

Getting Started with Aventra MyEID PKI Smart Card

Version 8.2



Change History

Version	Date	Comments
8.1	17.10.2024	Updated the product name and document title to be consistent with other product documentation.
8.2	18.8.2025	Added a note about applicability of this document to different MyEID versions. Internal review 22.8.2025 JS

Table of contents

1	Introduction	1
2	Hardware requirements	1
3	Usage as Secure Signature Creation Device	1
4	Middleware software	2
4.1	MyEID Minidriver	2
4.2	OpenSC	2
4.3	Other Solutions	3
5	Note: MyEID ATRs	3
6	Tutorial: MyEID Deployment with Windows, Minidriver and Certificate Services	4
6.1	Install Software	4
6.2	Initializing the Card	8
6.3	Request and Install Certificates	10
7	Troubleshooting	21
7.1	The Card Does not Appear in the Device Manager	21

1 Introduction

This quick start guide contains short instructions on how to set up Aventura's MyEID PKI Smart Card for typical PKI usage like smart card authentication. This document applies to all MyEID versions. Information about differences between versions is available in MyEID PKI Smart Card Reference Manual.

MyEID cards can be used in Windows, Linux, and Mac OS X environments. You need middleware software to initialize and use the cards. Initialization means creating the initial structure to the cards with desired PIN and PUK codes that protect the card. For this you can use the following free software:

- MyEID MiniDriver and Minidriver Utility
- OpenSC

After initialization, you need to generate or upload an RSA or elliptic curve key pair to the card and install a certificate. In Windows environment, the simplest way is to obtain a key pair and a certificate from your Windows domain's CA using Microsoft Certificate Services.

2 Hardware requirements

For using MyEID, you need a smart card reader compliant with the ISO 7816 1-4 standard. A smart card reader can be USB-connected or embedded into a laptop or keyboard. Most smart card readers on the market are PC/SC compliant. CCID compliant PC/SC readers do not require installation of drivers, because operating systems (at least Microsoft Windows) include built-in CCID drivers.

3 Usage as Secure Signature Creation Device

For using MyEID PKI Smart Card as a Secure Signature Creation Device which fulfills the requirements defined in Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), please verify that your operational environment complies with the requirements described in document "MyEID PKI JavaCard Applet Reference Manual 3-0-1 - Annex I - CC Requirements Mapping".

4 Middleware software

4.1 MyEID Minidriver

A minidriver for MyEID cards is available from Aventura. The minidriver integrates MyEID cards tightly with Windows. The minidriver works together with Cryptography API: Next Generation (CNG) and Microsoft Smart Card Key Storage Provider. The minidriver is a lightweight software component that provides lower-level interface to the card for the KSP. The minidriver also supports the deprecated CSP (Cryptographic Service Provider) interface. It is recommended to always use MyEID Minidriver with CNG / KSP instead of CSP.

The minidriver has passed Microsoft's Windows Hardware Certification Program. Latest certified version is 2.2.4. Aventura also releases versions which have not yet been certified. Non-certified versions are digitally signed by Aventura and have been tested with the same test tool which is used in the Hardware Certification Program.

The minidriver can be used with the following Windows versions: 7, 8, 8.1, 10, 11, 2008 Server, 2012 Server, 2016 Server, 2019 Server and 2022 Server.

The latest version of the minidriver can be freely downloaded from our web site at <https://aventra.fi/downloads/>

For Windows 10, the minidriver may be automatically installed from Windows Update when inserting a MyEID card for the first time, depending on Windows 10 version.

Download and install also MyEID Minidriver Utility. With this program you can initialize the card's file structure and perform other management tasks, for example import PKCS#12 files and unblock a blocked PIN.

4.2 OpenSC

OpenSC is an open-source project that has support for MyEID cards. You can use OpenSC in Windows, Linux, and Mac OS environments. The latest version can be downloaded from the project's website <https://github.com/OpenSC/OpenSC/wiki>.

OpenSC includes a PKCS#11 module, a minidriver for Windows, and some tools to initialize and manage the cards.

Please read the information at <https://github.com/OpenSC/OpenSC/wiki/Aventra-MyEID-PKI-card> about initializing and using MyEID cards with OpenSC.

4.3 Other Solutions

For personalising large quantities of MyEID cards, we recommend Aventra's Active Process Manager software. Please contact sales@aventra.fi for more information.

Fujitsu's mPollux DigiSign Client middleware is compatible with MyEID and includes a set of tools for card management and usage. DigiSign Client is available for Windows, Linux and Mac OS.

MyEID has been verified to be compatible with [Versasec's](#) vSEC:CMS. With easy installation and deployment, it is a good option for enrolling certificates and managing cards' lifecycles.

4.3.1 Preparing Cards for vSEC:CMS

Before a MyEID card can be used in vSEC:CMS, it must be initialized using MyEID Minidriver Utility. Use administrator key "000102030405060708090A0B0C0D0E0F1011121314151617". This will be changed when the card is registered. The PUK codes cannot be changed later, so be sure to use secure PUK codes and store them in a safe place, and NOT use the default codes in production environment.

We can deliver cards pre-initialized for vSEC:CMS upon request. Please notify us, for example in the "Add Comments About Your Order" field in our web shop, if you would like your cards to be prepared for vSEC:CMS.

5 Note: MyEID ATRs

MyEID cards have been delivered with two different ATRs:

New ATR: 3BF59600008131FE454D7945494414

Old ATR: 3BF51800008131FE454D794549449A

All cards are normally delivered with the new ATR. Cards with the old ATR version are available on request.

In the new ATR, third byte of the ATR, named TA1, has been changed from 18h to 96h to allow faster communication speed. Consequently, also the last checksum byte (TCK) has changed.

All the software presented in this document recognize both versions, so in normal usage this change does not cause compatibility issues. However, please note that OpenSC versions older than 0.16 do not recognize the new ATR directly. If you have written your own software that communicates with the card directly, please note this change if the card is recognized from the ATR.

If you have any technical questions, you can contact us at support@aventra.fi

6 Tutorial: MyEID Deployment with Windows, Minidriver and Certificate Services

This step-by-step tutorial shows, how to set up a MyEID Smart Card for Windows smart card logon.

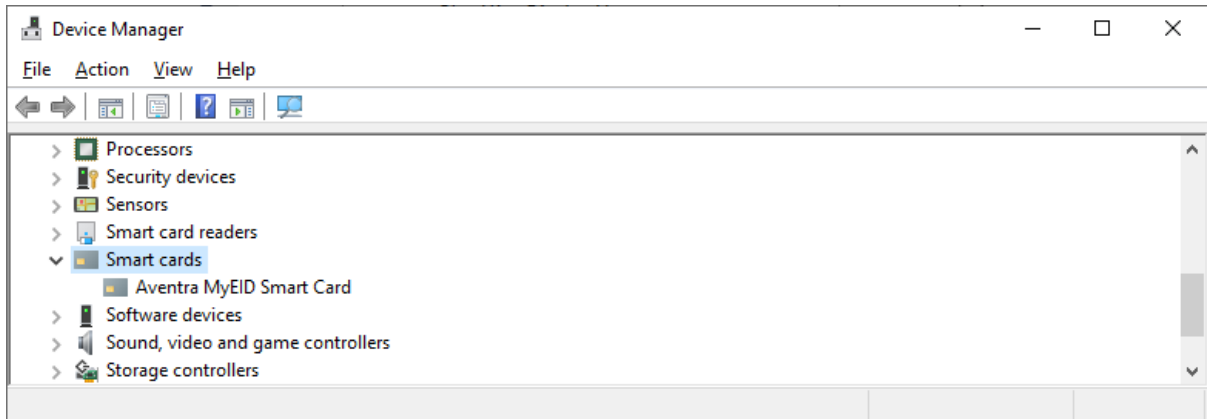
Prerequisites for this tutorial:

- a MyEID PKI Smart Card
- PS/SC compliant smart card reader
- a Windows 7 or 10 workstation that belongs to a domain
- Certificate Services running on your domain. If you don't have Certificate Services running yet, please refer to Aventura PKI Administrator's guide on how to set it up.

6.1 Install Software

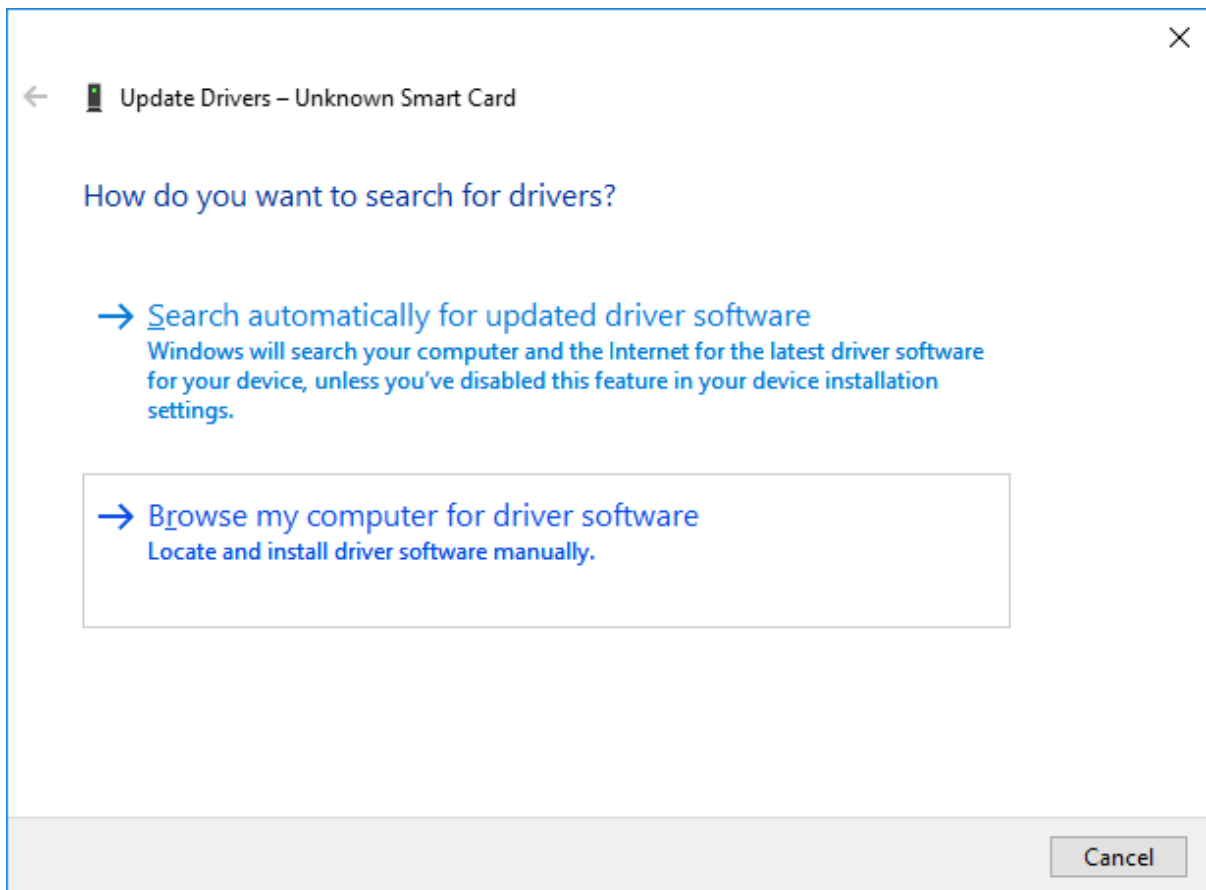
1. Insert a MyEID card to your smart card reader. Wait for a couple of minutes to give Windows a chance to install the driver automatically from Windows Update.
2. Open Device Manager (right click Windows logo and select Device Manager)

3. Locate and expand *Smart cards*. If you find Aventura MyEID Smart Card, the minidriver has been installed automatically. If this is the case, continue to step 6. If you see “Unknown smart card”, proceed to the following steps.

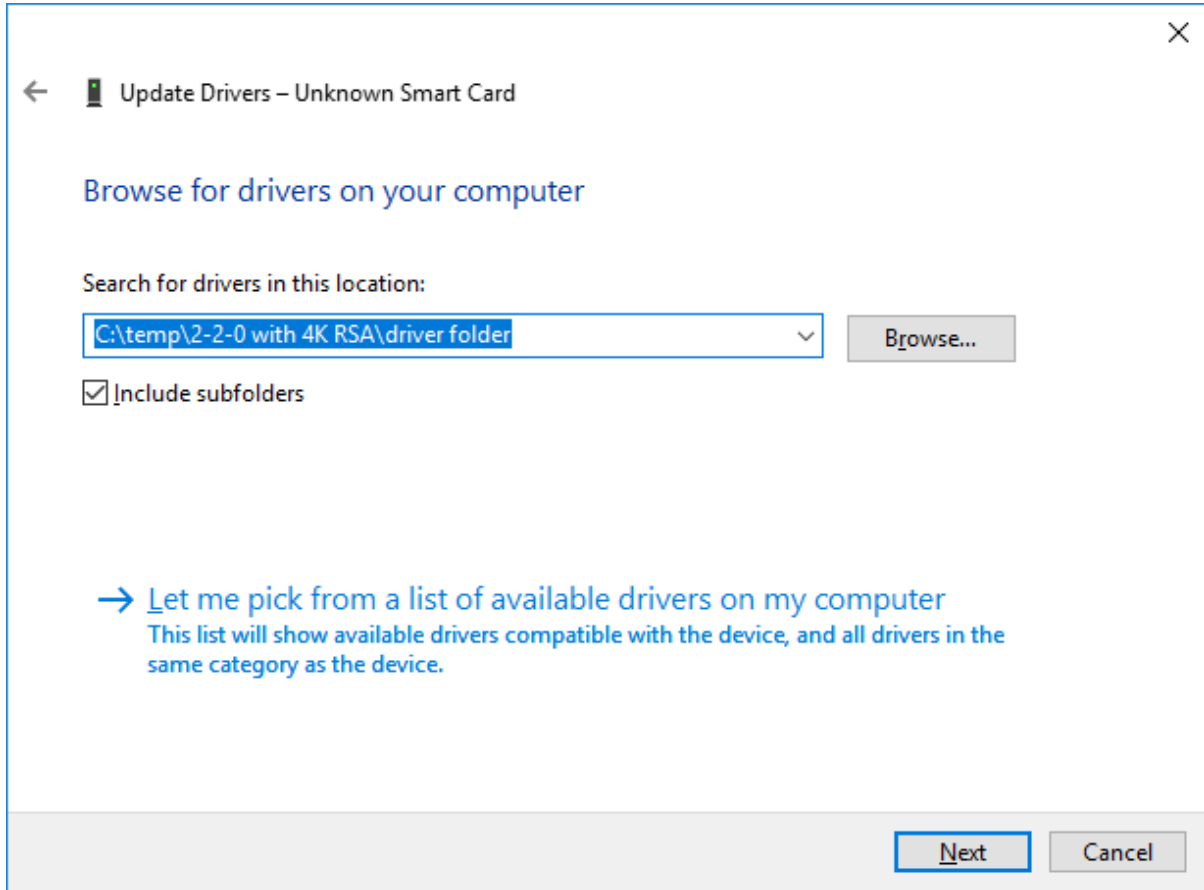


4. Go to <https://aventra.fi/downloads/> and download the newest versions of MyEID Minidriver (driver files). Extract it to your hard drive, for example to folder c:\temp

5. Right click "Unknown smart card" and select "Update driver". Select "Browse my computer for driver software".



6. Locate the folder containing MyEID Driver files.



7. The driver is now installed.
8. Download newest version of MyEID Minidriver Utility from <https://aventra.fi/downloads/>
9. Install the software by running the installer.

6.2 Initializing the Card

1. Run MyEID Minidriver Utility. If the card is not in the reader, insert it now.
2. Press "Initialise card" button.

3. Select your PIN codes.

Card initialization ? X

Hide PINs

User PIN (PIN #1) Confirm User PIN (PIN #1)

User PUK Confirm User PUK

Signature PIN (optional) Confirm Signature PIN (PIN #2)

Signature PUK Confirm Signature PUK

Administrator PIN / KEY

Challenge/Response Challenge length

Admin key source

User input Encrypted key file

Administrator key. ...

Confirm Administrator PIN / KEY

Administrator PUK

Confirm Administrator PUK

Activate applet

Create msroots file

You can create either Challenge/Response type or normal Administrator PIN. A Challenge/Response PIN can be used to unblock a blocked card using the built-in user interface of Windows. Challenge/Response is selected by default. If you uncheck it, enter a 4 to 8 characters long PIN code.

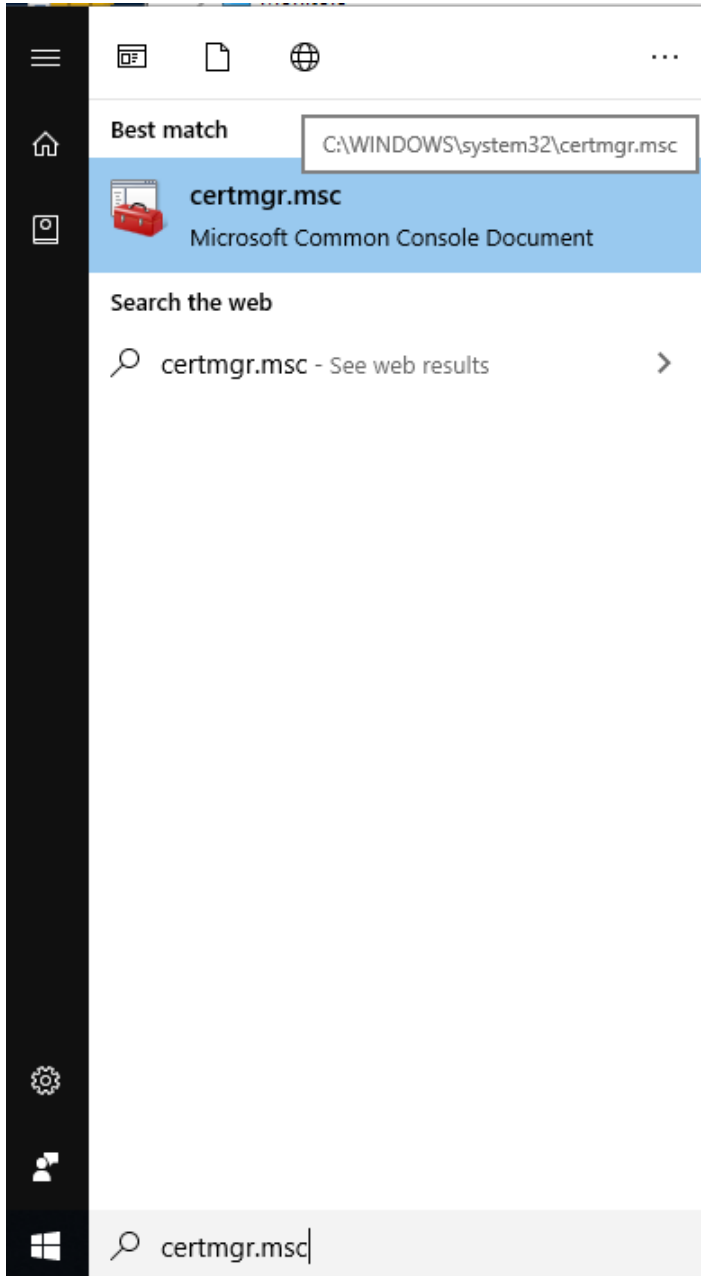
Use the default Administrator key or PIN values only for testing purposes. It is recommended to generate a random value for the Administrator key. Be sure to store your Administrator Key or PIN and PUK in a safe place. They will be needed if you later want to clear and reinitialise the card. If you use a Challenge/Response Admin PIN, you can select either 8 or 16 byte challenges. 16 bytes is the driver's default.

4. Press ok and wait for the card to be initialised. Remove and reinsert the card.

6.3 Request and Install Certificates

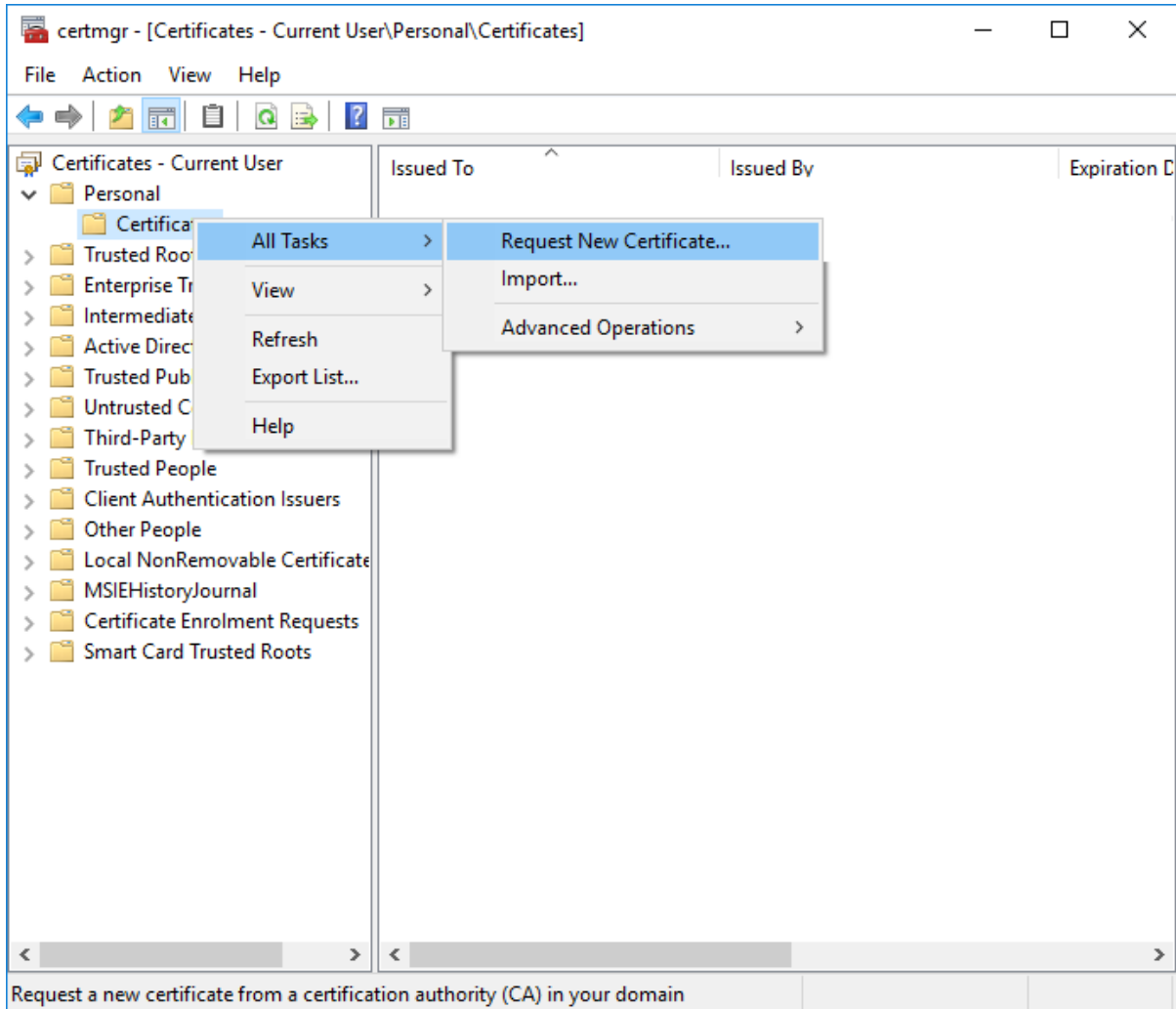
1. Before this step, you must set up Certificate Services, if it is not already running in your Windows domain.

2. Open Windows start menu and type "certmgr.msc". Press Enter.

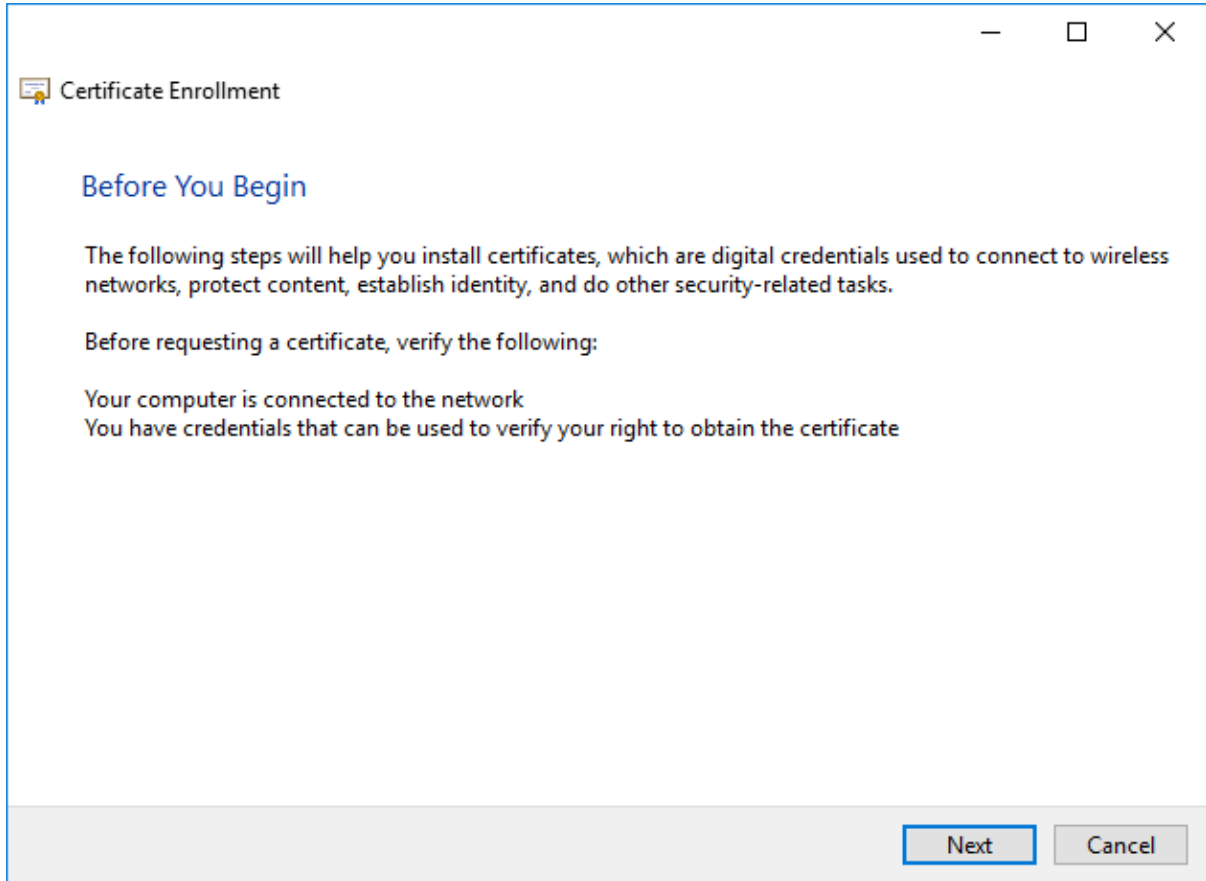


3. The Certificates management console snap-in opens.

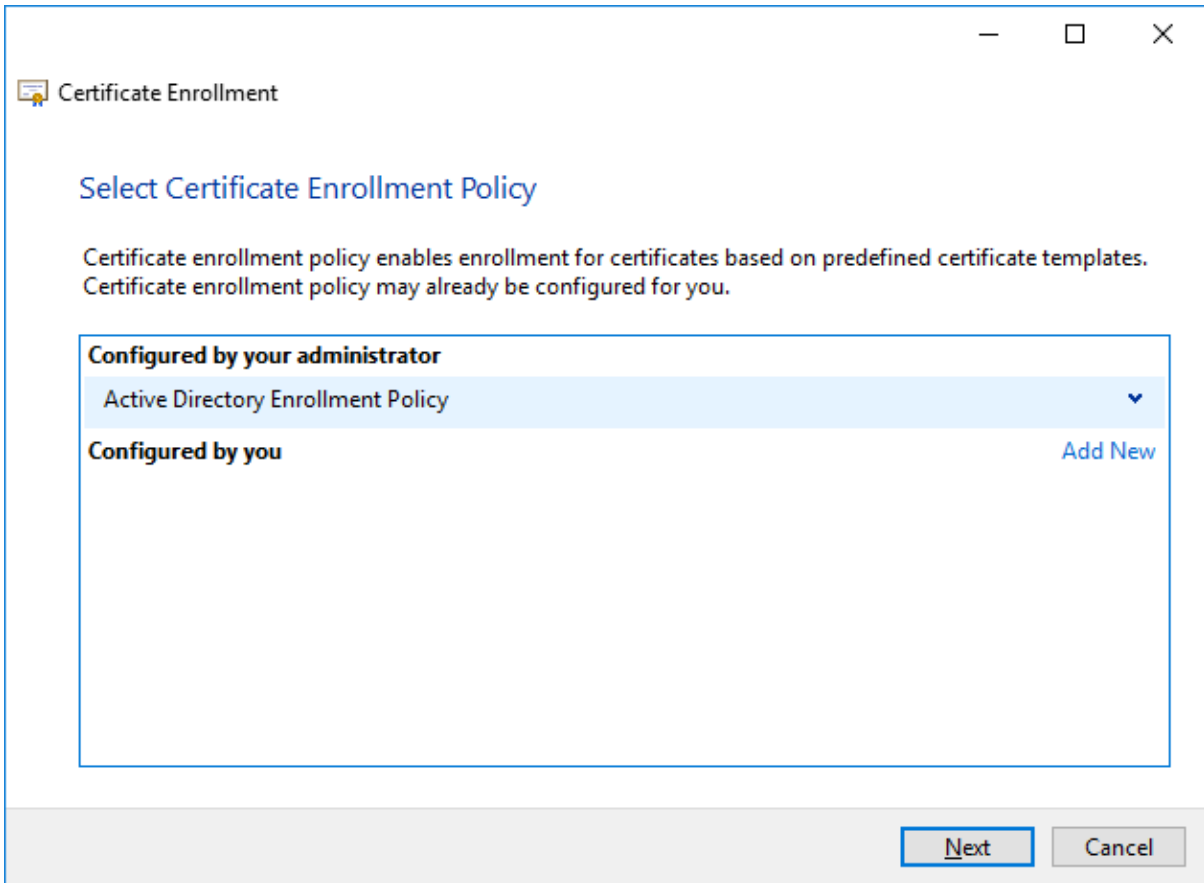
4. Expand Personal and right click Certificates. Select All Tasks -> Request New Certificate...



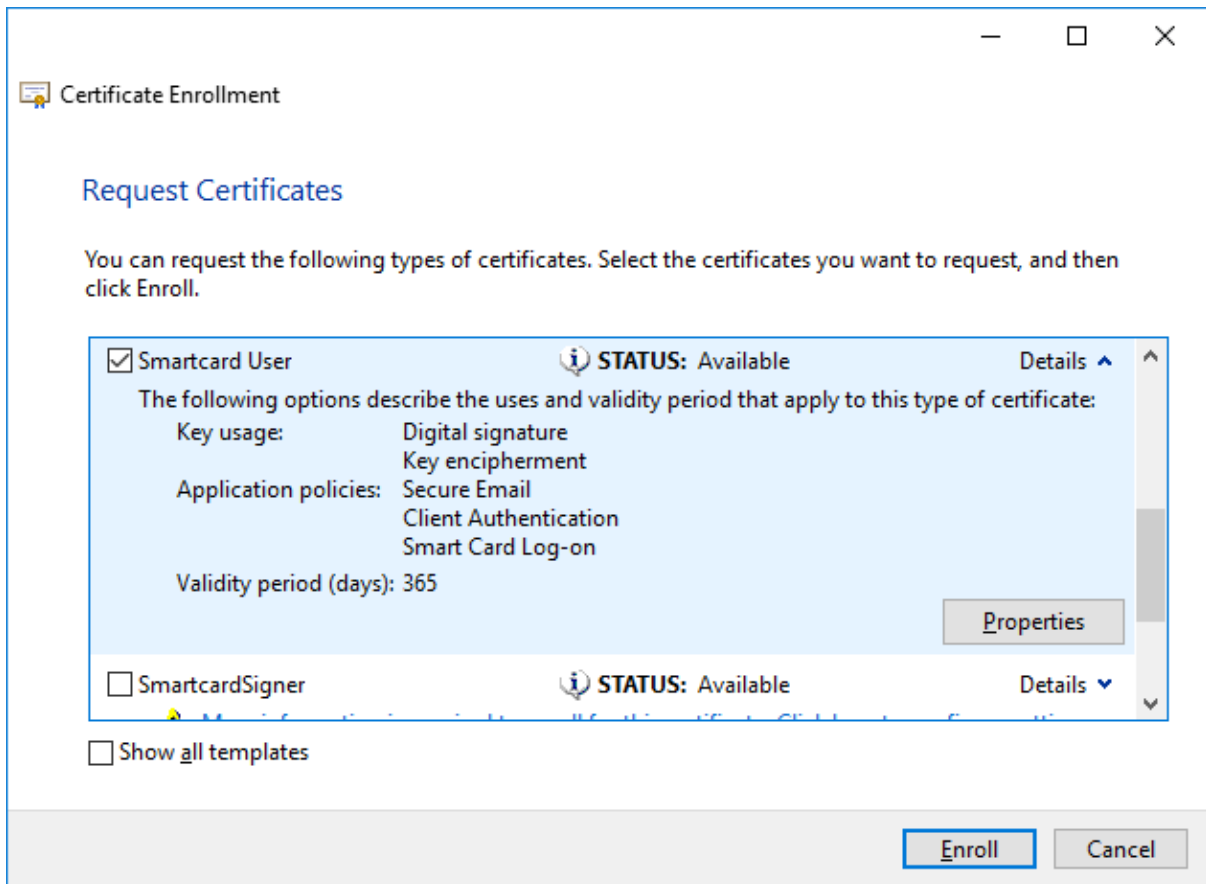
5. The wizard opens. Press Next.

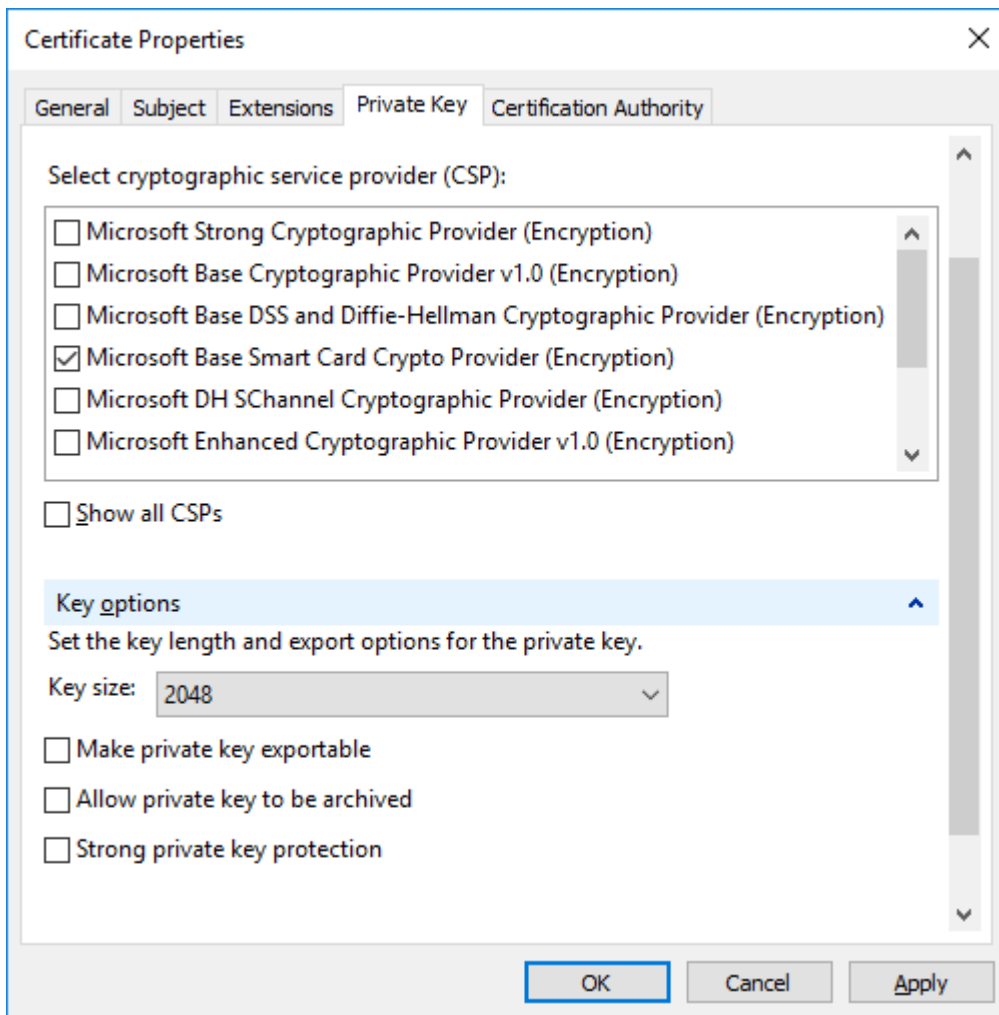


6. Press Next.



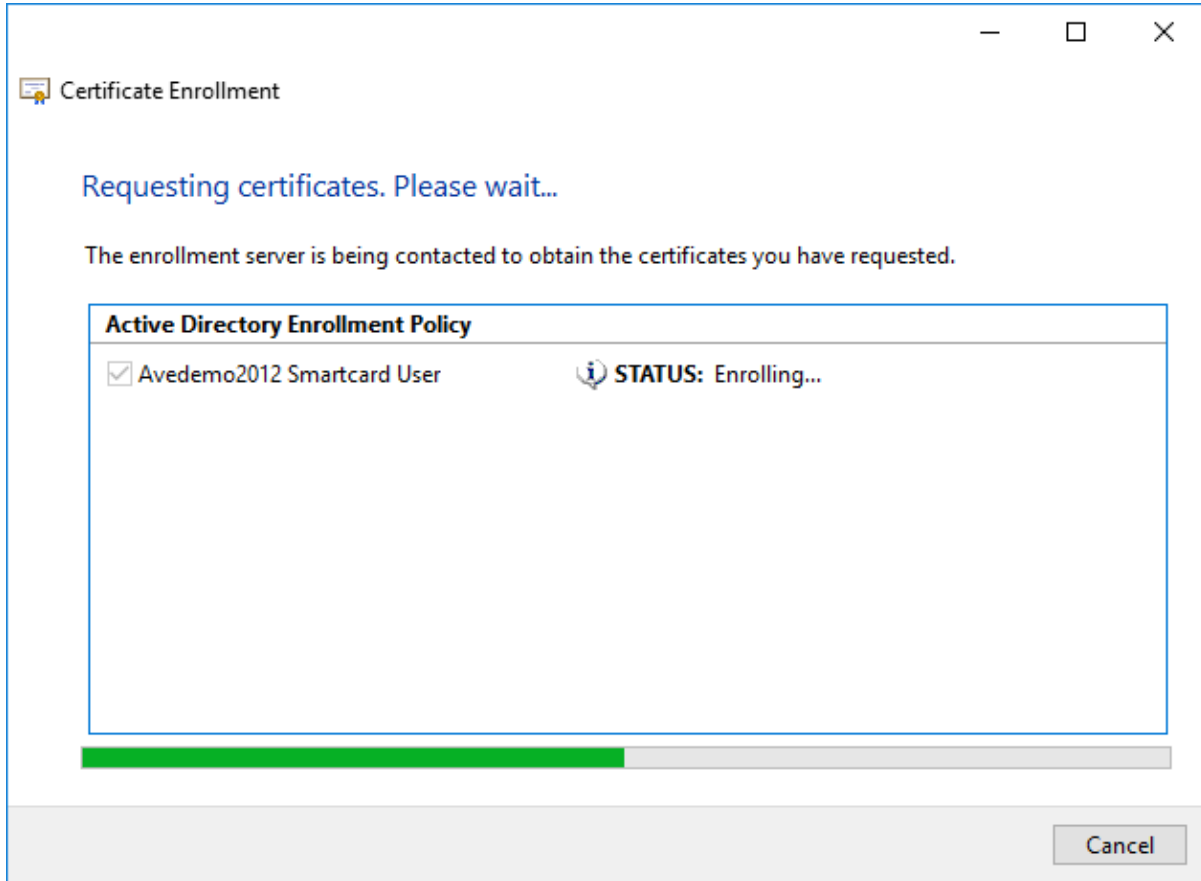
7. Select Smartcard User, or other certificate type that has been configured in Certificate Services for smart cards. Expand the certificate type and press the Properties button.



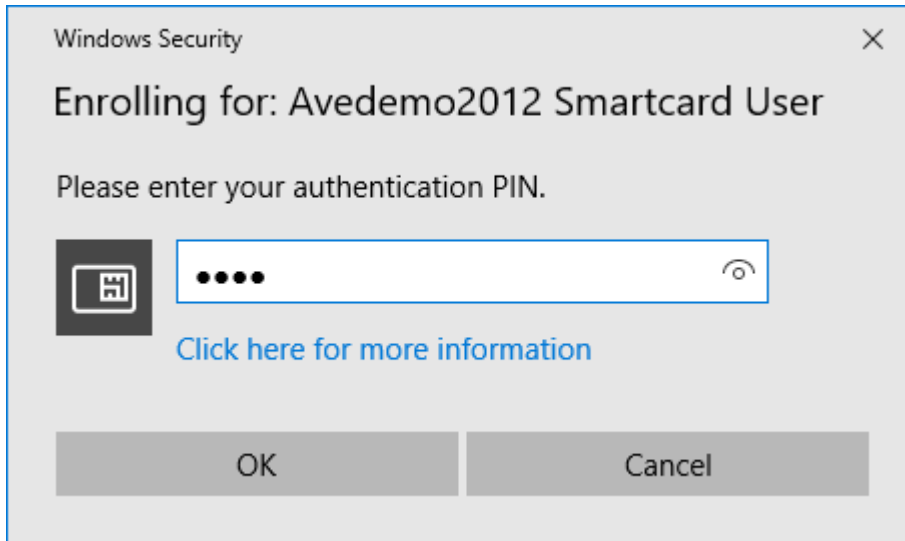


8. Select "Private Key" tab and verify that either "Microsoft Base Smart Card Crypto Provider" or "Microsoft Smart Card Key Storage Provider" is selected. Select desired key length. Recommended key lengths are 2048 or 4096 bits. You can also configure other options, which are not covered by this tutorial.

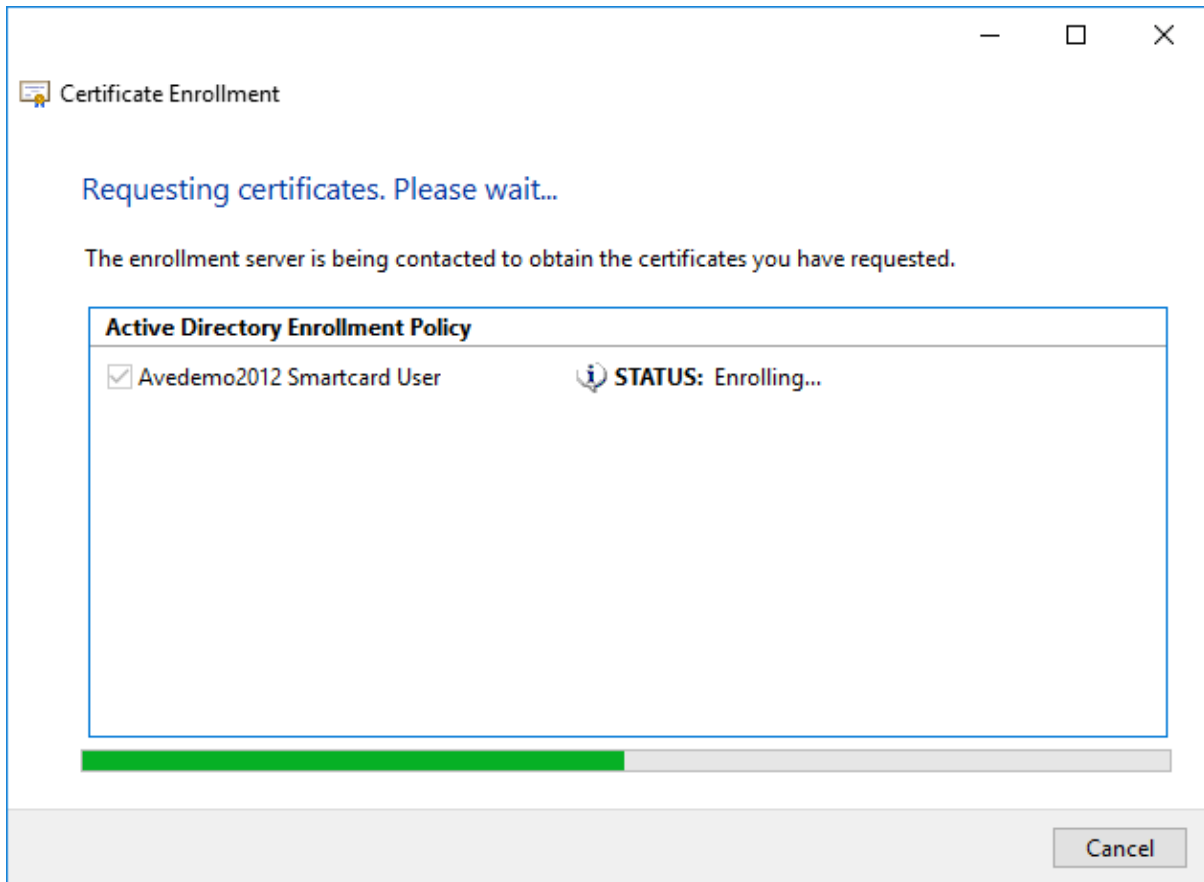
9. Press "Enroll". Certificate enrollment begins.



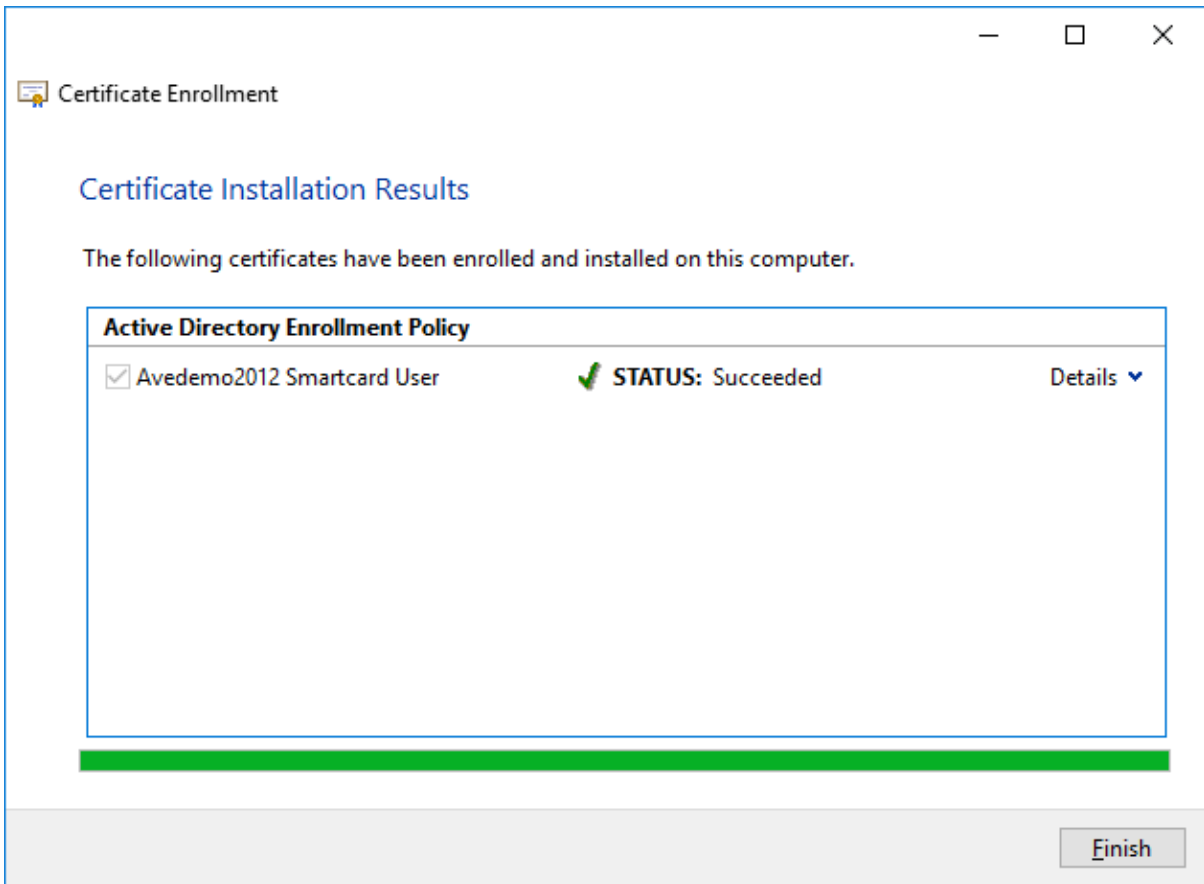
10. Enter your PIN code (The User PIN you selected in MyEID Minidriver Utility)



11. Wait until certificate enrollment completes. This may take a minute or two, because generating the key pair on smart card takes a varying amount of time.



12. When the certificate has been successfully received and installed, the following window is shown. You can now test smart card logon.



7 Troubleshooting

7.1 The Card Does not Appear in the Device Manager

Ensure that Smart Card Plug & Play is enabled.

You can enable Smart Card Plug & Play by setting the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ScPnP\EnableScPnP

REG_DWORD: 1

7.2 Windows does not find certificates from the Card

The minidriver architecture includes a cache mechanism. In some situations, the cache counters are not increased on the card when the card is updated. Windows fails to notice that the card has been updated and loads an outdated version of the card's contents from the cache. Use "Increase card counters" button in MyEID Minidriver Utility to increase the cache counters. Remove and reinsert the card, and Windows refreshes the cache.