mike@csis.dk

Contents

Introduction

This manual describes the CSIS Enrollment Station located at https://github.com/CSIS/EnrollmentStation. The Enrollment Station was created to facilitate enrollment of Yubico Smartcards (specifically using the Yubikey NEO Premium with CCID functionality) using a Windows AD CS (Active Directory Certificate Services) CA.

The current version of the Enrollment Station is coded in C#.Net Winforms and is a GUI application.

Requirements

There are a number of requirements for this system to work.

- The computer running the ES must be domain-joined.
- The Windows CA must also be domain-joined, and online.
- The user running the ES must have an Enrollment Agent certificate in their personal certificate store.
- The user running the ES must have permissions to manage certificates on the CA server.

Local files

The program creates and maintains a series of local files, listed below:

- settings.json
  This file contains all persistent settings in the application.

- store.json
  This file contains all enrolled certificates and their associated secret data, such as PUK keys.

- store.json.bak
  To combat corrupt stores, a backup is always created before saving.

Operations

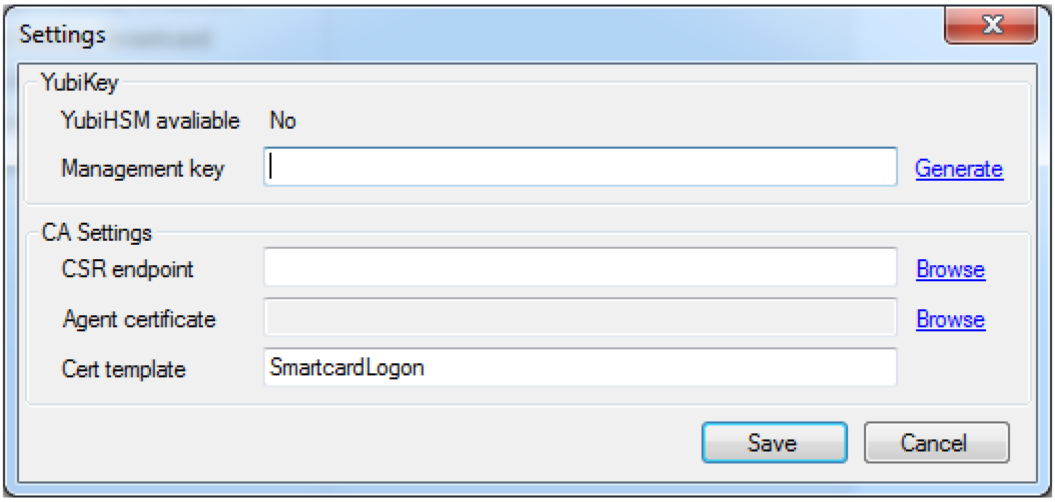
The following operations will achieve various purposes, but are not everyday tasks. The Procedures section will describe everyday tasks.

First run

When the program is first run, with no Smart Card inserted, it will show something similar to the below screenshot. This is the settings dialog, which can always be found in the top menu of the program. This dialog should be filled with the information relevant to your setup, so that program will function better.

The individual fields have helpful links which will help you fill out the details correctly.

Note that if a YubiHSM is present, it can be used to create a new Management Key.



Settings

YubiKey

YubiHSM avaliable No

Management key

CA Settings

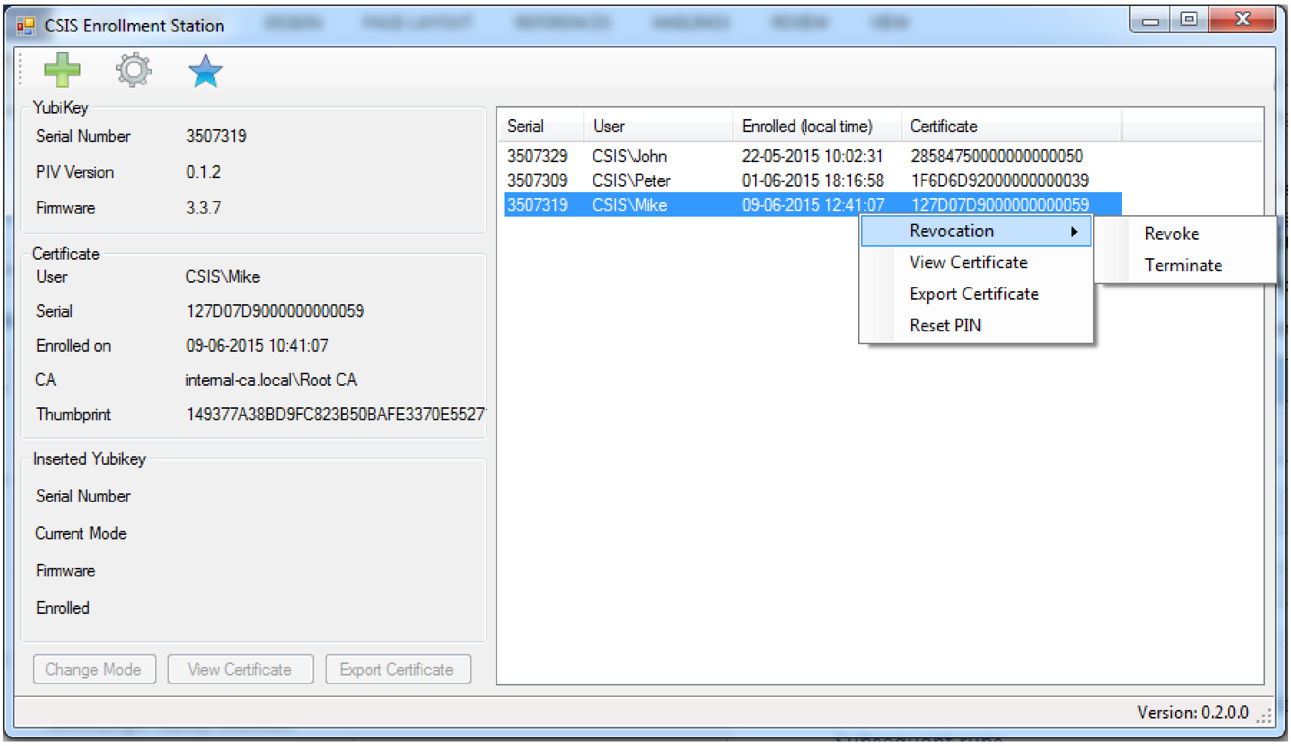
CSR endpoint

Agent certificate

Cert template SmartcardLogon

Subsequent runs

Once configured, the programs main window will be displayed, instead of the settings dialog. The window contains all previously enrolled keys, and allows you to enroll new keys easily. Right clicking a previously enrolled key allows you to manage this enrollment.



YubiKey

Serial Number	3507319
PIV Version	0.1.2
Firmware	3.3.7

Certificate

User	CSIS\Mike
Serial	127D07D9000000000059
Enrolled on	09-06-2015 10:41:07
CA	internal-ca.local\Root CA
Thumbprint	149377A38BD9FC823B50BAFE3370E5527

Inserted Yubikey

Serial Number	
Current Mode	
Firmware	
Enrolled	

Serial	User	Enrolled (local time)	Certificate
3507329	CSIS\John	22-05-2015 10:02:31	2858475000000000050
3507309	CSIS\Peter	01-06-2015 18:16:58	1F6D6D92000000000039
3507319	CSIS\Mike	09-06-2015 12:41:07	127D07D9000000000059

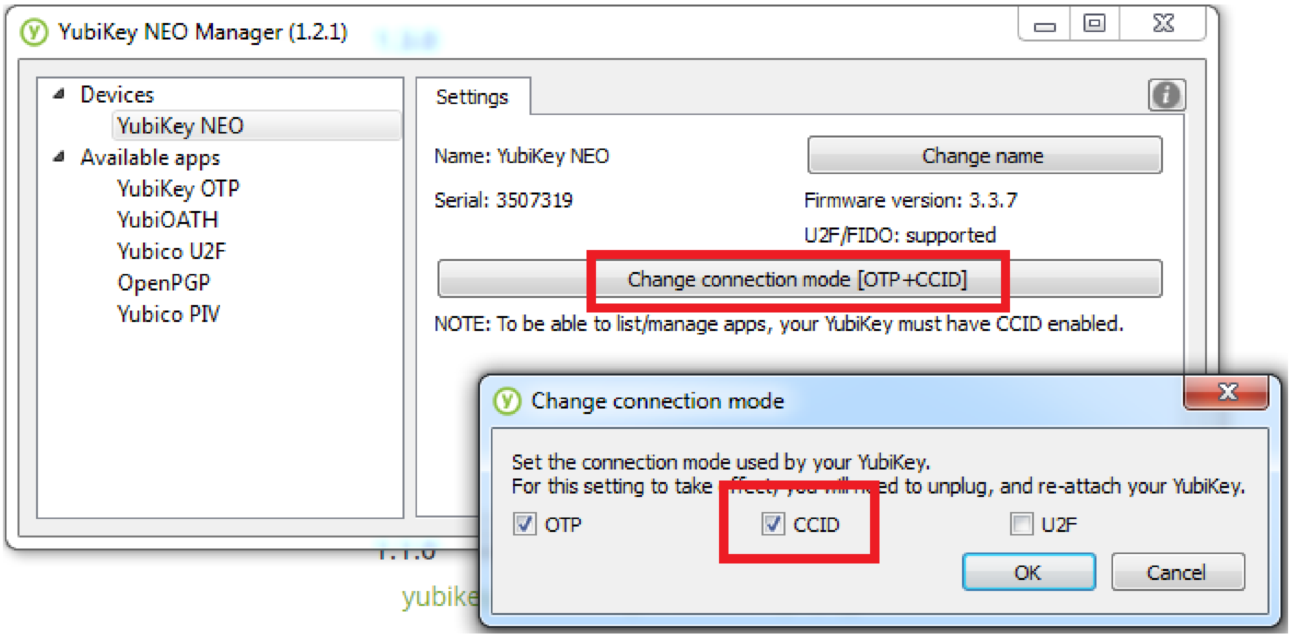
Preparing a Smartcard for enrollment

In our experience, Yubikey NEO Premiums are not set up to enable the CCID applet. This step has to be taken first, to allow the rest of the program to operate correctly. This is a one-time step for any new Yubikey.

It has not been possible to create this feature in code (yet), so for now a separate tool from Yubico is needed. There are two tools available to perform this task.

NEO Manager

This GUI will allow you to control various aspects of the NEO device. When the GUI is open and the Yubikey has been detected, click the “Change connection mode” and check the “CCID” option. Finally click “Ok” and unplug and plug the device again. It will now be ready for use with the ES.



Name: YubiKey NEO

Serial: 3507319

Firmware version: 3.3.7

U2F/FIDO: supported

NOTE: To be able to list/manage apps, your YubiKey must have CCID enabled.

Set the connection mode used by your YubiKey.
For this setting to take effect, you will need to unplug, and re-attach your YubiKey.

☑ OTP ☑ CCID □ U2F

Home page: https://developers.yubico.com/yubikey-neo-manager/

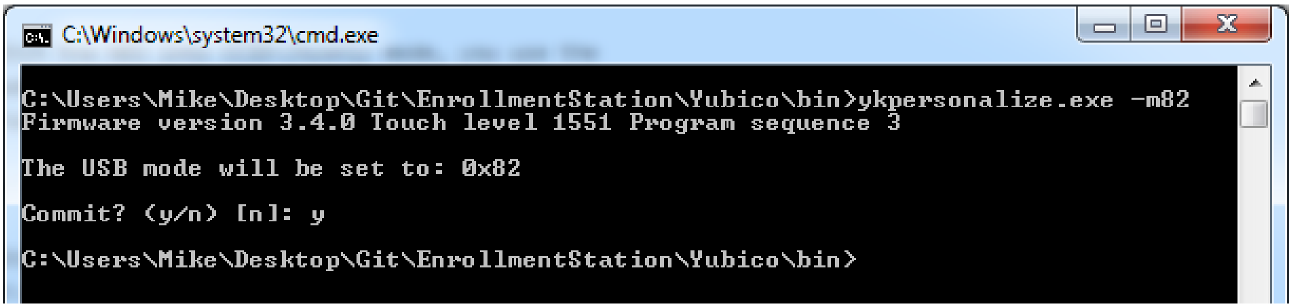
Download page: https://developers.yubico.com/yubikey-neo-manager/Releases/

Yubikey Personalize

This command line utility will set the mode for you using a simple argument. When downloaded, open a new command prompt and navigate to the directory. Run the following command:

```
ykpersonalize.exe –m82
```

The "-m" parameter sets the mode of the device, where 82 is an option found in the documentation. 82 enabled OTP and CCID and allows for button presses to eject/insert the Smartcard. After running the command, unplug and plug the Yubikey to enable the new mode.



```
C:\Users\Mike\Desktop\Git\EnrollmentStation\Yubico\bin>ykpersonalize.exe -m82
Firmware version 3.4.0 Touch level 1551 Program sequence 3

The USB mode will be set to: 0x82

Commit? (y/n) [n]: y

C:\Users\Mike\Desktop\Git\EnrollmentStation\Yubico\bin>
```

Home page: https://developers.yubico.com/yubikey-personalization/

Download page: https://developers.yubico.com/yubikey-personalization/Releases/

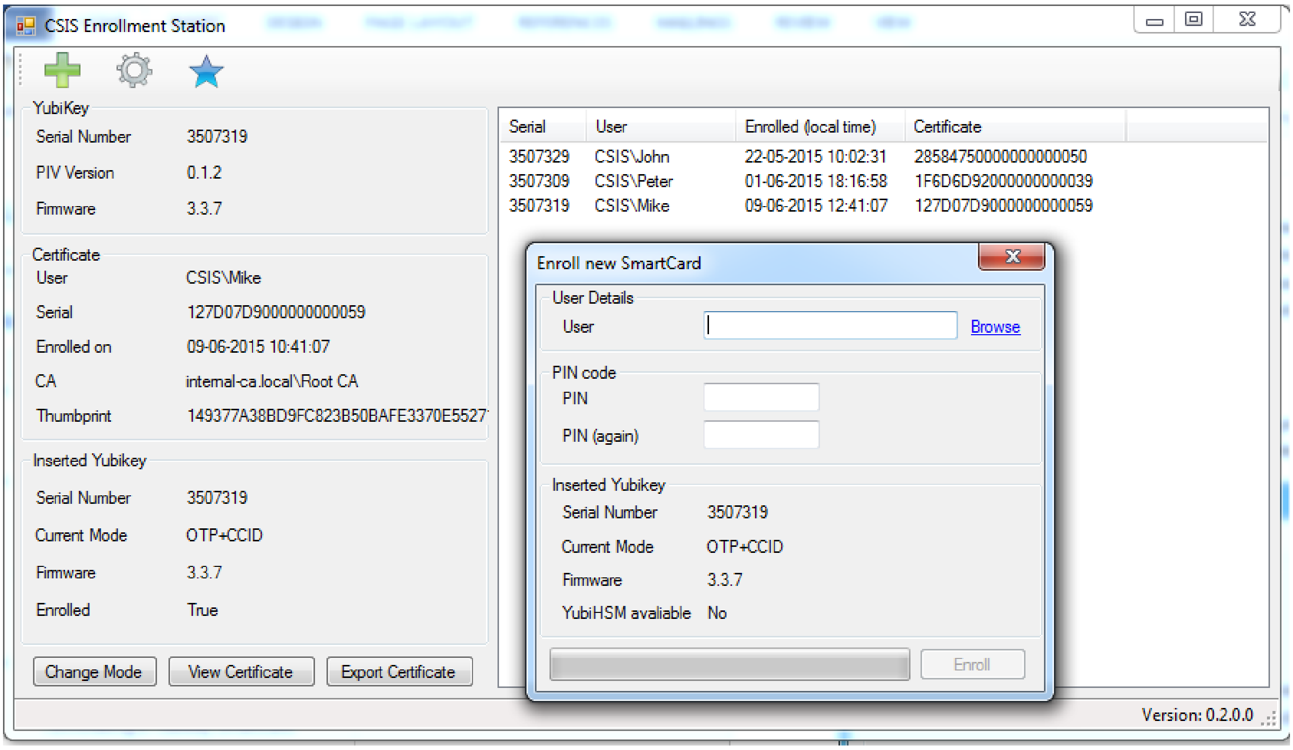
Documentation: https://yubico.github.io/yubikey-personalization/ykpersonalize.1.html

Procedures

Following is a series of different use cases, accompanied by screenshots.

Enrolling a Yubikey Smartcard

Enrolling a new Smartcard will present a new window requiring you to enter information. By using the information store in the Settings, the only information needed at this point is the username to enroll for, as well as a PIN code. The normal use case for this procedure is that the user is physically standing at the enrollment station, and will enter a PIN code that only they know. PIN codes can be 1 to 8 characters in length.



YubiKey

Serial Number	3507319
PIV Version	0.1.2
Firmware	3.3.7

Certificate

User	CSIS\Mike
Serial	127D07D9000000000059
Enrolled on	09-06-2015 10:41:07
CA	internal-ca.local\Root CA
Thumbprint	149377A38BD9FC823B50BAFE3370E5527

Inserted Yubikey

Serial Number	3507319
Current Mode	OTP+CCID
Firmware	3.3.7
Enrolled	True

Serial	User	Enrolled (local time)	Certificate
3507329	CSIS\John	22-05-2015 10:02:31	28584750000000000050
3507309	CSIS\Peter	01-06-2015 18:16:58	1F6D6D92000000000039
3507319	CSIS\Mike	09-06-2015 12:41:07	127D07D9000000000059

Inserted Yubikey

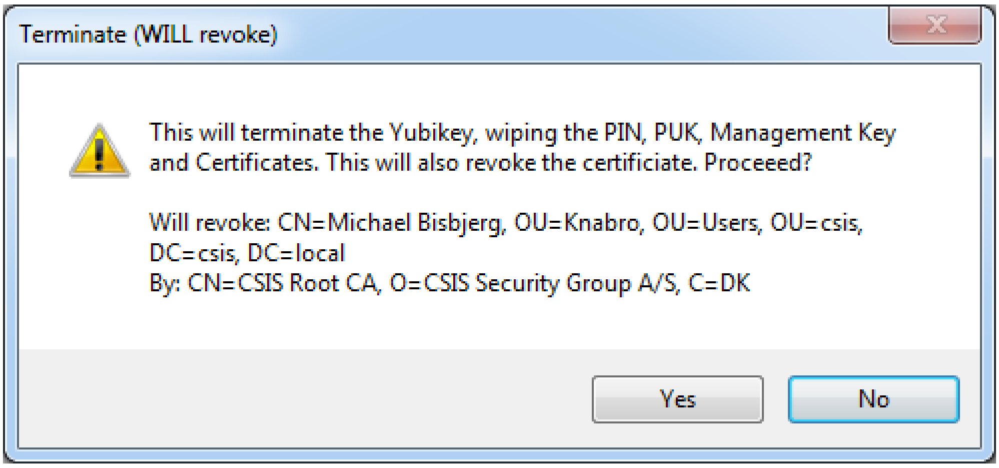
Serial Number	3507319
Current Mode	OTP+CCID
Firmware	3.3.7
YubiHSM avaliable	No

The enrollment process can take a little while, so a progress bar will indicate the progress. Once successful, the dialogue will close and the newly enrolled Yubikey is listed in the overview.

Terminating a Yubikey Smartcard

This is the process, in which a Smartcard is revoked and reset. This is the normal method of wiping a Smartcard as it will simultaneously revoke the active certificate and reset the Smartcard (making it possible to use the card again).

Selecting the Terminate context menu will start this process (asking you to insert the relevant Yubikey if necessary), at which point you'll be presented with a dialog asking you to confirm the operation.



Terminate (WILL revoke)

This will terminate the Yubikey, wiping the PIN, PUK, Management Key and Certificates. This will also revoke the certificiate. Proceeed?

Will revoke: CN=Michael Bisbjerg, OU=Knabro, OU=Users, OU=csis, DC=csis, DC=local
By: CN=CSIS Root CA, O=CSIS Security Group A/S, C=DK

Terminating the Yubikey will take a short while, but in the end the Yubikey is removed from the store and it is ready to be enrolled again.

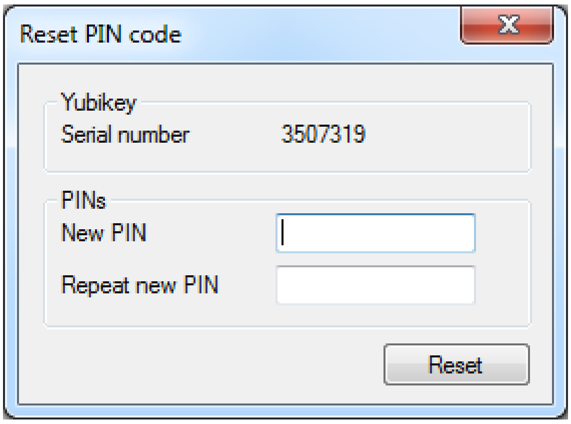
Revoking a lost Smartcard

When a user loses a Smartcard, it should be revoked as soon as possible. When a key is to be revoked, find it in the list of users, and select the Revoke option from the context menu. When revoking, a confirmation dialogue will be shown presenting all the information known to the application. It is not possible to un-revoke Smartcards later on, as they are revoked with "Cease of Operations".

Other procedures

Changing or resetting a PIN code

When a user has forgotten their PIN code or wishes to change it, it is possible directly in the application to do so. From the context menu for the user, select “Reset PIN” and enter the new details. If necessary, you’ll be prompted to insert the relevant Yubikey.



Reset PIN code

Yubikey
Serial number 3507319

PINs
New PIN
Repeat new PIN