

SmartCard-HSM Tutorials Getting started with XCA

Author Version Date Andreas Schwier V1.0 06.December 2013



© 2013 CardContact Software & System Consulting

The authors of this documentation make no representation or warranty regarding whether any particular physical implementation of any part of these specifications does or does not violate, infringe, or otherwise use the patents, copyrights, trademarks, trade secrets, know-how, and/or other intellectual property of third parties, and thus any person who implements any part of these specifications should consult an intellectual property attorney before any such implementation.



Content

1	Overview	.5
2	Installation	.5
3	Configuration	.5
3.1	Creating a Database	.5
3.2	Selecting the PKCS#11 Module	.5
3.3	Initializing the SmartCard-HSM	.7
4	Create a Certification Authority	.9
5	İssue Certificates	13



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 <u>http://sourceforge.net/projects/xca/</u>. 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:



of X Certificate and Key management	? 🛛				
XCA Options					
countryName	▼	Add Delete			
Default hash algorithm	SHA 1	×			
String types	Printable string or UTF8 (def	ault) 🔽			
Suppress success messages					
Don't colorize expired certificates					
PKCS#11 provider					
C:/WINDOWS/system32/sc-hsm-pkcs11.dll		Add Remove Search			
	ОК	Cancel			

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



of X Certificate and Key management	? 🛛
Directory C:\WINDOWS\system32 include sub directorys The following files are possible PKCS#11 libraries C:\WINDOWS\system32\opensc-pkcs11.dll C:\WINDOWS\system32\sc-hsm-pkcs11.dll	Start
OK Open	Cancel

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:



✓ X Certificate and Key management	? 🛛
PIN	
Please enter the original SO PIN (PUK) of the token 'SmartCard-HSM (L Required PIN size: 4 - 16	JserPIN) (#UTCC0100405)'
PIN Take as HEX string	
	OK Cancel

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.

🖍 X Certificate and Key management 🛛 🔹 💽		
The new label of the token 'SmartCard-HSM (UserPIN) (#UTCCC OK Ca)100405)' ancel	

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



of X Certificate and Key manageme	nt ? 🔀
PIN	
Please enter the SO PIN (PUK) of the toke	n SmartCard-HSM (UserPIN)
PIN	
Take as HEX string	
	OK Cancel

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.

🝼 X Certific	ate and Key management 🛛 🛛 🔀
PIN	E
Please enter Required PIN	the new PIN for the token: 'SmartCard-HSM (UserPIN)' size: 4 - 16
PIN	•••••
Repeat PIN	•••••
🔲 Take as H	IEX string
	OK Cancel

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:





🖌 X Certificate and Key management	
<u>File Import Token Help</u>	
Private Keys Certificate signing requests Certificates Templates Revocati	ion lists
Private Keys Certificate signing requests Certificates Templates Revocati Internal name commonName CA Serial Expiry date	In lists
Database:C:/Dokumente und Einstellungen/asc/Eigene Dateien/tutorial.xdb	Taumineeta Divisiono Tima

Press New Certificate



🖋 X Certificate and Key management	29
Create x509 Certificate	Community of the second s
Source Subject Extensions Key usage Netscape	Advanced
Signing request	
Sign this Certificate signing request	×
Copy extensions from the request	Show request
Modify subject of the request	
Signing	
• Create a self signed certificate with the serial 1	
O Use this Certificate for signing	✓
Signature algorithm	SHA 1
[default] CA	
	Apply extensions Apply subject Apply all
	OK Cancel

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



Source Subject Key usage Netscape Advanced Distinguished name organizationName CardContact Image: Control of CardContact Internal name rootca organizationalUnitName CardContact Test Root CA Internal name rootca organizationalUnitName CardContact Test Root CA Internal name rootca organizationalUnitName CardContact Test Root CA Internal name rootca commonName CardContact Test Root CA Internal name rootca mailAddress Add Delete Type Content Add Delete Delete Private key Image:	🖌 X Certii	ficate and K	ey manage	ment				? 🛛
Source Subject Extensions Key usage Advanced Distinguished name organizationName CardContact Internal name rootca organizationalUnitName countryName DE organizationalUnitName stateOrProvinceName commonName CardContact Test Root CA localityName emailAddress Add Type Content Add Delete Plete Plete Private key Used keys too generate a new key OK Cancel	Create	Create x509 Certificate						
Distinguished name Internal name rootca organizationName CardContact stateOrProvinceName cormonName cardContact Test Root CA localityName emailAddress Type Content Add Delete Private key	Source	Subject	Extensions	Key usage	Netscape	Advanced		
Internal name rootca organizationName CardContact countryName DE organizationalUnitName Image: CardContact Test Root CA localityName emailAddress Type Content Add Delete Private key Vertice key Image: Content Vertice key OK Cancel	Distingu	ished name —						
countryName DE organizationalUnitName CardContact Test Root CA localityName emailAddress Type Content Add Delete Private key Vintek key Vintek key Vintek key Vintek key Vintek key Vintek key Vintek key Vintek key Vintek key Vintek key Vintek key too Cancel OK	Interna	Iname	rootca			organizationName	CardContact	
stateOrProvinceName CardContact Test Root CA localityName emailAddress Type Content Add Delete Private key Vised keys too Generate a new key OK	country	Name	DE			organizationalUnitName		
IncalityName emailAddress Type Content Delete Delete Private key Private key Y Used keys too GK Cancel	stateOr	ProvinceName				commonName	CardContact Test Root C	A
Type Content Add Delete Private key V Used keys too Generate a new key OK Cancel	locality	Name				emailAddress		
Private key		Tue	•			Content		
Delete Delete Delete Private key Image: Comparison of the set of th		UVP	6			Concent		Add
Private key								Delete
Private key								
Private key								
Private key								
Private key								
Private key Used keys too Generate a new key								
Private key Used keys too Generate a new key								
Private key Used keys too Generate a new key OK Cancel								
Private key Used keys too Generate a new key OK Cancel								
Private key Used keys too Generate a new key OK Cancel								<u> </u>
Used keys too Generate a new key OK Cancel		Land State						
Used keys too Generate a new key OK Cancel	Private	кеу					_	
OK Cancel						*	Used keys too Gen	erate a new key
OK Cancel								
							ОК	Cancel

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.

of X Certificate and Key manager	nent 🛛 🛛 🛛
PIN	II 🖌
Please enter the PIN of the token Smar	tCard-HSM (UserPIN)
PIN •••••• Take as HEX string	
L	OK Cancel

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.

🖋 X Certificate and Key management 🛛 🔀	
(Successfully created the token key 'rootca'
	ОК

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.