CardContact
smart system architects

SmartCard-HSM
n-of-m Authentication HowTo

Author	Andreas Schwier
Version	0.1
Date	2015-09-07

Table of Contents

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

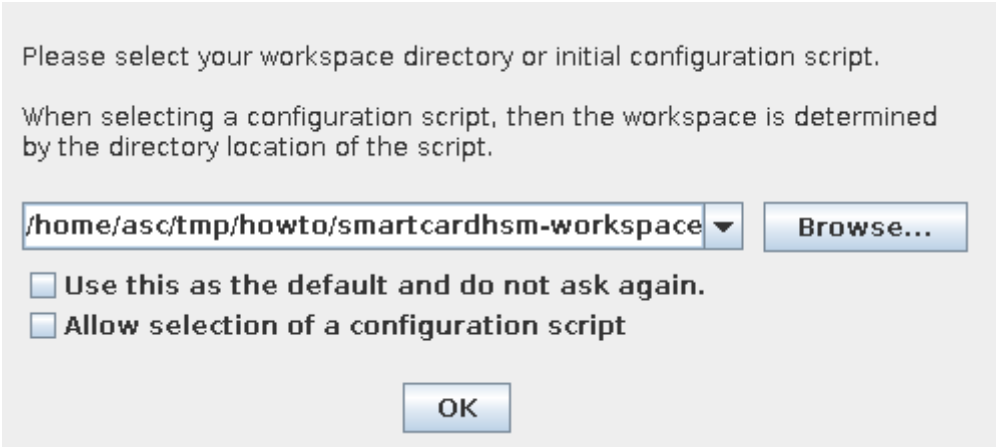
Create a directory on your disk to serve as a workspace (e.g. smartcardhsm-workspace).

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

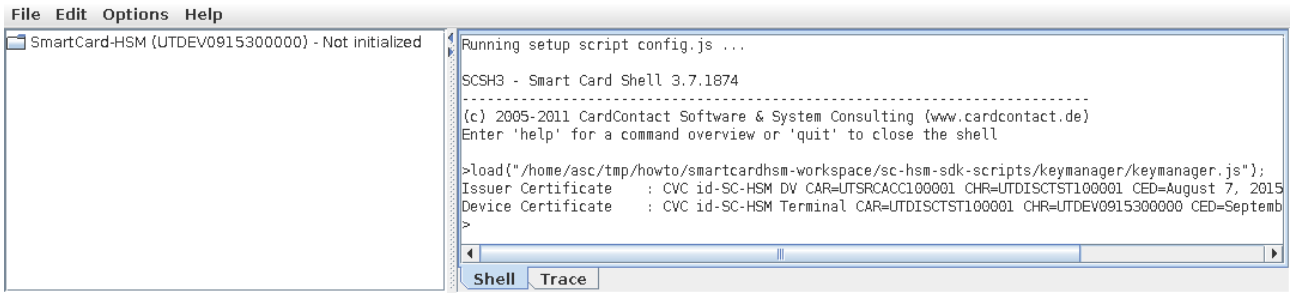
```
$ mkdir smartcardhsm-workspace
$ cd smartcardhsm-workspace
$ ssh-add -s /usr/local/lib/opensc-pkcs11.so
$ git clone ssh://git@devnet.cardcontact.de:222/scsh-mods scsh
$ git clone ssh://git@devnet.cardcontact.de:222/sc-hsm-sdk-scripts
```

2.3 Starting the Smart Card Shell

Start the Smart Card Shell and select the workspace directory.



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

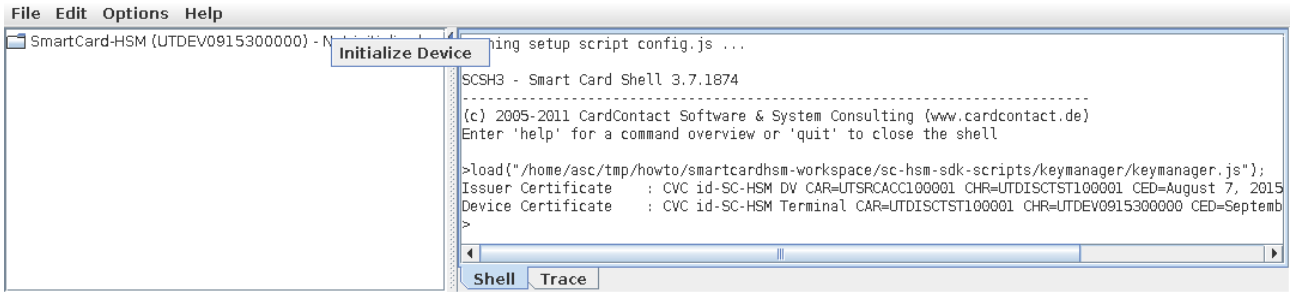


The shell shows some status information of the device, in particular the device id.

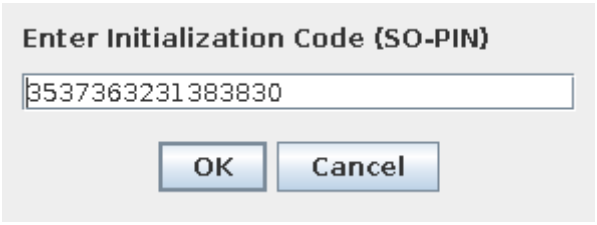
3 Creation of Authentication Keys

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

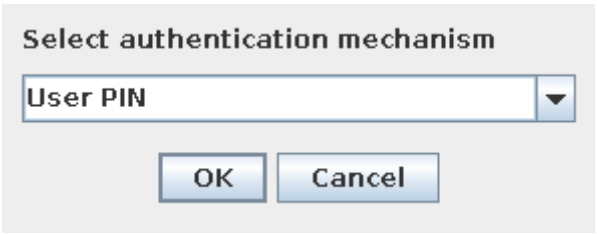
Right-click on the SmartCard-HSM node to see the context menu and select "Initialize Device".



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.

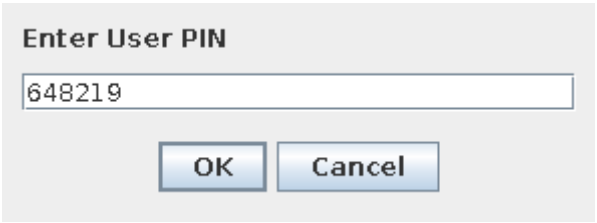


On the next prompt select "User PIN" as authentication mechanism.

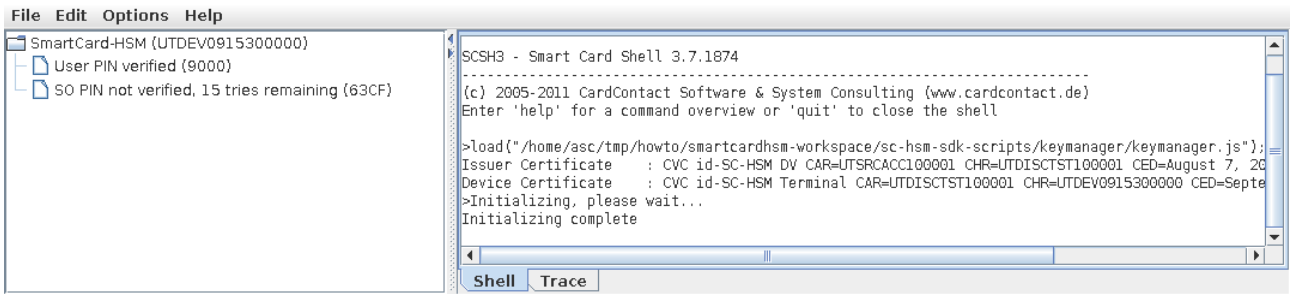


On the next prompt select "Resetting PIN with SO-PIN not allowed".

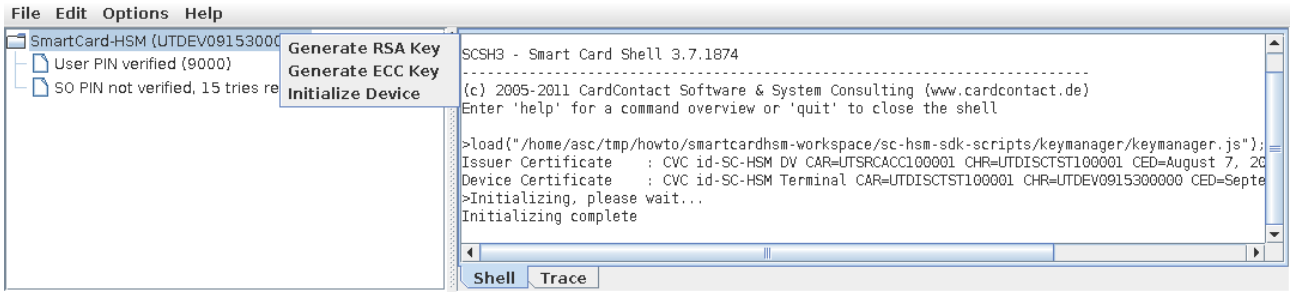
The key manager will prompt for the User PIN value. Please have the key custodian enter a self-selected PIN. The dialog is pre-set with the default User PIN used throughout the tutorials.



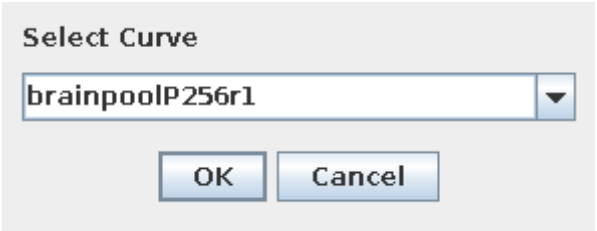
The SmartCard-HSM is now initialized. The procedure can be repeated as often as desired.



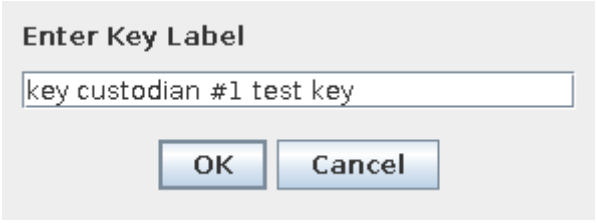
Next you will need to generate an ECDSA key. Right-click on the SmartCard-HSM node and select "Generate ECC Key".



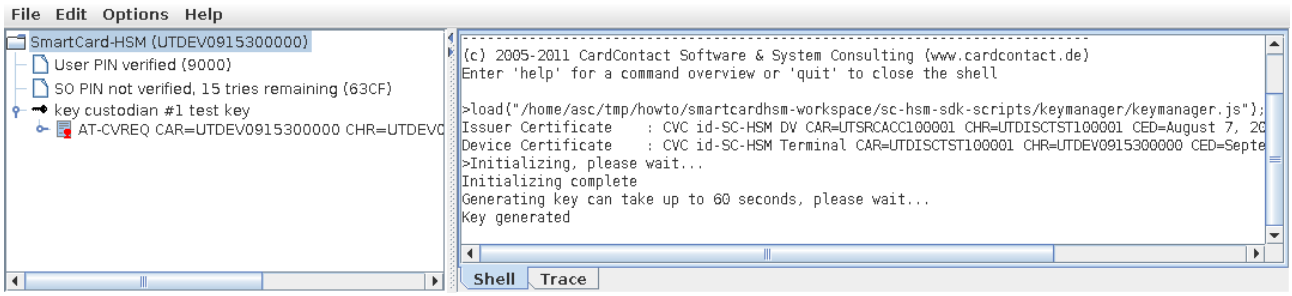
Select "brainpoolP256r1" as curve.



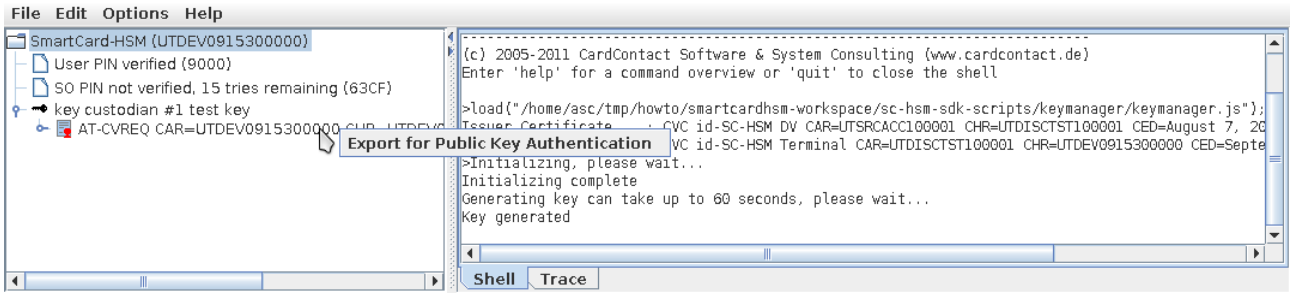
Enter a label for the key in the next dialog.



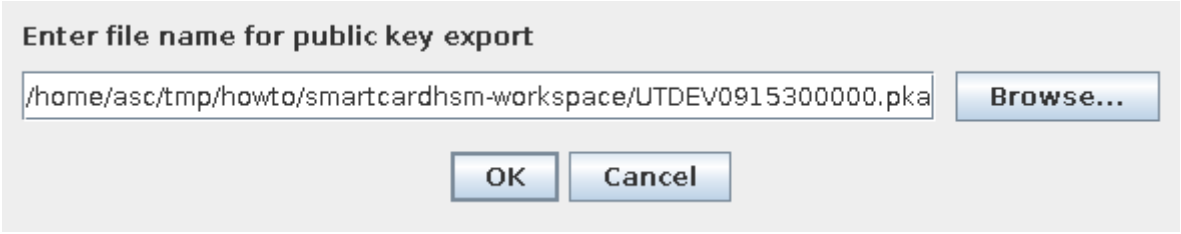
The key is now generated and the public key certification signing request prepared.



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



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



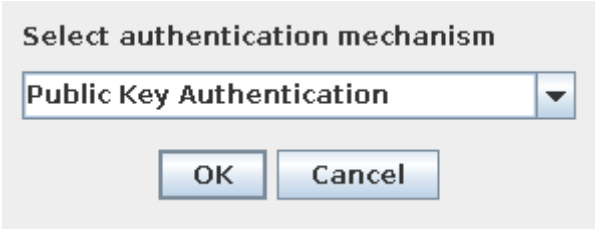
Please note, that the proposed file name matches the device id of the SmartCard-HSM on which the key resides.

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.

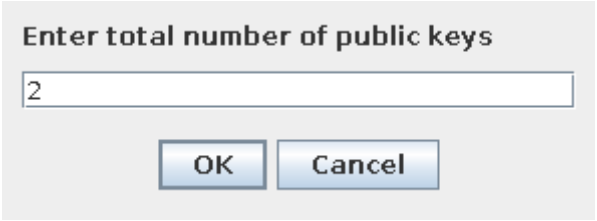
4 Configuration for n-of-m Authentication

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".

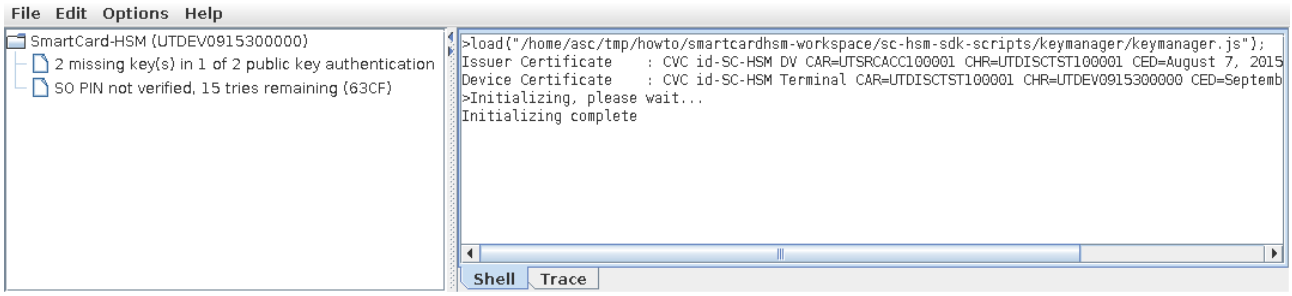


The next dialog allows you to select the total number of public keys that shall be registered for public key authentication. This is the m parameter in n-of-m.

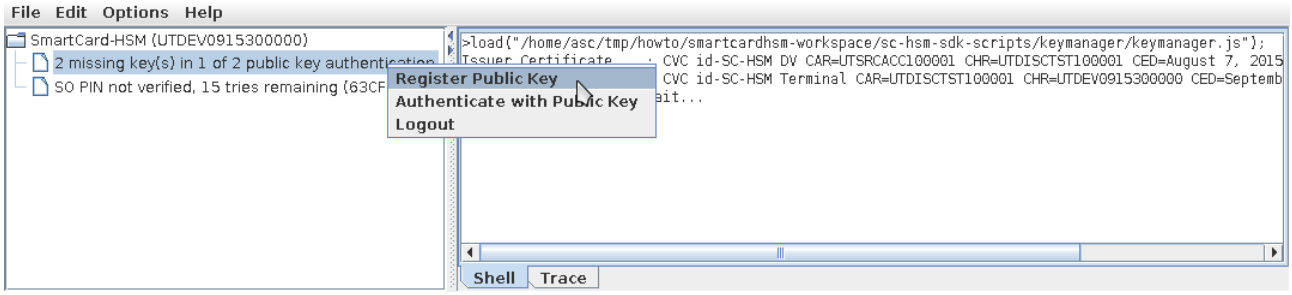


This is followed by a dialog that allows to set the threshold of required public key authentication before access is granted (Parameter n in n-of-m). The value must be between 1 and the total number of public keys.

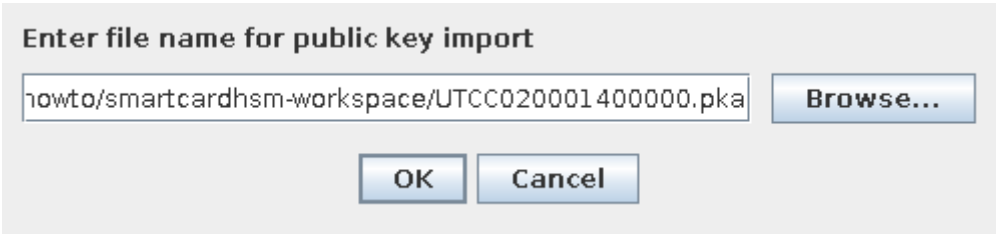
The device is now initialized and ready to register public keys.



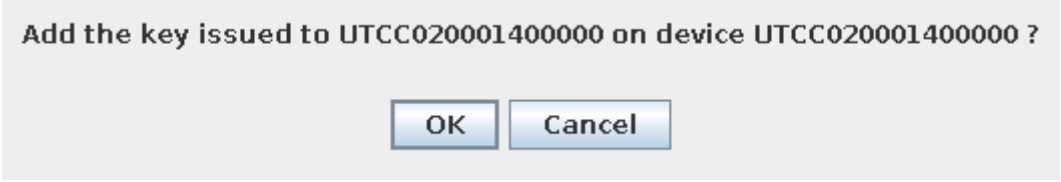
As the authentication status indicates, two public keys are missing to complete the registration. Right-click on the authentication state and select "Register Public Key".



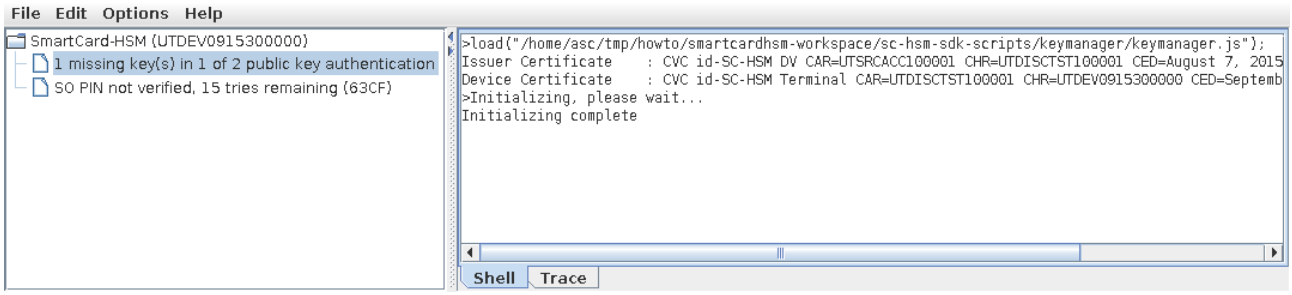
Select the public key previously exported from the key custodians SmartCard-HSM.



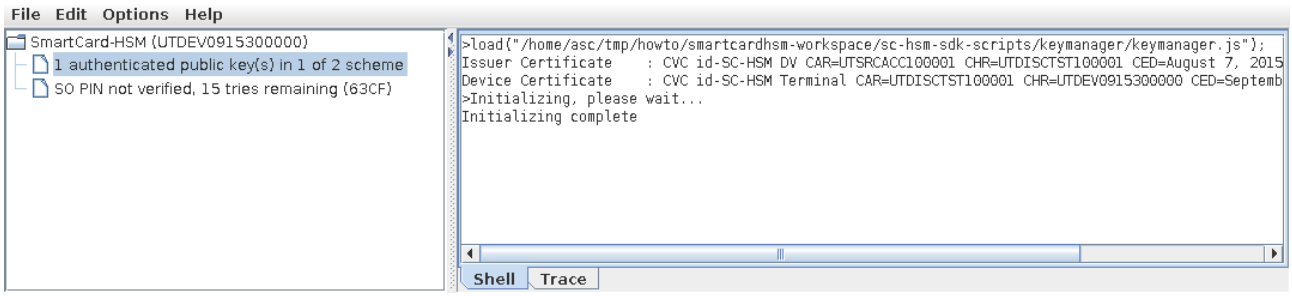
The key manager validates the certificate and signatures applied to the public key and display the identification information extracted from the certificate.



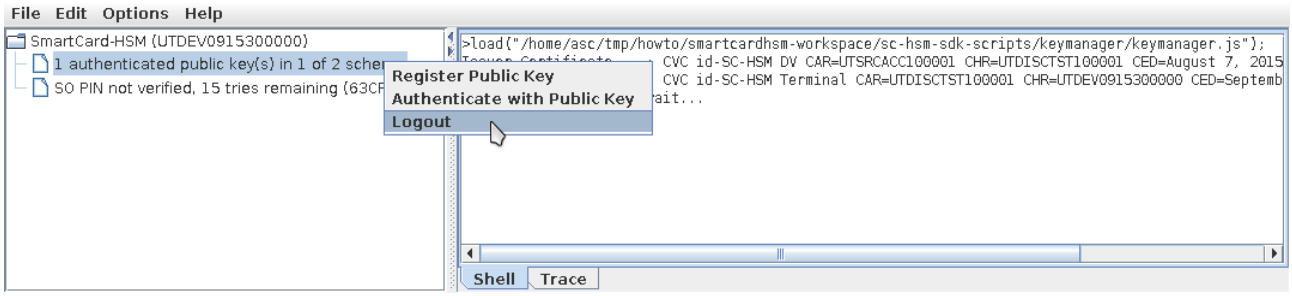
The authentication status is updated to reflect that one more public key must be registered.



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.



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

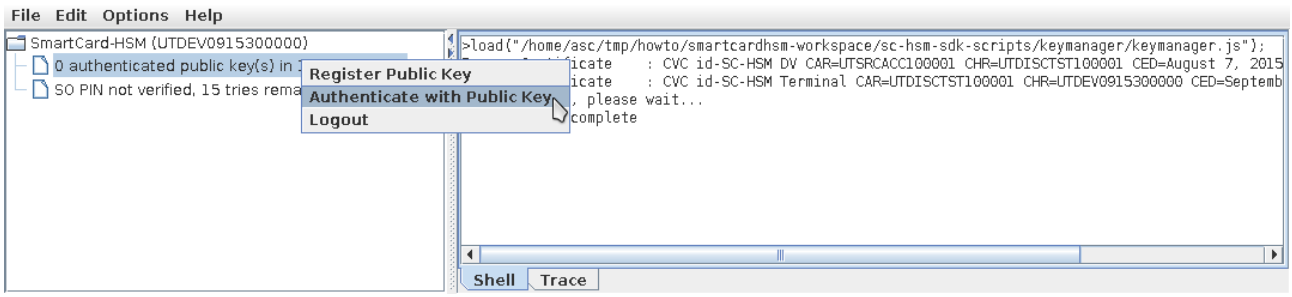


Now the device is protected with public key authentication and one of the registered keys must be used to authenticate.

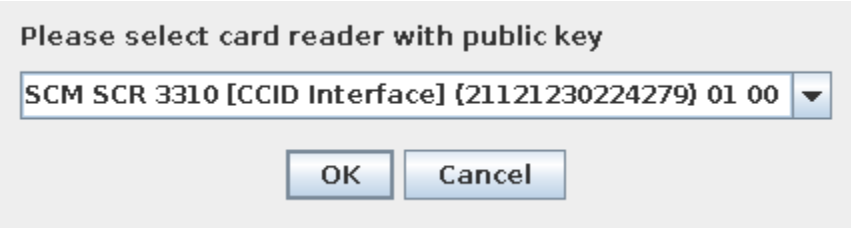
5 Performing Public Key Authentication

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.

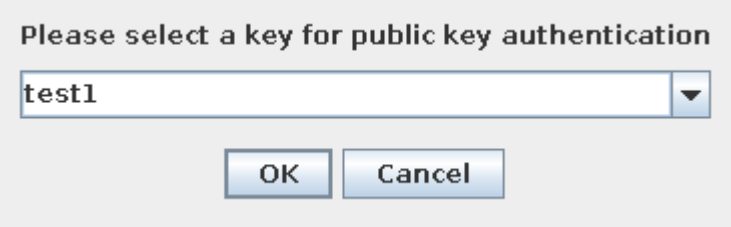
Right-click on the authentication status and select "Authenticate with Public Key".



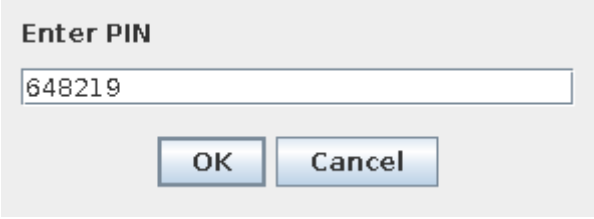
The key manager prompts for the card reader name for the device with the authentication key.



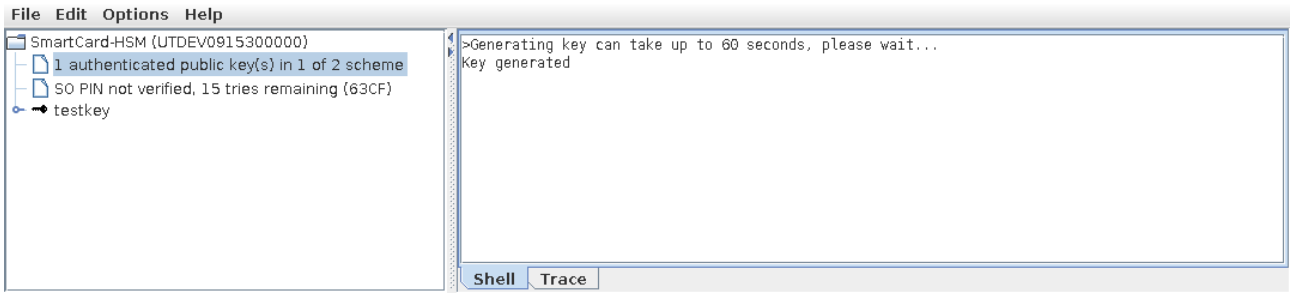
The key manager then prompts for the key label of the authentication key (In the example, a different key than the one created earlier in this how-to is used).



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



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.