Creating X.509 certificates

Quick Reference Guide
QRG_037_EN_01_Creating-X509-certificates.docx

Certificates are required for a secure VPN connection.
Certificates can be acquired from certification authorities or you can create them using the appropriate software. For example, X.509 certificates are created using Version 0.9.3 of the XCA program.

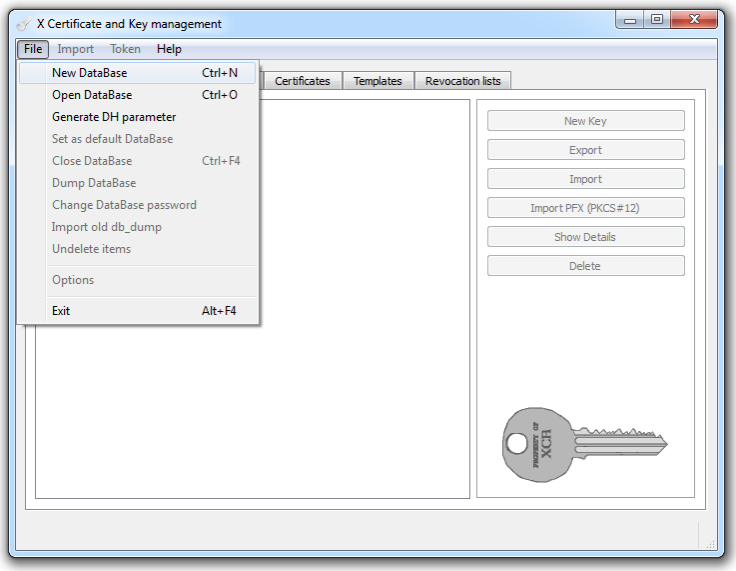
The XCA program can be downloaded at http://xca.sourceforge.net.

1 Installing XCA

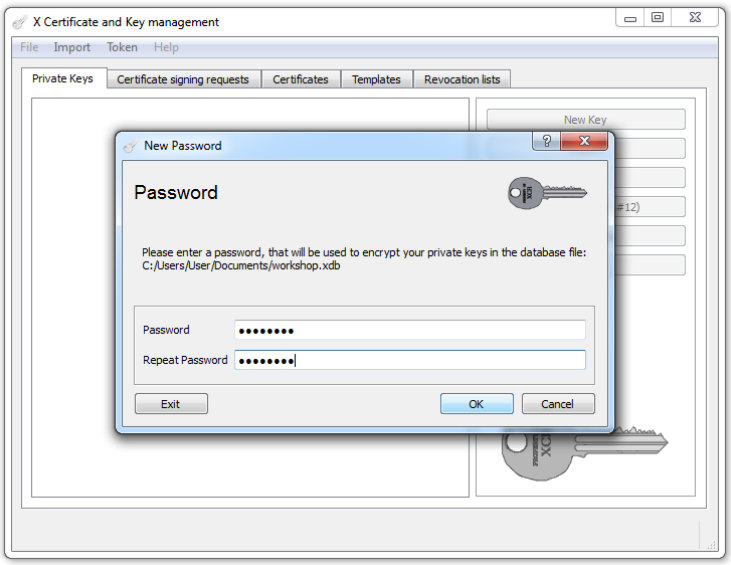
Start the setup_xca-0.9.3.exe setup file and follow the on-screen instructions of the setup program.

2 Creating a database

Once installed, start the XCA program and create a new database via the "File… New Database" menu item.

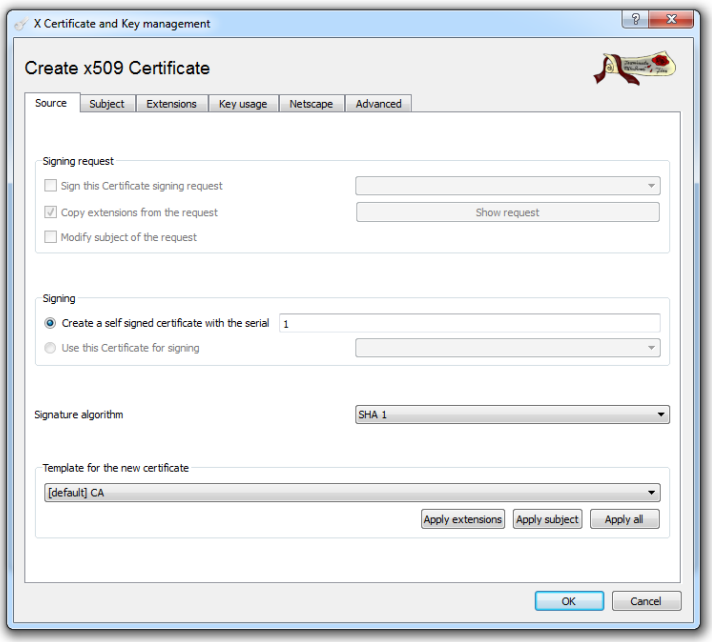


Assign a password to encrypt the database.

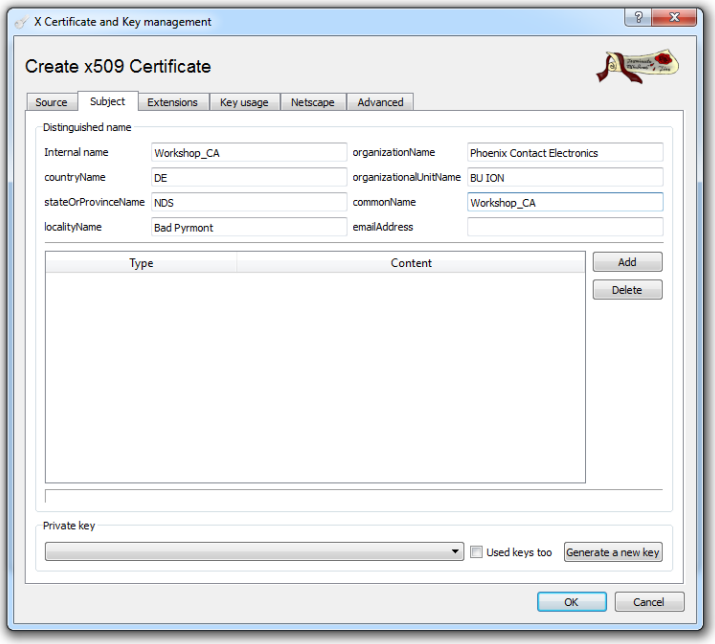


3 Creating a CA certificate

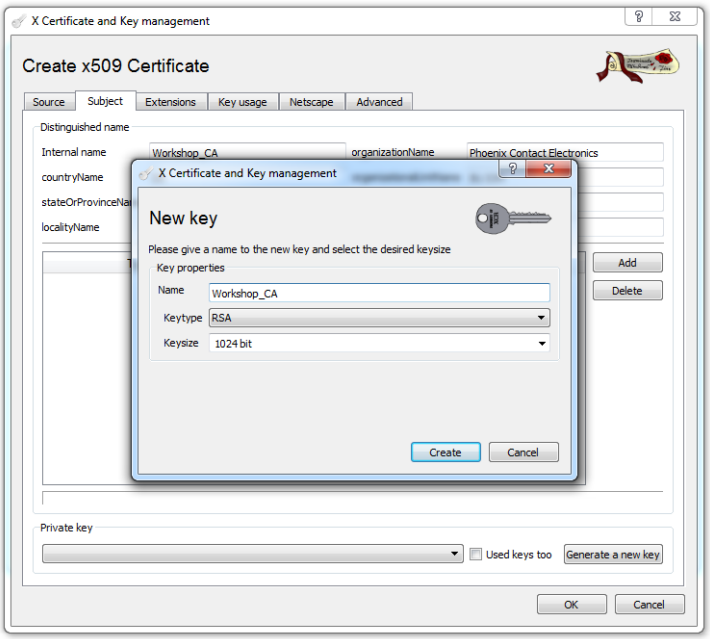
First you have to create a certification authority (CA) certificate. This root certificate acts as an entity that certifies and authenticates the signing of all certificates that are derived from it and thus guarantees the authenticity of the certificate that is in circulation. Switch to the "Certificates" tab and click on "New Certificate". In the program window shown, there is already a preset self-signed certificate with the signature algorithm SHA-1.



Switch to the "Subject" tab. Here, enter the information about the owner of the root certificate.

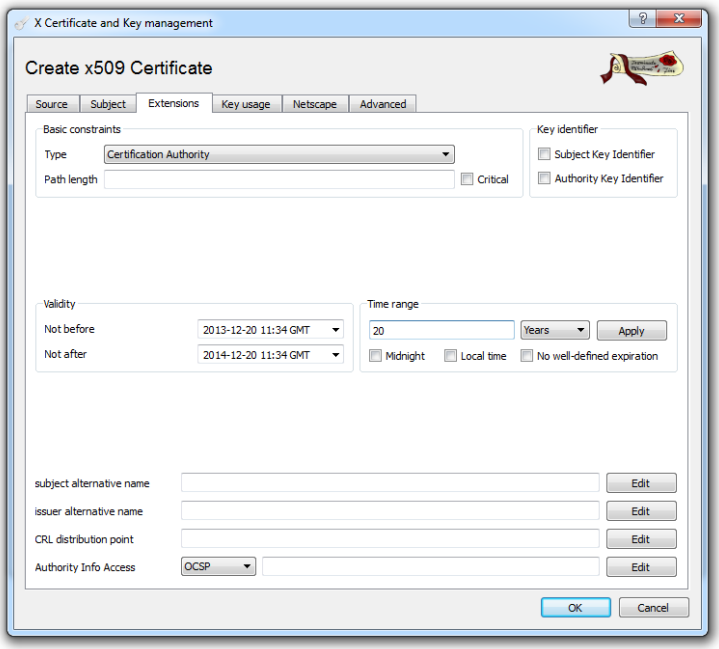


Click on "Generate a new key" for the certificate. You can keep the default key size and type as well as the name.



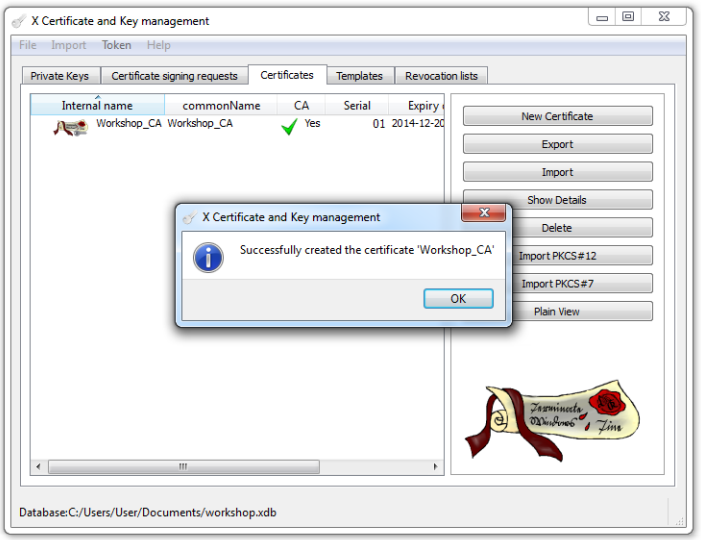
Switch to the "Extensions" tab.

The period of validity of the certificate is specified on the "Extensions" tab. The root certificate should have a longer period of validity than the machine certificates that are to be created later. In this example, the period of validity is set to 10 years. The certificate type is already set to "Certificate Authority" by default. Activate all the options as shown in the Figure.



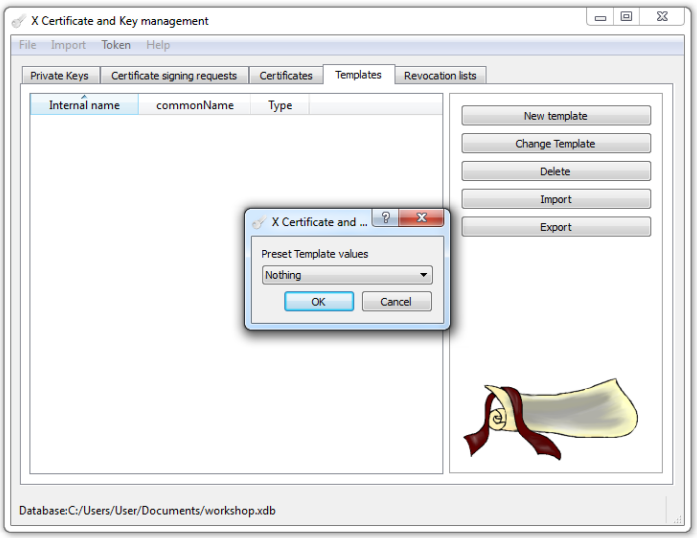
Click "OK" to complete root certificate creation.

A new root certificate from which further machine certificates can be derived now appears in the overview.

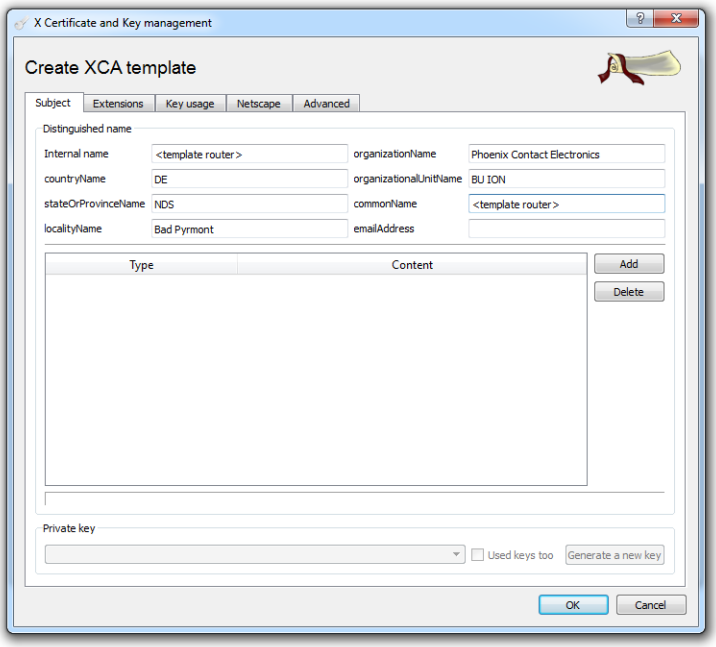


4 Creating templates

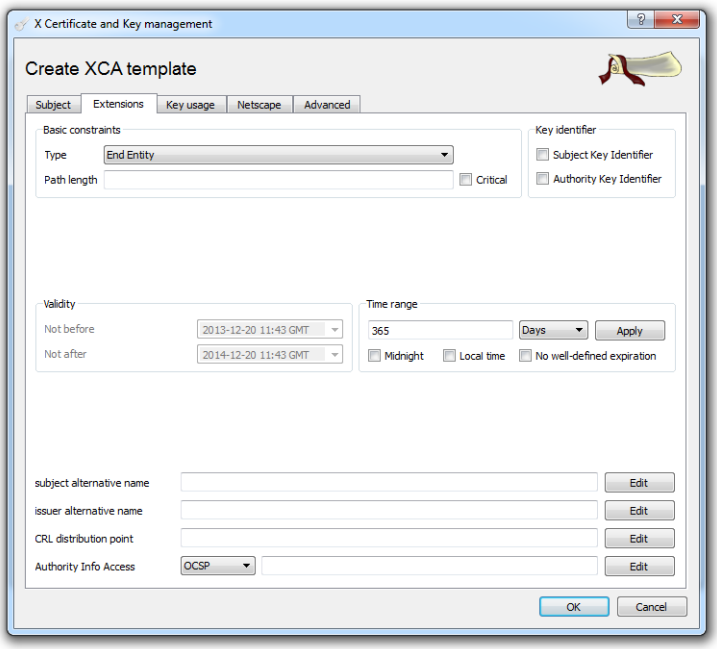
The further creation of machine certificates can be simplified by using templates. Switch to the "Templates" tab. Click on "New Template" to create a terminal certificate. In the "Preset Template Values" prompt that appears, select "Nothing".



On the "Subject" tab, specify the settings for the certificates that are to be created later. Two names appear in angular brackets ("Internal name" and "Common name"). The names in the angular brackets are simply placeholders, as the actual names are assigned to the certificates. When using the template, the names are set individually.



Switch to the "Extensions" tab. Change the certificate type to "End Entity", as the template is to be used for machine certificates. 365 days should be specified as the period of validity of the certificates to be created. After the resulting end date, the certificates can no longer be used.

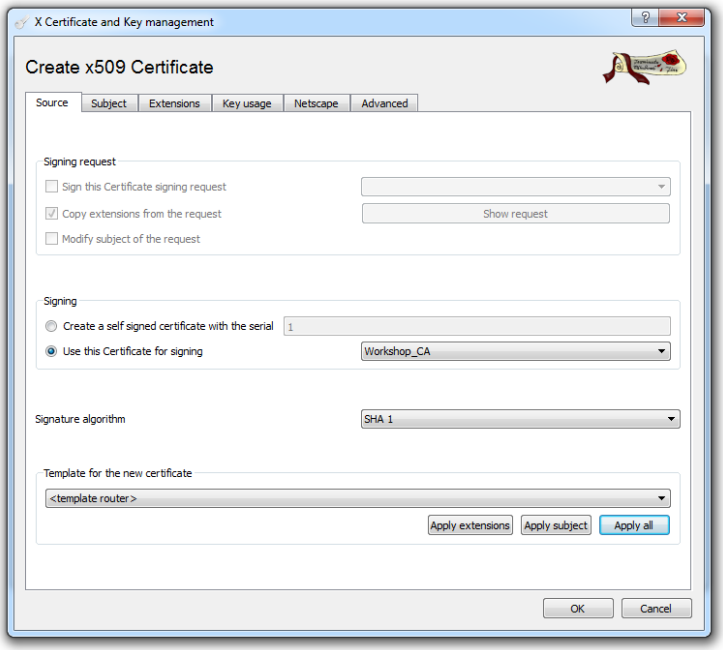


Click "OK" to create the template.
The template can now be used as a basis to create certificates signed with the root certificate.

5 Creating machine certificates based on a template

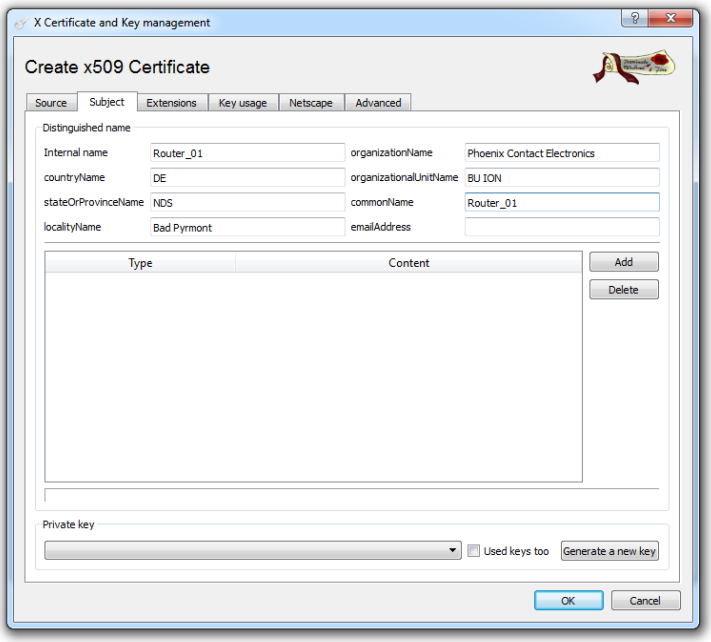
A template can be used to create certificates signed with the root certificate.

Switch to the "Certificates" tab and click on "New Certificate".
On the "Source" tab, specify the root certificate that is to be used for signing. In addition, you can select a template that has been created and read it in by clicking "Apply All".

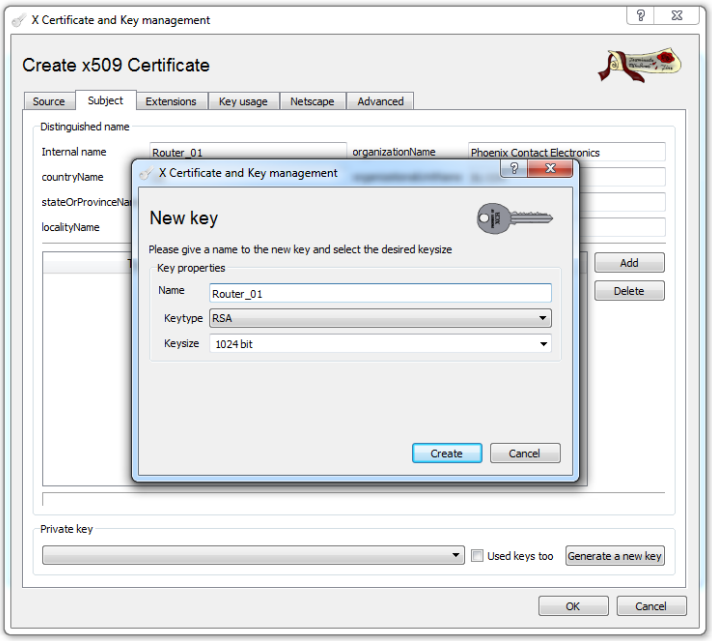


Switch to the "Subject" tab.

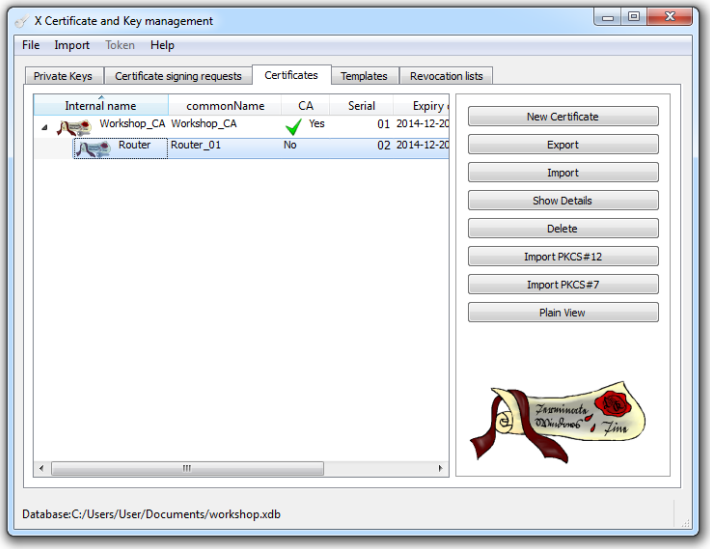
Here, enter the information about the owner of the machine certificate. When entering information on this tab, please note that the certificates must differ at least with regard to their name ("Internal name" and "Common name"). The equipment identification of the machine or router, for example, can be used as the name.



Click on "Generate a new key". Do not change the default key size, type, and name.

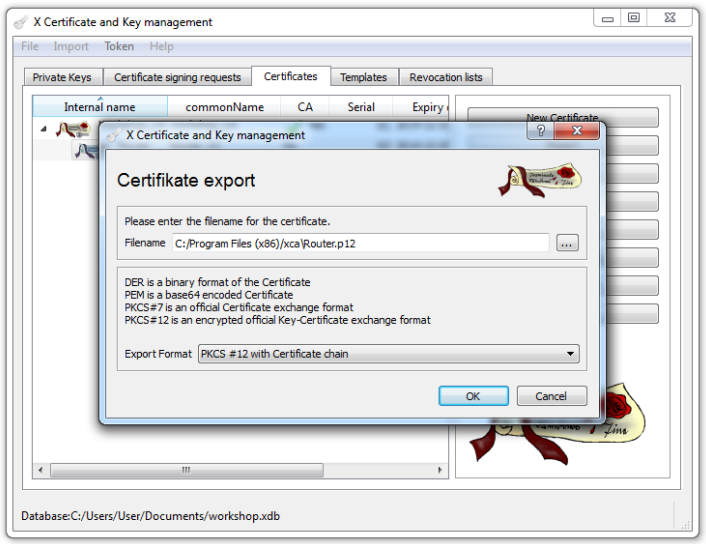


Click on “OK” to finish the creation of the machine certificate.
You now made machine certificate , which has been signed by the CA certificate.

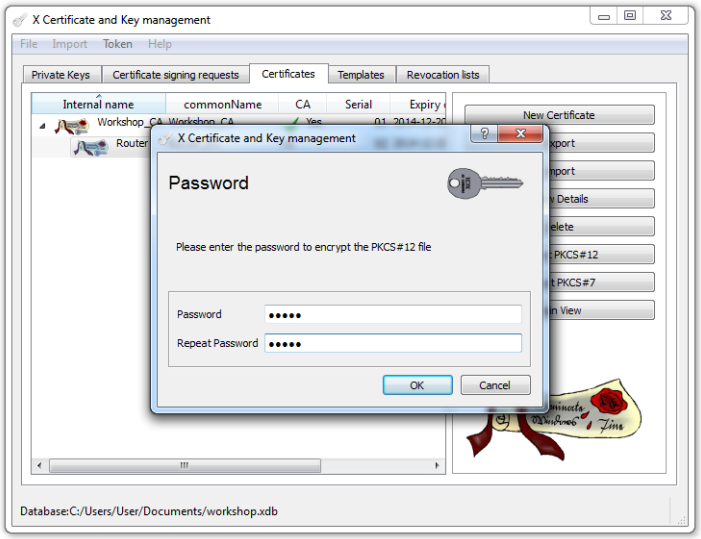


6 Exporting machine certificates

The machine certificate must be exported so that it can be used on the router. Select the relevant certificate from the list and click on "Export". The entire certificate including the private key must be in PKCS#12 format with certificate chain and can then be uploaded to the relevant component as a own machine certificate.



For security reason the machine certificate is encrypted with a password. Enter a password. This password is needed to load the machine certificate to the device.



The partner certificate should also be exported. This is stored in PEM format without the private key.