CSIS Enrollment Station

For Yubikey smart card management in Windows Active Directory environment.

Created by Ian Qvist and Michael Bisbjerg

Table of Contents

Introduction

This manual describes the CSIS Enrollment Station (ES) located at https://github.com/CSIS/EnrollmentStation. The Enrollment Station was created to facilitate enrollment of Yubico Smartcards, using the Yubikey NEO Premium with CCID functionality in a Windows Active Directory environment with an associated Windows Certificate Authority.

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

Requirements

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

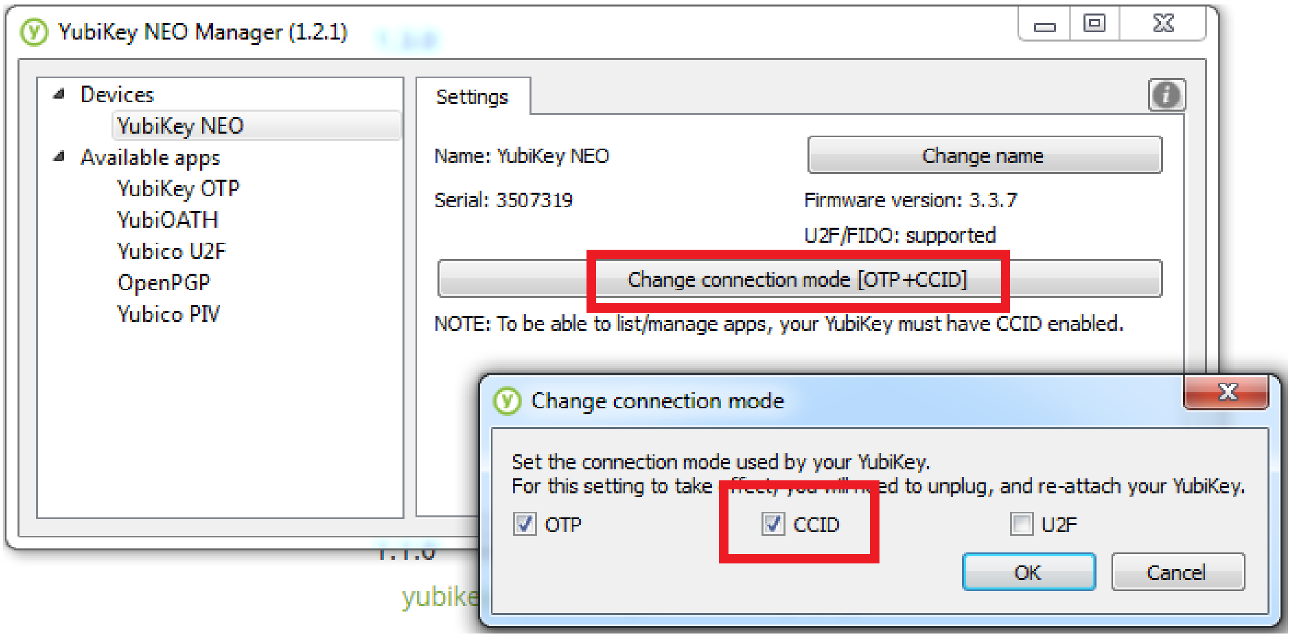
- A Microsoft Windows Active Directory domain
- A computer running the ES software joined to the domain.
- A Windows Certificate Authority (CA) published in the domain.
- The user running the ES must have an Enrollment Agent certificate in their personal certificate store.
- The user running the ES must have permissions to manage certificates on the CA server.

Preparing a Yubikey for enrollment

Directly from the factory, Yubikey NEO Premium keys are not set up to with the CCID mode, which activates the smartcard applet. You have 2 applications available directly from Yubico to activate the CCID mode, which both are described below.

Using NEO Manager (recommended)

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.



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

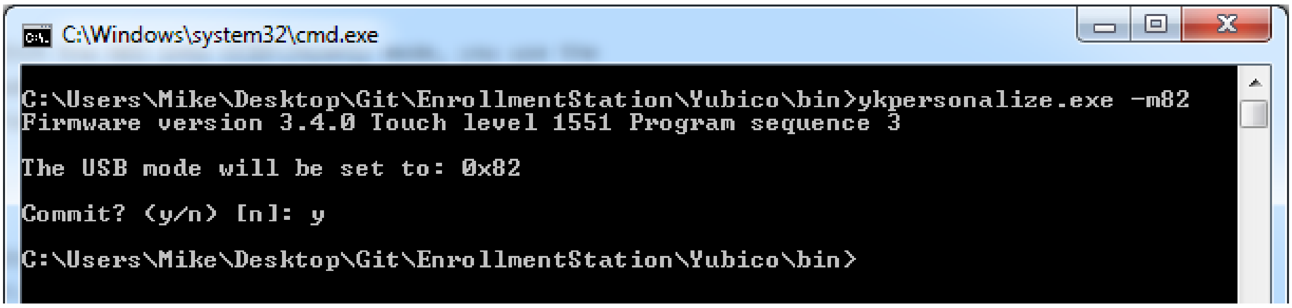
Home page: https://developers.yubico.com/yubikey-neo-manager/
Download page: https://developers.yubico.com/yubikey-neo-manager/Releases/

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.

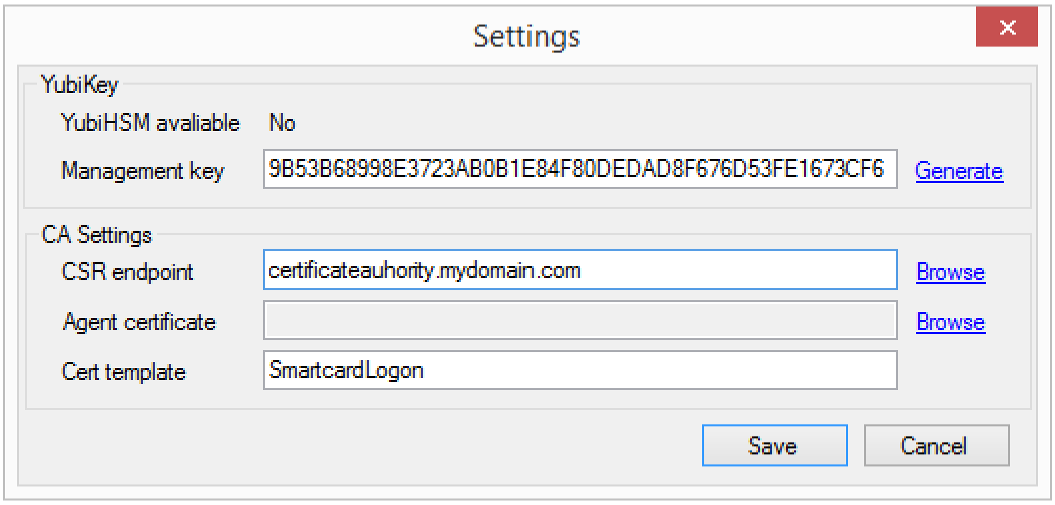


```
C:\Users\Mike\Desktop\Git\EnrollmentStation\Yubico\bin>ykpersonalize.exe -m82
Firmware version 3.4.0 Touch level 1551 Program sequence 3

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.



Settings

YubiKey

YubiHSM avaliable No

Management key 9B53B68998E3723AB0B1E84F80DEDAD8F676D53FE1673CF6

CA Settings

CSR endpoint certificateauhority.mydomain.com

Agent certificate

Cert template SmartcardLogon

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.

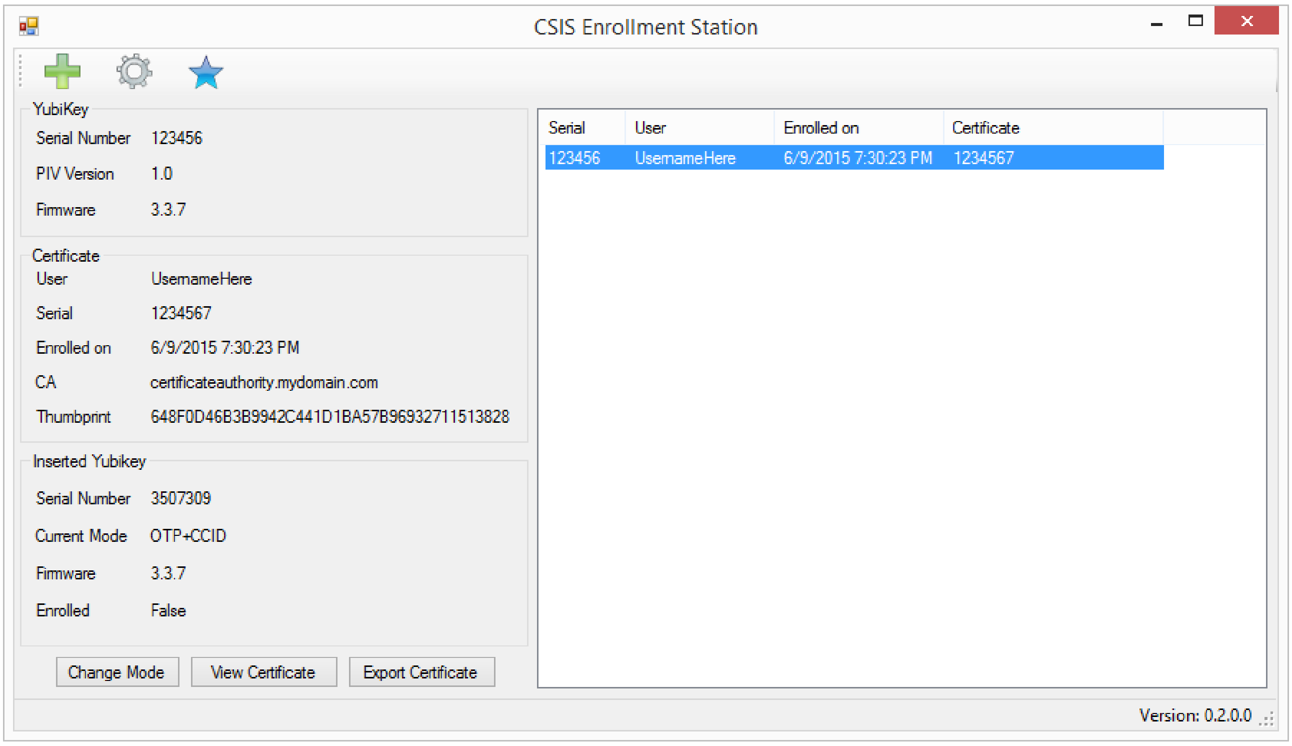
To be able to send signing requests on behalf of another user, you will have to have an enrollment agent certificate. See the guide here for more information on how to enroll an agent certificate. Once it is installed in your personal certificate store, you can select it using the *Browse* button next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



YubiKey

Serial Number	123456
PIV Version	1.0
Firmware	3.3.7

Certificate

User	UsernameHere
Serial	1234567
Enrolled on	6/9/2015 7:30:23 PM
CA	certificateauthority.mydomain.com
Thumbprint	648F0D46B3B9942C441D1BA57B96932711513828

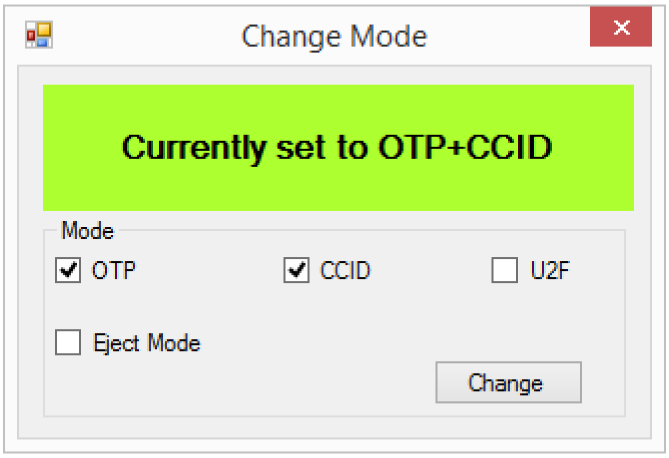
Inserted Yubikey

Serial Number	3507309
Current Mode	OTP+CCID
Firmware	3.3.7
Enrolled	False

Serial	User	Enrolled on	Certificate
123456	UsernameHere	6/9/2015 7:30:23 PM	1234567

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.



Currently set to OTP+CCID

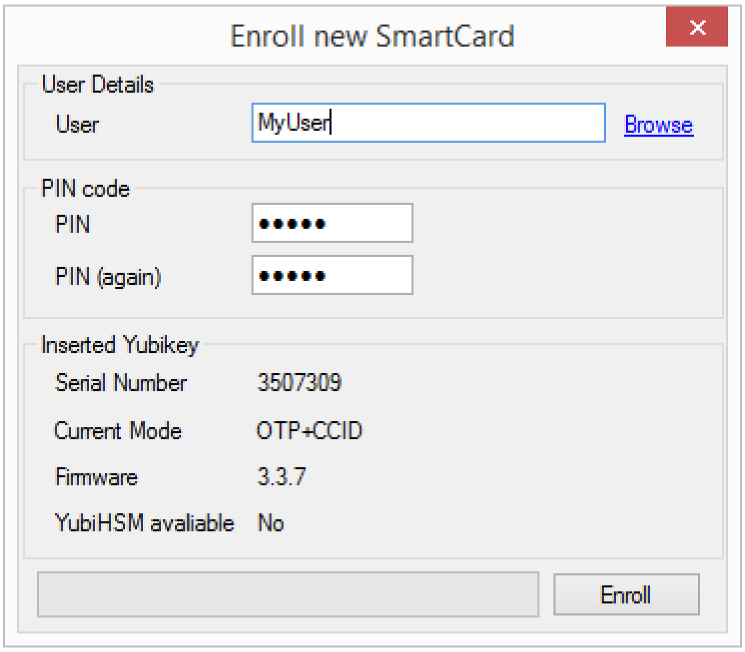
Mode

☑ OTP ☑ CCID ☐ U2F

☐ Eject Mode

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.



Enroll new SmartCard

User Details

User MyUser

PIN code

PIN: •••••

PIN (again): •••••

Inserted Yubikey

Serial Number: 3507309

Current Mode: OTP+CCID

Firmware: 3.3.7

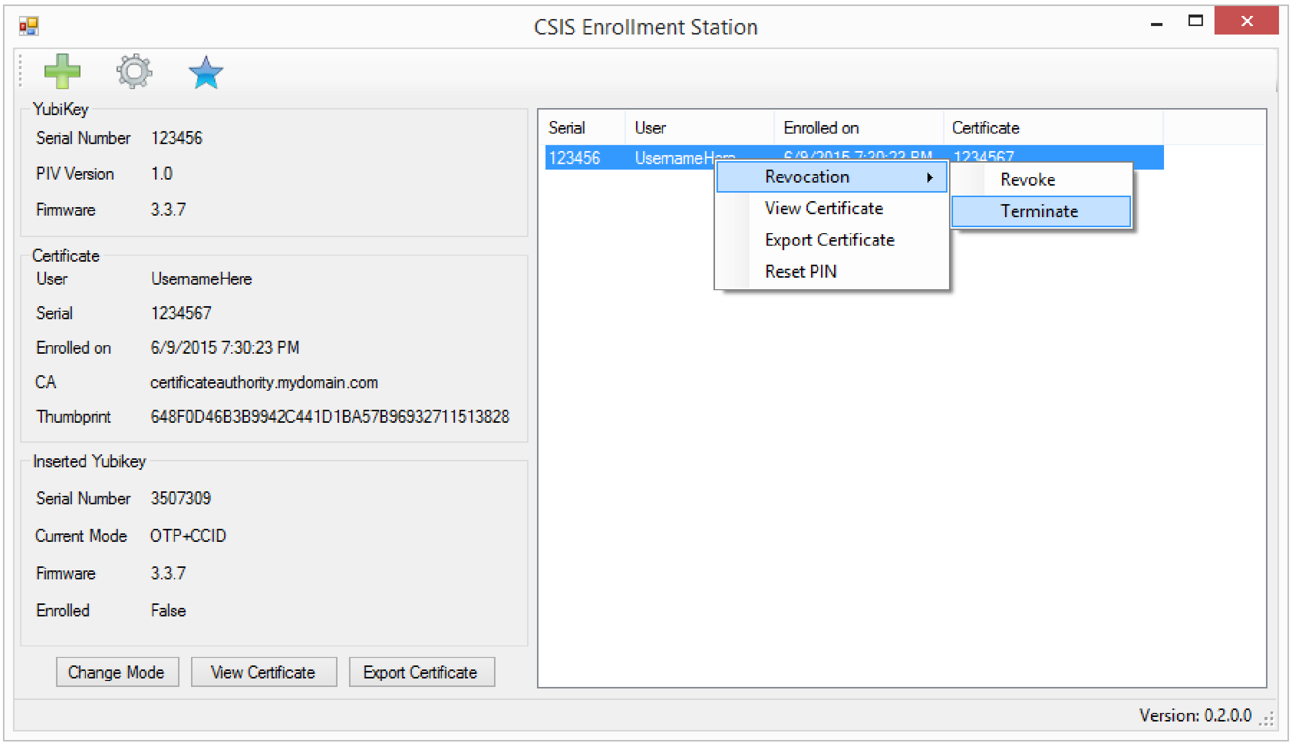
YubiHSM avaliable: No

The enrollment process can take a little while, so a progress bar will indicate the progress. Once successful, the 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.



YubiKey

Serial Number	123456
PIV Version	1.0
Firmware	3.3.7

Certificate

User	UsernameHere
Serial	1234567
Enrolled on	6/9/2015 7:30:23 PM
CA	certificateauthority.mydomain.com
Thumbprint	648F0D46B3B9942C441D1BA57B96932711513828

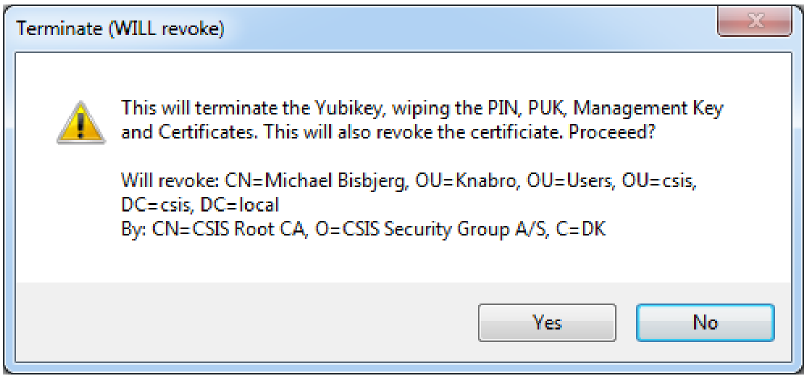
Inserted Yubikey

Serial Number	3507309
Current Mode	OTP+CCID
Firmware	3.3.7
Enrolled	False

Serial	User	Enrolled on	Certificate
123456	UsernameHere	6/9/2015 7:30:23 PM	1234567

Version: 0.2.0.0

The application will ask to confirm the operation.



Terminate (WILL revoke)

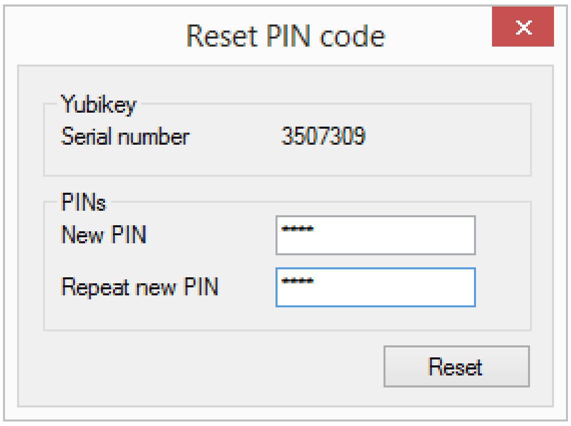
This will terminate the Yubikey, wiping the PIN, PUK, Management Key and Certificates. This will also revoke the certificate. Proceeed?

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 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 ****

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

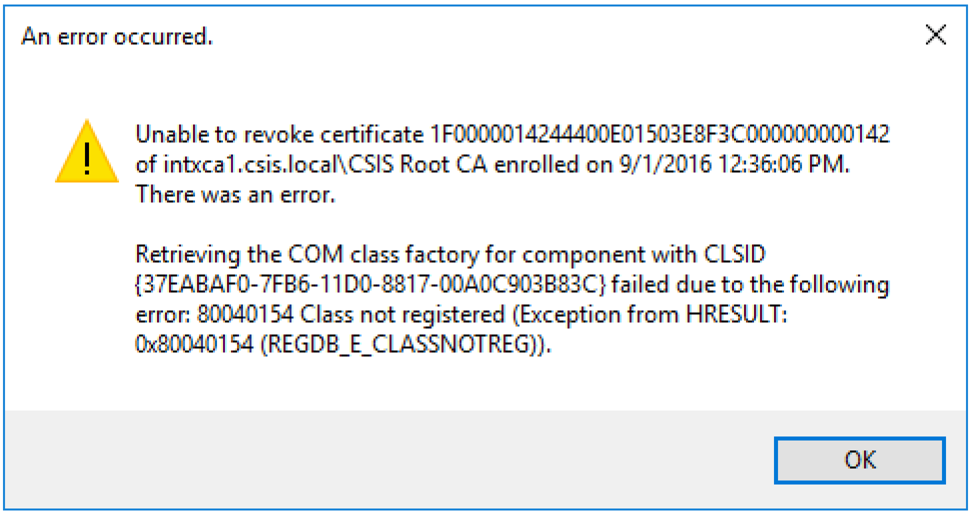
Note: The PIN must be at least 6 characters in length.

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.



An error occurred.

Unable to revoke certificate 1F0000014244400E01503E8F3C000000000142 of intxca1.csis.local\CSIS Root CA enrolled on 9/1/2016 12:36:06 PM.
There was an error.

Retrieving the COM class factory for component with CLSID {37EABAF0-7FB6-11D0-8817-00A0C903B83C} failed due to the following error: 80040154 Class not registered (Exception from HRESULT: 0x80040154 (REGDB_E_CLASSNOTREG)).

Cause

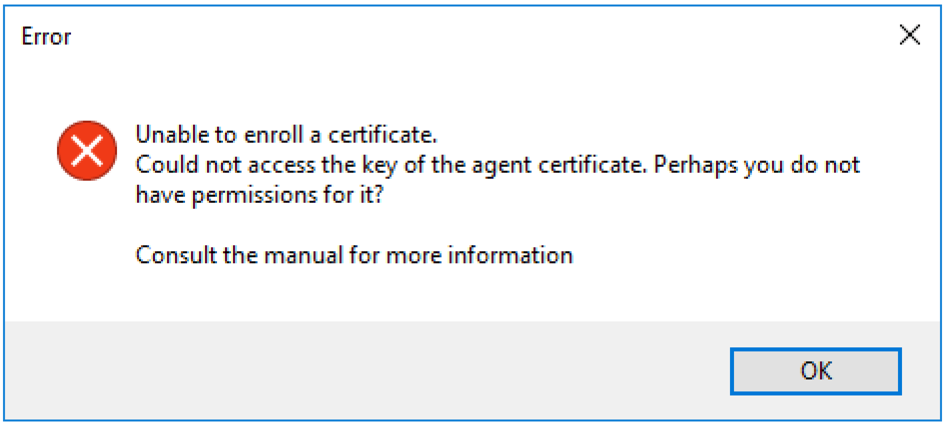
The Microsoft CertAdmin library is not present and registered.

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.

Could not access the key of the agent certificate

This error has to do with permissions.



Unable to enroll a certificate.
Could not access the key of the agent certificate. Perhaps you do not have permissions for it?

Consult the manual for more information

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.