

| Author | Andreas Schwier |
|---------|-----------------|
| Version | 0.1 |
| Date | 2015-09-07 |

Table of Contents

| 1 Introduction | 4 |
|---|----|
| 2 Prerequisite | 4 |
| 2.1 Installing Software | 4 |
| 2.2 Prepare the script workspace | 4 |
| 2.3 Starting the Smart Card Shell | 4 |
| 3 Creation of Authentication Keys | 5 |
| 4 Configuration for n-of-m Authentication | 7 |
| 5 Performing Public Key Authentication | 10 |
| | |

1 Introduction

This document is a step-by-step description for configuring n-of-m authentication with a SmartCard-HSM EA+ Edition.

2 Prerequisite

2.1 Installing Software

You need to install the Smart Card Shell at least in version 3.7.1874 available from www.openscdp.org/scsh3.

You need to install git in order to checkout the software from the CDN.

You need to have a CDN certificate on your SmartCard-HSM to access the repository. See http://www.cardcontact.de/cdn/gitaccess.html for details.

2.2 Prepare the script workspace

Create a directory on your disk to serve as a workspace (e.g. smartcardhsm-workspace).

Open a console in the workspace and checkout the scsh-mods project from the CDN.

- \$ mkdir smartcardhsm-workspace
- \$ cd smartcardhsm-workspace
- \$ ssh-add -s /usr/local/lib/opensc-pkcs11.so
- \$ git clone ssh://git@devnet.cardcontact.de:222/scsh-mods scsh
- \$ git clone ssh://git@devnet.cardcontact.de:222/sc-hsm-sdk-scripts

2.3 Starting the Smart Card Shell

Start the Smart Card Shell and select the workspace directory.

| Please select your workspace directory or initial configuration script. | | |
|--|--|--|
| When selecting a configuration script, then the workspace is determined by the directory location of the script. | | |
| /home/asc/tmp/howto/smartcardhsm-workspace 💌 Browse | | |
| Use this as the default and do not ask again. Allow selection of a configuration script | | |
| ОК | | |

Run the keymanager.js script from sc-hsm-sdk-scripts/keymanager

File Edit Options Help

| 🚍 SmartCard-HSM (UTDEV0915300000) - Not initialized | Running setup script config.js |
|---|---|
| | SCSH3 - Smart Card Shell 3.7.1874 |
| | (c) 2005-2011 CardContact Software & System Consulting (www.cardcontact.de) Enter 'help' for a command overview or 'quit' to close the shell |
| | >load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); Issuer Certificate : CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August 7, 2015 Device Certificate : CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septemb > |
| | Shell Trace |

The shell shows some status information of the device, in particular the device id.

3 Creation of Authentication Keys

You will need to create a key pair on each SmartCard-HSM given to a key custodian.

Right-click on the SmartCard-HSM node to see the context menu and select "Initialize Device".

| File Edit Options Help | | | | |
|--|--|--|--|--|
| SmartCard-HSM (UTDEV0915300000) - N is in the setup script config.js | | | | |
| | SCSH3 - Smart Card Shell 3.7.1874 | | | |
| | (c) 2005-2011 CardContact Software & System Consulting (www.cardcontact.de) Enter 'help' for a command overview or 'quit' to close the shell | | | |
| | <pre>>load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); Issuer Certificate : CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August 7, 2015</pre> | | | |
| | Device Certificate : CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septemb > | | | |
| | | | | |
| | Shell Trace | | | |

The key manager will prompt for the Initialization Code. The dialog is pre-set with the default value used in all tutorials. Replace with your own 16 digit hex code for productive cards.

| Enter Initialization Code (SO-PIN) | | | |
|------------------------------------|----------|--------|--|
| 35373632 | 31383830 |) | |
| | OK | Cancel | |
| | | cancer | |

On the next prompt select "User PIN" as authentication mechanism.

| Select authentication mechanism | | | |
|---------------------------------|----|--------|---|
| User PIN | | | - |
| | ОК | Cancel | |

On the next prompt select "Resetting PIN with SO-PIN not allowed".

| Allow RESET RETRY COUNTER | | | |
|---|--|--|--|
| Resetting PIN with SO-PIN not allowed 💌 | | | |
| OK Cancel | | | |

The key manager will prompt for the User PIN value. Please have the key custodian enter a self-selected PIN. The dialog is pre-set with the default User PIN used throughout the tutorials.

| Enter Use | r PIN | | |
|-----------|-------|--------|--|
| 648219 | | | |
| | | | |
| | ок | Cancel | |

The SmartCard-HSM is now initialized. The procedure can be repeated as often as desired.

| File Edit Options Help | |
|---|--|
| 🚍 SmartCard-HSM (UTDEV0915300000) — 🗋 User PIN verified (9000) | SCSH3 - Smart Card Shell 3.7.1874 |
| └ 🗋 SO PIN not verified, 15 tries remaining (63CF) | (c) 2005-2011 CardContact Software & System Consulting (www.cardcontact.de) Enter 'help' for a command overview or 'quit' to close the shell |
| | <pre>>load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); Issuer Certificate : CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August 7, 20 Device Certificate : CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septe >Initializing, please wait Initializing complete</pre> |
| | ▼ ↓ Trace |

Next you will need to generate an ECDSA key. Right-click on the SmartCard-HSM node and select "Generate ECC Key".

| File Edit Options Help | |
|---|---|
| SmartCard-HSM (UTDEV09153000 User PIN verified (9000) SO PIN not verified, 15 tries re Initialize Device | SCSH3 - Smart Card Shell 3.7.1874 (c) 2005-2011 CardContact Software & System Consulting (www.cardcontact.de) Enter 'help' for a command overview or 'quit' to close the shell >load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); Issuer Certificate : CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August 7, 2C Device Certificate : CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septe >Initializing, please wait Initializing complete |

Select "brainpoolP256r1" as curve.

| Select Curve | |
|-----------------|--------|
| brainpoolP256r1 | - |
| ОК | Cancel |

Enter a label for the key in the next dialog.

| Enter Key | Label | | |
|---------------------------|-------|--------|--|
| key custodian #1 test key | | | |
| | ок | Cancel | |
| | | | |

The key is now generated and the public key certification signing request prepared.

| FI | le Edit Options Help | |
|----|---|---|
| • | SmartCard-HSM (UTDEV0915300000) User PIN verified (9000) SO PIN not verified, 15 tries remaining (63CF) → key custodian #1 test key ▲ AT-CVREQ CAR=UTDEV0915300000 CHR=UTDEV0 | <pre>(c) 2005-2011 CardContact Software & System Consulting (www.cardcontact.de) Enter 'help' for a command overview or 'quit' to close the shell >load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); Issuer Certificate : CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August 7, 2C Device Certificate : CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septe >Initializing, please wait Initializing complete Cenerating key can take up to 60 seconds, please wait</pre> |
| 1 | M. 🕨 | Key generated |

The final step is to export the public key. Right-click on the certificate and select "Export for public key authentication".

| File Edit Options Help | | | | |
|---|--|--|--|--|
| 🗂 SmartCard-HSM (UTDEV0915300000) | | | | |
| - 🗋 User PIN verified (9000) | [c) 2005-2011 CardContact Software & System Consulting (www.cardcontact.de) Exter (balo) for a command exercise or (multi to close the chall | | | |
| – 🗋 SO PIN not verified, 15 tries remaining (63CF) | | | | |
| 👇 🕶 key custodian #1 test key | >load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); | | | |
| ► AT-CVREQ CAR=UTDEV0915300000 CUB_UTDEV0 | Construction of the second sec | | | |
| VC 1d-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septe | | | | |
| >initializing, please walt | | | | |
| | Constraint key can take up to 60 cocondo, pleace voit | | | |
| | Key can take up to 60 seconds, pitease wait | | | |
| | rey generated | | | |
| | | | | |
| | | | | |
| | Shell Trace | | | |

The key manager will prompt for a file name to store the public key and certificate chain.

| Enter file name for public key export | |
|--|--------|
| /home/asc/tmp/howto/smartcardhsm-workspace/UTDEV0915300000.pka | Browse |
| OK Cancel | |

Please note, that the proposed file name matches the device id of the SmartCard-HSM on which the key resides.

The procedure must be repeated for each key custodian. The procedure can be done remotely, as the resulting public key file includes all information necessary for the next steps.

4 Configuration for n-of-m Authentication

The SmartCard-HSM to be used as key store with n-of-m authentication must be initialized with a right-click on the SmartCard-HSM node and selecting "Initialize Device". This is identical with the above procedure for the key custodian device.

At the prompt "Select authentication mechanism" select "Public Key Authentication".

| Select authentication mechanism | | | |
|---------------------------------|--------|--|--|
| Public Key Authentication | | | |
| ОК | Cancel | | |

The next dialog allows you to select the total number of public keys that shall be registered for public key authentication. This is the m parameter in n-of-m.

| Enter total number of public keys | | | |
|-----------------------------------|----|--------|--|
| 2 | | | |
| | ок | Cancel | |
| | | | |

This is followed by a dialog that allows to set the threshold of required public key authentication before access is granted (Parameter n in n-of-m). The value must be between 1 and the total number of public keys.

| Enter number of public keys required for authentication | n |
|---|---|
| 1 | |
| OK Cancel | |

The device is now initialized and ready to register public keys.

File Edit Options Help

| SmartCard-HSM (UTDEV0915300000) 2 missing key(s) in 1 of 2 public key authentication SO PIN not verified, 15 tries remaining (63CF) Image: Solution of the second | -hsm-sdk-scripts/keymanager/keymanager.js"); C100001 CHR=UTDISCTST100001 CED=August 7, 2015 TDISCTST100001 CHR=UTDEV0915300000 CED=Septemb |
|--|--|

As the authentication status indicates, two public keys are missing to complete the registration. Right-click on the authentication state and select "Register Public Key".

| File Edit Options Help | | | |
|---------------------------------|---|---|-----------------------------|
| SmartCard-HSM (UTDEV0915300000) | Register Public Key Authenticate with Public Key Logout | ovto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager. - CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED= ait | js"); 7, 2015 Septemb |
| | Shell Trace | | |

Select the public key previously exported from the key custodians SmartCard-HSM.

| Enter file name for public key import | |
|---|--------|
| howto/smartcardhsm-workspace/UTCC020001400000.pka | Browse |
| OK Cancel | |

The key manager validates the certificate and signatures applied to the public key and display the identification information extracted from the certificate.

| Add the key | issued to UTCC020001400000 on device UTCC02 | 20001400000 ? |
|-------------|---|-----------------|
| Add the Reg | | -vvvvt ivvvvv i |

The authentication status is updated to reflect that one more public key must be registered.

| File Edit Options Help | |
|---------------------------------|--|
| SmartCard-HSM (UTDEV0915300000) | <pre>>load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); Issuer Certificate : CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August 7, 2015 Device Certificate : CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septemb >Initializing, please wait Initializing complete</pre> |
| | |
| | Shell Trace |

After import of the missing public keys the authentication state indicates that the setup is complete. With the completion of the setup, the authentication state is assumed as authenticated until logout or the next reset. This ensures, that initial keys can be generated as part of the key management procedure without explicit authentication of the public key.

| File Edit Options Help | |
|---|--|
| SmartCard-HSM (UTDEV0915300000) 1 authenticated public key(s) in 1 of 2 scheme SO PIN not verified, 15 tries remaining (63CF) | <pre>>load("/home/asc/tmp/howto/smartcardhsm-workspace/sc-hsm-sdk-scripts/keymanager/keymanager.js"); Issuer Certificate : CVC id-SC-HSM DV CAR=UTSRCACC100001 CHR=UTDISCTST100001 CED=August 7, 2015 Device Certificate : CVC id-SC-HSM Terminal CAR=UTDISCTST100001 CHR=UTDEV0915300000 CED=Septemb >Initializing, please wait Initializing complete</pre> |
| | |
| | Shell Trace |

Select "Logout" from the context menu to lock the device.

File Edit Options Help

| SmartCard-HSM (UTDEV0915300000) D 1 authenticated public key(s) in 1 of 2 scher S0 PIN not verified, 15 tries remaining (63CF | Register Public Key Authenticate with Public Key | howto/smartcardhsm-workspace/sc-hsm-sdk-s OVC id-SC-HSM DV CAR=UTSRCACC100001 CH CVC id-SC-HSM Terminal CAR=UTDISCTST10 ait | cripts/keymanager/keymanager.js"); R=UTDISCTST100001 CED=August 7, 2015 Ю001 CHR=UTDEV0915300000 CED=Septemb |
|---|---|--|--|
| | Logout | | |
| | Shell Trace | M | ► |

Now the device is protected with public key authentication and one of the registered keys must be used to authenticate.

5 Performing Public Key Authentication

To perform a Public Key Authentication you need to insert both SmartCard-HSMs, the target device and the device that contains the authentication private key.

Right-click on the authentication status and select "Authenticate with Public Key".

| File Edit Options Help | | | | |
|--------------------------------|---|---|--|--|
| SmartCard-HSM (UTDEV0915300000 |) >load ("/ht Register Public Key Authenticate with Public Ke Logout | me/asc/tmp/howto/smartcardhsm- icate : CVC id-SC-HSM DV icate : CVC id-SC-HSM Te , please wait complete | workspace/sc-hsm-sdk-scripts/keyma 'CAR=UTSRCACC100001 CHR=UTDISCTST1 rminal CAR=UTDISCTST100001 CHR=UTD | nager/keymanager.js"); 00001 CED=August 7, 2015 EV0915300000 CED=Septemb |
| | ▲ | Trace | | |

The key manager prompts for the card reader name for the device with the authentication key.

| Please select card reader with public key | | | |
|--|--|--|--|
| SCM SCR 3310 [CCID Interface] (21121230224279) 01 00 💌 | | | |
| OK Cancel | | | |

The key manager then prompts for the key label of the authentication key (In the example, a different key than the one created earlier in this how-to is used).

| Please select a key for public key authentication | | | |
|---|---|--|--|
| testl | - | | |
| OK Cancel | | | |

Enter the PIN of the device with the authentication private key.

| Enter PIN | | | |
|-----------|----|--------|--|
| 648219 | | | |
| | ОК | Cancel | |

If authentication was successful, then the authentication state reflects that one public key is authenticated. As the threshold is 1, you can now perform operations that require user authentication.



If more than one key is required for authentication, then the procedure must be repeated for other keys.