Logging into Windows domain with eID smart card

Technical overview

Document information	
Date of creation	21.01.2019
Receivers	RIA
Author	Urmas Vanem, OctoX
Version	22.09/1

Version information

Date	Version	Changes/Notices
21.01.2019	19.01/1	Public version, bases on software version 18.12.
10.03.2022	22.03/1	Updated version, bases on software version eID-22.1.0.1922. Changed by: Urmas Vanem
14.09.2022	22.09/1	Added description of new requirements from Microsoft for mapping user and eID card certificate. Changed by: Urmas Vanem

Background

Since Windows Server 2008 SP2 and Windows Vista SP2 we can use Estonian eID cards for Windows domain login. This possibility has been actual since autumn 2008, when first successful tests were made. This document describes platforms and configurations which ones enable Windows domain login, we can do it using only standard Microsoft and eID software.

Logging into Windows domain using eID card is currently quite popular in Estonian enterprises. Using smart card for domain logging has many benefits, like users do not need remember their password and change it regularly, two factor authentication is more secure etc. Creating technical configuration is also not too hard using the guidance you currently read.

Windows domain logging with eID smart card is supporter and tested on following platforms:

- Servers: All supported Windows Server versions including Windows Server 2022.
- Clients: All supported Windows operating systems including Windows 11.

Implementation

Configuring ID login requires a set of systemic preparations for both the domain and client computers. In addition, domain user accounts must be linked to eID authentication certificates.

To enable eID card logging into Windows domain following options must be enabled:

- Domain controllers must have specific certificate to identify themselves, certificate must also be trusted by clients/computers.
- Domain controllers must trust root and intermediate level certificates from eID card chains.
- Client computers must have supported eID card management software installed (today, 02.09.2022 we recommend version 22.6.0.1930).
- Client computers must support certificates that do not have a special Smart Card Logon EKU property and the use of ECC certificates for logging purposes into computers must also be allowed.
- In the domain, the authentication certificate of the eID card must be linked to specific user in a certain way.

In following chapters, we describe exact steps to create working configuration for eID domain logging.

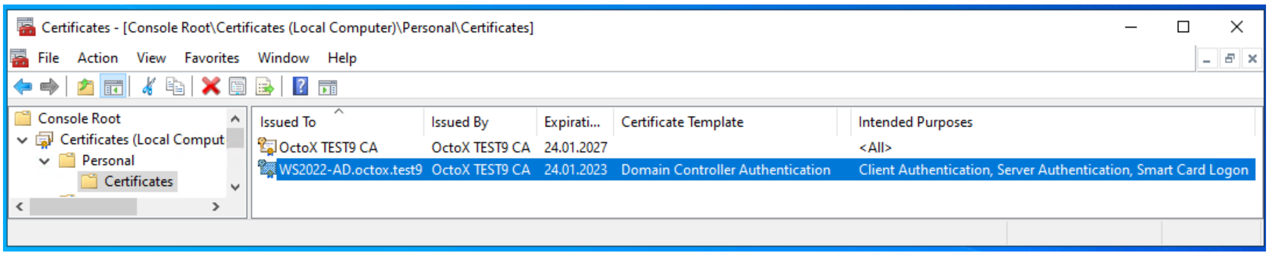
Domain settings

To prepare Windows domain for eID logging we must create specific policies for domain controllers and client computers. As prerequisite domain controller must have specific certificate (*server authentication*, *smart card logon*) to identify itself and allow smart card logon.

Domain controller certificate

As already mentioned, domain controllers need certificates, with which they can prove their identity and enable smart card logon for client clients/computers. The most common way to ask for these certificates is to use local PKI solution. If PKI services have been implemented in Windows domain, it will be easy to assign mandatory certificate to domain controllers. By default, *Domain Controller Authentication* certificate template, which one fulfills all needs for eID logging, can be published for domain controllers. If certificate autoenrollment for domain controllers is enabled (and if certificate template is published in domain of course), then all domain controllers automatically install mandatory certificate. If not, certificate can be requested manually.

Domain controller certificates can be found from domain controller certificates personal store:


Certificates - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Issued To	Issued By	Expirati...	Certificate Template	Intended Purposes
OctoX TEST9 CA	OctoX TEST9 CA	24.01.2027		<All>
WS2022-AD.octox.test9	OctoX TEST9 CA	24.01.2023	Domain Controller Authentication	Client Authentication, Server Authentication, Smart Card Logon

Picture 1 – domain controller authentication certificate in personal store

If PKI services are not implemented in domain, it can be good idea to change the situation now. It can also be possible to get mandatory certificate from other sources.

Policies

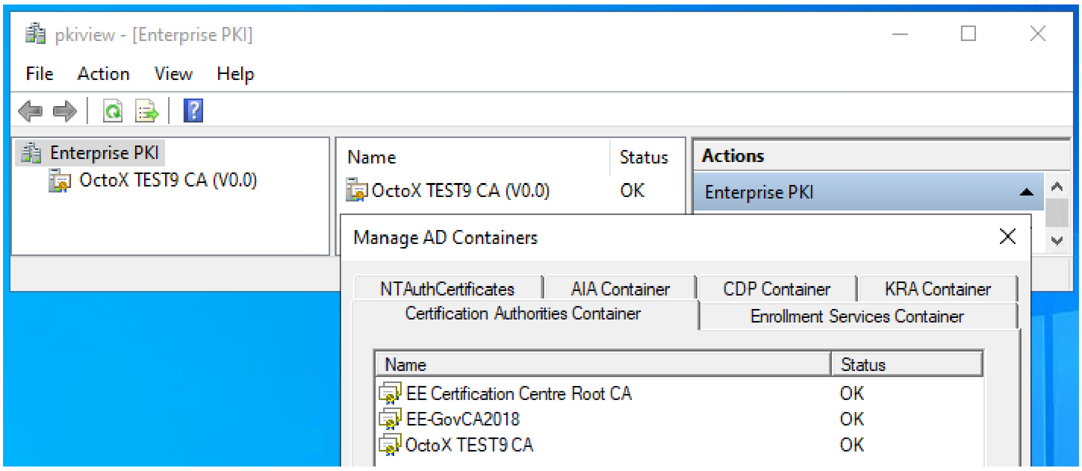
Publishing certificates

To use eID cards and related certificates for domain logging, domain controllers must trust those certificates. Both root and intermediate certificates form eID certificate chains must be trusted, installed into correct certificate containers. Domain controllers must also have access to the OCSP service and/or certificate revocation lists (CRLs) described in certificates to check the validity of certificates.

In order to enable domain logging with an eID card, intermediate level certificates (ESTEID-SK 2015 and ESTEID2018) must be installed in the NTAuthCertificates container of the domain. We can do this with the command “certutil -dspublish -f ’CERTIFICATE NAME’ NTAuthCA”. We can also add a root-level certificates to the domain container with command "certutil -dspublish -f 'CERTIFICATE NAME' RootCA".

Certificates can be downloaded from http://www.sk.ee/certs. Today, we need the following certificates from two chains:

- “Old” chain (Gemalto):
  - EE Certification Center Root CA - trusted root certificate;
  - ESTEID-SK 2015 – intermediate level certificate.
- "New" chain (Idemia):
  - EE-GovCA2018 - trusted root certificate;
  - ESTEID2018 - intermediate level certificate.



Name	Status
OctoX TEST9 CA (V0.0)	OK

Name	Status
EE Certification Centre Root CA	OK
EE-GovCA2018	OK
OctoX TEST9 CA	OK

Picture 2 – root certificates in AD containers

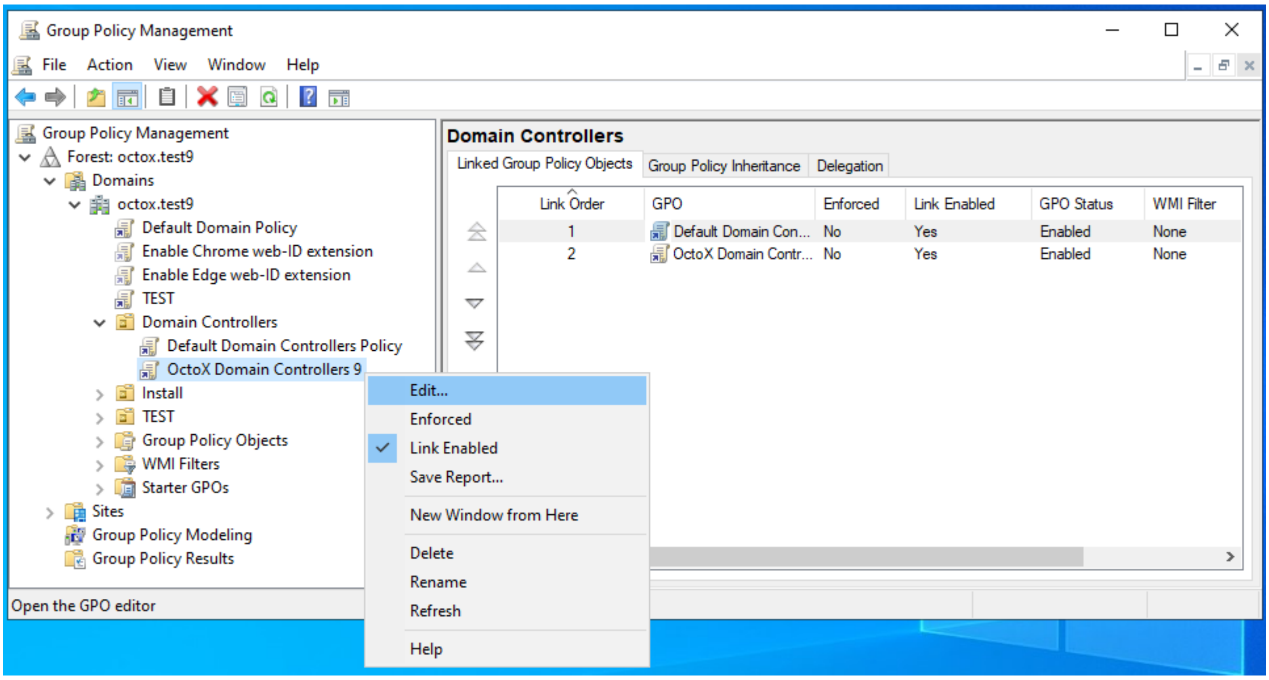
In addition, both SK root and intermediate certificates can be published in the domain for domain controllers and/or all other Windows computers or computer groups using group policies.[1]

So, if we want to publish certificates to domain controllers automatically with group policy, we recommend that you modify the Default Domain Controllers or any other OU-level policy for domain controllers. Certificates must be placed into containers according to the list and type, root certificates into *Trusted Root Certification Authorities* and intermediate certificates into *Intermediate Certification Authorities* container.

Here's how to publish root and intermediate certificates. To publish certificates in the Trusted and Intermediate Certificate stores on domain controllers:

1. Open the Group Policy Management console and select the appropriate GPO, click Edit ...:

[1] If we have already published both the middle and root level certificates in the domain using the previously described method, there is no direct need for republishing. We can, however, publish the intermediate certificate by placing it in the domain NTAuthCertificates container and the root certificate with a normal domain policy, as described below. It's actually a bit confusing, because although in theory Microsoft requires that the CA certificate that issued the card certificate belongs to the NTAuthCertificates container in the domain (check https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/enabling-smart-card-logon-third-party-certification-authorities), then in practice the login with the eID card works even if it hasn't been done and the chain is simply trusted. Anyway, we recommend to follow Microsoft's technical requirements when creating eID login configuration.



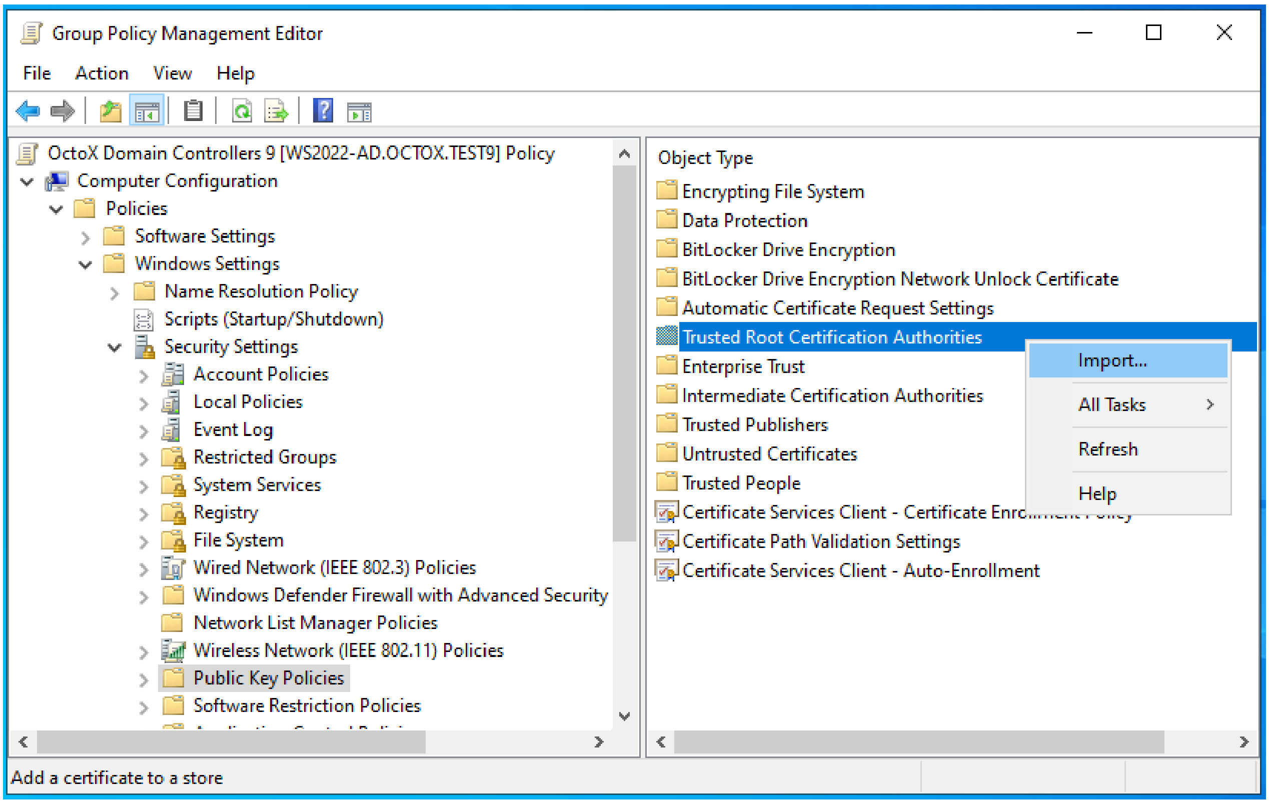
Domain Controllers

Linked Group Policy Objects | Group Policy Inheritance | Delegation

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Default Domain Con...	No	Yes	Enabled	None
2	OctoX Domain Contr...	No	Yes	Enabled	None

Picture 3 – starting GPO editing

2. Select folder „*Computer Configuration/Policies/Windows Settings/Security Setting/Public Key Policies*“

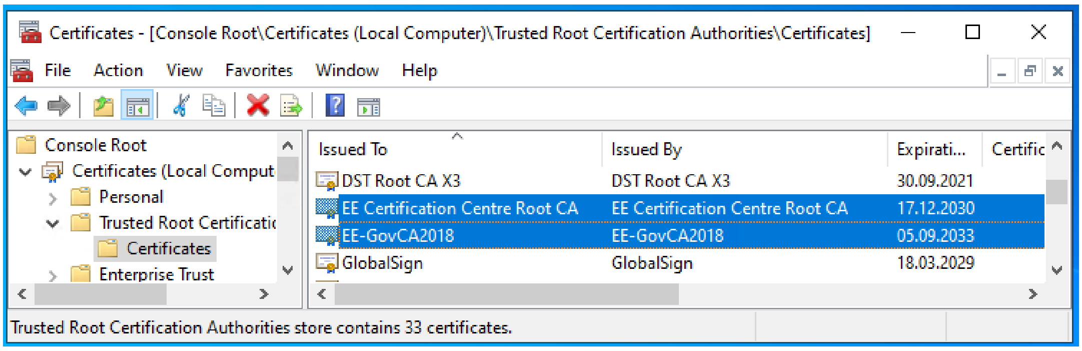


Group Policy Management Editor
File
Action
View
Help
OctoX Domain Controllers 9 [WS2022-AD.OCTOX.TEST9] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment
Import...
All Tasks
Refresh
Help

Add a certificate to a store

Picture 4 – starting certificate import

3. To import „EE Certification Centre Root CA“ and EE-GovCA2018 certificates:
   a. Right-click on folder *Trusted Root Certification Authorities* ja select *Import;*
      i. Click *Next*, select „EE Certification Centre Root CA“ certificate and import it.
      ii. Click *Next*, select „EE-GovCA2018“ certificate and import it.



Certificates - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Comput
Personal
Trusted Root Certificatio
Certificates
Enterprise Trust

Issued To	Issued By	Expirati...	Certific
DST Root CA X3	DST Root CA X3	30.09.2021	
EE Certification Centre Root CA	EE Certification Centre Root CA	17.12.2030	
EE-GovCA2018	EE-GovCA2018	05.09.2033	
GlobalSign	GlobalSign	18.03.2029	

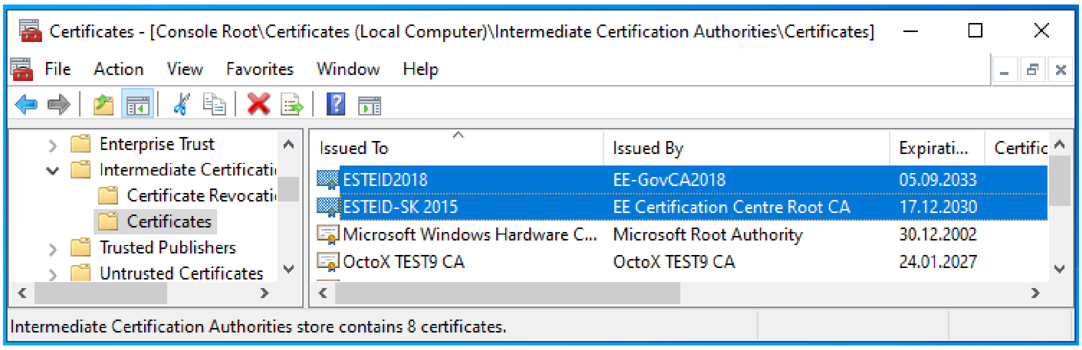
Trusted Root Certification Authorities store contains 33 certificates.

Picture 5 - root level certificates are correctly published

4. To add intermediate certificates:
   a. Right-click on folder *Intermediate Certification Authorities* ja select *Import;*

iii. Click *Next*, select „ESTEID-SK 2015“ certificate and import it.

iv. Click *Next*, select „ESTEID2018“ certificate and import it.



Issued To	Issued By	Expirati...	Certific
ESTEID2018	EE-GovCA2018	05.09.2033	
ESTEID-SK 2015	EE Certification Centre Root CA	17.12.2030	
Microsoft Windows Hardware C...	Microsoft Root Authority	30.12.2002	
OctoX TEST9 CA	OctoX TEST9 CA	24.01.2027	

Intermediate Certification Authorities store contains 8 certificates.

Picture 6 - intermediate level certificates are correctly published

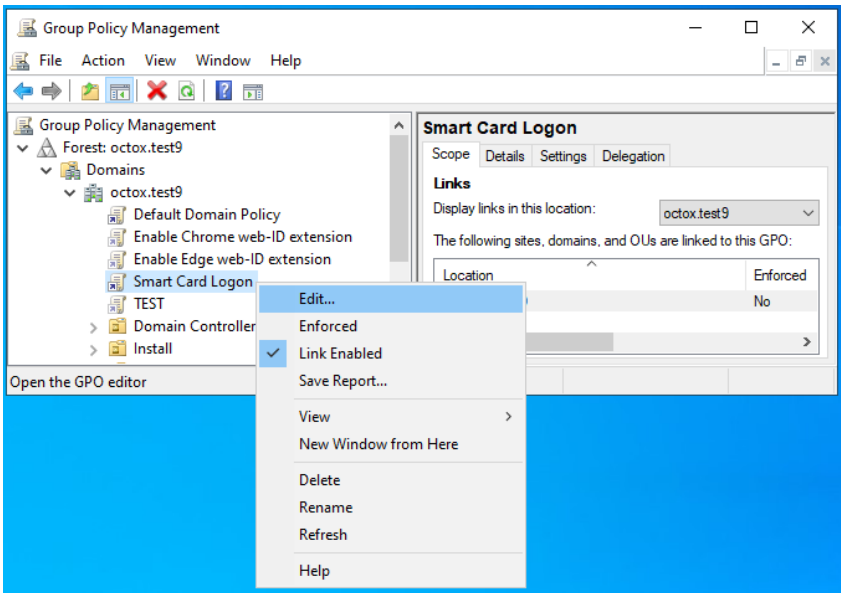
As you can see in the previous illustrations, the certificates become visible in the *Trusted Root Certification Authorities* and *Intermediate Certificate Authorities* containers, respectively. With next policy cycle the settings will be applied to all domain controllers. We can force policies by running gpupdate (/force) on domain controllers. And as already said, in the same way the required certificates can be published to all other Windows workstations and servers.

Configuring eID card properties in domain

To support eID card domain logging centrally on all client computers, we use a domain-level policy in our example [2]:

1. Open the Group Policy Management console and select the appropriate GPO to add properties, click Edit:

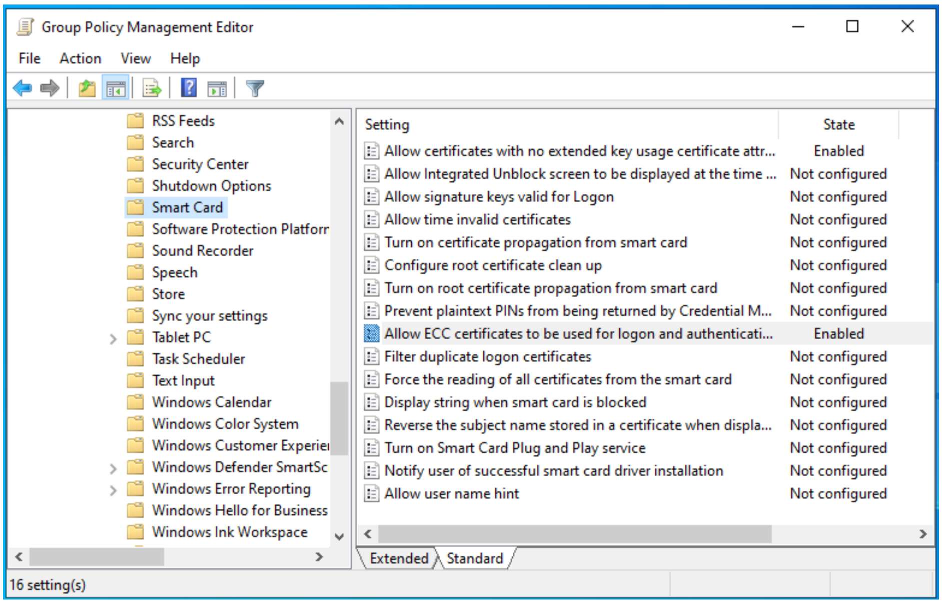
[2] Of course, we can apply policy from any level or group we like, for only client computers for example.



Picture 7 - selecting GPO, starting editing

2. Select folder *„Computer Configuration/Policies/Administrative Templates/Windows Components/Smart Card*“ and add following configuration:
    a. *„Allow certificates with no extended key usage certificate attribute = Enabled“* – to enable certificates without *„Smart Card Logon“ setting in EKU;*
    b. *„Allow ECC certificates to be used for logon and authentication = Enabled“ – to enable using certificates based on ECC cryptography for logon.*

After changes our policy should look like presented on following picture:



Setting	State
Allow certificates with no extended key usage certificate attr...	Enabled
Allow Integrated Unblock screen to be displayed at the time ...	Not configured
Allow signature keys valid for Logon	Not configured
Allow time invalid certificates	Not configured
Turn on certificate propagation from smart card	Not configured
Configure root certificate clean up	Not configured
Turn on root certificate propagation from smart card	Not configured
Prevent plaintext PINs from being returned by Credential M...	Not configured
Allow ECC certificates to be used for logon and authenticati...	Enabled
Filter duplicate logon certificates	Not configured
Force the reading of all certificates from the smart card	Not configured
Display string when smart card is blocked	Not configured
Reverse the subject name stored in a certificate when displa...	Not configured
Turn on Smart Card Plug and Play service	Not configured
Notify user of successful smart card driver installation	Not configured
Allow user name hint	Not configured

Picture 8 - smart card settings in policy

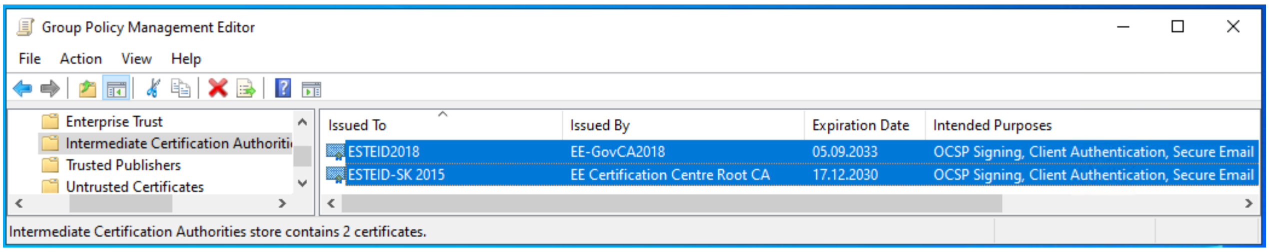
Supporting eID card domain logging in single computer

If you want to support eID card to log in from a non-domain, for example from home computer to any domain server over an RDP connection, you must configure the home computer to support eID cards. To do this, run the local policy manager gpedit.msc as an administrator on the computer. In the policy manager, the exact same change as described in the upper chapter (setting the properties of the eID card) must be made in the computer configuration, "Allow certificates with no extended key usage certificate attribute" and also "Allow ECC certificates to be used for logon and authentication" must be enabled! After making the described change, you must wait for policy to apply, update the policies with the “gpupdate / force” command or restart the computer. Now it is possible to log into domain servers with an eID card (if supported by domain and server of course).

Requiring OCSP revocation check

To configure OCSP-based certificate validation requirement, the properties of published intermediate certificates must be set as follows:

1. Open the policy where intermediate eID certificates are described for domain controllers and select „Computer Configuration / Policies / Windows Settings / Security Settings / Public Key Policies / Intermediate Certification Authorities / Certificates" folder:



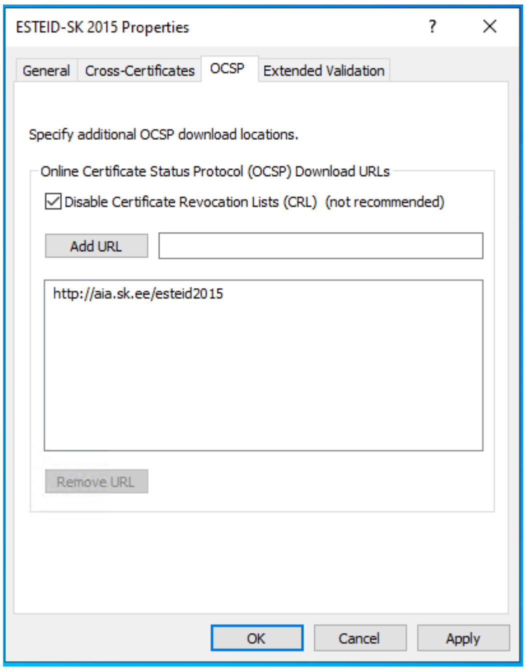
Group Policy Management Editor

Issued To	Issued By	Expiration Date	Intended Purposes
ESTEID2018	EE-GovCA2018	05.09.2033	OCSP Signing, Client Authentication, Secure Email
ESTEID-SK 2015	EE Certification Centre Root CA	17.12.2030	OCSP Signing, Client Authentication, Secure Email

Intermediate Certification Authorities store contains 2 certificates.

Picture 9 – policy with published intermediate certificates

2. Open properties for certificate „ESTEID-SK 2015“ and select tab *OCSP*. Add path http://aia.sk.ee/esteid2015 to define OCSP server and disable certificate revocation lists:



ESTEID-SK 2015 Properties

Specify additional OCSP download locations.

Online Certificate Status Protocol (OCSP) Download URLs

☑ Disable Certificate Revocation Lists (CRL) (not recommended)

http://aia.sk.ee/esteid2015

Picture 10 - intermediate certificate settings, defining OCSP server

Notes

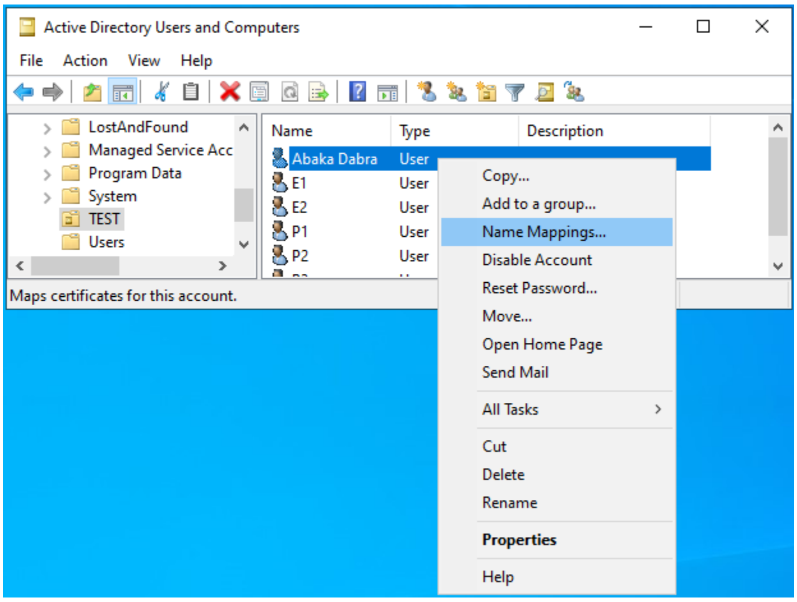
- For certificates issued from the end of 2018, we no longer need to describe the OCSP path centrally, as it is already included in the certificate. There is no CRL path in those certificates.
- Both OCSP and CRL paths are described inside the 2015 chain certificates. The above configuration for the 2015 chain certificate only makes sense if we want to disable the use of CRL revocation check.
- Our guidance here describes so-called free OCSP service. If you need a high-availability OCSP, you can get more information at https://www.skidsolutions.eu/en/services/validity-confirmation-services. If you have already this service, use http://ocsp.sk.ee as the OCSP path for both 2018 and 2015 chains.

- If using OCSP, familiarize yourself with the concept of OCSP magic number also[3].

The advantage of using OCSP over a CRL[4]-based solution is greater security, the validity of the certificate is checked "more" in real time. Updated CRLs are generated twice a day and must be downloaded twice a day. However, with the CRL verification method, the user can log in for up to almost 12 hours with a certificate that is no longer valid (cycle between CRL list updates). In the case of OCSP-based certificate revocation verification, the certificate status is validated near real time by OCSP service, which may be more efficient and is certainly more secure in a temporal view.

Mapping users and certificates

Due to the Microsoft software updates described in article KB5014754, it is no longer recommended to use the AD GUI to associate a user with a certificate (as of 05.09.2022). With AD GUI the *issuer* and *subject* fields from user certificate are mapped to user. From now on, however, it is considered insecure. Recommended way is to map user account with *issuer* and *serialnumber* fields of the certificate.



Name	Type	Description
Abaka Dabra	User	
E1	User	
E2	User	
P1	User	
P2	User	

Maps certificates for this account.

Picture 11 – example of AD GUI

There are different ways to get a user eID authentication certificate:

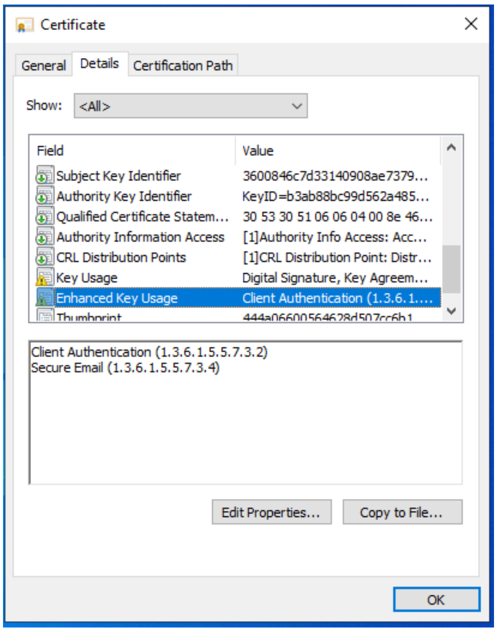
1. Request a user certificate from the central LDAP database using personal identification code.

[3] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee619754(v=ws.10)

[4] Certificate Revocation List

2. If the ID card has been previously registered on the computer, the certificate can also be obtained from the user certificate store using MMC (Certificates snap-in, Personal / Certificates).
3. With the command "certutil.exe –scinfo" if the eID card is in the reader.
4. …

I would like to draw attention to the fact that eID cards have two certificates. To log into domain with eID card, we must use the certificate with *Client Authentication* described under EKU.



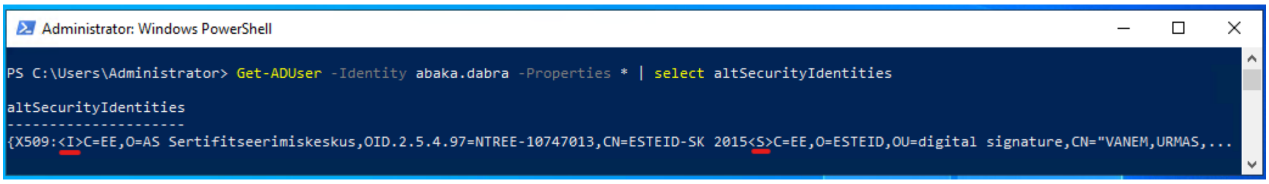
Field	Value
Subject Key Identifier	3600846c7d33140908ae7379...
Authority Key Identifier	KeyID=b3ab88bc99d562a485...
Qualified Certificate Statem...	30 53 30 51 06 06 04 00 8e 46...
Authority Information Access	[1]Authority Info Access: Acc...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Key Usage	Digital Signature, Key Agreem...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Thumbprint	444a06600564628d507cc6b1

Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)

Picture 12 – EKU contains Client Authentication

How to map user and authentication eID certificate

As already stated, using the AD GUI, the certificate is associated with the user using the *Issuer* and *Subject* fields, and this combination is no longer recommended by Microsoft. In addition, in the case of Estonian eID cards, *issuer* field is identical at least on the ID card and on the Digi-Id card.



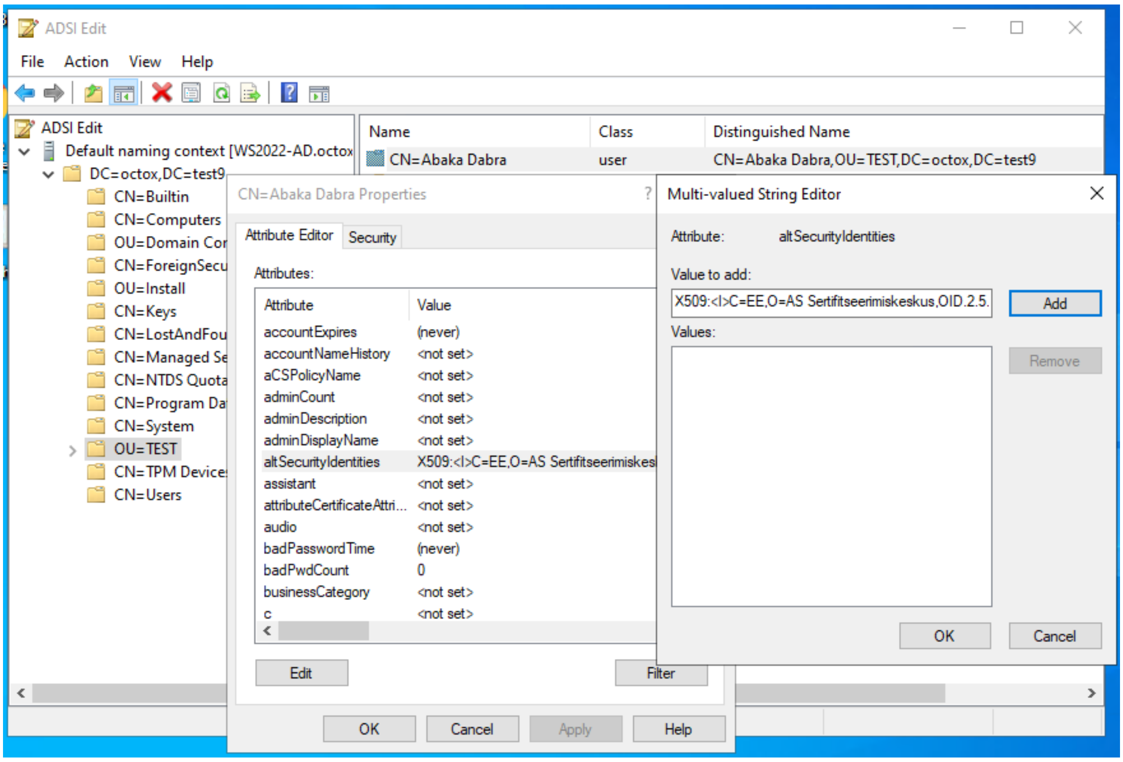
```
PS C:\Users\Administrator> Get-ADUser -Identity abaka.dabra -Properties * | select altSecurityIdentities

altSecurityIdentities
---------------------
{X509:<I>C=EE,O=AS Sertifitseerimiskeskus,OID.2.5.4.97=NTREE-10747013,CN=ESTEID-SK 2015<S>C=EE,O=ESTEID,OU=digital signature,CN="VANEM,URMAS,...
```

Picture 13 - <I> ja <S> are pointing to certificate fields Issuer ja Subject.

So, it is probably reasonable to follow Microsoft's recommendation and associate the certificate with the user using the *issuer* and *serialnumber* fields. We can do this via the *ADSI Edit* GUI. It should be noted that both *issuer* and *serialnumber* strings must be reversed when pairing! This means that if:

1. Issuer is described in the certificate as "CN = ESTEID-SK 2015 / 2.5.4.97 = NTREE-10747013 / O = AS Sertifitseerimiskeskus / C = EE", in AD it must be "<I>C=EE,O= AS Sertifiseterimiskeskus,OID.2.5.4.97=NTREE-10747013,CN=ESTEID-SK 2015";
2. The serial number is described in the certificate as 8958ee38a565845e9107720de61ca64d, in AD it must be 4da61ce60d7207915e8465a538ee5889. Please also pay attention to the fact that the reversal takes place two symbols at a time!

The correct user and certificate binding string in the *ADSI Edit* utility looks like this for the 2015 chain: "X509:<I>C=EE,O=AS Sertifitseerimiskeskus,OID.2.5.4.97=NTREE-10747013,CN=ESTEID-SK 2015<SR>4da61ce60d7207915e8465a538ee5889".[5]



Name	Class	Distinguished Name
CN=Abaka Dabra	user	CN=Abaka Dabra,OU=TEST,DC=octox,DC=test9

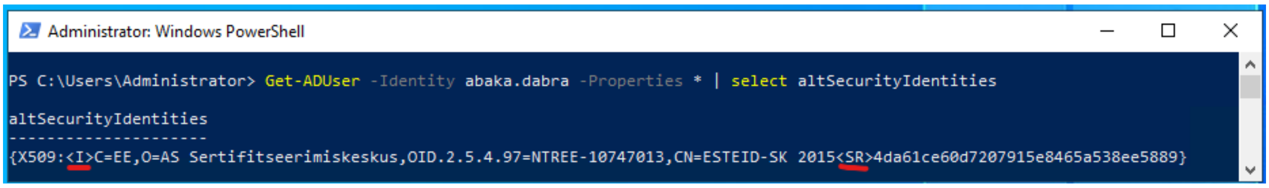
Attribute	Value
accountExpires	(never)
accountNameHistory	<not set>
aCSPolicyName	<not set>
adminCount	<not set>
adminDescription	<not set>
adminDisplayName	<not set>
altSecurityIdentities	X509:<I>C=EE,O=AS Sertifitseerimiskes
assistant	<not set>
attributeCertificateAttri...	<not set>
audio	<not set>
badPasswordTime	(never)
badPwdCount	0
businessCategory	<not set>
c	<not set>

Attribute: altSecurityIdentities

Value to add: X509:<I>C=EE,O=AS Sertifitseerimiskeskus,OID.2.5.

Picture 14 – modifying altSecurityIdentities value with ADSI Edit

[5] If, as a rule, we have the *issuer* as a constant (across the chain), then the *serialnumber* must be changed for every user. There are certainly several automation measures here, but as an example, I'll give Excel's way to make this change: "=CONCAT(MID(B4;31;2);MID(B4;29;2);MID(B4;27;2);MID(B4;25;2);MID(B4;23;2);MID(B4;21;2);MID(B4;19;2);MID(B4;17;2);MID(B4;15;2);MID(B4;13;2);MID(B4;11;2);MID(B4;9;2);MID(B4;7;2);MID(B4;5;2);MID(B4; 3;2);MID(B4;1;2))", where B4 is then the cell where the original serial number is located.



```
PS C:\Users\Administrator> Get-ADUser -Identity abaka.dabra -Properties * | select altSecurityIdentities

altSecurityIdentities
---------------------
{X509:<I>C=EE,O=AS Sertifitseerimiskeskus,OID.2.5.4.97=NTREE-10747013,CN=ESTEID-SK 2015<SR>4da61ce60d7207915e8465a538ee5889}
```

Picture 15 - <I> ja <SR> are pointing to certificate fields Issuer ja SerialNumber.

For larger environments and bigger number of users, you must definitely think about automating the previously described activities!

Preparing client computers

Software

The eID card management software must be installed on the client computers (today, 02.09.2022 we recommend version 22.6.0.1930) and minidrivers must work correctly.

Settings

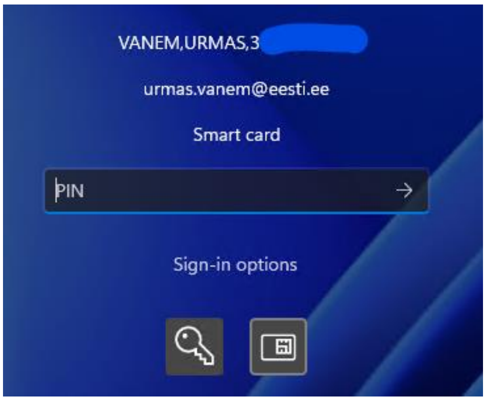
All required configurations apply to client computers at the domain level with the predefined central policies described above.

Final implementation

To actually implement the ID login, just do it as it is described previously. Obvious prerequisites are:

1. Testing the solution in a test and/or development environment;
2. Implementation of the solution in the work environment;
3. Training of administrators;
4. Training of users.

After the configuration takes effect on the client computer, we can select the smart card as the login method in the login window .



VANEM,URMAS,3[redacted]

urmas.vanem@eesti.ee

Smart card

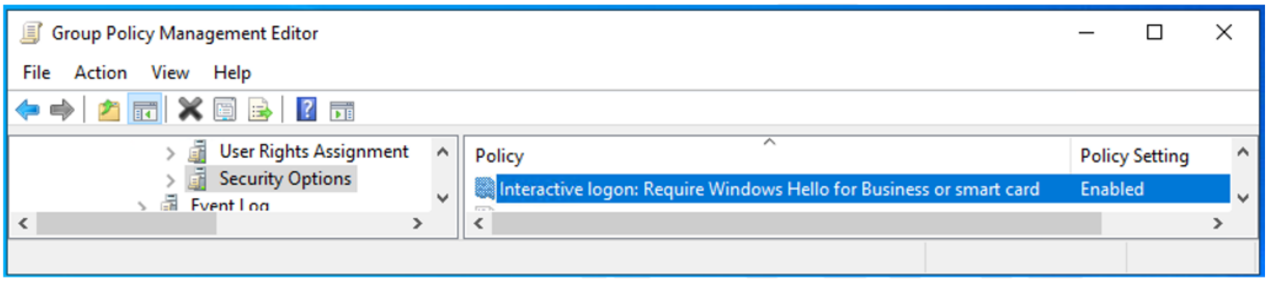
PIN

Picture 16 – eID card domain login window, waiting for PIN

Requiring eID card for domain logging

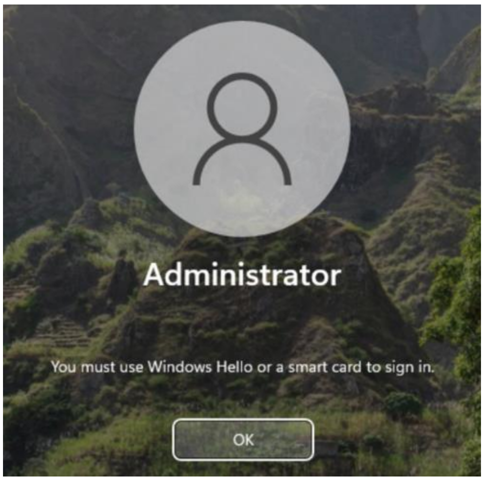
Sometimes we may want users to be able to log in to systems only with an eID card (in other words, we prohibit the use of user passwords). This can be applied to common or specific workstations and/or RDP servers. To apply the requirement, the following policy must be applied to the desired computers:

"Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Security Options : Interactive logon: Require Windows Hello for Business or Smart Card" = Enabled.



Policy	Policy Setting
Interactive logon: Require Windows Hello for Business or smart card	Enabled

Picture 17 – a username and password are no longer enough to log into a computer or server!


Administrator

You must use Windows Hello or a smart card to sign in.

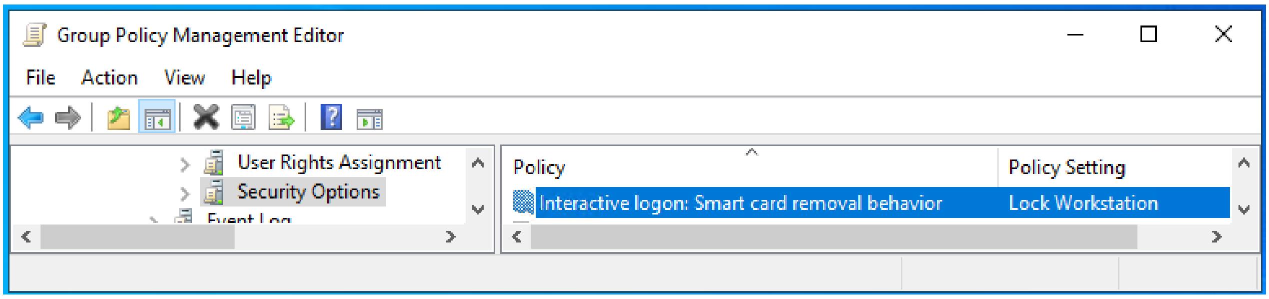
Picture 18 – error message in case user tries to log into domain with username and password, but smart card is required

Controlling the behavior of the computer when the smart card is removed

We can also configure the behavior of a computer or a group of computers when the smart card is removed. (It works of course only, when we use smart card for domain logon.) Options include:

1. No Action (default);
2. Lock Workstation;
3. Force Logoff;
4. Disconnect if a remote Remote Desktop Services session.

To apply the change, one of the above values must be set to the policy "Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Security Options : Interactive logon: Smart card removal behavior".



Policy	Policy Setting
Interactive logon: Smart card removal behavior	Lock Workstation

Picture 19 – in this example, after applying the policy, removing the smart card from reader the computer locks

Possible problems

Proxy

If the domain has a proxy configured to access external HTTP sites and this policy also applies to the domain controllers' system account, the certificate will not be validated and the login will fail.

What to do: Create a proxy setup for your domain controllers. See netsh.exe options.

Same certificate is mapped to more than one user

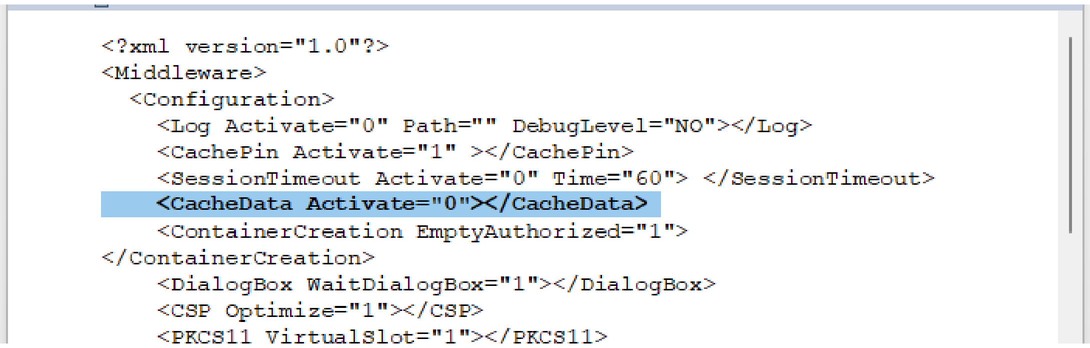
If one authentication certificate is associated with more than one user in the domain, logging into domain with eID card will fail.

What to do: Remove the certificate association from the "wrong" user(s).

Mess with 2018 certificates and RDP login

There may be a problem of "certificate confusion" for the first portions of certificates issued from the 2018 chain. Under certain conditions, the certificate cannot be associated with correct user and the user may be shown a description of other logged in user while trying to log on. This problem is mainly detected on RDP (terminal) servers.

You must disable the use of caching in Idemia software to overcome this problem. To do this, modify parameter "CacheData Activate" value to 0 in the OCSMiddlewareConf.xml configuration file on the RDP server or workstation. The configuration file can be found in "C:\Program Files (x86)\IDEMIA\AWP" or "C:\Program Files\IDEMIA\AWP" folder. You must restart your computer or server for the change to take effect.



```
<?xml version="1.0"?>
<Middleware>
  <Configuration>
    <Log Activate="0" Path="" DebugLevel="NO"></Log>
    <CachePin Activate="1" ></CachePin>
    <SessionTimeout Activate="0" Time="60"> </SessionTimeout>
    <CacheData Activate="0"></CacheData>
    <ContainerCreation EmptyAuthorized="1">
</ContainerCreation>
    <DialogBox WaitDialogBox="1"></DialogBox>
    <CSP Optimize="1"></CSP>
    <PKCS11 VirtualSlot="1"></PKCS11>
```

Picture 20 – disabling caching in Idemia software

Summary

Domain login based on eID smartcards is a good way to simplify user domain logging process and increase system security at the same time.

In the users' view, it is definitely a convenient feature to avoid forgetting the password - all you need to remember is the authorization PIN (which eID card users probably know anyway).

The experience of system administrators and support persons is also expected to be positive, as in addition to the increase in security, there are fewer problems with users who forget their passwords. Creating such a configuration is also quite easy. And interesting :)