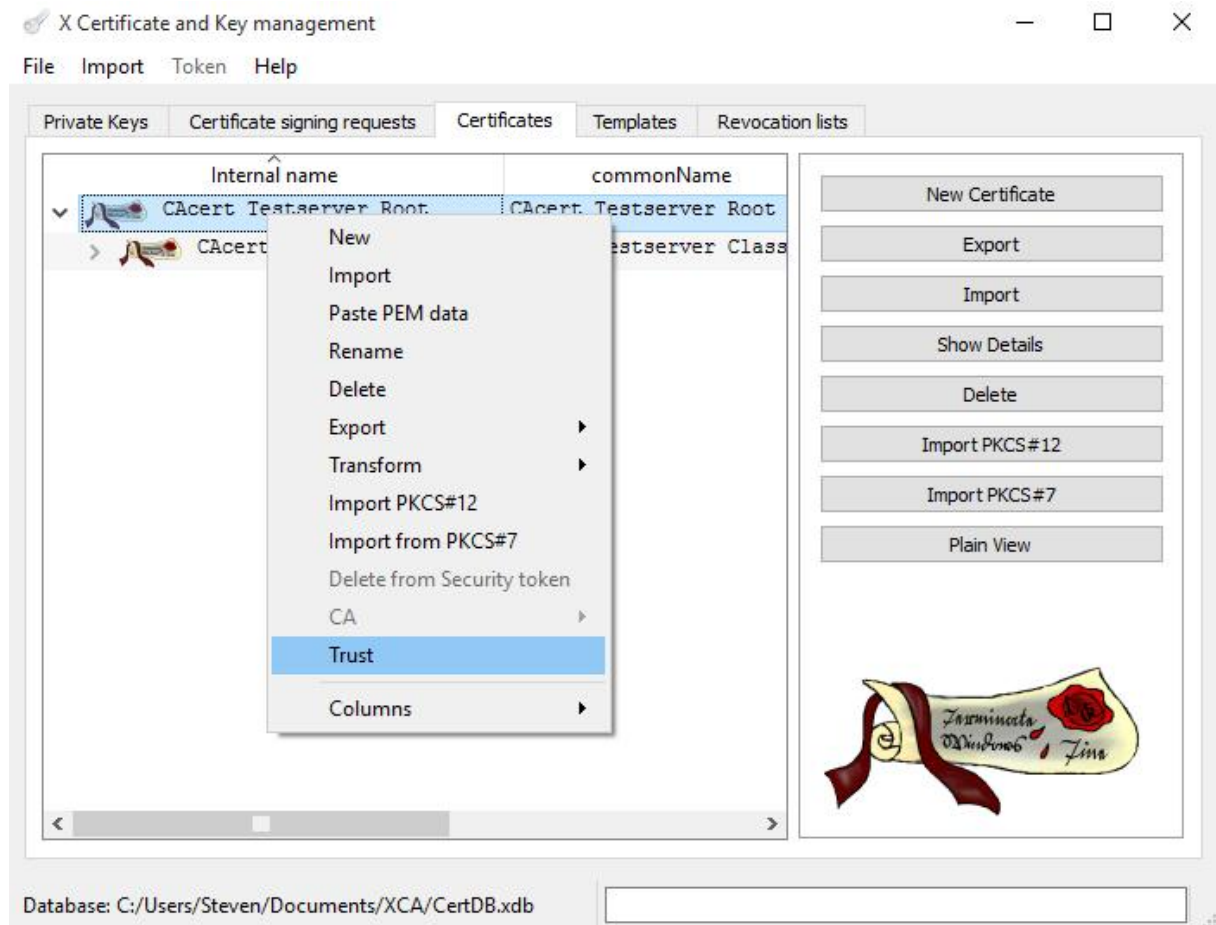
Go into tab "Certificates".



Use "Import" to allow XCA to recognize certificates of CAcert.

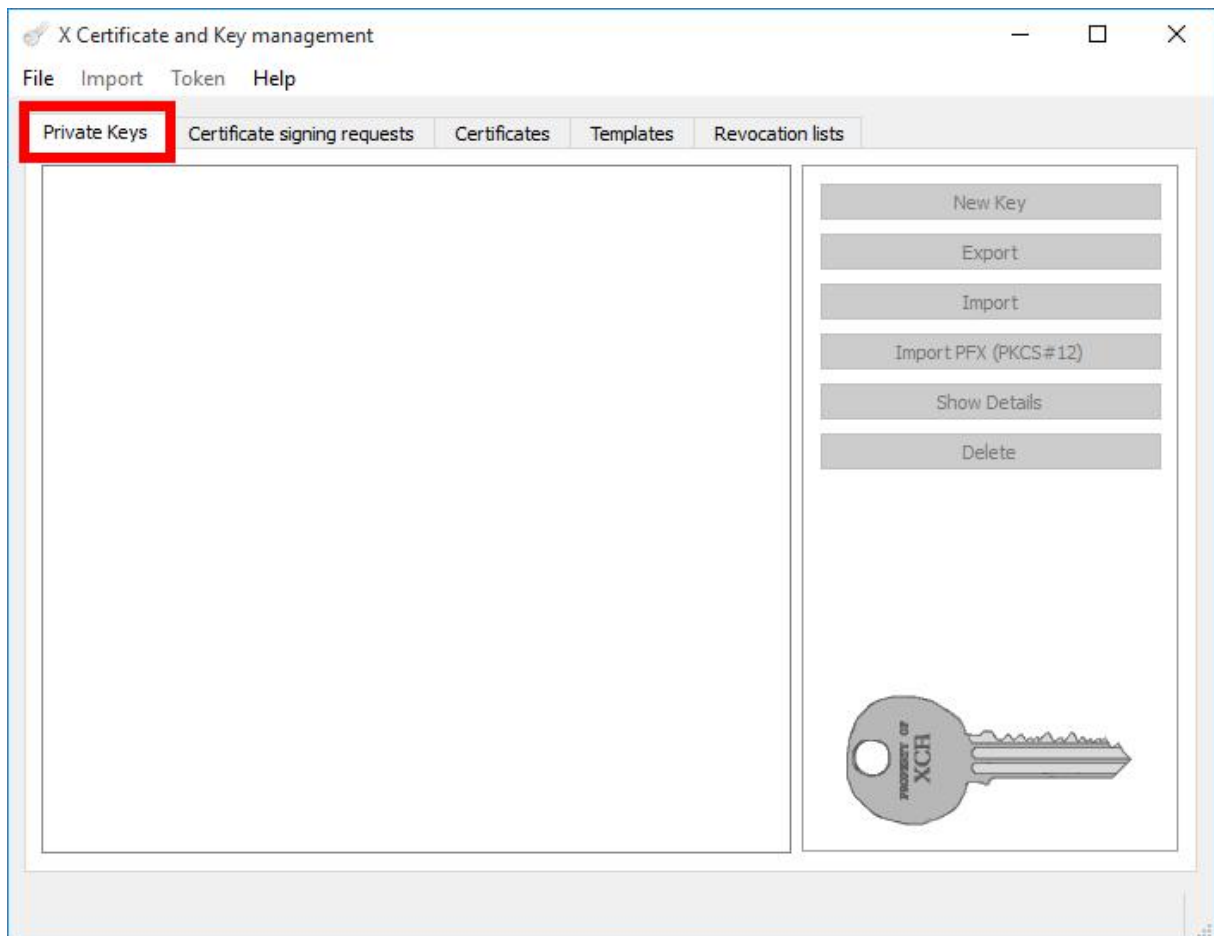


Import the "CAcert Public Root Certificates" "root" and "class3" in this order.

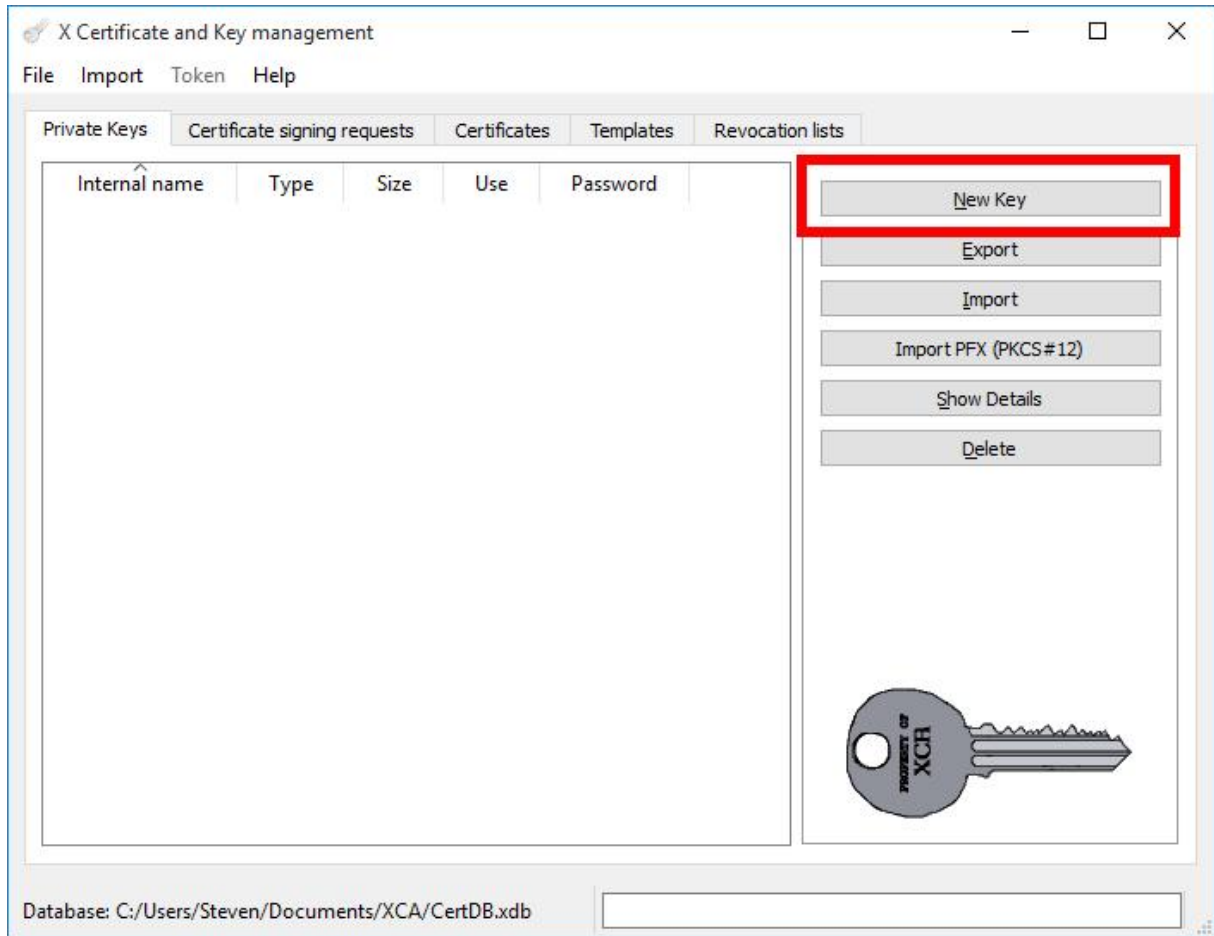


Trust the imported "CAcert Public Root Certificates" in the Context Menu with "Trust".

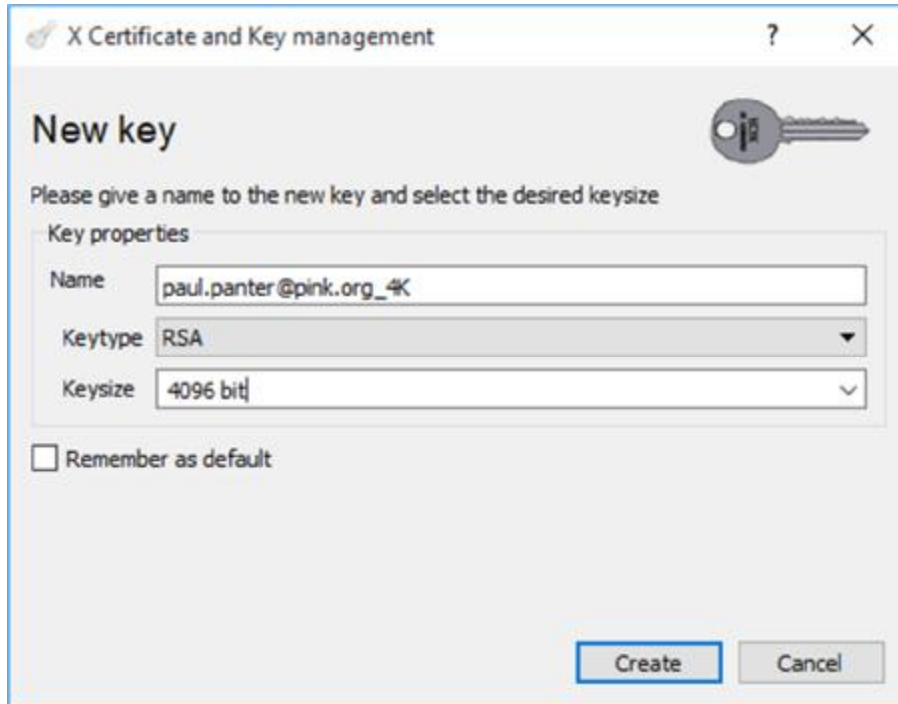
Private Key



Go into tabs "Private Keys".

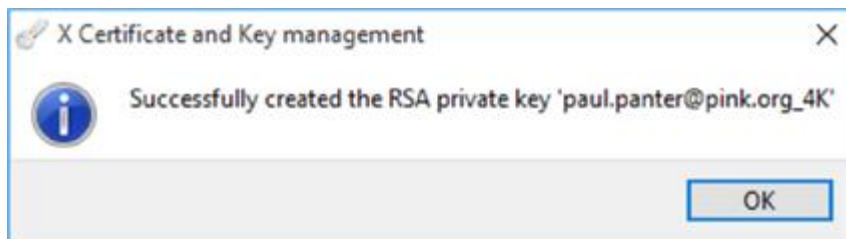


Use "New Key" for a new Private Key.

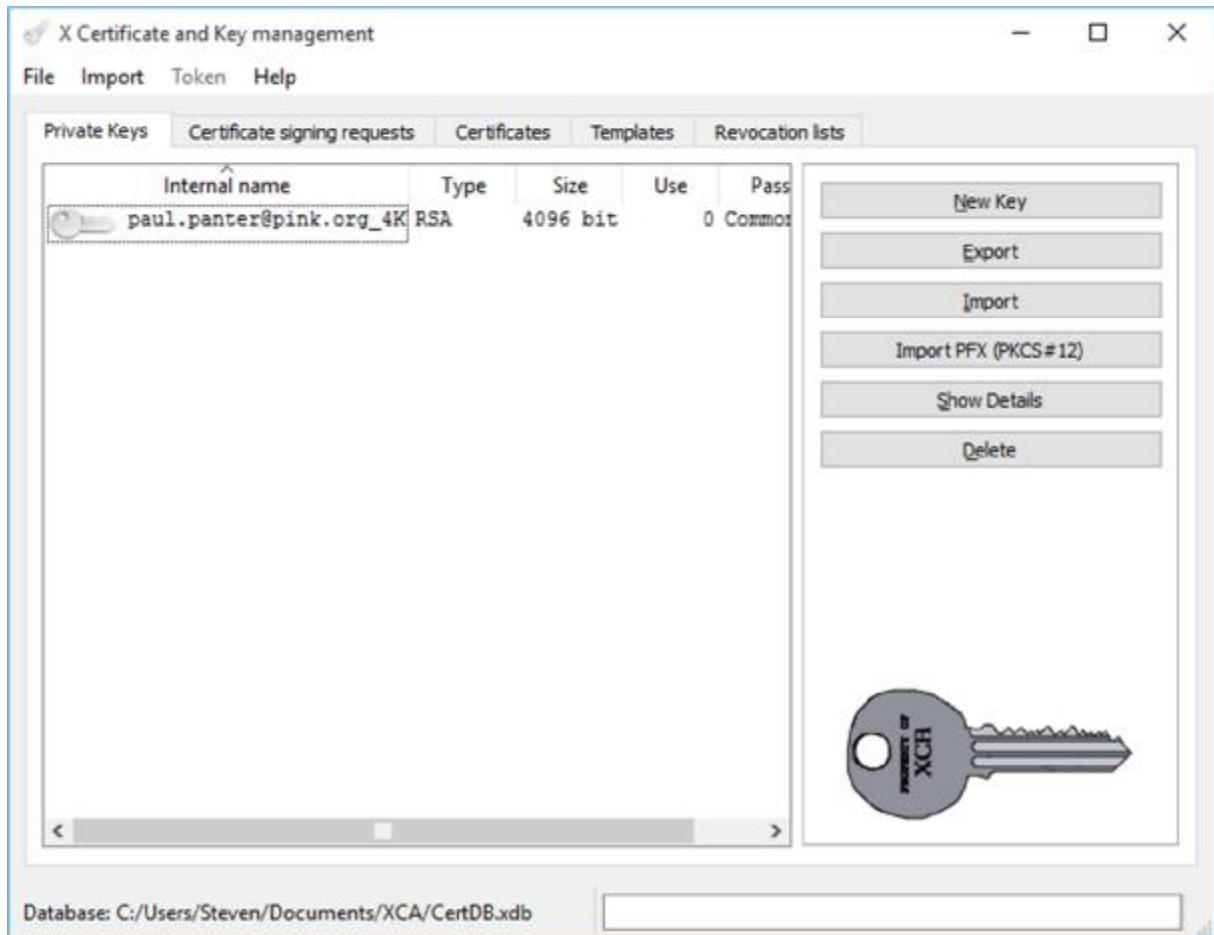


Choose a name for the new key with e.g. the intended purpose included. This name is for your reference only.

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.

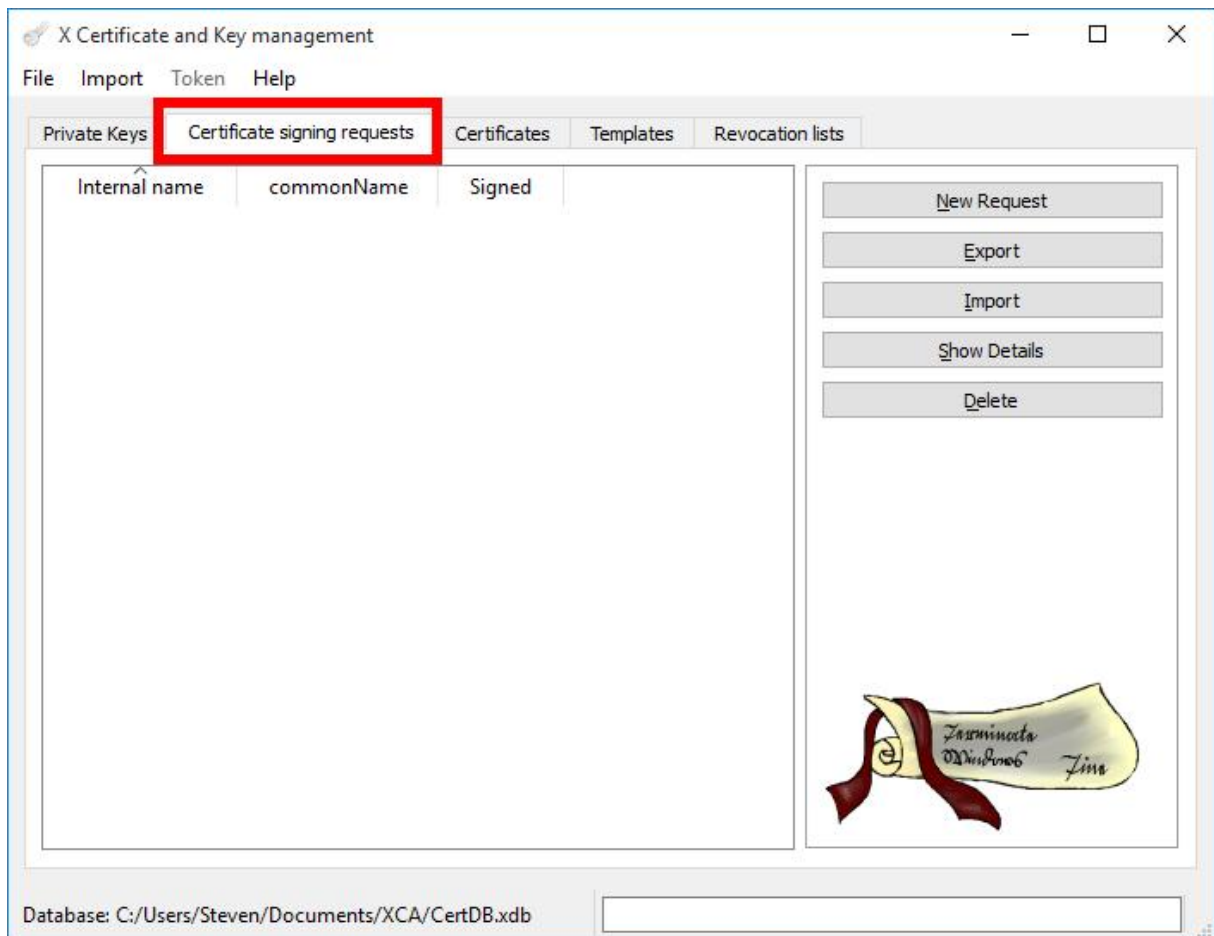


The new Private Key is ready and...

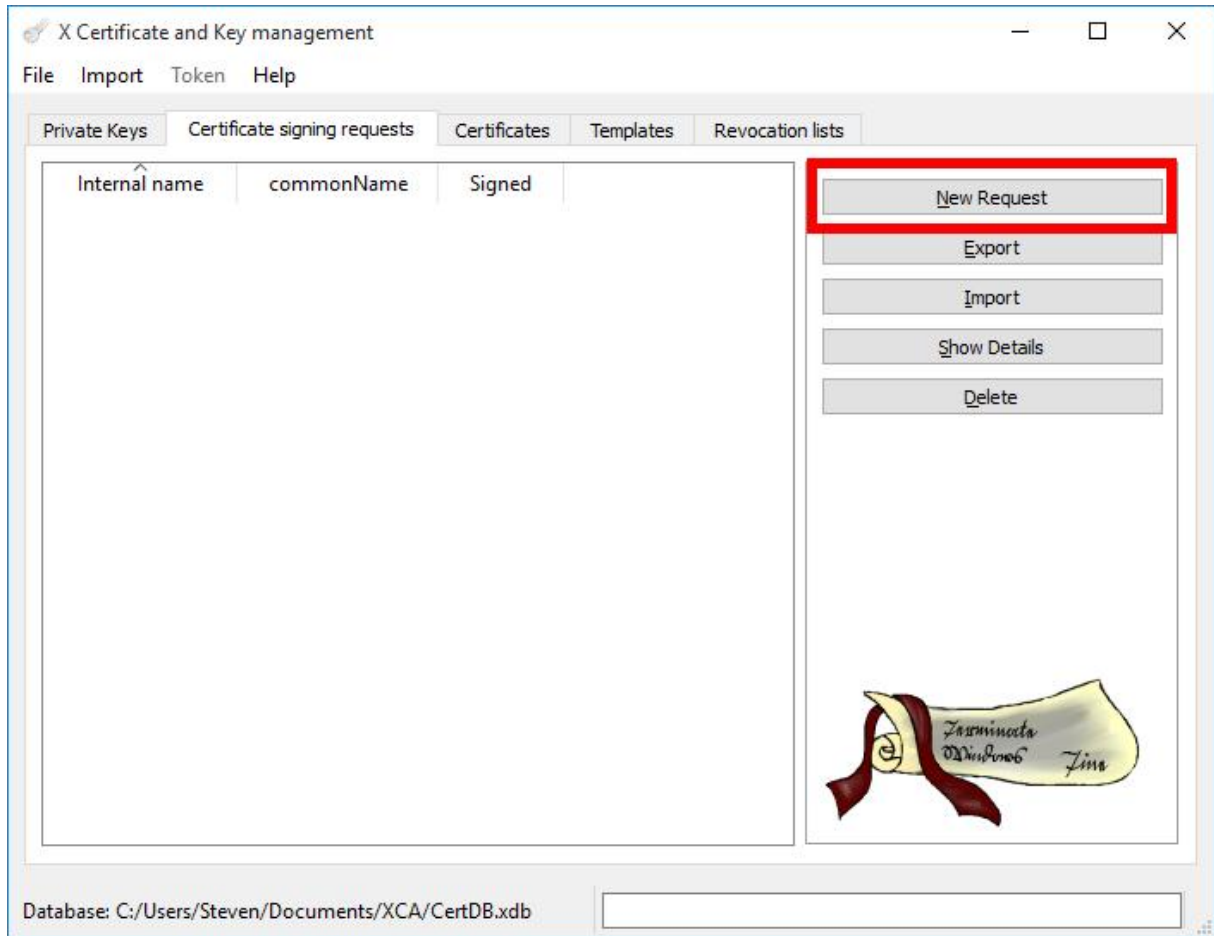


...appears in your list of private Keys.

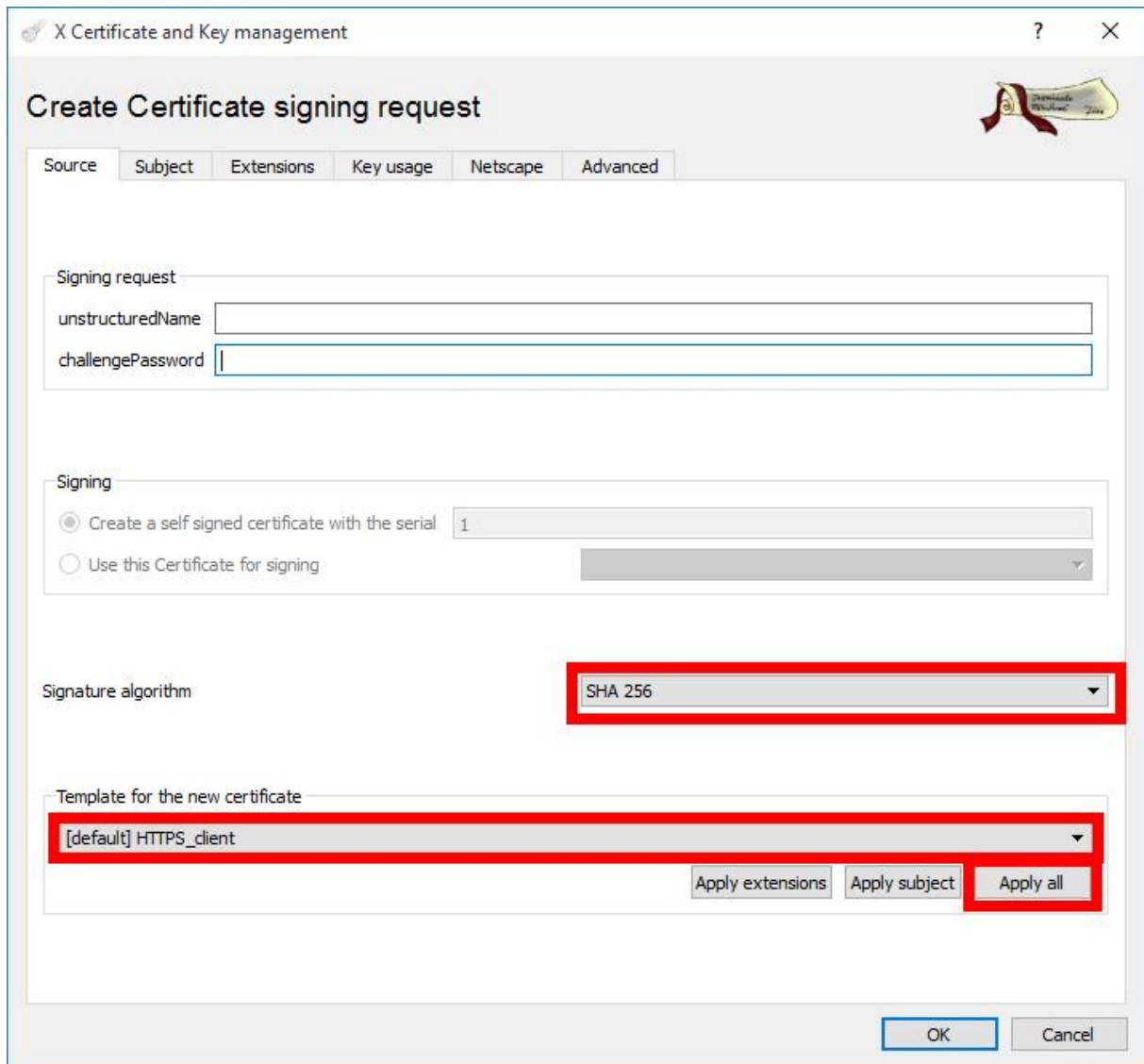
Certificate Signing Request – CSR



For the next step go into tab "Certificate signing requests"



Use "New Request" to create a CSR.



X Certificate and Key management

Create Certificate signing request

Source Subject Extensions Key usage Netscape Advanced

Signing request

unstructuredName

challengePassword

Signing

Create a self signed certificate with the serial

Use this Certificate for signing

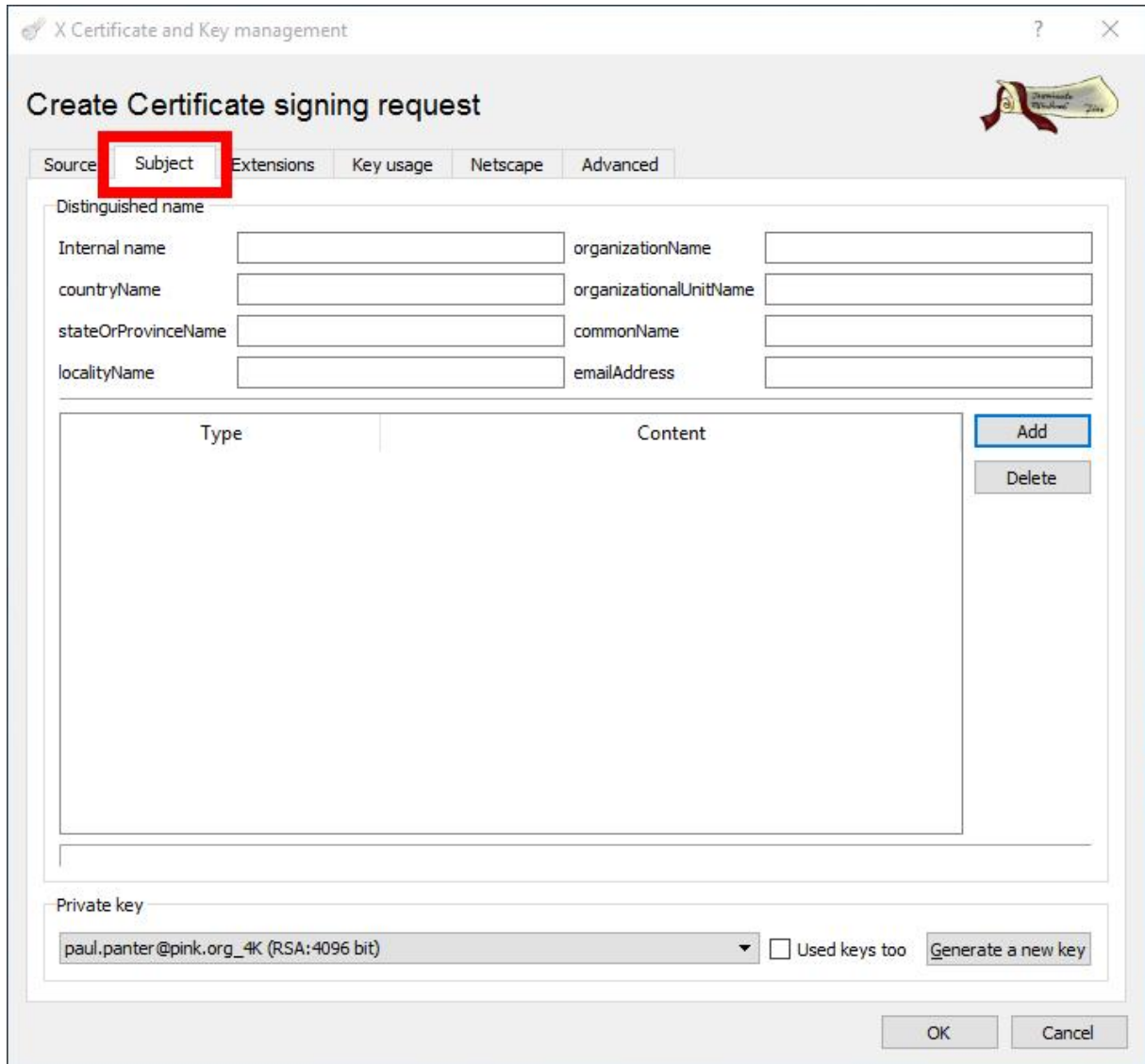
Signature algorithm

Template for the new certificate

Apply extensions Apply subject **Apply all**

OK Cancel

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



X Certificate and Key management

Create Certificate signing request

Source **Subject** Extensions Key usage Netscape Advanced

Distinguished name

Internal name	<input type="text"/>	organizationName	<input type="text"/>
countryName	<input type="text"/>	organizationalUnitName	<input type="text"/>
stateOrProvinceName	<input type="text"/>	commonName	<input type="text"/>
localityName	<input type="text"/>	emailAddress	<input type="text"/>

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

Private key

paul.panter@pink.org_4K (RSA:4096 bit) Used keys too

Go into tab "Subject".

X Certificate and Key management

Create Certificate signing request

Source Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name: Paul Panter organizationName: []

countryName: [] organizationalUnitName: []

stateOrProvinceName: [] commonName: []

localityName: [] emailAddress: paul.panter@pink.org

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

Private key

paul.panter@pink.org_4K (RSA:4096 bit) Used keys too Generate a new key

OK Cancel

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.

X Certificate and Key management

Create Certificate signing request

Source Subject Extensions Key usage Netscape Advanced

X509v3 Basic Constraints

Type: End Entity

Path length: Critical

Key identifier

Subject Key Identifier

Authority Key Identifier

Validity

Not before: 2015-10-11 17:37 GMT

Not after: 2016-10-10 17:37 GMT

Time range

365 Days

Midnight Local time No well-defined expiration

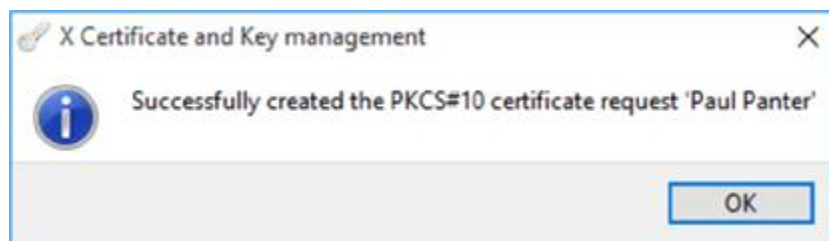
X509v3 Subject Alternative Name

X509v3 Issuer Alternative Name

X509v3 CRL Distribution Points

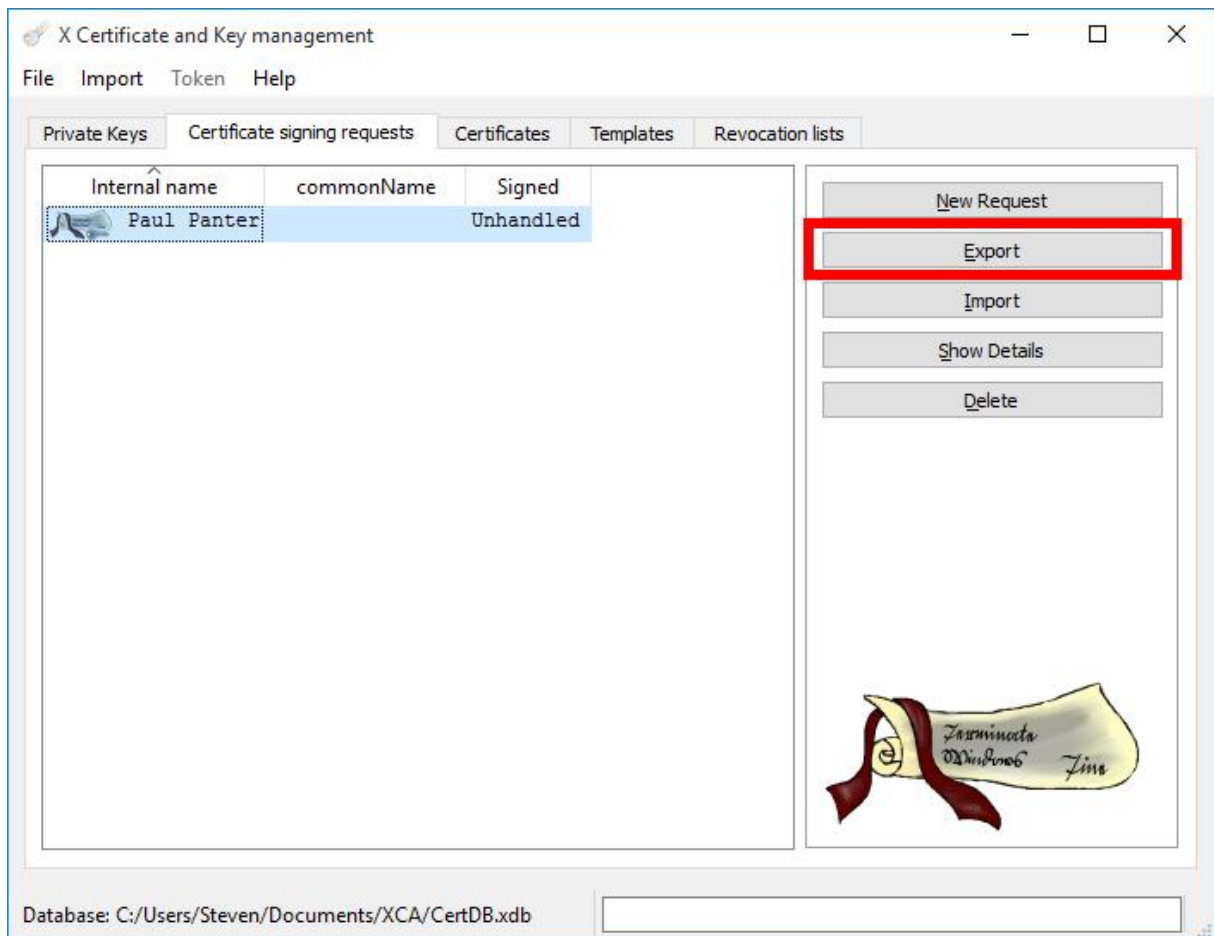
Authority Information Access: OCSP

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

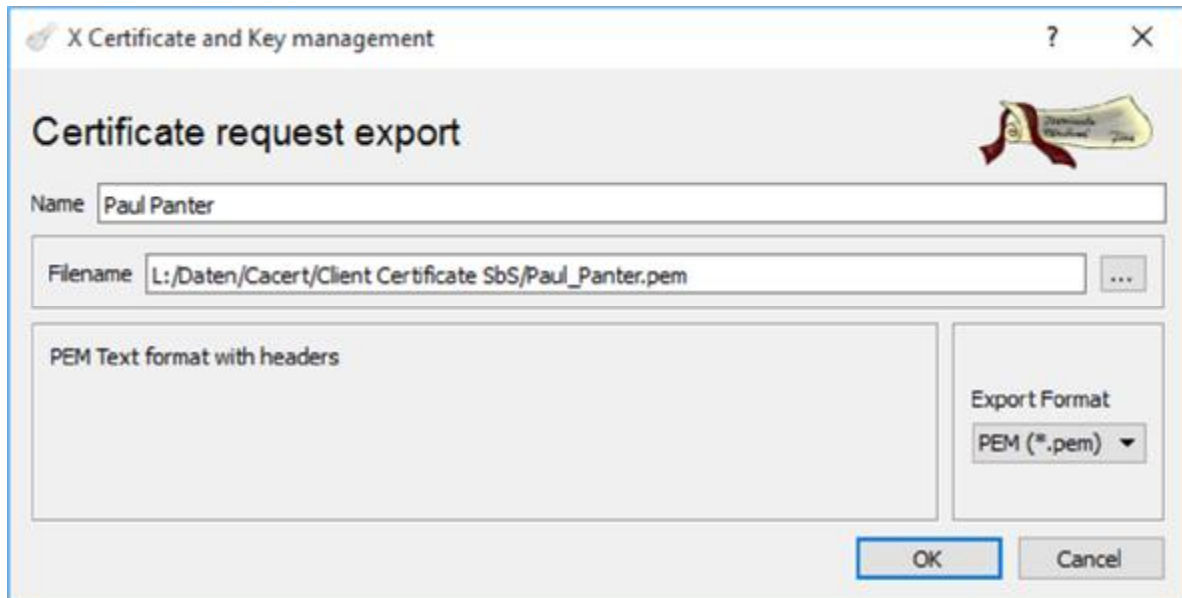


The CSR is ready.

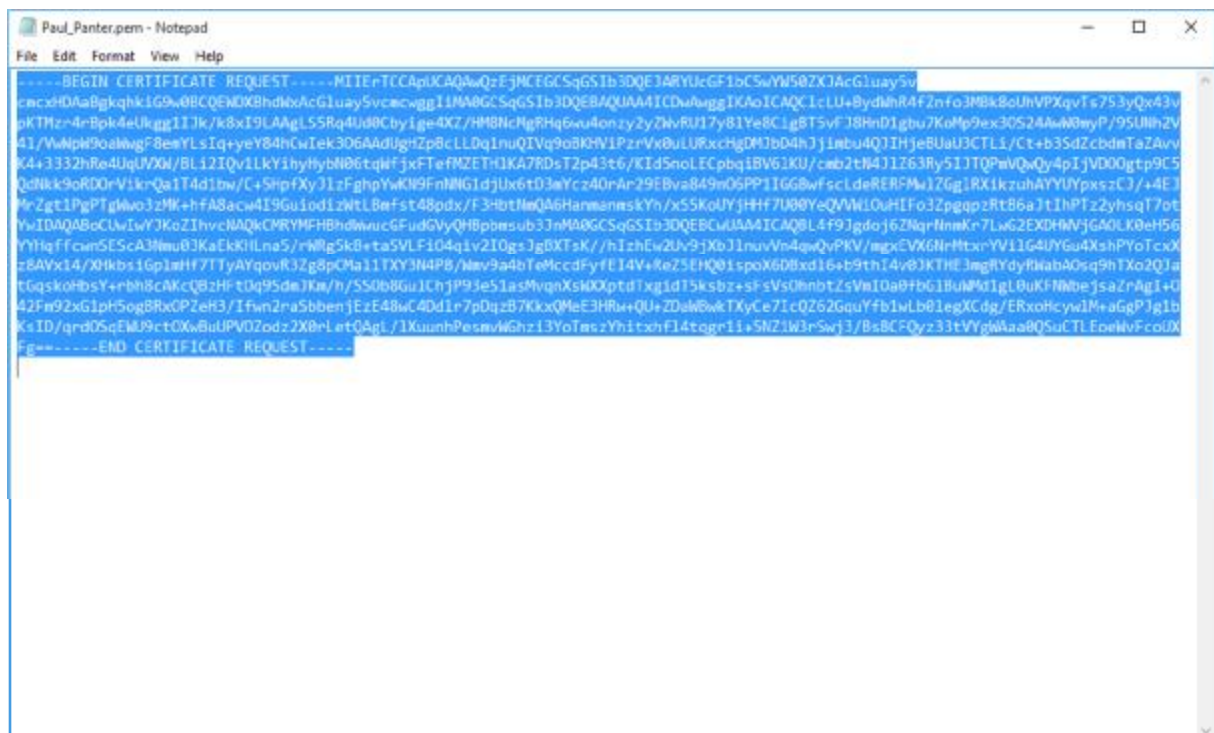
Signing Process



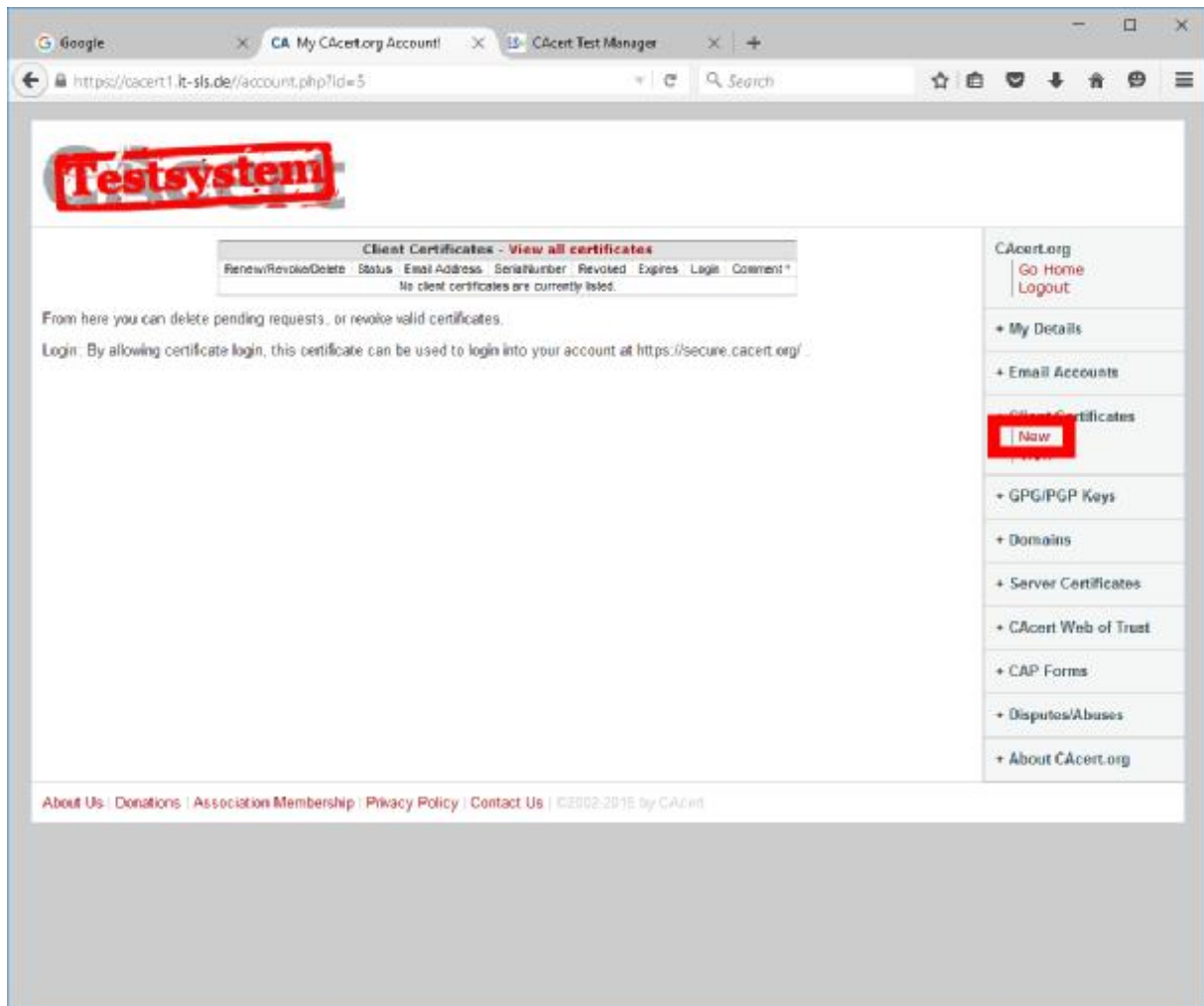
Select the new CSR and "Export".



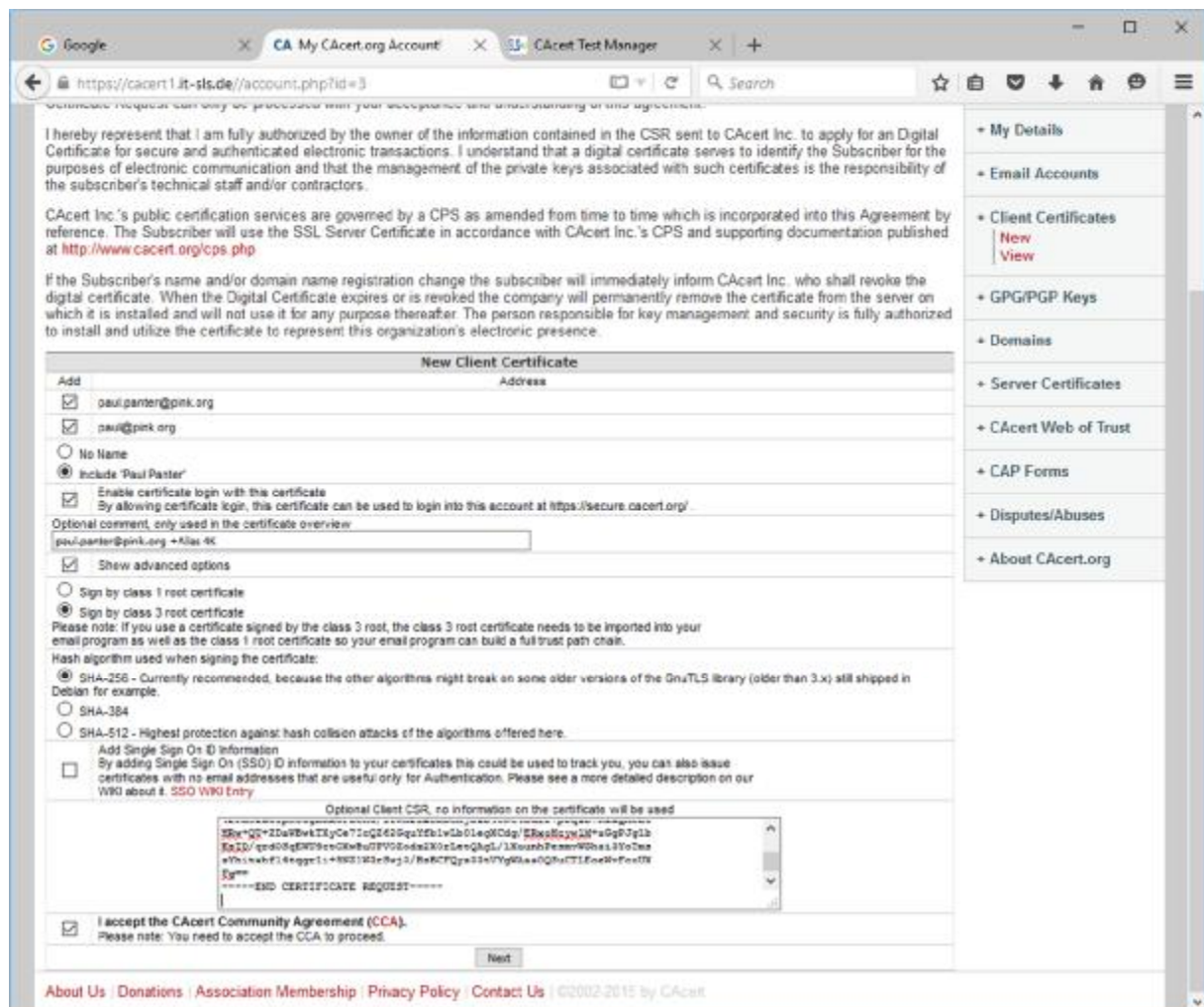
Save the CSR to file in pem Format but with extension .csr



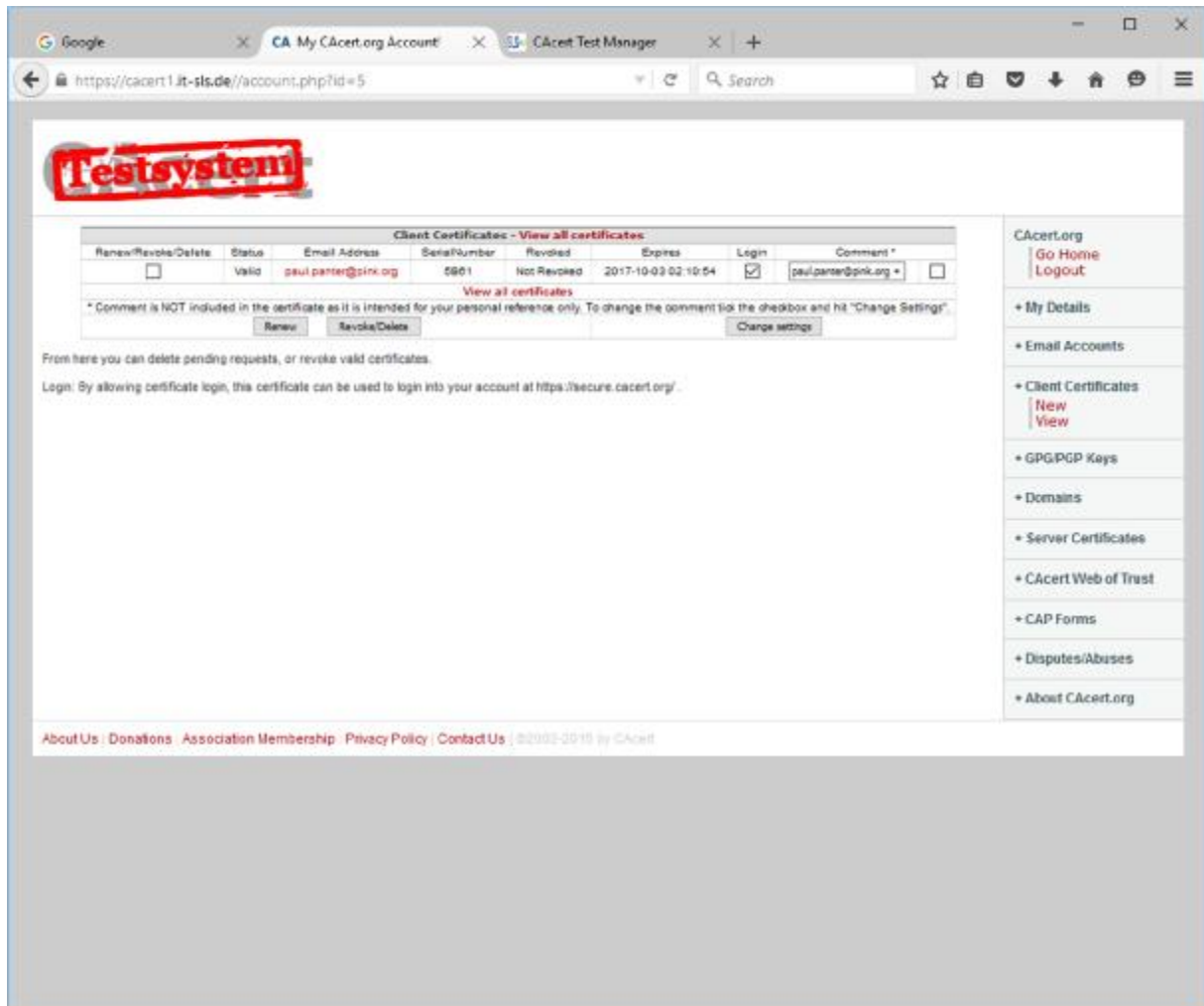
Open the CSR in an editor, select ALL and copy the content.



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"



The screenshot shows a web browser window with the URL <https://cacert1.it-sls.de/account.php?id=5>. The page features a red "Testsystem" stamp at the top left. The main content area is titled "Client Certificates - View all certificates" and contains a table with the following data:

Renew/Revoke/Delete	Status	Email Address	Serial Number	Revoked	Expires	Login	Comment *
<input type="checkbox"/>	Valid	paul.panter@pink.org	5801	Not Revoked	2017-10-03 02:10:54	<input checked="" type="checkbox"/>	paul.panter@pink.org *

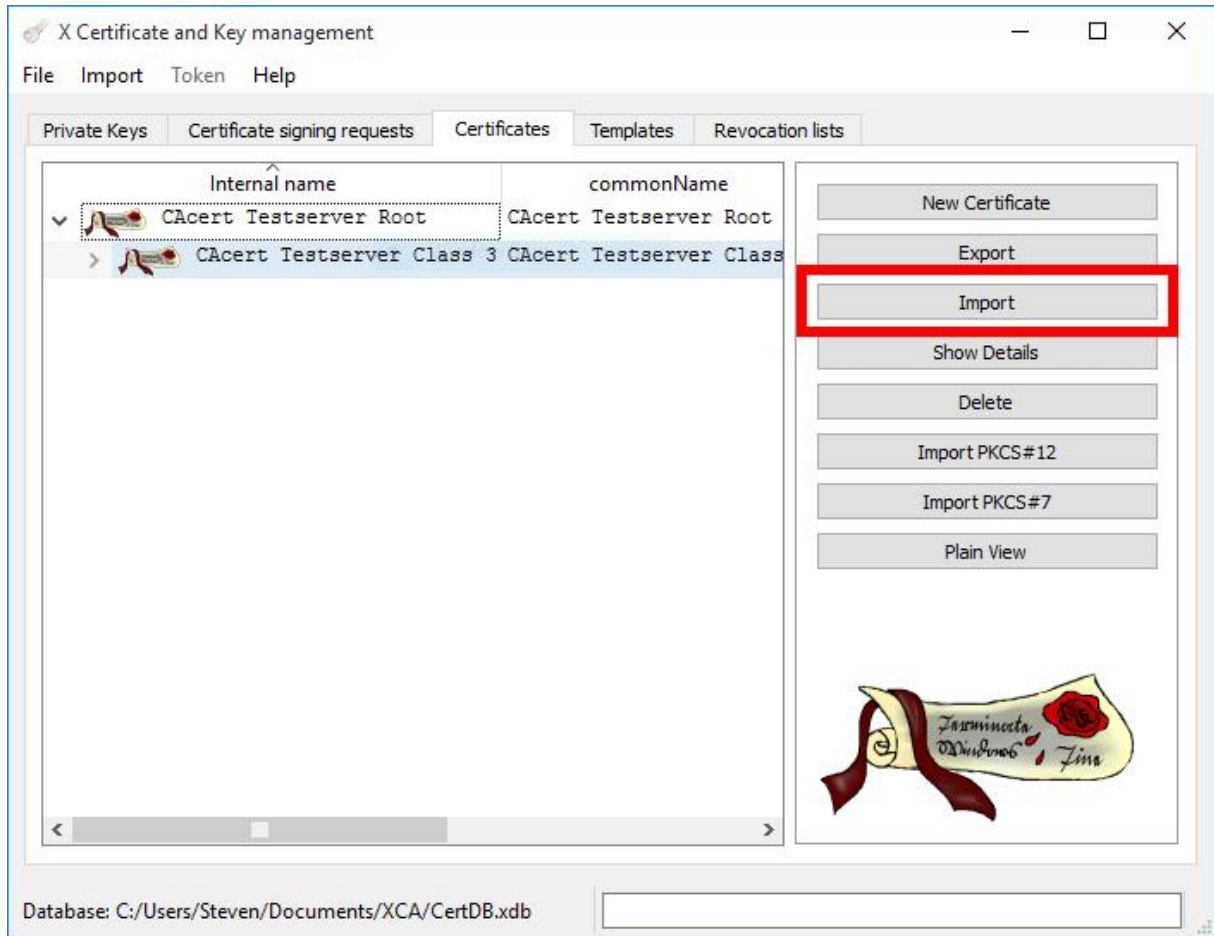
Below the table, there are buttons for "Renew", "Revoke/Delete", and "Change settings". A note states: "From here you can delete pending requests, or revoke valid certificates. Login: By allowing certificate login, this certificate can be used to login into your account at <https://secure.cacert.org/>."

The right sidebar contains a navigation menu with the following items:

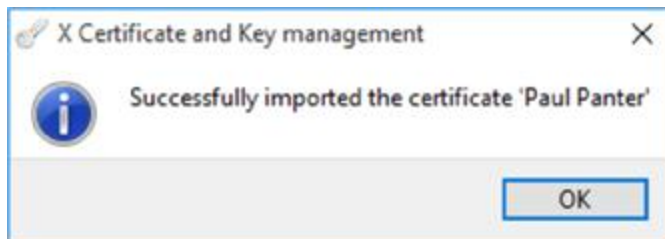
- CAcert.org
- Go Home
- Logout
- + My Details
- + Email Accounts
- + Client Certificates
 - New
 - View
- + GPG/PGP Keys
- + Domains
- + Server Certificates
- + CAcert Web of Trust
- + CAP Forms
- + Disputes/Abuses
- + About CAcert.org

At the bottom of the page, there is a footer with links for "About Us", "Donations", "Association Membership", "Privacy Policy", and "Contact Us", along with the copyright notice "©2002-2015 by CAcert".

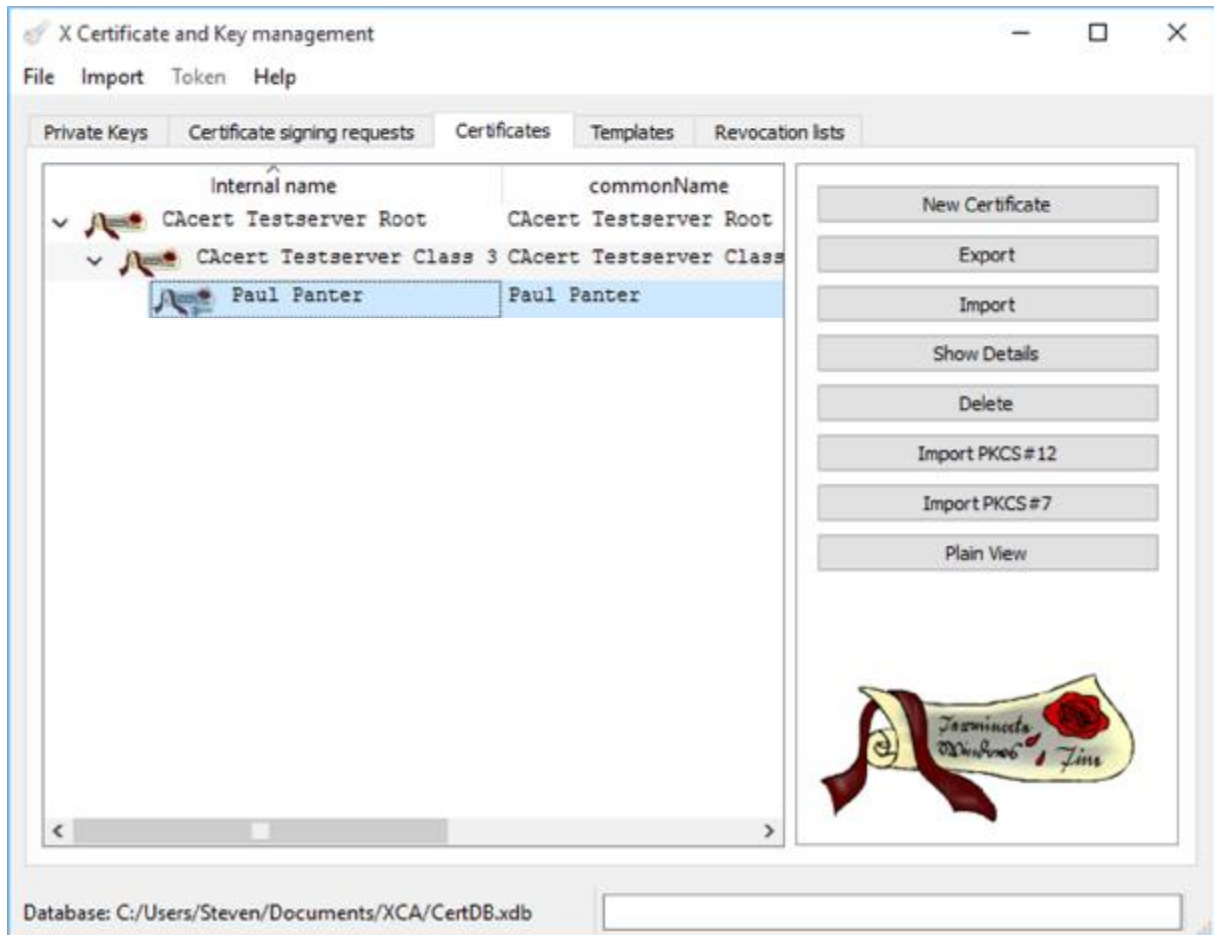
See the certificate in "Client Certificates" and "View".



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

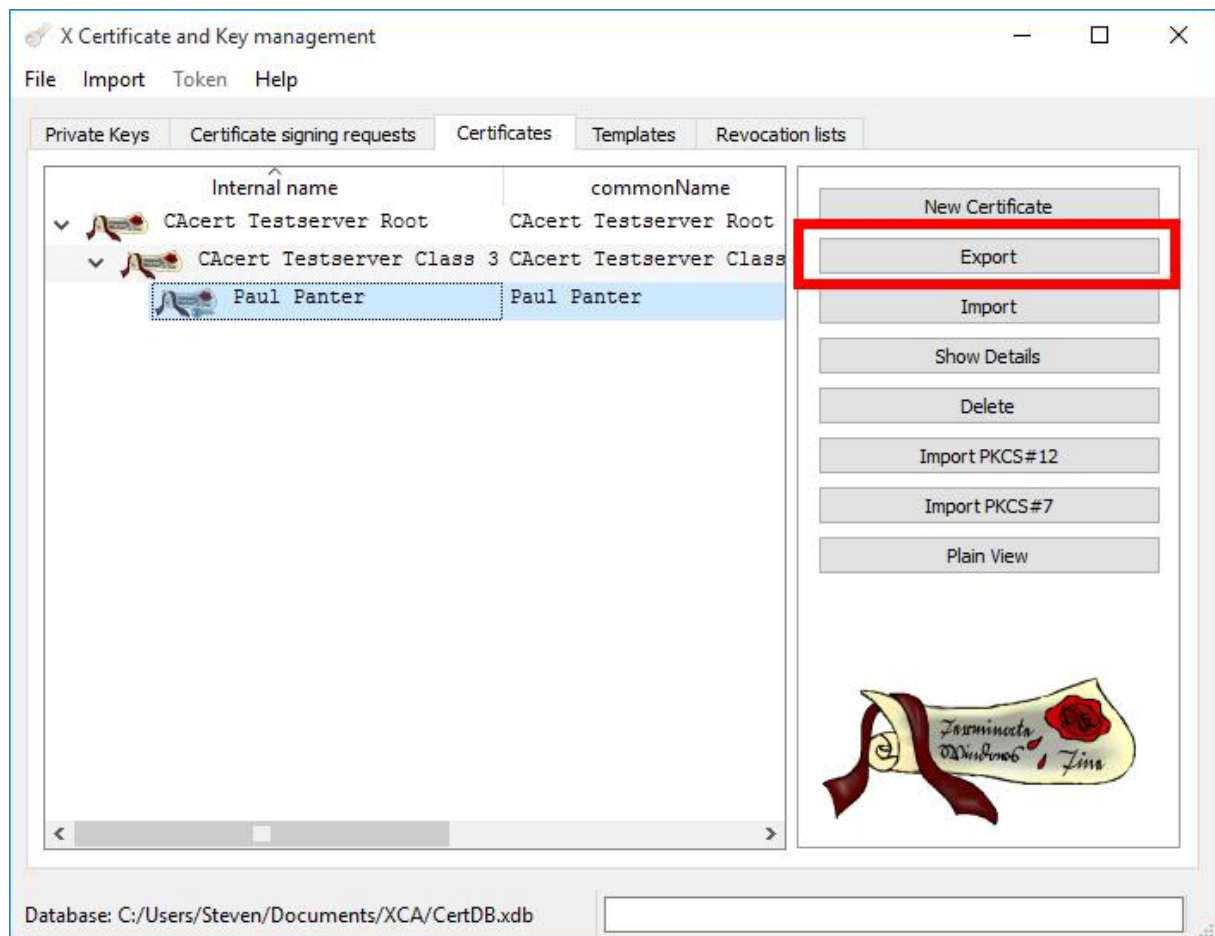


Import was successful.

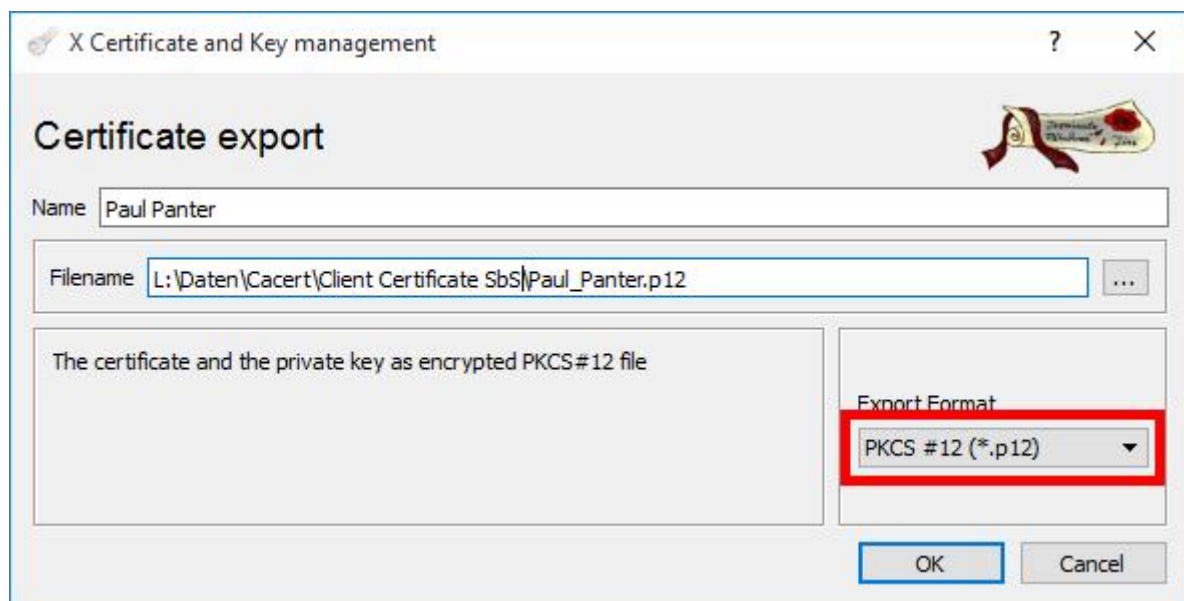


The certificate is listed below the signer certificate you choose earlier.

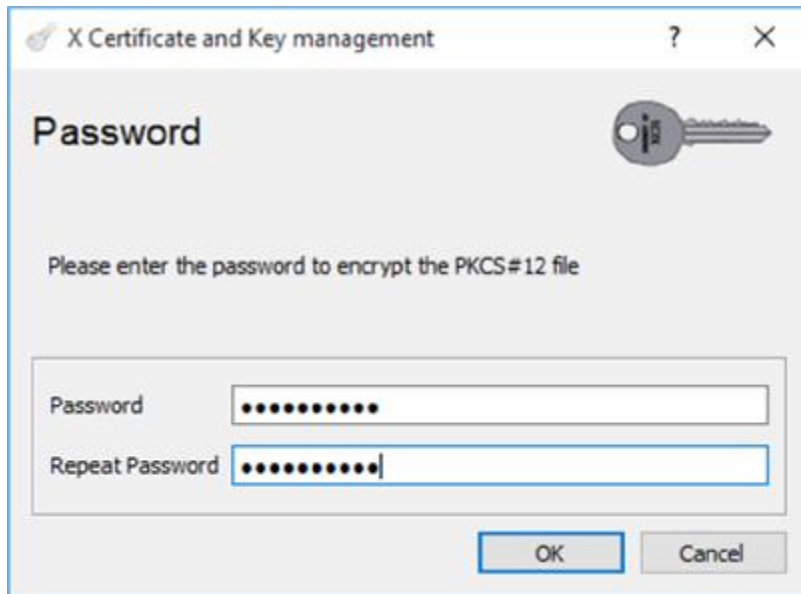
Export PKCS#12 File



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!