

5.9.2023

Getting Started with MyEID Cards and Tokens



Table of contents

1	Ir	ntroduction	1
2	N	1yEID Minidriver	1
3	0	penSC	2
4	0	Other Solutions	2
4	4.1	Preparing Cards for vSEC:CMS	3
5	Ν	lote: MyEID ATRs	3
6	Т	utorial: MyEID Deployment with Windows, Minidriver and Certificate Services	4
(5.1	Install Software	4
(5.2	Initializing the Card	8
(5.3	Request and Install Certificates	10
7	Т	roubleshooting	21
-	7.1	The Card Does not Appear in the Device Manager	21
-	7.2	Windows does not find certificates from the Card	21

MyEID Getting Started Guide



5.9.2023

1 Introduction

This quick start guide contains short instructions on how to set up Aventra's MyEID PKI Smart Card for typical PKI usage like smart card authentication.

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 MyEID Minidriver

A minidriver for MyEID cards is available from Aventra. 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. Aventra releases also versions which have not yet been certified. Non-certified versions are digitally signed by Aventra 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: XP, Vista, 7, 8, 8.1, 10, 11, 2003 Server, 2008 Server and 2012 Server, 2016 Server, 2019 Server and 2022 Server.



MyEID Getting Started Guide

2

The minidriver is automatically installed from Windows Update when inserting a MyEID card for the first time. If you are using an older version of Windows or cannot use Windows Update, The latest version of the minidriver can be freely downloaded from our web site at https://webservices.aventra.fi/downloads/

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.

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

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

4 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 <u>Versasec's</u> vSEC:CMS. With easy installation and deployment, it is a good option for enrolling certificates and managing cards' lifecycles.

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



5.9.2023

4.1 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

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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 readeraa
- > 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 Aventra 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)

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



3. Locate and expand *Smart cards.* If you find Aventra 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.

📇 Device Manager	_	×
<u>File Action View H</u> elp		
> Processors		^
> 🛐 Security devices		
> 🔚 Sensors		
> 📮 Smart card readers		
✓ III Smart cards		
Aventra MyEID Smart Card		
> 📱 Software devices		
> 🕡 Sound, video and game controllers		
> 🍇 Storage controllers		\sim

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

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



п

6

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

		×
÷	Update Drivers – Unknown Smart Card	
	How do you want to search for drivers?	
	→ <u>Search automatically for updated driver software</u> Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.	
	→ B <u>r</u> owse my computer for driver software Locate and install driver software manually.	
		Cancel

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



6. Locate the folder containing MyEID Driver files.

		\times
←	Update Drivers – Unknown Smart Card	
	Browse for drivers on your computer	
	Search for drivers in this location:	
	C:\temp\2-2-0 with 4K RSA\driver folder	
	✓ Include subfolders	
	→ Let me pick from a list of available drivers on my computer This list will show available drivers compatible with the device, and all drivers in the same category as the device.	
	<u>N</u> ext Cance	

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

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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.

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



5.9.2023

3. Select your PIN codes.

Card initialization	?	×
Hide PINs		
User PIN (PIN #1)	Confirm User PIN (PIN #1)	
1111		
User PUK	Confirm User PUK	
12345678]	
Signature PIN (optional)	Confirm Signature PIN (PIN #	2)
2222		
Signature PUK	Confirm Signature PUK	
12345678		
Administrator PIN / KEY		
Challenge/Response	Challenge length 8	-
Admin key source		
User input	O Encrypted key file	
Administrator key.		
000102030405060708090A0B0C0D0E0	F1011121314151617	
Confirm Administrator PIN / KEY		
Administrator PUK		
12345678		
Confirm Administrator PUK		
Clear PINs and PUKs		
Activate applet		
Create msroots file		
	ОК	Cancel

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.

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



MyEID Getting Started Guide

10

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.

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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



3. The Certificates management console snap-in opens.

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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



Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



5. The wizard opens. Press Next.

		—		\times
🗐 C	Certificate Enrollment			
	Before You Begin			
	The following steps will help you install certificates, which are digital credentials used networks, protect content, establish identity, and do other security-related tasks.	to conne	ct to wire	less
	Before requesting a certificate, verify the following:			
	Your computer is connected to the network You have credentials that can be used to verify your right to obtain the certificate			
		Next	Can	cel

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



MyEID Getting Started Guide

14

6. Press Next.

		—		×
🔄 Ce	ertificate Enrollment			
	Select Certificate Enrollment Policy			
	Certificate enrollment policy enables enrollment for certificates based on predefined of Certificate enrollment policy may already be configured for you.	ertificate	template	s.
	Configured by your administrator			
	Active Directory Enrollment Policy			*
	Configured by you		Add Ne	ew
		<u>N</u> ext	Cano	el:

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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.

		_		\times
🔄 Certificate Enrollment				
Request Certificates				
You can request the following click Enroll.	types of certificates. Select the certificates you want	t to request, a	and then	
Smartcard User	i) STATUS: Available	۵	etails 🔺	
The following options de	scribe the uses and validity period that apply to this	type of cert	ificate:	
Key usage:	Digital signature			
Application policies:	Key encipherment Secure Email			
	Client Authentication			
Validity period (days):	365			
runary period (days).		<u>P</u> rop	erties	_
SmartcardSigner	(i) STATUS: Available	D	etails 💌	•
Show <u>a</u> ll templates		·		
		<u>E</u> nroll	Can	cel

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



Certificat	e Propert	ties					\times
General	Subject	Extensions	Private Key	Certification Autho	rity		
Select	cryptogra	phic service	provider (CS	P):			^
Mi	crosoft St	rong Crypto	graphic Prov	ider (Encryption)		^	
	crosoft Ba	ase Cryptogr	aphic Provid	er v1.0 (Encryption)		
	crosoft Ba	ase DSS and	Diffie-Hellma	in Cryptographic P wider (Engruption)	rovider (Encryption)		
	crosoft DI	H SChannel	Crypto Pro Cryptographi	c Provider (Encryption)	tion)		
	crosoft Er	nhanced Cry	ptographic P	rovider v1.0 (Encry	ption)	~	
	w all CSP	5					
Key <u>o</u>	otions					~	
Set the	key leng	th and expo	rt options for	the private key.			
Key siz	e: 2048			~			
🗌 Mak	e private	key exportal	ble				
Allo	w private	key to be ar	chived				
Stro	ng privat	e key protec	tion				
							~
				01	Canad		
				OK	Cancel	Apply	

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.

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



9. Press "Enroll". Certificate enrollment begins.

ficate Enrollment			
equesting certificates. Please w	ait		
ne enrollment server is being contacted t	o obtain the certificates you have req	uested.	
Active Directory Enrollment Policy			
Avedemo2012 Smartcard User	③ STATUS: Enrolling		
			_
			C

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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



Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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.

			_		\times
🔄 Ce	ertificate Enrollment				
	Requesting certificates. Please wait				
	The enrollment server is being contacted to o	btain the certificates you have requested	l.		
	Active Directory Enrollment Policy				
	Avedemo2012 Smartcard User	i STATUS: Enrolling			
				Can	cel

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



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

			—		Х
🔄 Ce	rtificate Enrollment				
	Certificate Installation Results				
	The following certificates have been enrolled a	nd installed on this computer.			
	Active Directory Enrollment Policy				
	Avedemo2012 Smartcard User	STATUS: Succeeded		Details	~
				<u>F</u> ini:	sh

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland



7 Troubleshooting

7.1The 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.

Aventra Ltd. Kutomotie 16 00380 Helsinki Finland