

CSIS Enrollment Station

For Yubikey smart card management in Windows Active Directory environment.

Created by Ian Qvist and Michael Bisbjerg

Modified by Jürgen Fechter

Table of Contents

Introduction	2
Note	2
Requirements	2
Preparing a Yubikey for enrollment	4
Using Yubikey Manager (recommended)	4
Using NEO Manager (obsolete)	6
Using Yubikey Personalize	7
Using the Enrollment Station application.....	8
Main interface	9
Enrolling a Yubikey Smartcard	11
Terminating a Yubikey Smartcard	12
Resetting a PIN code.....	13
Troubleshooting	14
COM Class not registered	14
MSVCP140.dll not found	14
Could not access the key of the agent certificate	15

Introduction

This manual describes the CSIS Enrollment Station (ES). It was original located at <https://github.com/CSIS/EnrollmentStation> and is archived. The Enrollment Station was created to facilitate enrollment of Yubico Smartcards, using the Yubikey NEO, Yubikey 4, Yubikey 5 with CCID functionality in a Windows Active Directory environment with an associated Windows Certificate Authority. The keys are using the standard PIV format for the certificates.

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

Note

The CSIS Enrollment Station is not working with container based the Yubico Windows smartcard minidriver!

Requirements

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

- A Microsoft Windows Active Directory domain
- A computer running the ES software joined to the domain.
- A Windows Certificate Authority (CA) published in the domain.
- 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.
- We used .NET Framework 4.6.1 which will run on Windows 10/Windows Server 2016, too.

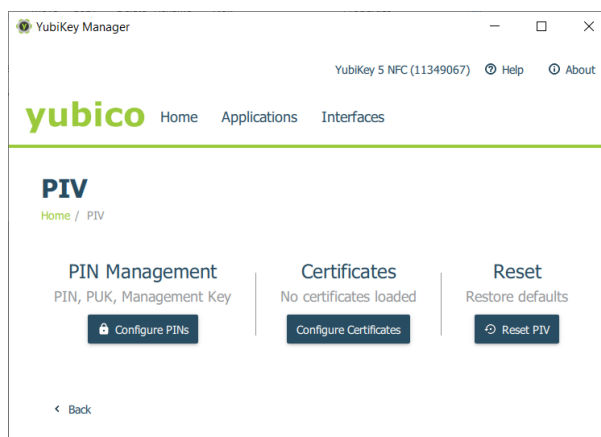
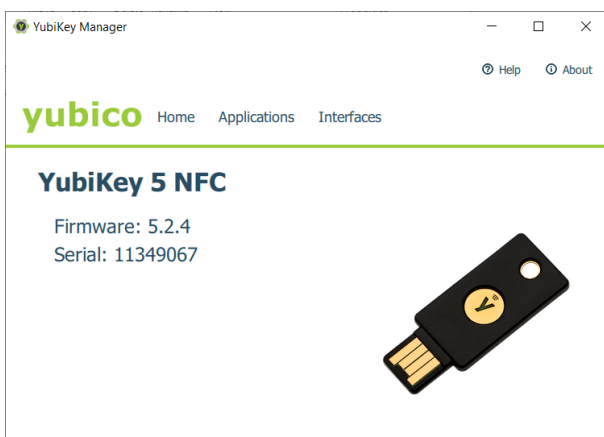
- We embedded the following libraries/programs into the application.
 - yubikey-manager-qt-1.1.3-win32
 - yubico-piv-tool-1.7.0-win32
 - Because ykpiv_get_serial() was added to API.

Preparing a Yubikey for enrollment

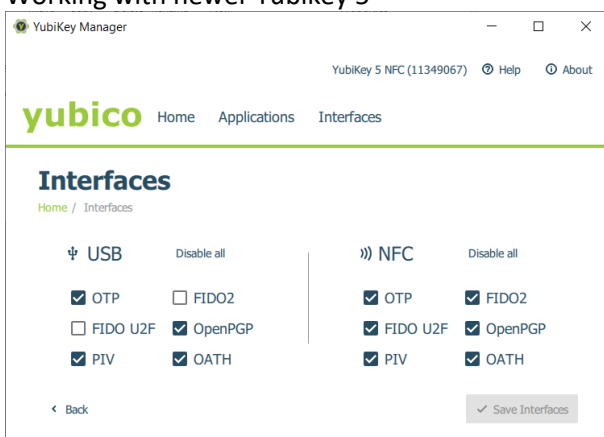
Directly from the factory, Yubikey keys are not set up to with the CCID mode, which activates the smartcard applet. You have several applications available directly from Yubico to activate the CCID mode, which both are described below.

Using Yubikey Manager (recommended)

There are two version of this application: One with GUI and other other with commandline (CLI).

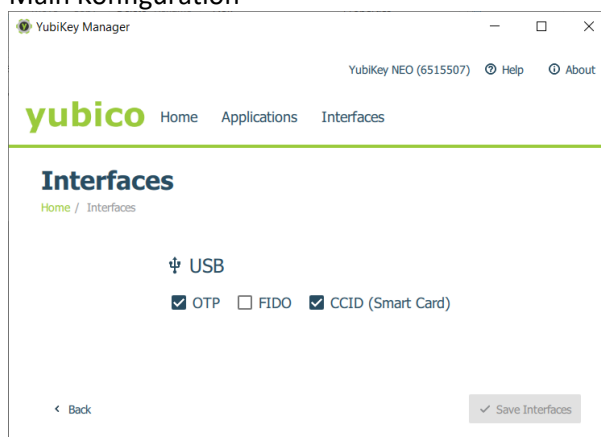


Working with newer Yubikey 5



CCID is not shown but instead PIV

Main Konfiguration



Support of CCID with older smartcards

Commandline

The name of the tool is ykman.

```
Parameter info
C:\Program Files (x86)\Yubico\YubiKey Manager>ykman info
Device type: YubiKey 5 NFC
Serial number: 11349067
Firmware version: 5.2.4
Form factor: Keychain (USB-A)
Enabled USB interfaces: OTP+CCID
NFC interface is enabled.

Applications      USB      NFC
OTP               Enabled  Enabled
FIDO U2F          Disabled Enabled
OpenPGP           Enabled  Enabled
PIV               Enabled  Enabled
OATH              Enabled  Enabled
```

FIDO2	Disabled	Enabled
Parameter mode to get and set the mode		
<pre>C:\Program Files (x86)\Yubico\YubiKey Manager>ykman mode Current connection mode is: OTP+FIDO+CCID Supported USB interfaces are: OTP, FIDO, CCID C:\Program Files (x86)\Yubico\YubiKey Manager>ykman mode OTP+CCID -f C:\Program Files (x86)\Yubico\YubiKey Manager>ykman mode OTP+CCID Mode is already OTP+CCID, nothing to do... C:\Program Files (x86)\Yubico\YubiKey Manager>ykman mode CCID Set mode of YubiKey to CCID? [y/N]: y C:\Program Files (x86)\Yubico\YubiKey Manager>ykman mode Current connection mode is: CCID Supported USB interfaces are: OTP, FIDO, CCID</pre>		
Parameter mode list		
<pre>C:\Program Files (x86)\Yubico\YubiKey Manager>ykman list -s 11349067 C:\Program Files (x86)\Yubico\YubiKey Manager>ykman list YubiKey NEO [OTP+CCID] Serial: 6515507 YubiKey 5 NFC [OTP+CCID] Serial: 11349067</pre>		
Parameter piv to manage the smartcard CCID /PIV		
<pre>C:\Program Files (x86)\Yubico\YubiKey Manager>ykman piv -? Usage: ykman piv [OPTIONS] COMMAND [ARGS]... Try "ykman piv -h" for help. Error: no such option: -? C:\Program Files (x86)\Yubico\YubiKey Manager>ykman piv -h Usage: ykman piv [OPTIONS] COMMAND [ARGS]... Manage PIV Application. Examples: Generate an ECC P-256 private key and a self-signed certificate in slot 9a: \$ ykman piv generate-key --algorithm ECCP256 9a pubkey.pem \$ ykman piv generate-certificate --subject "yubico" 9a pubkey.pem Change the PIN from 123456 to 654321: \$ ykman piv change-pin --pin 123456 --new-pin 654321 Reset all PIV data and restore default settings: \$ ykman piv reset Options: -h, --help Show this message and exit. Commands: attest Generate a attestation certificate for a key. change-management-key Change the management key. change-pin Change the PIN code. change-puk Change the PUK code. delete-certificate Delete a certificate. export-certificate Export a X.509 certificate. generate-certificate Generate a self-signed X.509 certificate. generate-csr Generate a Certificate Signing Request (CSR). generate-key Generate an asymmetric key pair. import-certificate Import a X.509 certificate. import-key Import a private key. info Display status of PIV application. read-object Read arbitrary PIV object. reset Reset all PIV data. set-ccc Generate and set a CCC on the YubiKey. set-chuid Generate and set a CHUID on the YubiKey.</pre>		

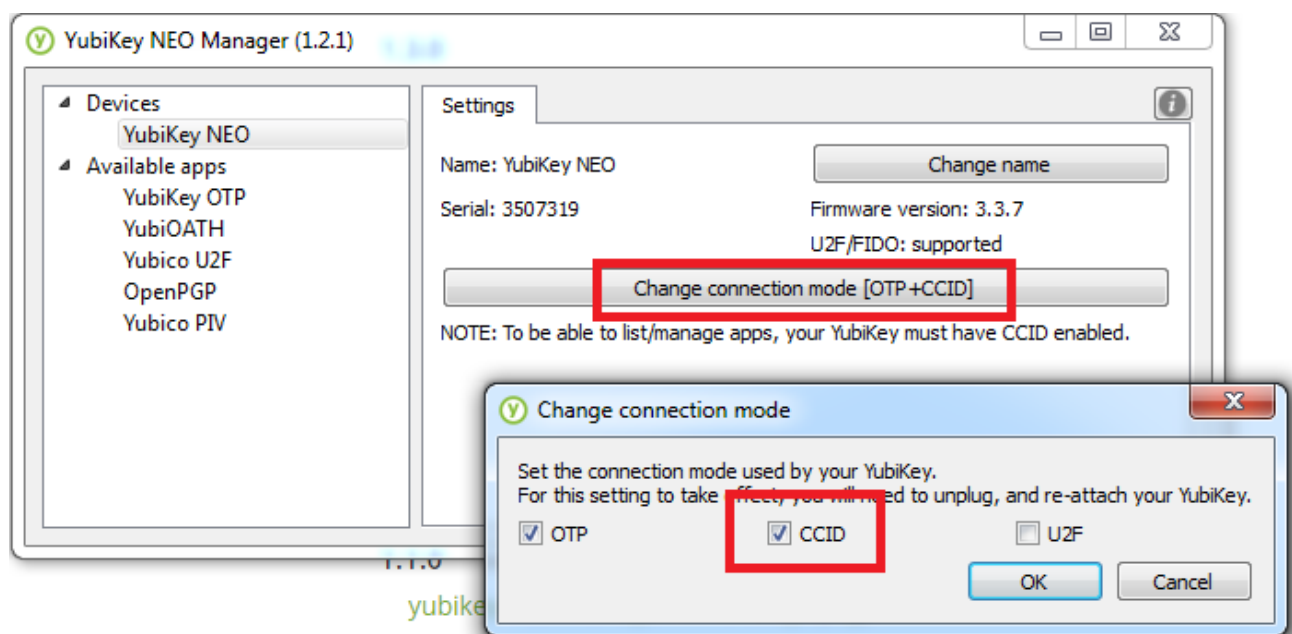
set-pin-retries	Set the number of PIN and PUK retries.
unlock-pin	Unblock the PIN.
write-object	Write an arbitrary PIV object.

Example to show the PIV contents with multiple devices using the device serial number

```
C:\Program Files (x86)\Yubico\YubiKey Manager>ykman --device=6515507 piv info
PIV version: 1.0.5
PIN tries remaining: 3
Management key is stored on the YubiKey, protected by PIN.
CHUID:
3019d4e739da739ced39ce739d836858210842108421c84210c3eb341005d0cf0e1f51069c189478e5f8cdf7de35083230
3330303130313e00fe00
CCC:
f015a000000116ff020bcdff690cca8620e18892bd33af10121f20121f300f40100f50110f600f700fa00fb00fc00fd00
fe00
Slot 9a:
  Algorithm:      RSA2048
  Subject DN:     DC=zz,DC=corpdir,OU=dev,OU=Users,CN=View User
  Issuer DN:      DC=zz,DC=corpdir,OU=dev,CN=Root-CA-dev
  Serial:         2586886443396826733924789446049828889205669958
  Fingerprint:    4a4f341ecc627f54d0e59c9d04d9156e31e29959479a9fe164b32b1403c7d2eb
  Not before:     2019-08-02 10:18:57
  Not after:      2022-08-01 10:18:57
```

Using NEO Manager (obsolete)

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 application.



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

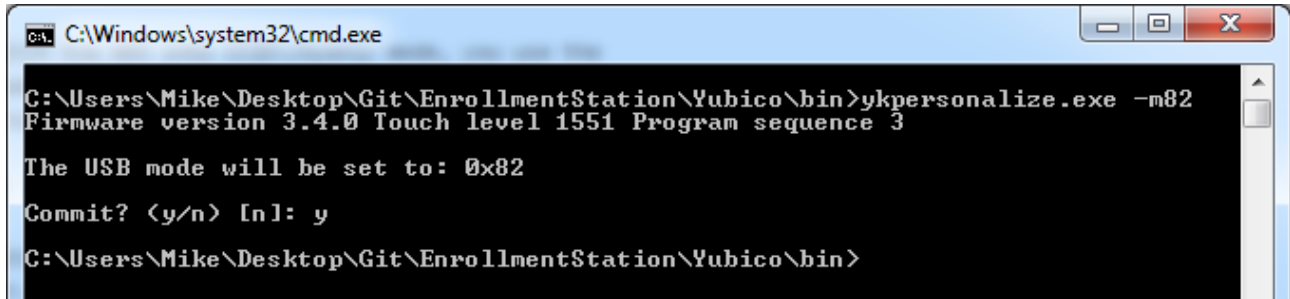
Download page: <https://developers.yubico.com/yubikey-neo-manager/Releases/>

Using 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 enable 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.

A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe'. The command prompt shows the following text: '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', and 'C:\Users\Mike\Desktop\Git\EnrollmentStation\Yubico\bin>'.

```
C:\Windows\system32\cmd.exe
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>
```

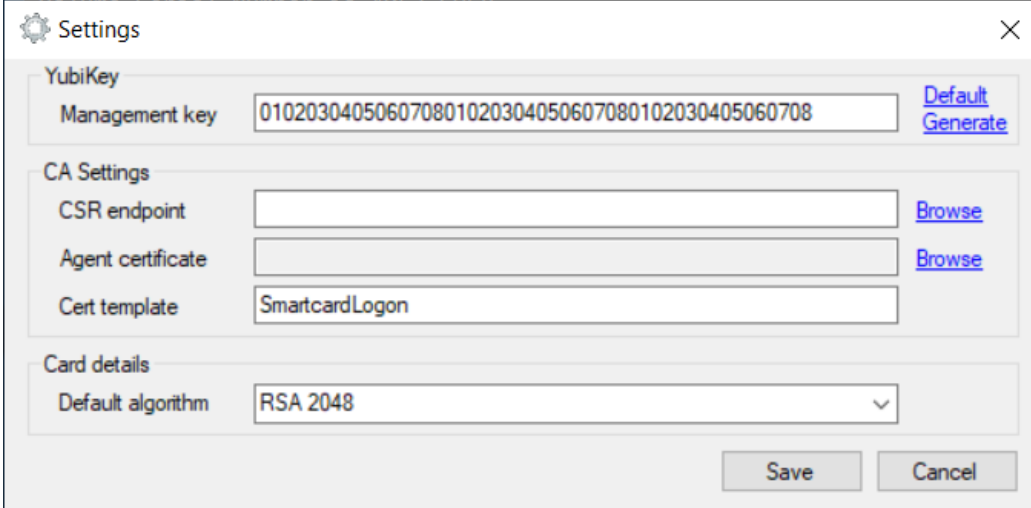
Home page: <https://developers.yubico.com/yubikey-personalization/>

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

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

Using the Enrollment Station application

On the first run of the application, you will be asked to fill out settings for the application. Here you can create a management key used to configure Yubikeys. You can click *Generate* to have the application securely generate a new key for you. If a YubiHSM is attached to the machine, the secure random number generator on the device will automatically be used for added security.



The screenshot shows a 'Settings' dialog box with a close button (X) in the top right corner. It is divided into three sections: 'YubiKey', 'CA Settings', and 'Card details'.
- The 'YubiKey' section contains a 'Management key' text field with the value '010203040506070801020304050607080102030405060708' and two buttons: 'Default' and 'Generate'.
- The 'CA Settings' section contains three fields: 'CSR endpoint', 'Agent certificate', and 'Cert template'. The 'CSR endpoint' and 'Agent certificate' fields have 'Browse' buttons to their right. The 'Cert template' field has the value 'SmartcardLogon'.
- The 'Card details' section contains a 'Default algorithm' dropdown menu with 'RSA 2048' selected.
At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

Set the Certificate Signing Request (CSR) endpoint to the Active Directory published Certificate Authority server. You can also click the *Browse* button to pick among a list of published CA in your domain.

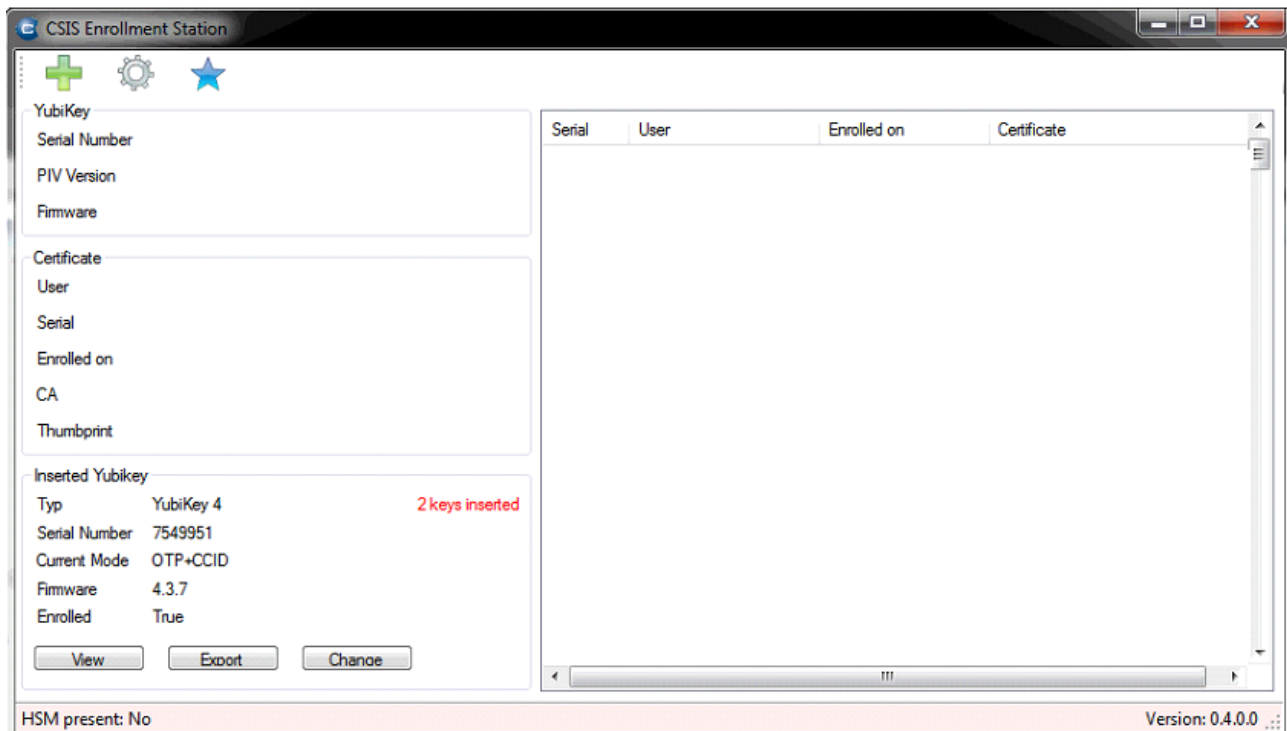
To be able to send signing requests on behalf of another user, you will have to have an enrollment agent certificate. See the [guide here](#) for more information on how to enroll an agent certificate. Once it is installed in your personal certificate store, you can select it using the *Browse* button next to the field.

The cert template field defines what kind of template to use in the CA. Smartcard Logon and Smartcard User templates are the most commonly used.

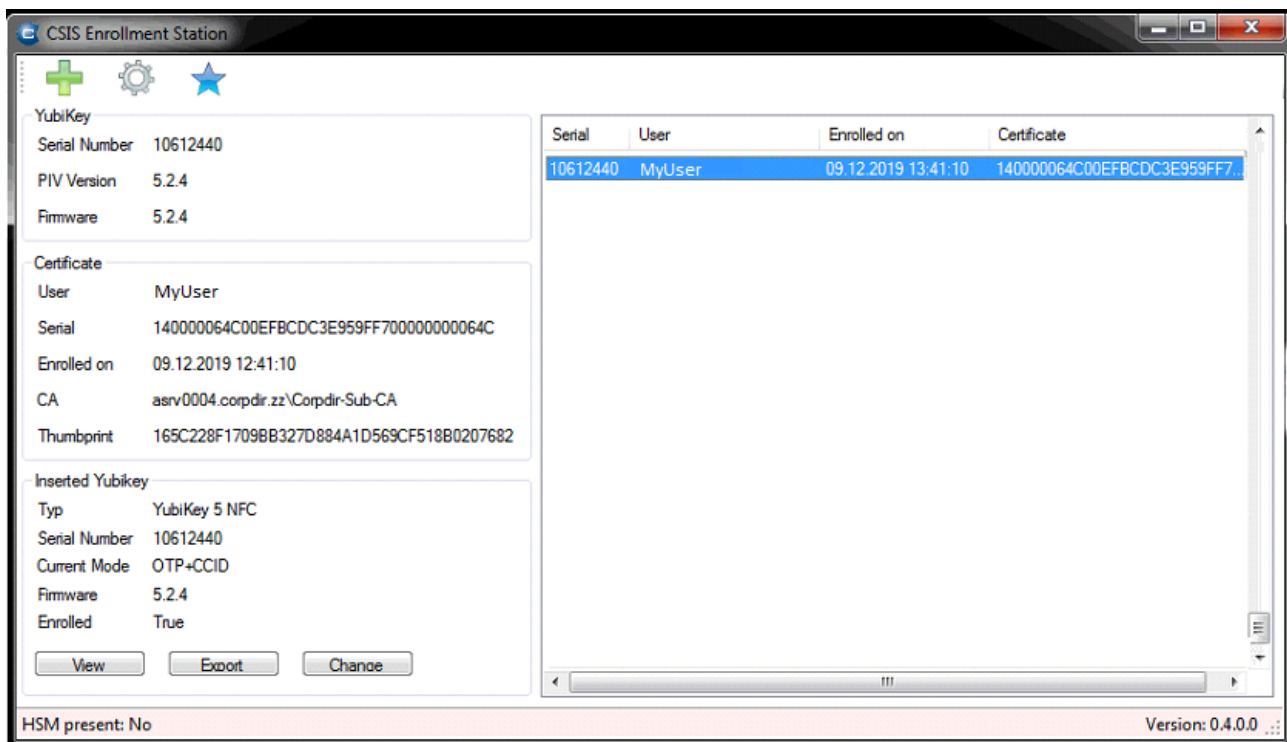
Fill out all the field and click *Save* to save the settings. The settings will be stored in the *settings.json* file.

Main interface

Once you have filled out the settings, you will be presented with the main interface. To the right there is a list of enrolled users, and once a user is selected, detailed information is presented to the left.



if several keys are added the displayed one will be enrolled. In this way you can add an administrative key for authentication and a second one to deploy. Maybe you have to change the USB-slots.

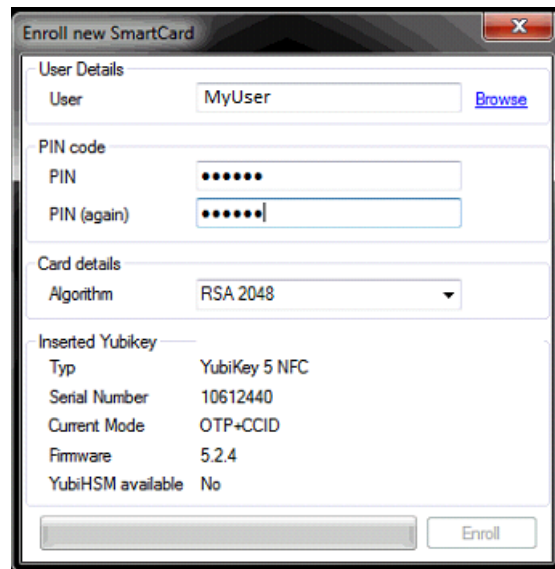


There are 3 buttons in the toolbar for common actions. The first one to the left is *enroll user*, see the section titled “Enrolling a Yubikey Smartcard” for more information. The second button shows the *settings*. See the “Using the application” section above for more information. The third button is *about*, which shows information about the application.

Once a Yubikey is inserted, its information will be displayed in the lower left corner of the application. Here you can quickly change the mode of the Yubikey, view the associated certificate or export the certificate to a file.

Enrolling a Yubikey Smartcard

Enrolling a new Smartcard will present a window requiring you to enter the user information. Enter the username, or click the *Browse* button to select from a list of Active Directory users, and then select a new PIN code for the user, from 6 to 8 in length. PUK code will be automatically generated and saved along with the user. If a YubiHSM is inserted in the machine, it will automatically be used to generate the PUK code for added security.



The screenshot shows a Windows-style dialog box titled "Enroll new SmartCard". It contains several sections: "User Details" with a "User" text box containing "MyUser" and a "Browse" button; "PIN code" with "PIN" and "PIN (again)" text boxes, both containing six dots; "Card details" with an "Algorithm" dropdown menu set to "RSA 2048"; and "Inserted Yubikey" with a table of details. At the bottom, there is a progress bar and an "Enroll" button.

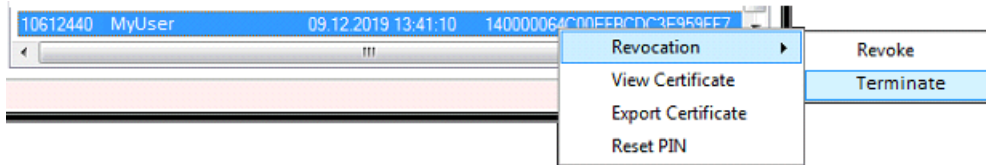
Inserted Yubikey	
Type	YubiKey 5 NFC
Serial Number	10612440
Current Mode	OTP+CCID
Firmware	5.2.4
YubiHSM available	No

The enrollment process can take a little while, so a progress bar will indicate the progress. Once successful, the dialog will close and the newly enrolled Yubikey is displayed in the users list. Users will be saved in the *store.json* file inside the application directory.

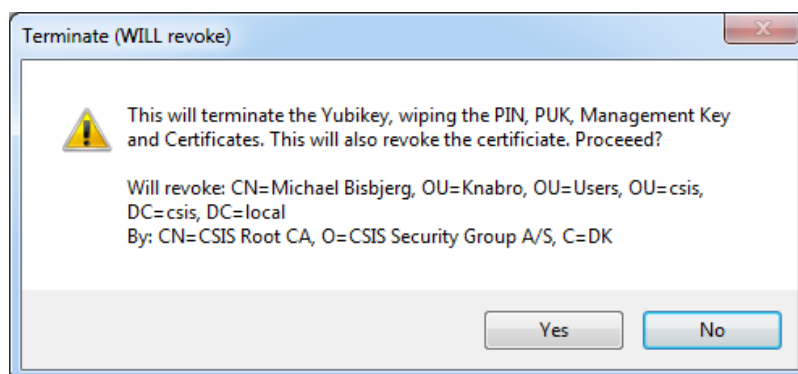
Note: The PIN must be at least 6 characters in length.

Terminating a Yubikey Smartcard

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). Right-click a user in the users list, click *Revocation* and click the *Terminate* action.



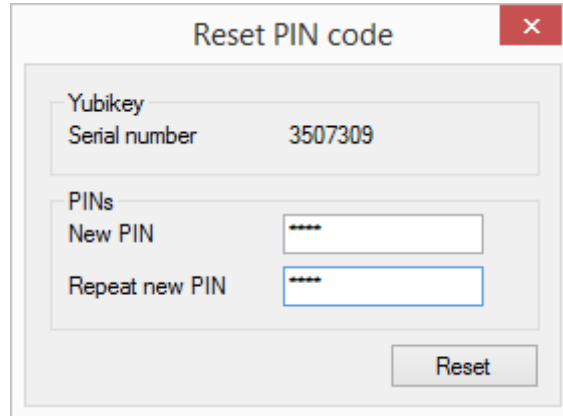
The application will ask to confirm the operation.



Terminating a Yubikey will, in addition to revoking the associated certificate, remove it from the user database. If you wish to simply revoke the certificate (in case the Yubikey has been lost), right click the user, click *Revocation* and then *Revoke*. You will then be presented with a confirmation dialog to revoke the certificate.

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 reset the PIN. When the Yubikey was enrolled in the application, a PUK code was automatically created, which is then used to reset the PIN code of the Yubikey without losing the details on the Smartcard,



Reset PIN code	
Yubikey	
Serial number	3507309
PINs	
New PIN	****
Repeat new PIN	****
Reset	

Enter the new PIN code and click *Reset*. The new PIN code will take effect immediately.

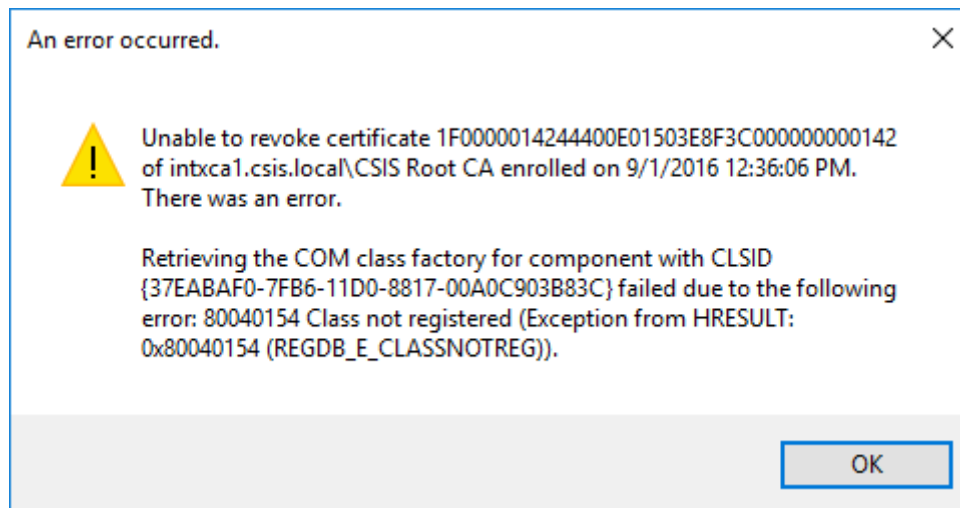
Note: The PIN must be at least 6 characters in length.

Troubleshooting

Occasionally, something will happen that prevents a successful enrollment or revocation of a Smart Card. This section will detail some of the more common cases, and the solutions for them.

COM Class not registered

This error typically occurs when the enrollment program is run for the first time on a computer. It will occur either when enrolling or revoking certificates, and indicates that a library used by the CSIS Enrollment Agent to communicate with the Microsoft AD CS.



Cause

The Microsoft CertAdmin library is not present and registered.

Resolution

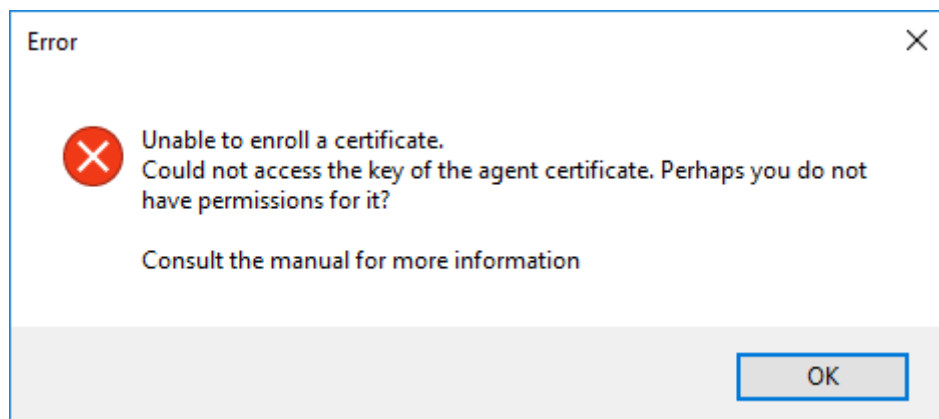
Install the Windows RSAT (Remote Server Administration Toolkit - KB2693643) on the computer. This should also install the Certificate management tools, which will include this library.

MSVCP140.dll not found

This error typically occurs when the Visual C Redist Package is not found. Please install yubikey-manager-qt-1.1.3-win32.exe. Currently the project is using the 32 Bit version of ykman. The 64 Bit version is working, too.

Could not access the key of the agent certificate

This error has to do with permissions.



Cause

Most commonly the agent certificate will be stored in the LocalMachine's certificate store. Usually, regular users do not have permissions to use these certificates for signing.

Resolution

Grant the user permissions by locating the certificate in the certificate store and managing its private keys. To utilize a certificate, a given user must have the Read permission.