CardContact
smart system architects

# SmartCard-HSM Tutorials
# Getting started with XCA


| | |
|---|---|
| **Author** | **Andreas Schwier** |
| **Version** | **V1.0** |
| **Date** | **06.December 2013** |

# Content

# Revisions

| Date | Author | Changes | Version |
|---|---|---|---|
| 2013-12-06 | A.Schwier | Initial release | 1.0 |

# 1 Overview

XCA is a great tool to setup a PKI key infrastructure using X.509 certificates. As XCA has support for PKCS#11 modules, you can use a SmartCard-HSM to store keys managed by XCA.

This tutorial provides a step-by-step explanation how to set up your own PKI.

# 2 Installation

XCA accesses the SmartCard-HSM card using the OpenSC PKCS#11 module. Please install the OpenSC module using the installer provided on the SmartCard-HSM Starterkit/SDK CD (opensc-0.13.0g20130929205541-win32.msi).

As XCA is a 32-bit Windows application, you will need to install the 32-bit version of OpenSC, even on a 64-bit Windows version. The same is true for Mozilla Firefox, which is also only available as 32-bit application.

A binary distribution of XCA is included in the SmartCard-HSM Starterkit. The project can be found at http://sourceforge.net/projects/xca/. Please use the XCA installer in the SmartCard-HSM Starterkit/SDK CD (setup_xca-0.9.3.exe).

# 3 Configuration

## 3.1 Creating a Database

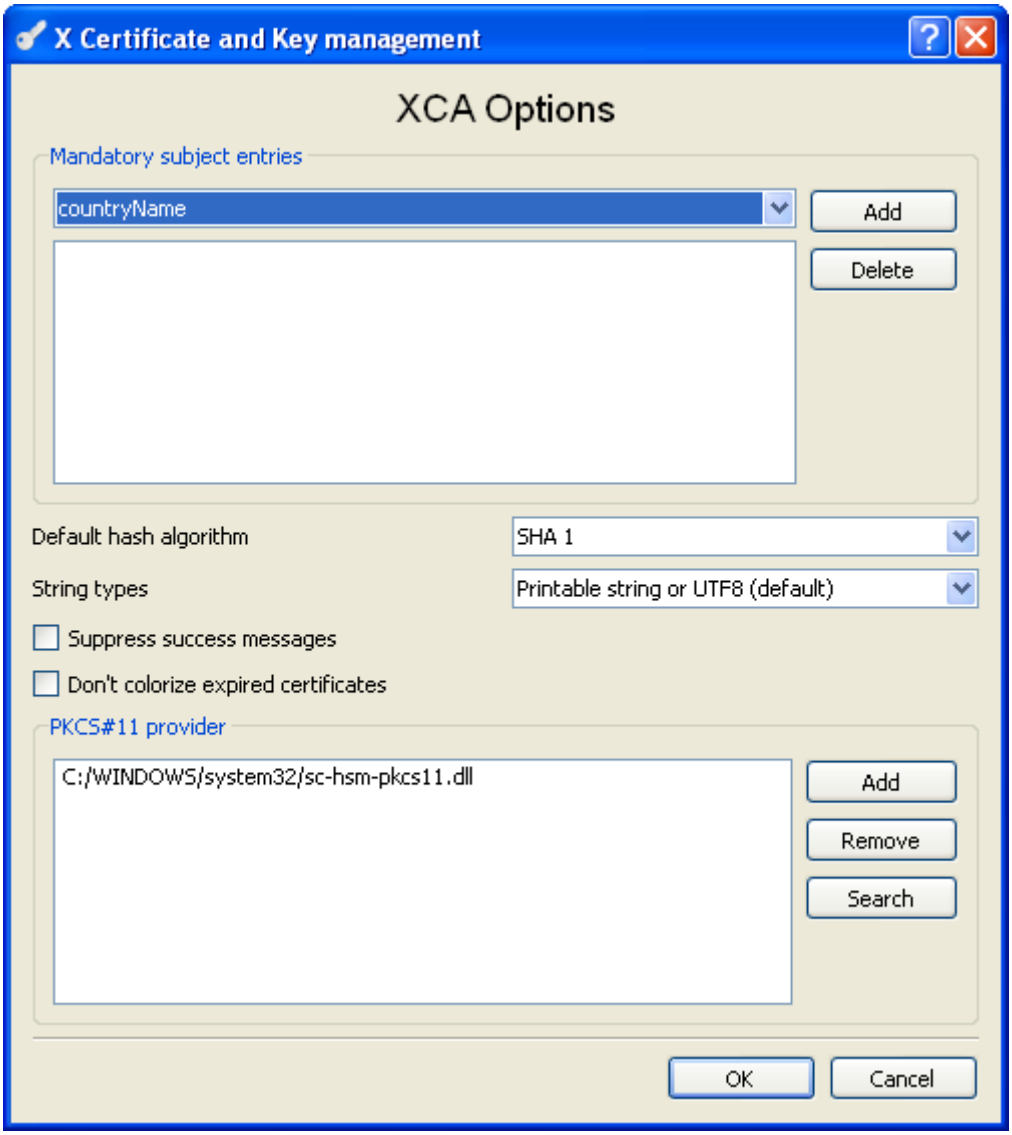
XCA requires a database to store local configuration information. Start XCA and use **File** / **New DataBase** to create a new database.

XCA will ask for a password which is used to control access to the database.

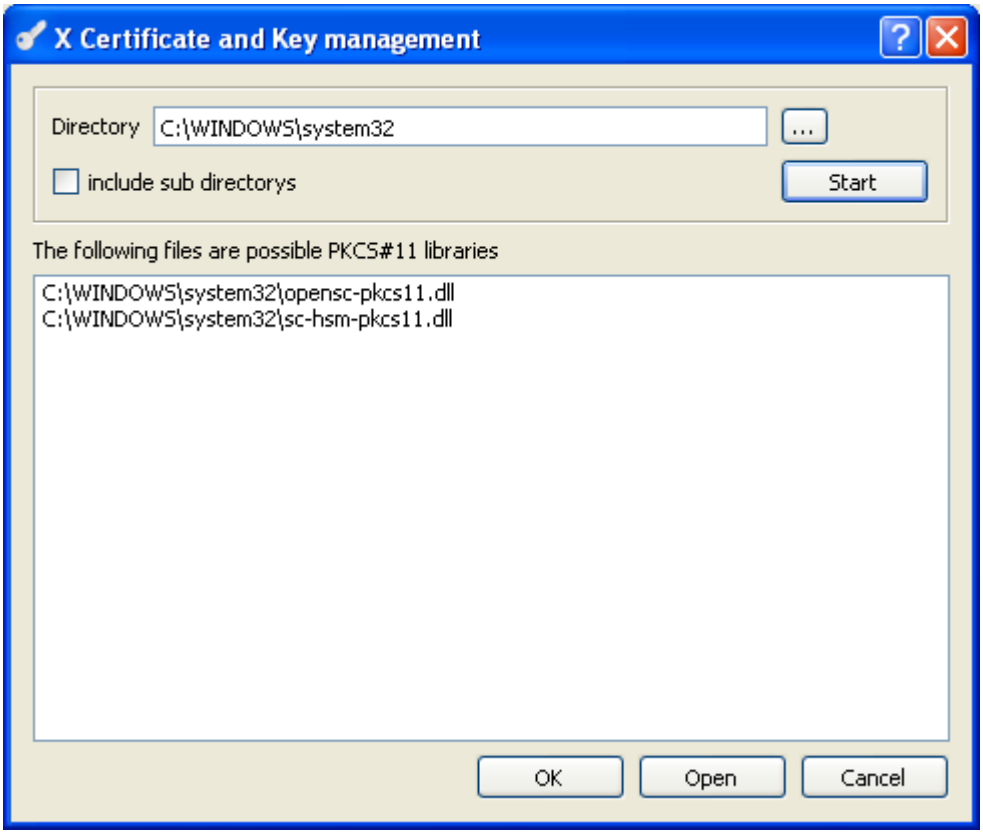
## 3.2 Selecting the PKCS#11 Module

To use the SmartCard-HSM as a key store in XCA, you will need to configure the OpenSC PKCS#11 module.

Open **File** / **Options**:




You can either define the PKCS#11 module directly using the **Add** button or search for the module using the **Search** button and dialog.



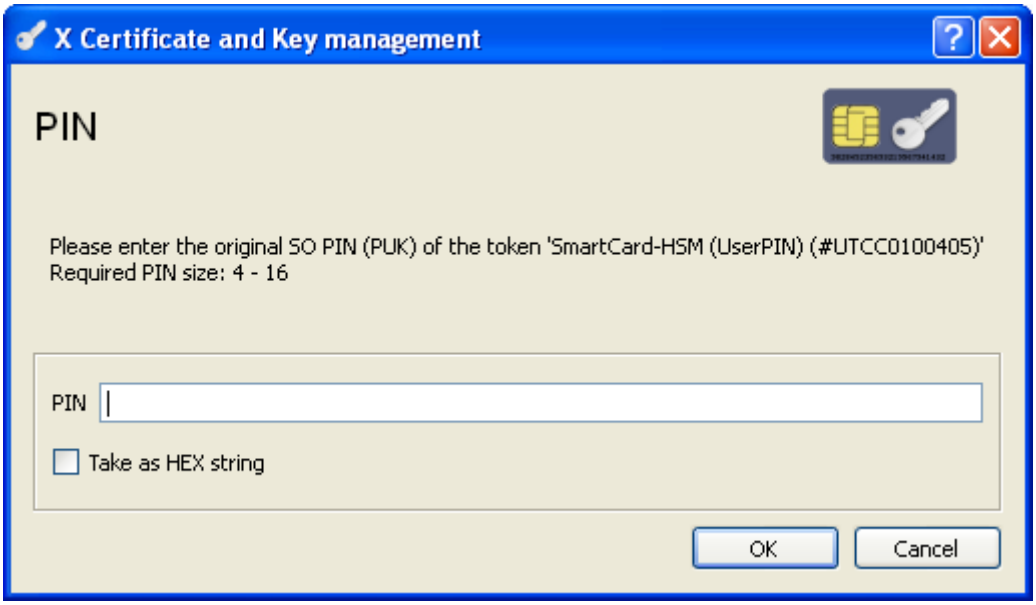

If you installed the light-weight PKCS#11 module for the SmartCard-HSM as well, it should be included in the list. Select the opensc-pkcs11.dll module, as only this module provides read/write access.

## 3.3 Initializing the SmartCard-HSM

If the SmartCard-HSM has never been used before and is not yet initialized, you will need to initialize the device first.

If the device has been initialized before (e.g. using sc-hsm-tool or pkcs11-tool from OpenSC) you can skip this step.

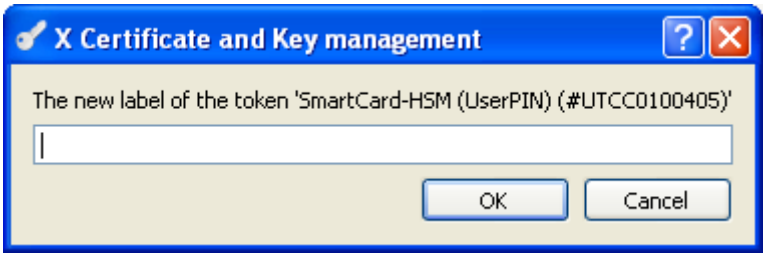
Select **Token** / **Init Security token** from the menu:



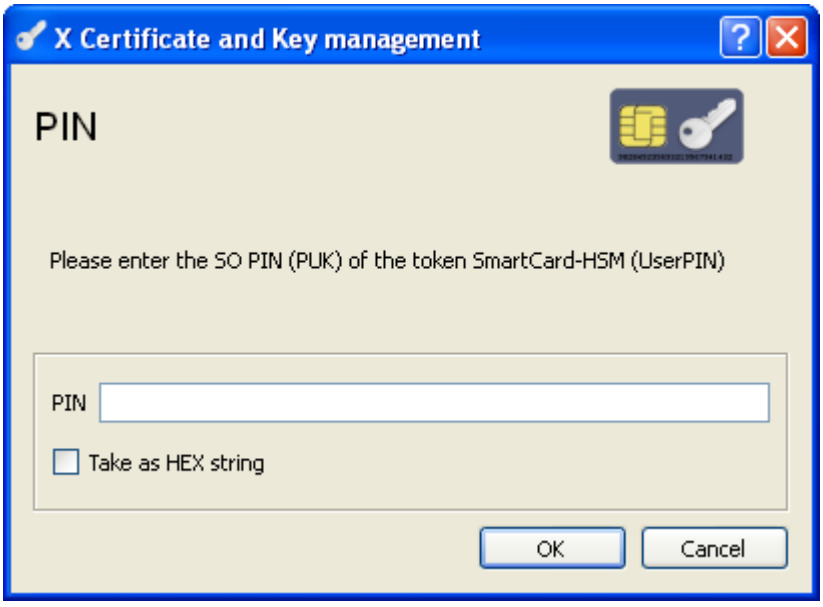

The Default SO PIN used throughout the tests is "3537363231383830". Please select your own secret SO PIN if you use a SmartCard-HSM in a productive environment. You will need the SO PIN to re-initialize a SmartCard-HSM or to reset the User PIN

Contrary to the XCA display, the SO PIN must contain 16 hexadecimal characters.

XCA will ask you for a label. You can leave the label empty as it is not used by the SmartCard-HSM.



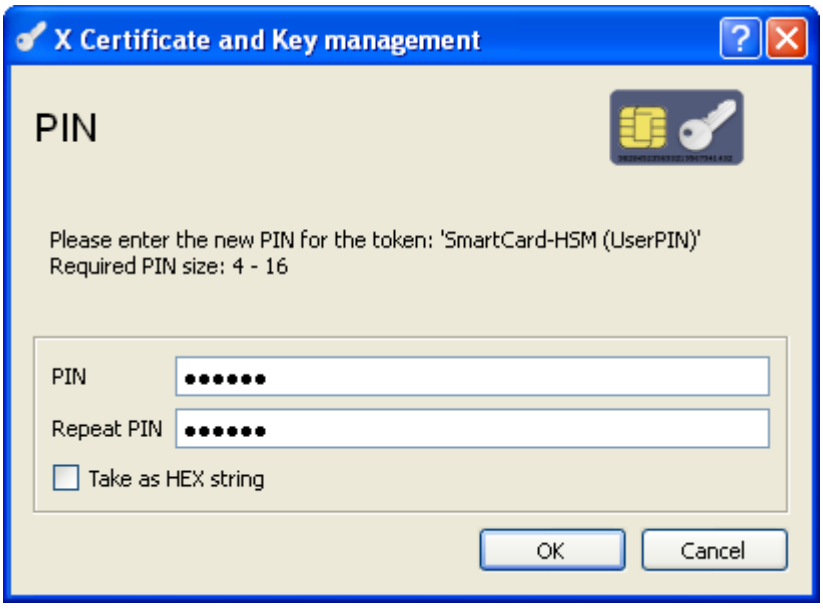

Next select **Token** / **Init PIN** to set the User PIN:




Again you will need to enter the SO PIN use before.

XCA will ask you for the User PIN. This PIN is required for all subsequent operations with the SmartCard-HSM.

Contrary to the XCA display, the PIN must be at least 6 digits long.

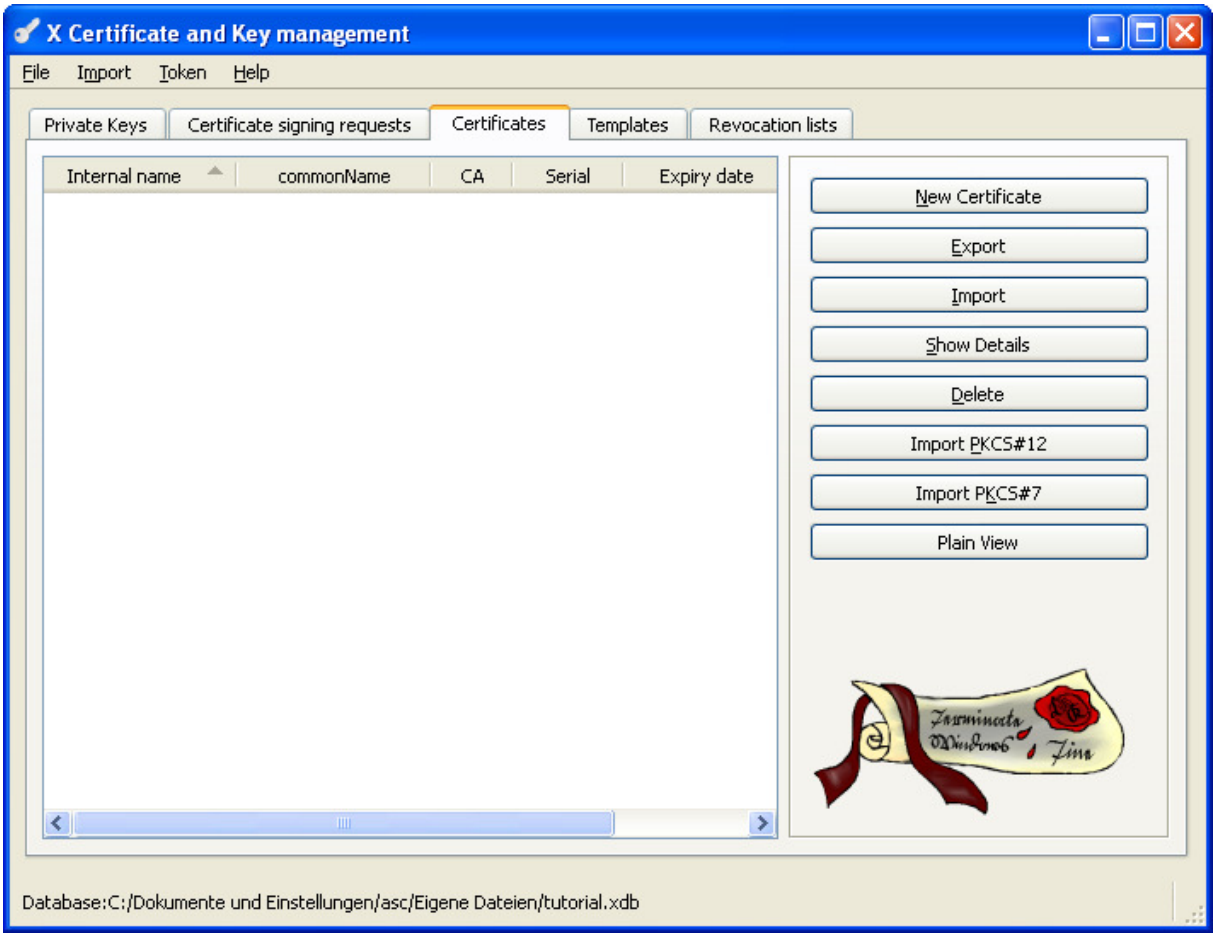



Now the SmartCard-HSM is initialized and has a User PIN set. You can start creating keys now.

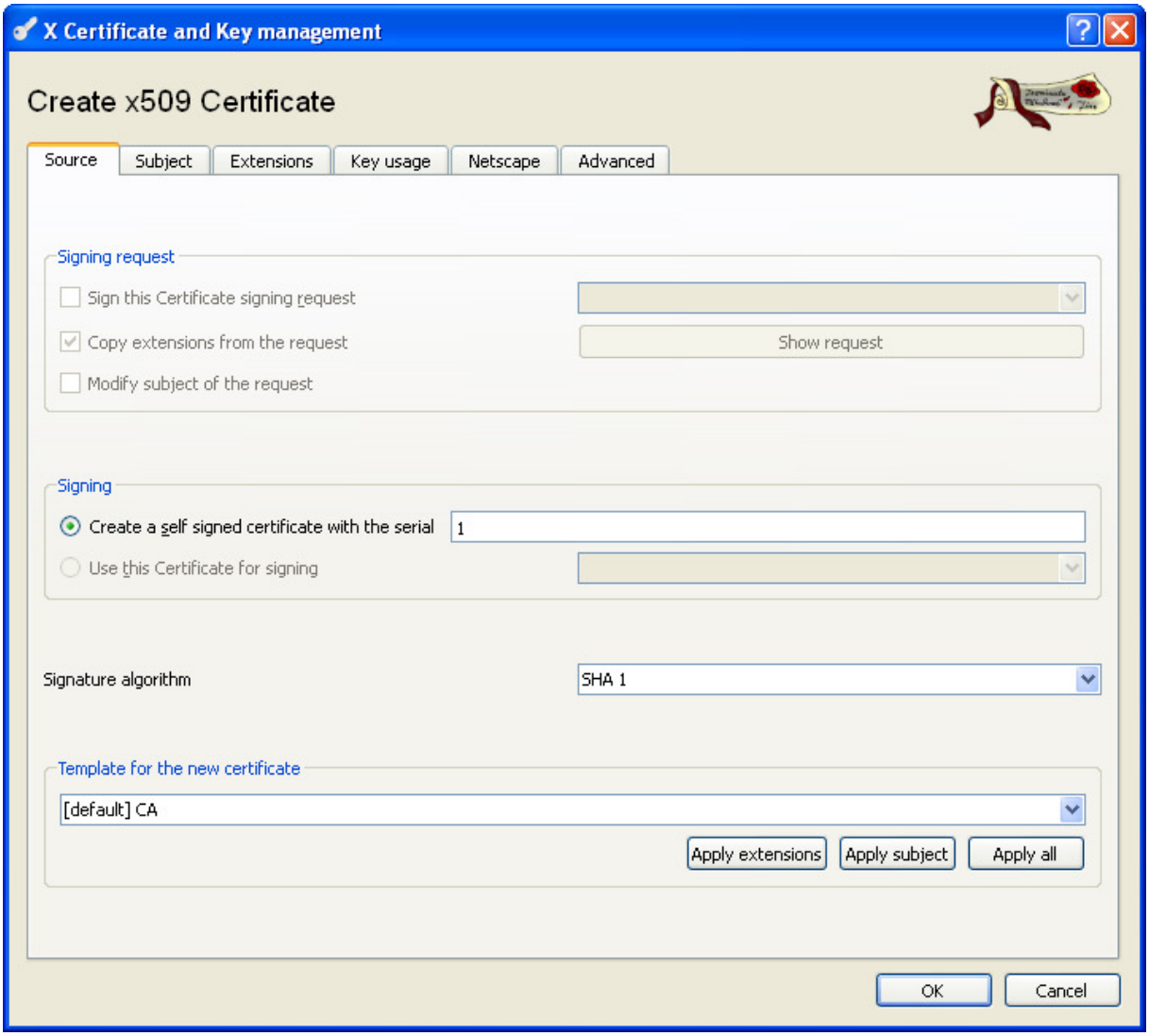
## 4 Create a Certification Authority

A Certification Authority can issue certificates to others. A certification authority has a private key and a certificate. Use the following steps to create a CA.

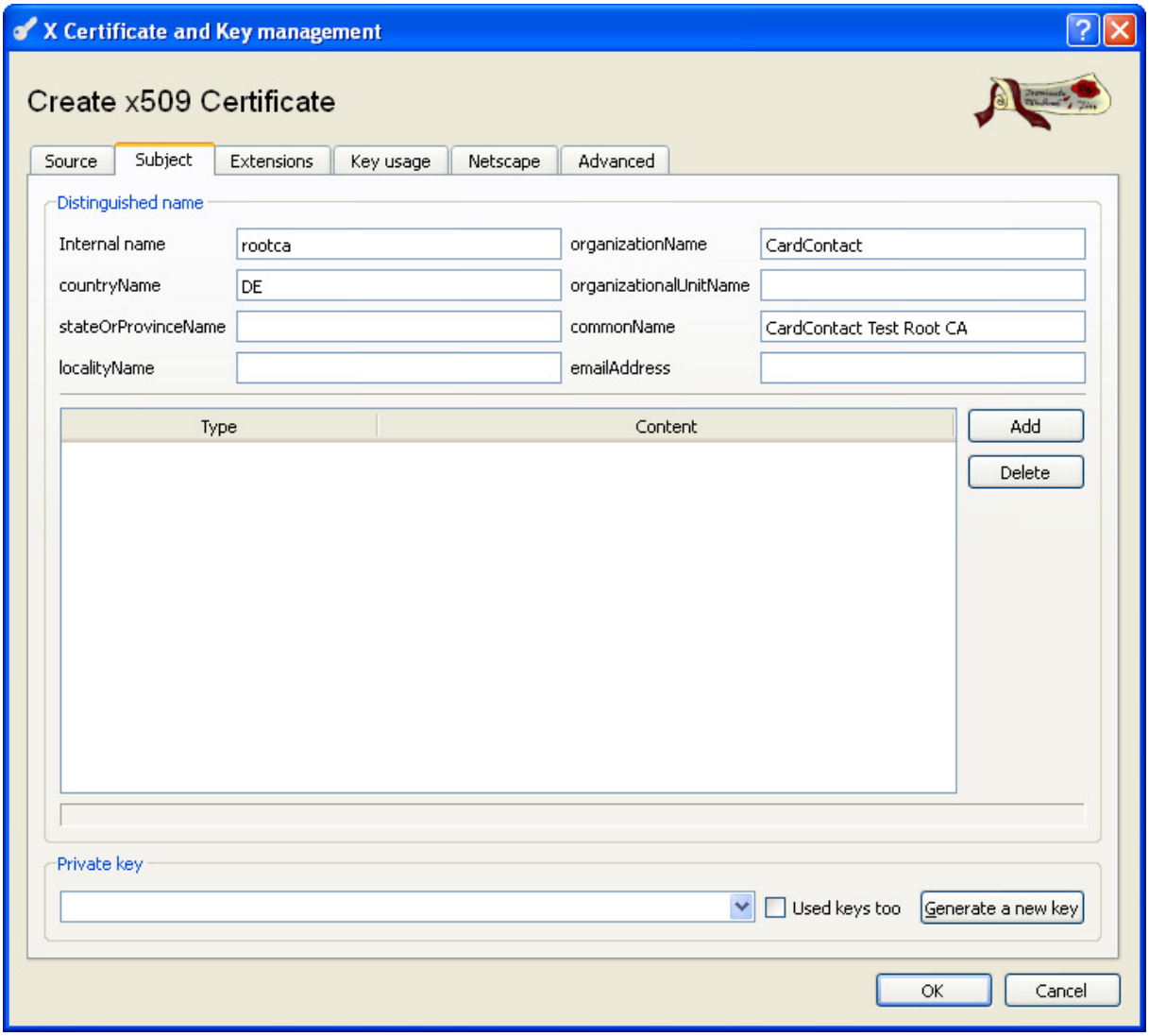
Select the **Certificates** tab:



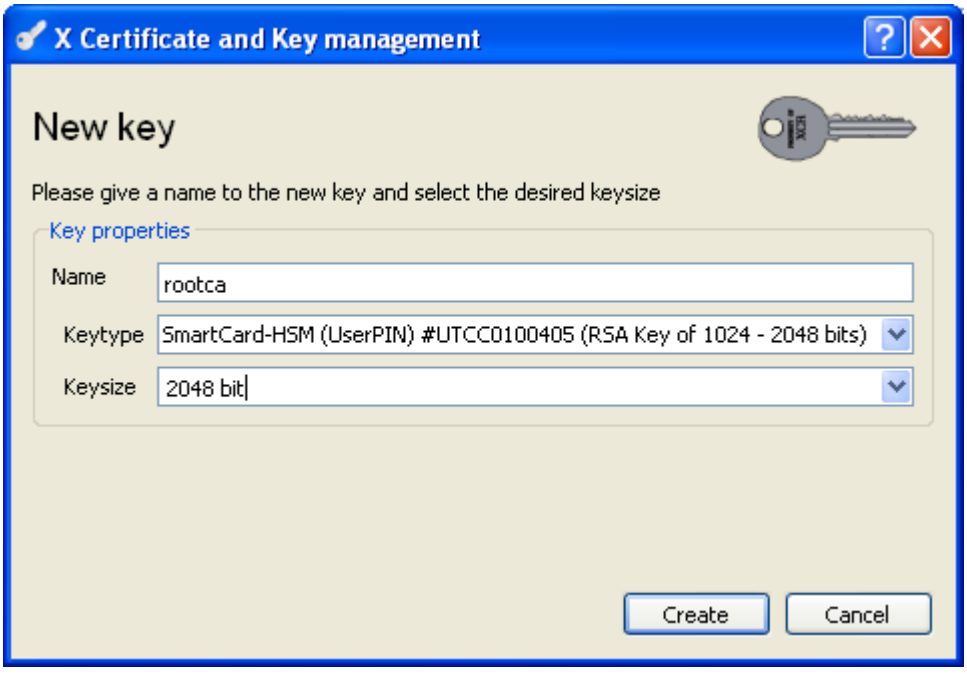

Press **New Certificate**



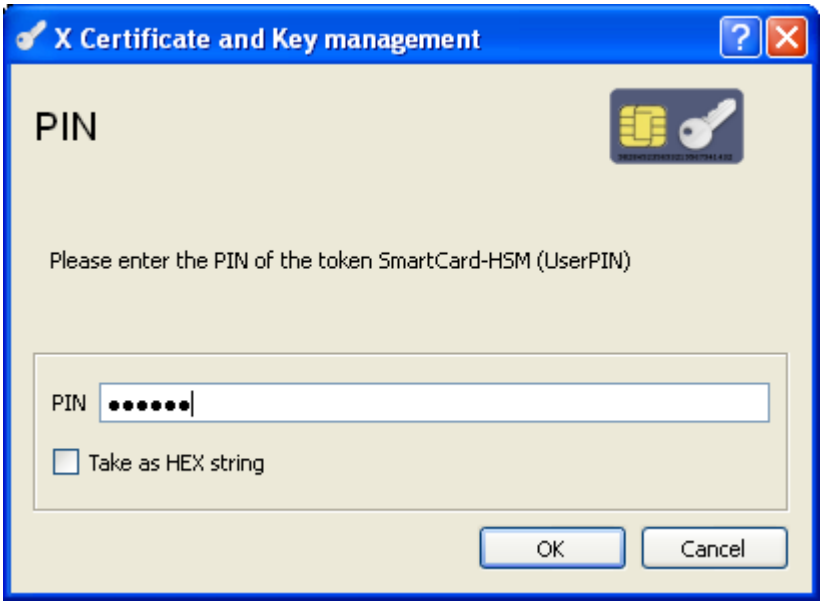

Press **Apply all** to set reasonable defaults for the CA certificate. Select **Subject** to enter the name of your CA:



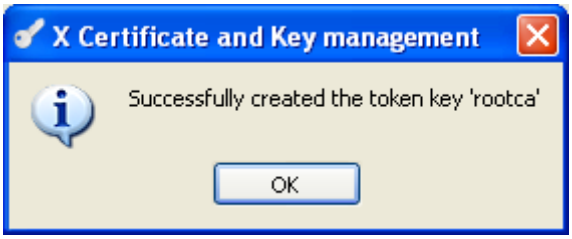

Next you will need to generate a new key for the CA. Press **Generate a new key**.



On the **Keytype** field you must select "SmartCard-HSM (UserPIN)…". The **Keysize** can be either 1024 or 2048 bit. Press **Create** to enter the User PIN.

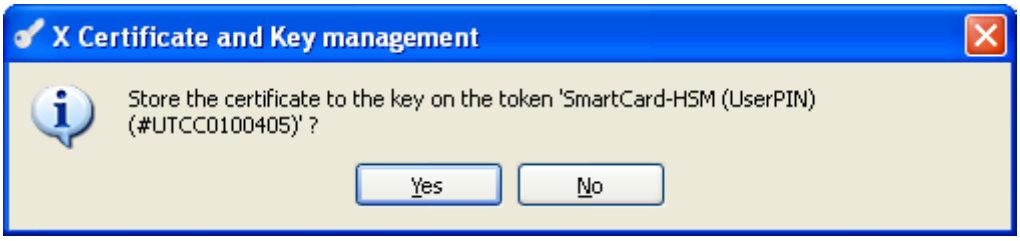



After pressing **OK** it will take up to 60 seconds to generate the new key. During this time the display will not be refreshed. Just be patient.




After the key has been created you can press **OK** to generate the certificate. You will be prompted again to enter the User PIN.

After the certificate has been signed using the key on the SmartCard-HSM you will be prompted if the certificate shall also be stored on the token.




This is optional and the certificate will be stored in the database anyway.

## 5 Issue Certificates

Once a CA certificate has been created, you can use that CA to certify end-entity certificates.

Issuing a certificate works the same way as issuing the CA certificate. You generate a certificate signing request first, send that to the CA and the CA issues the certificate. Later you receive the certificate and store it on the SmartCard-HSM.