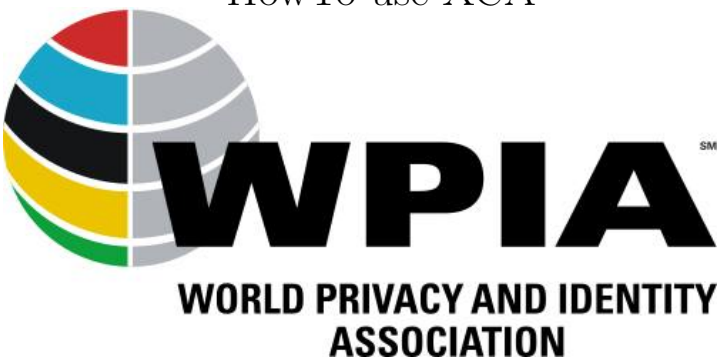
HowTo use XCA



2018-12-12

Contents

1 Obtain Software **1**

2 Create Certificate Signing Request (CSR) **1**

3 Copy CSR To Clipboard **4**

4 Import Public Key Via Clipboard **5**

5 Export Certificate **7**

1 Obtain Software

XCA is an open source tool to manage private und public keys.

XCA is available under [https://www.hohnstaedt.de/xca/index.php/download] (https://www.hohnstaedt.de/xca/index.php/download).

Please download the newest version at the top of the page.

Windows users can press the download button, Apple or Linux users select their appropriate file. Then install the program on your system. During the installation you can choose from several languages.

2 Create Certificate Signing Request (CSR)

At the first program start you have to create a new database. To do this, press "STR + N", choose a directory and name the new database, e.g. WPIA.xdb. You can continue to use this database at any time later. A password for this database is required; without entering a password later export is not possible.

To create a new CSR open a xca database and go to the Certificate Signing Request tab.

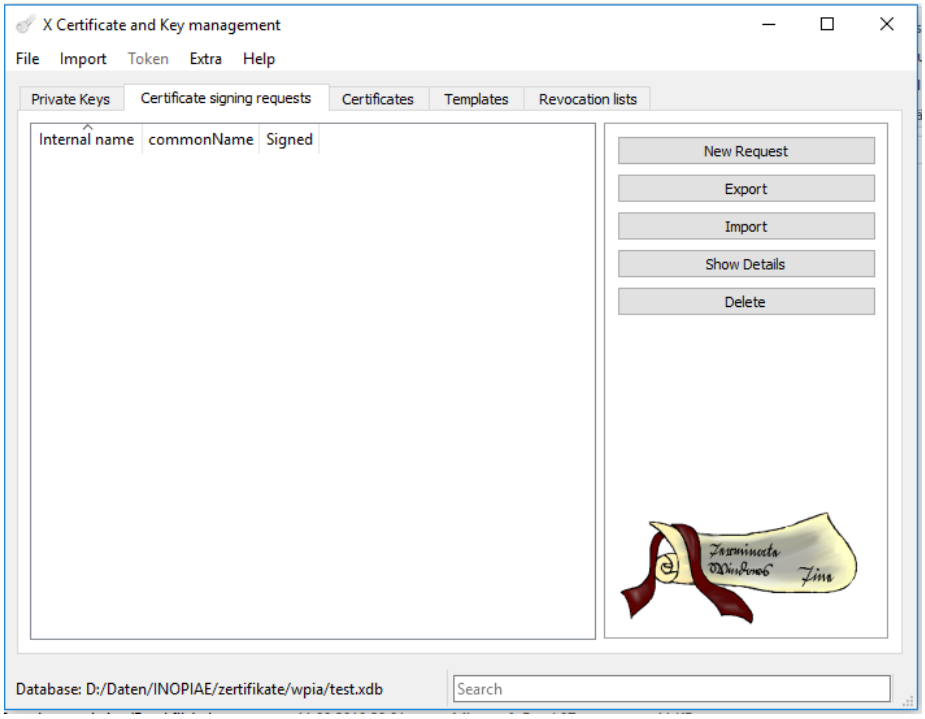


Figure 1: Screenshot Certificate Signing Request tab

Use 'New Request' to create a new request.

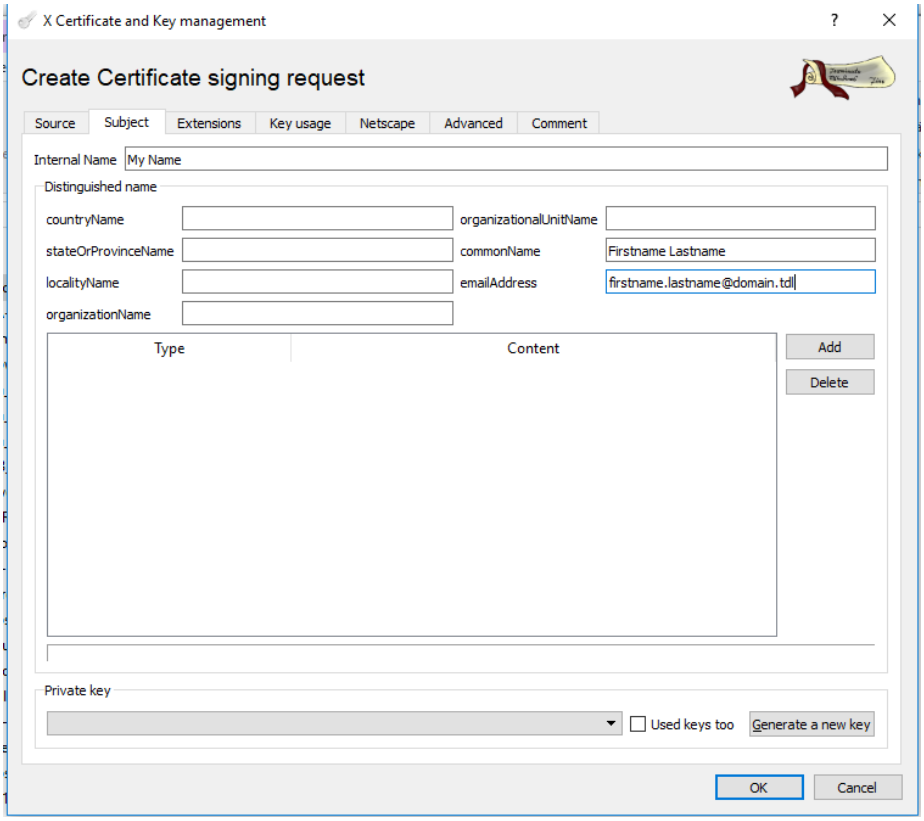


Figure 2: Screenshot New Request

You only need to fill data on the Subject tab.

Fill in:

- Internal name - any data, it is for you to find the entry later, but no special characters
- CommonName - your Firstname and Lastname
- emailAddress - an email address used in your CA account

Generate a new private key with 'Generate a new key'.

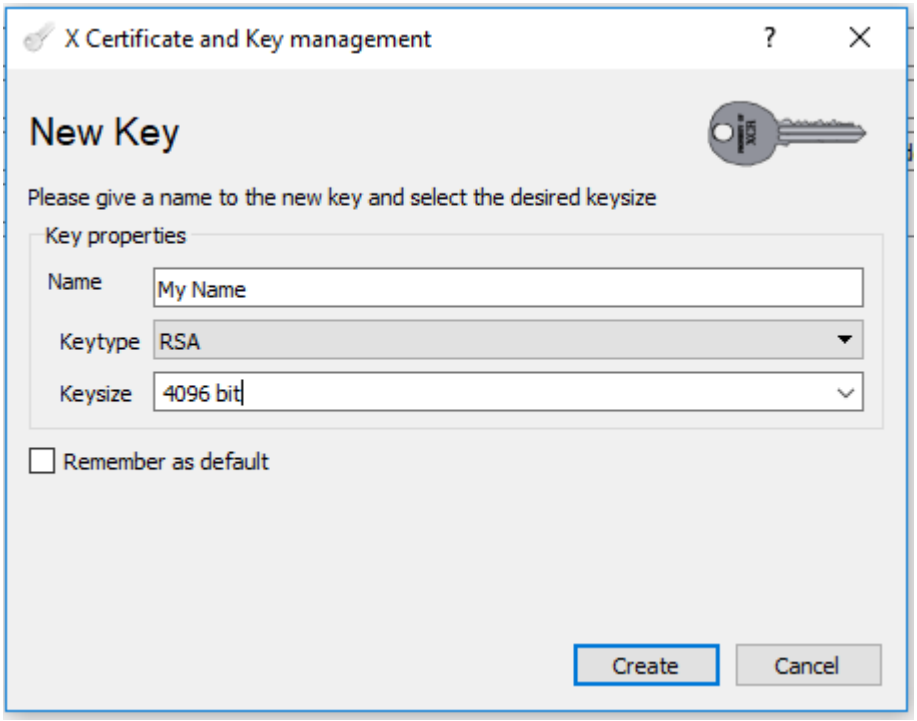


Figure 3: Screenshot New Key

It is recommended to use the keytype RSA with a keysize of 4096 bit. It is advised to change the default setting of 2048 bit to 4096 bit. Then create a new key by pressing the “Create” button. After a moment, the message appears that the key was successfully created; please confirm this with the “OK” button. Close the window with “OK” and the newly created key appears.

Once you have the data filled and a private key finish with ‘Create’.

3 Copy CSR To Clipboard

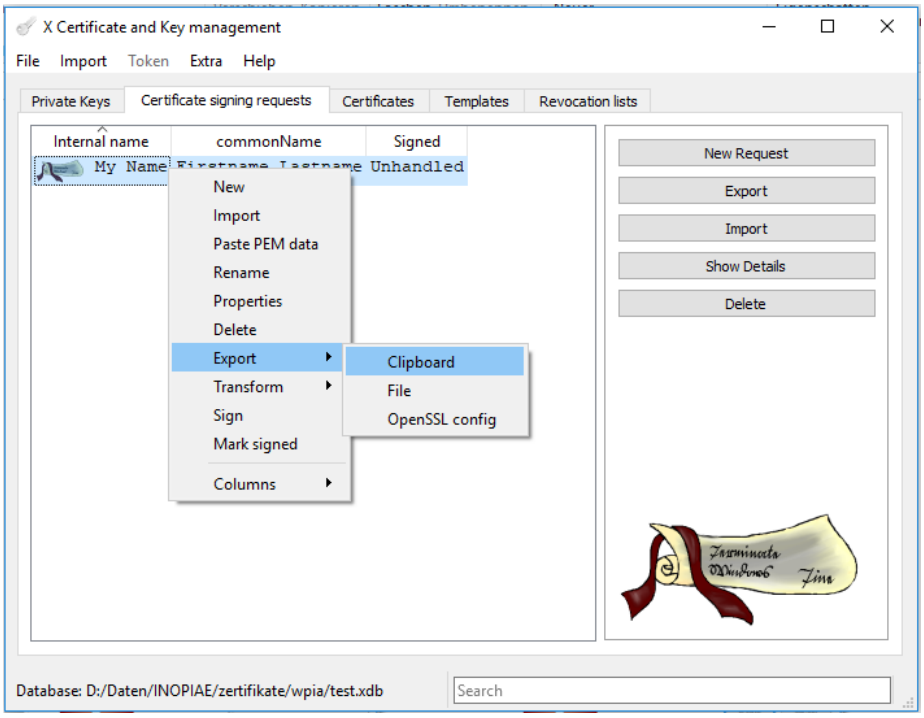


Figure 4: Screenshot Paste CSR to clipboard

Select the CSR and use a right mouse click to Export - Clipboard.

Now the CSR can be pasted to an email, to a file or into a CA application.

4 Import Public Key Via Clipboard

If you receive your public key in an CA application or as text in an email copy the public key from

```
-----BEGIN CERTIFICATE-----
until
-----END CERTIFICATE-----
```

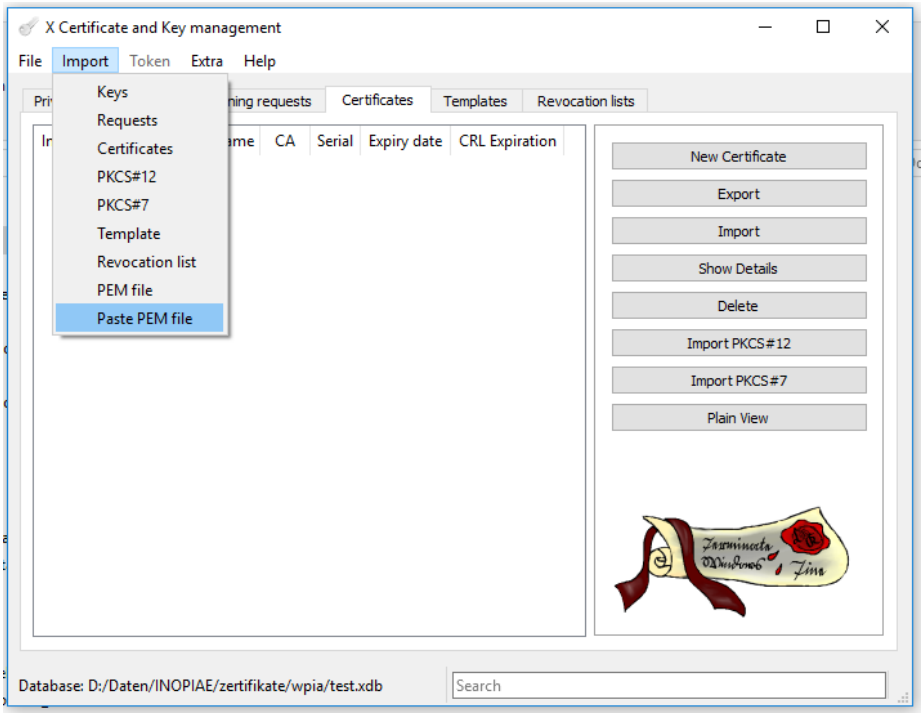


Figure 5: Screenshot Import PEM file via clipboard

To import the public key go to the Cerificates tab and choose from the menu Import - 'Paste PEM file'

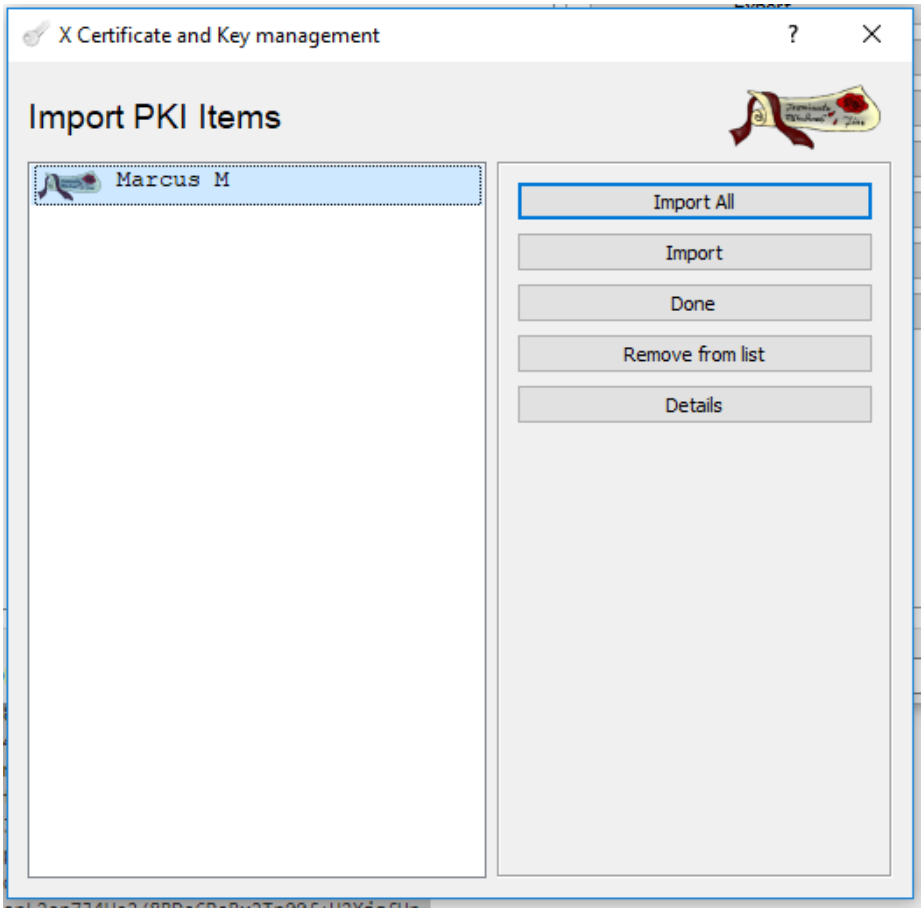


Figure 6: Screenshot Import key

Use ‘Import’ to import the public key to the XCA database.

5 Export Certificate

To export a certificate from the XCA database select the certifcate on the Certificates tab and use the button ‘Export’.

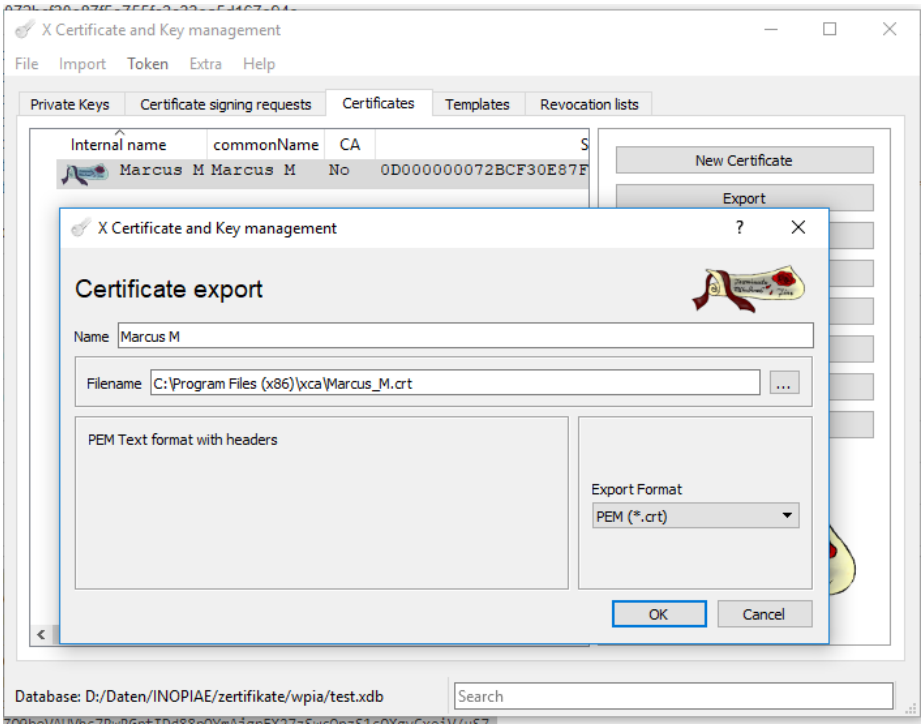


Figure 7: Screenshot Export certificate

Select a file name and define the export format.

To use the certificate with Windows you should export the file as PKCS#12 (*.p12).

Finish the export with ‘OK’.