eID KAARDIGA WINDOWS DOMEENI LOGIMINE

Tehniline ülevaade

Dokumendi info	
Loomise aeg	21.01.2019
Tellija	RIA
Autor	Urmas Vanem, OctoX
Versioon	22.09/1

Versiooni info		
Kuupäev	**Versioon**	**Muutused/märkused**
21.01.2019	19.01/1	Avalik versioon, baseerub 18.12 tarkvaral
10.03.2022	22.03/1	Uuendatud versioon, baseerub EID-22.1.0.1922 tarkvaral. Muutja: Urmas Vanem
14.09.2022	22.09/1	Lisatud uute Microsoft poolsete nõuete kirjeldus kasutaja ja eID kaardi sertifikaadi sidumiseks. Muutja: Urmas Vanem

Taust

Alates Windows Server 2008 SP2 ja Windows Vista SP2 sümbioosist on võimalik kasutada Eesti eID kaarte domeeni sisselogimiseks. See teema on olnud aktuaalne juba 2008 aasta sügisest, mil tehti ka vastavad esimesed õnnestunud katsetused. Käesolev dokument kirjeldab platvormid ja konfiguratsioonid, millised täna meil eID logimise funktsionaalsust lihtsalt ja edukalt võimaldavad rakendada - kasutusel on vaid Microsofti operatsioonisüsteemid ja eID tarkvara.

eID kaardiga sisselogimine on teenus, mis on tänaseks Eesti ettevõtetes juba üsna levinud. eID logini rakendamisel on palju häid omadusi nagu lihtsustatud sisselogimine – kasutajatel pole vaja enam parooli meeles pidada, turvalisuse kasv tänu kahefaktorilisele autentimisele jpm. Ja ka tehniline konfiguratsioon selle lubamiseks ei ole ülemäära keeruline.

eID login on täna toetatud ja testitud järgmistel platvormidel:

- Serverid: Kõik ametlikult toetatud Windows serverite versioonid, k.a. Windows Server 2022.
- Kliendid: Kõik ametlikult toetatud Windows operatsioonisüsteemide versioonid, k.a. Windows 11.

Rakendamine

ID logini rakendamine eeldab kogumit süsteemseid ettevalmistusi nii domeeni kui klientide häälestusel. Lisaks tuleb kasutajakontod domeenis siduda eID autentimise sertifikaatidega.

eID kaartidega domeeni logimiseks tuleb keskkond konfigureerida järgnevalt:

- Domeeni kontrollerid peavad omama endi tuvastamiseks spetsiifiliste omadustega sertifikaati, mida usaldavad ka kliendid.
- Domeeni kontrollerid peavad usaldama sertifitseerimiskeskuse eID kaartide harude juur- ja kesktasemete sertifikaate.
- Klientarvutitel peab olema installeeritud toetatud eID kaartide haldustarkvara (täna, 02.09.2022 soovitame versiooni 22.6.0.1930).
- Klientarvutid peavad toetama sertifikaate, millistel puudub spetsiaalne kiipkaardiga logimise toe atribuut (*Smart Card Logon EKU*) ja samuti peab lubatud olema ECC sertifikaatide kasutamine arvutisse logimise eesmärgil.
- Domeenis peab eID kaartide autentimissertifikaat olema seotud kindlal viisil kindla kasutajaga.

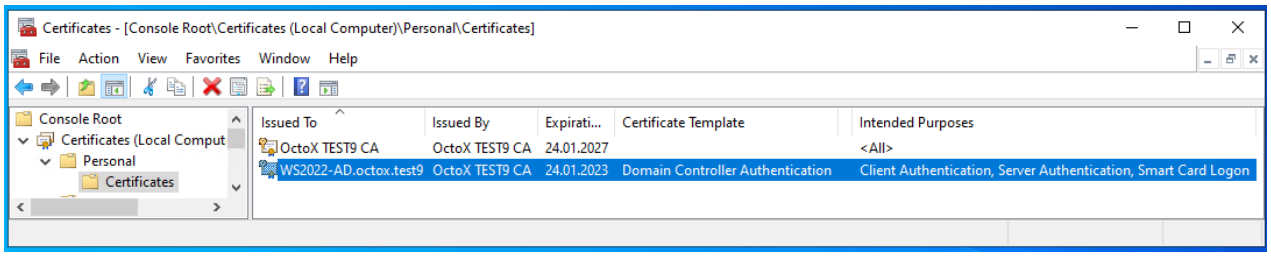
Täpsemalt käsitleme konfiguratsiooni ettevalmistust järgmistes alampunktides.

Domeenist

Domeeni ettevalmistuse osadeks on poliitikate häälestus domeeni kontrolleritele ja töökohtadele. Samuti peab domeeni kontrolleril olema kindlatele omadustele vastav (*server authentication*, *smart card logon*) sertifikaat enda tuvastamiseks ja kiipkaardiga logimise võimaldamiseks.

Domeeni kontrolleri sertifikaat

Nagu juba öeldud, domeeni kontrollerid vajavad eID logini toimimiseks sertifikaate, millistega nad suudavad klientarvutitele endi identiteeti ja kiipkaardiga logimise võimekust tõestada. Kõige mõistlikum tundub võimalusel need sertifikaadid küsida lokaalse PKI lahenduse käest. Vaikimisi Windows CA konfiguratsioonis on võimalik publitseerida „*Domain Controller Authentication*“ mall, mida reeglina küsivad endale kõik domeeni kontrollerid. Juhul kui domeeni kontrolleritel sertifikaatide *autoenrollment* ei ole lubatud, tuleb nimetatud sertifikaadid küsida “käsitsi”. Piltlikult väljendub nõutav domeeni kontrollerite sertifikaatide konfiguratsioon järgmisel joonisel:



Pilt 1 - domeeni kontrolleri autentimissertifikaat domeeni kontrolleri sertifikaadihoidlas

Juhul, kui ettevõttel PKI lahendus puudub, tundub mõistliku otsusena selle loomine. Alternatiivina võib mõelda domeeni kontrolleri sertifikaadi hankimisele kolmandatest allikatest.

Poliitikad

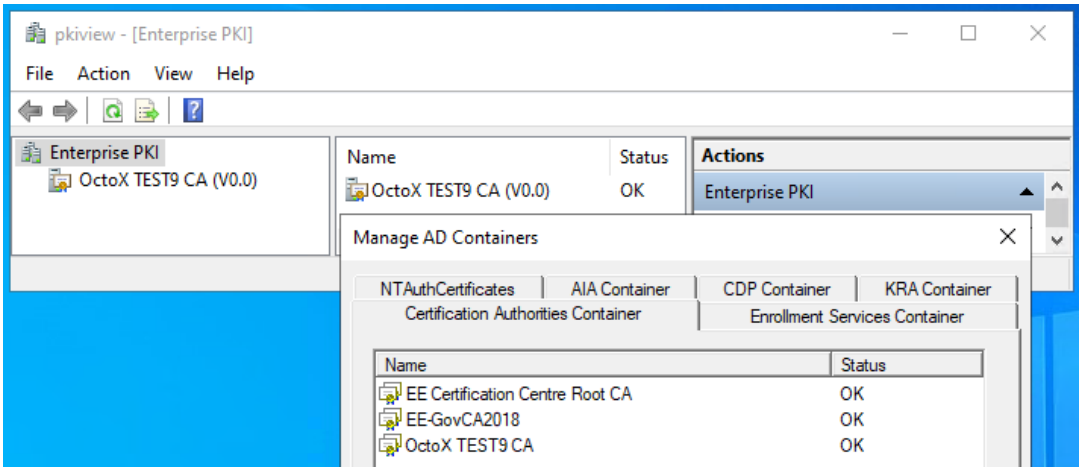
Sertifikaatide publitseerimine

eID kaartide ja nendega seotud sertifikaatide kasutamisel domeeni sisselogimisel peavad domeeni kontrollerid neid usaldama, nii kesk- kui juurtaseme sertifikaadid peavad paiknema õigetes konteinerites. Sertifikaatide kehtivuse kontrolliks peab olema ligipääs SK OCSP teenusele ja/või sertifikaatide tühistusnimekirjadele (CRL).

eID kaardiga domeeni logimise võimaldamiseks tuleb kesktaseme sertifikaadid (ESTEID-SK 2015 ja ESTEID2018) paigaldada ka domeeni NTAuthCertificates konteinerisse. Seda saame teha käsuga „certutil -dspublish -f ’SERDINIMI’ NTAuthCA“. Samuti võime domeeni konteinerisse lisada ka juurtaseme sertifikaadid, siis on käsuks „certutil -dspublish -f ’SERDINIMI’ RootCA“.

Sertifikaadid on allalaetavad lehelt http://www.sk.ee/certs. Tänase seisuga vajame järgmiseid sertifikaate kahest ahelast:

- „Vana“ haru (Gemalto):
    a. EE Certification Centre Root CA – usaldusväärne juursertifikaat;
    b. ESTEID-SK 2015 - usaldusväärne kesktaseme sertifikaat.
- „Uus“ haru (Idemia):
    a. EE-GovCA2018 – usaldusväärne juursertifikaat;
    b. ESTEID2018 - usaldusväärne kesktaseme sertifikaat.



Pilt 2 - juurtaseme sertifikaadid AD konteinerites

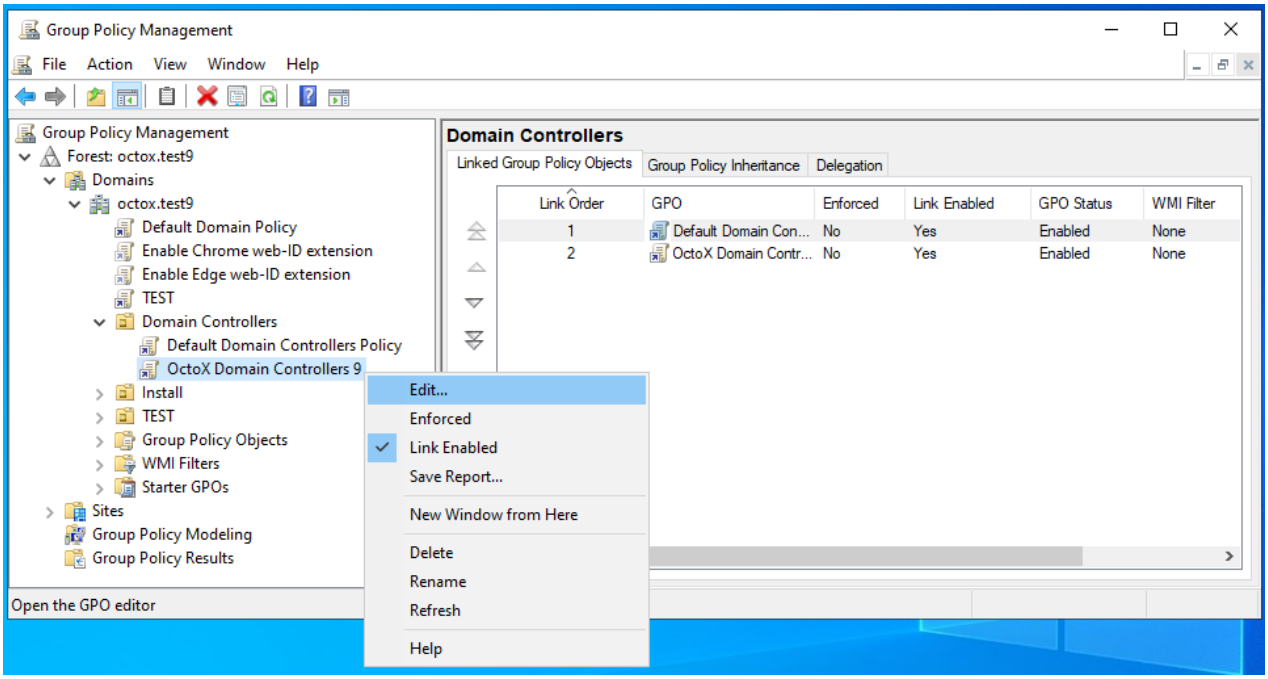
Lisaks võime SK juur- ja kesktaseme sertifikaadid publitseerida kas ainult domeeni kontrolleritele või ka kõikidele domeeni serveritele ja/või tööjaamadele või nende gruppidele kesksete poliitikate abil.[1]

Kui soovime publitseerida sertifikaate domeeni kontrolleritel automaatselt, siis soovitame modifitseerida *Default Domain Controllers* või mõnda teist domeeni kontrollerite OU tasemelt rakenduvat poliitikat. Sertifikaadid tuleb paigutada konteineritesse vastavalt tüübile, juursertifikaadid juur- ja kesktaseme sertifikaadid kesktaseme konteineritesse. Sertifikaadid võib keskse poliitika abil automaatselt paigutada ka kõikidele domeeni serveritele ja/või tööjaamadele.

Järgnevalt näitame, kuidas publitseerida juur- ning kesktaseme sertifikaate. Sertifikaatide publitseerimiseks domeeni kontrollerite usaldatud ja kesktaseme sertifikaatide kaustades:

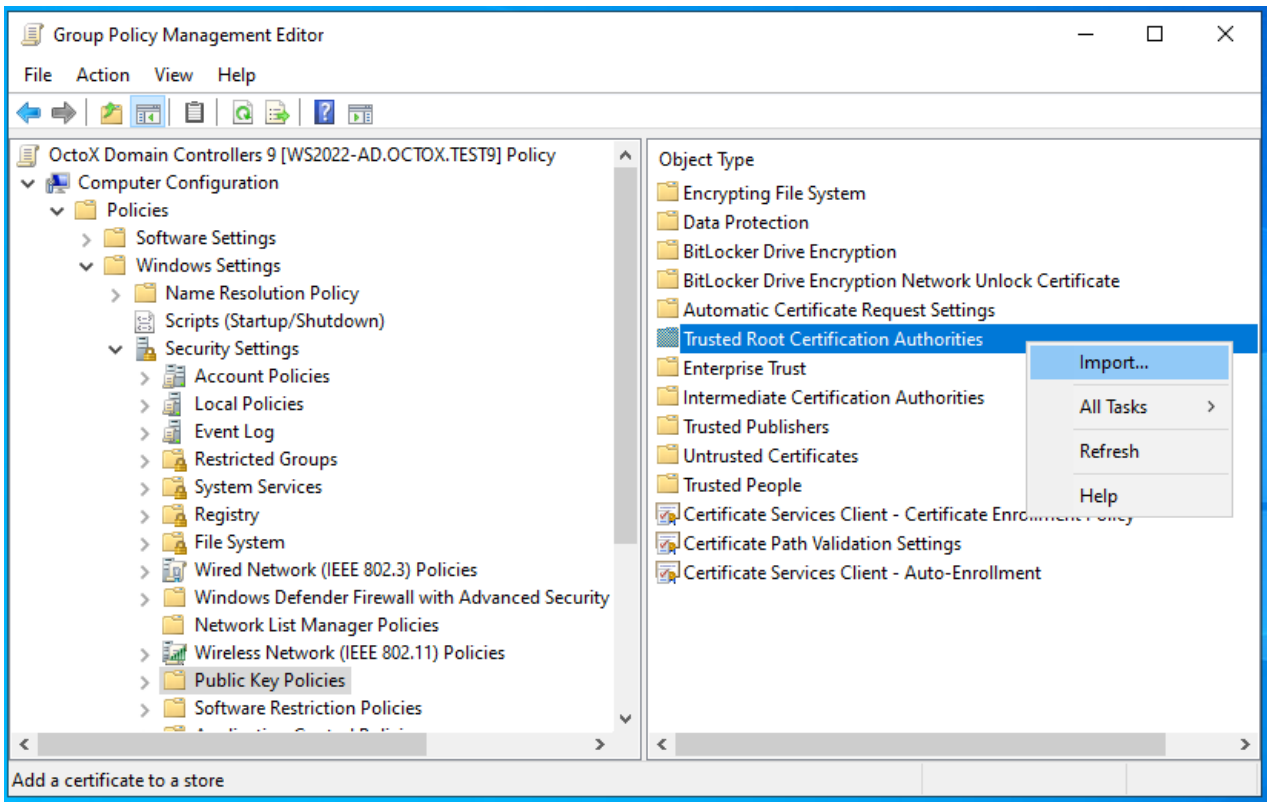
1. Ava *Group Policy Management* konsool ja vali omaduste lisamiseks sobilik GPO, kliki *Edit...:*

[1] Kui oleme eelnevalt kirjeldatud meetodil nii kesk- kui juurtaseme sertifikaadid juba domeenis publitseerinud, puudub selleks küll otsene vajadus. Saame samas näiteks kesktaseme sertifikaadi publitseerida domeeni NTAuthCertificates konteinerisse paigutamisega ja juurtaseme sertifikaadi tavalise domeeni poliitikaga, nagu kirjeldatud allpool. Sellega on lugu tegelikult üldse natuke segane, sest kuigi teoreetiliselt Microsoft nõuab, et kaardi sertifikaadi väljastanud CA sertifikaat kuuluks domeeni NTAuthCertificates konteinerisse (vt. https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/enabling-smart-card-logon-third-party-certification-authorities), siis praktikas töötab eID kaardiga login ka siis, kui seda pole tehtud ja ahel on lihtsalt usaldatud. Siiski soovitame konfiguratsiooni luues järgida Microsofti tehnilisi nõudeid.



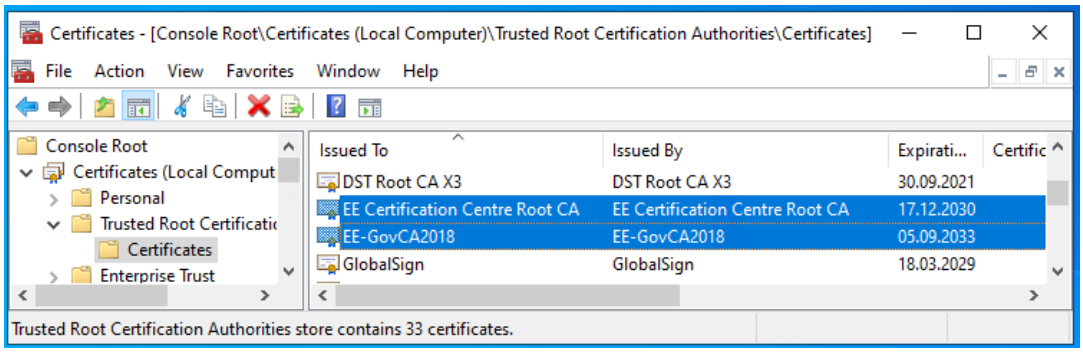
Pilt 3 - sobiva GPO valik

2. Vali kaust „*Computer Configuration/Policies/Windows Settings/Security Setting/Public Key Policies*“



Pilt 4 - sertifikaadi importimisega alustamine

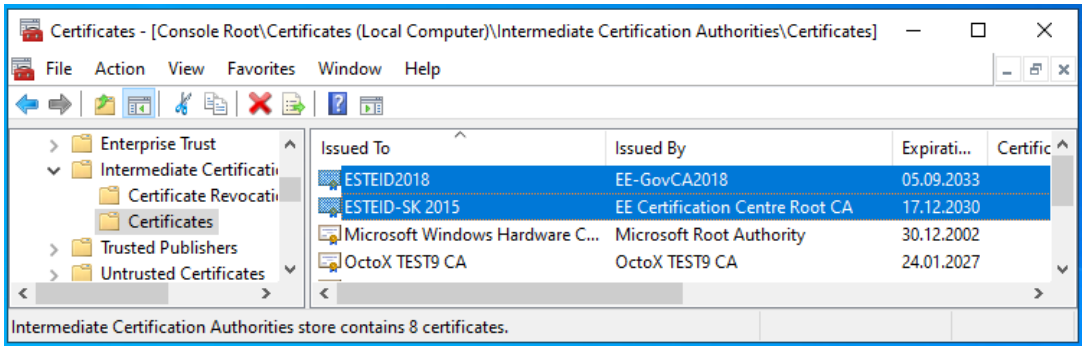
3. „EE Certification Centre Root CA“ ja EE-GovCA2018 sertifikaatide lisamiseks:
    a. Paremkliki kaustal *Trusted Root Certification Authorities* ja vali *Import*
        i. Kliki *Next*, vali „EE Certification Centre Root CA“ sertifikaat ja impordi see.
        ii. Kliki *Next*, vali „EE-GovCA2018“ sertifikaat ja impordi see.



Pilt 5 - juurtaseme sertifikaadid on korrektselt publitseeritud

4. Kesktaseme sertifikaatide lisamiseks:
    a. Paremkliki kaustal *Intermediate Certification Authorities* ja kliki *Import*

i. Kliki *Next*, vali sertifikaat „ESTEID-SK 2015“ ja impordi see.
ii. Kliki *Next*, vali sertifikaat „ESTEID2018“ ja impordi see.



Pilt 6 - kesktaseme sertifikaadid on korrektselt publitseeritud

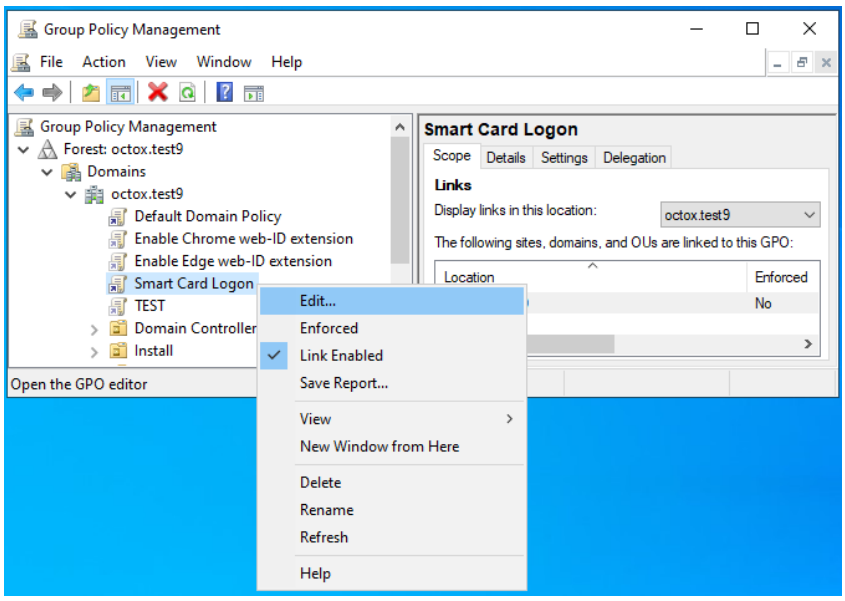
Nagu eelnevatelt illustreerivatelt piltideltki näha on, muutuvad sertifikaadid nähtavateks vastavalt *Trusted Root Certification Authorities* ja *Intermediate Certificate Authorities* konteinerites. Kuna tegemist on kesksete poliitikatega siis rakenduvad kirjeldatud omadused järgmise poliitikate uuendustsükli ajal kõikidele domeeni kontrolleritele. Poliitikate rakendumise kiirendamiseks võib kasutada käsku *gpupdate (/force)*. Ja nagu juba mainitud, siis samal viisil võib vajalikud sertifikaadid publitseerida ka kõikidele teistele Windows tööjaamadele ja serveritele.

eID kaardi omaduste häälestus domeenis

Toetamaks eID kaardiga domeeni logimist keskselt kõikidel klientarvutitel kasutame siin näites domeeni taseme poliitikat[2]:

1. Ava *Group Policy Management* konsool ja vali omaduste lisamiseks sobilik GPO, kliki *Edit...:*

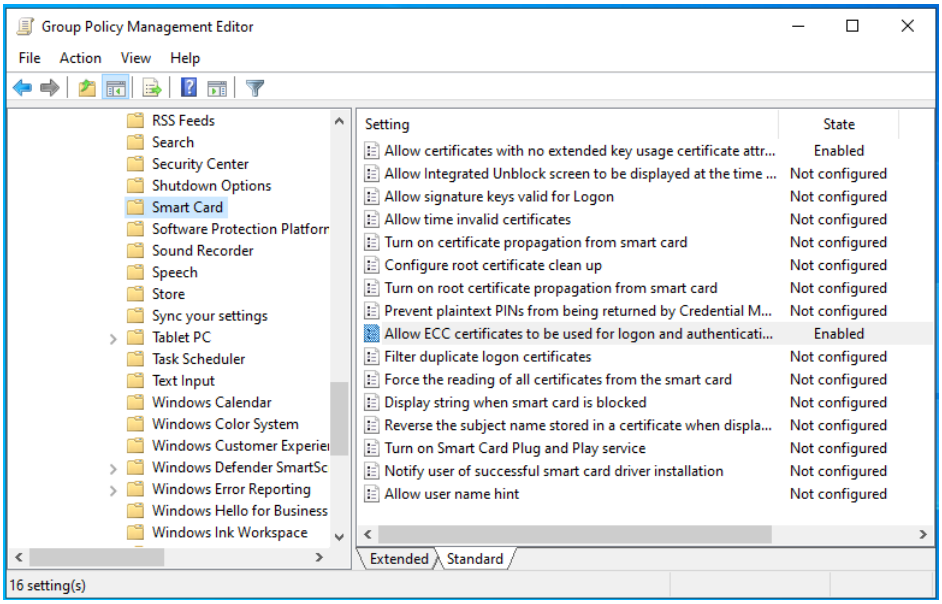
[2] Muidugi võime vastava poliitika rakendada ka ainult klientarvutite ja/või serverite OU baasilt või mõnel muul loogikal baseeruvalt.



Pilt 7 - sobiva GPO valik

2. Vali kaust *„Computer Configuration/Policies/Administrative Templates/Windows Components/Smart Card“* ja muuda järgmiseid omadusi:
   a. *„Allow certificates with no extended key usage certificate attribute = Enabled“* – lubamaks sertifikaate, milliste EKU-s on kirjeldamata *„Smart Card Logon“;*
   b. *„Allow ECC certificates to be used for logon and authentication = Enabled“ – lubamaks domeeni logimine kaartidega milliste krüptograafia baseerub elliptilistel kõveratel.*

Peale muudatuste sisseviimist näeb loodud poliitika välja järgmine:



Pilt 8 - Smart Card määrangud keskses poliitikas

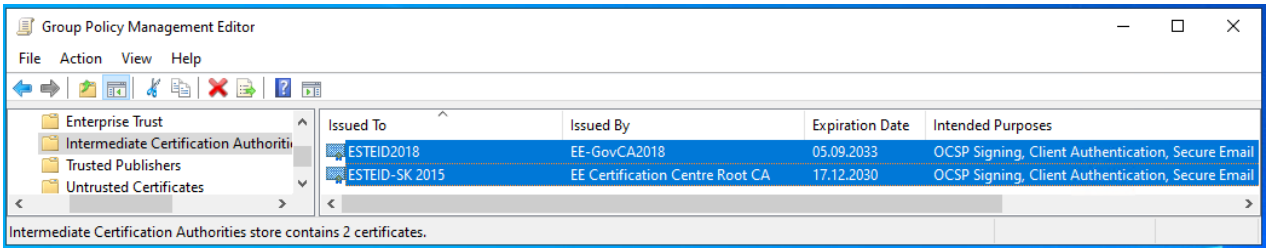
eID kaartide toetamine domeeni logimiseks üksikarvutitel

Juhul, kui eID kaartidega tahetakse logida näiteks domeenivälisest koduarvutist domeeni serverisse üle RDP ühenduse, tuleb koduarvuti häälestada toetama eID kaarte (logimise vaates). Selleks tuleb koduarvutil administraatori õigustes käivitada lokaalne poliitikate haldur käsuga *gpedit.msc*. Poliitikate halduris tuleb arvuti konfiguratsiooni viia sisse täpselt sama muudatus mis kirjeldatud ülemises peatükis (eID kaardi omaduste häälestus), tuleb lubada *„Allow certificates with no extended key usage certificate attribute“ ja ka „Allow ECC certificates to be used for logon and authentication“*! Peale kirjeldatud muudatuse sisseviimist tuleb kas oodata poliitika rakendumist, uuendada poliitikaid käsuga *„gpupdate /force“* või restartida arvuti, ja eID kaartidega logimine osutubki võimalikuks (kui domeen ja server seda toetab muidugi).

OCSP sertifikaadikontrolli meetodi keskne nõue

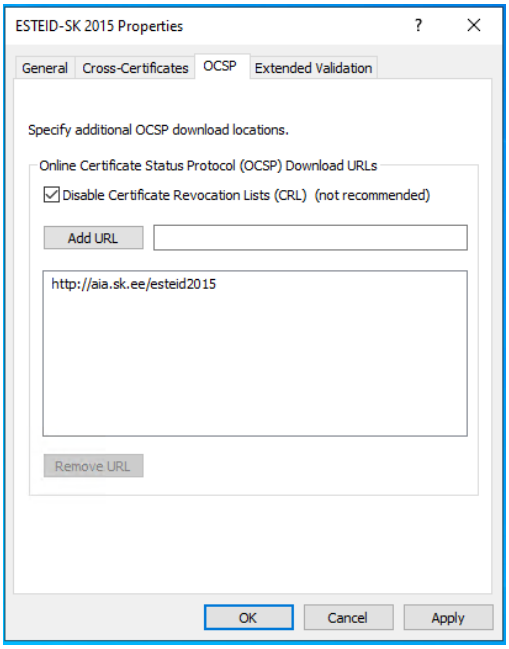
Kasutamaks OCSP-põhist sertifikaadi kehtivuse nõuet tuleb häälestada publitseeritud kesktaseme sertifikaatide omadused järgmiselt:

1. Ava domeeni kontrolleritele suunatud poliitika, millises kirjeldatakse eID kesktaseme sertifikaatide usaldussidemeid ja vali „Computer Configuration / Policies / Windows Settings / Security Settings / Public Key Policies / Intermediate Certification Authorities / Certificates“:



Pilt 9 – poliitika publitseeritud kesktaseme sertifikaatidega

2. Ava publitseeritud sertifikaat „ESTEID-SK 2015“ hiire topelt klõpsuga ja vali leht *OCSP*. Lisa tee http://aia.sk.ee/esteid2015 SK OCSP teenuse juurde ja keela sertifikaadi kehtivuse kontroll üle CRL-i:



Pilt 10 – kesktaseme sertifikaadi omadused, OCSP teenuse häälestus.

Märkuseid

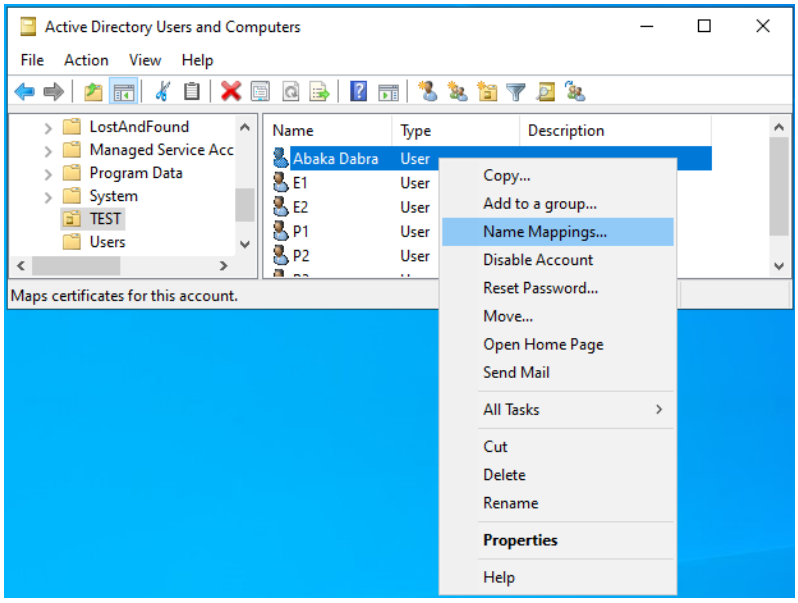
- 2018 aasta lõpust väljastatavate sertifikaatide puhul ei ole meil vajalik OCSP teed enam keskselt kirjeldada, kuna see on sertifikaadis juba sees. CRL tee neis sertifikaatides puudub.
- 2015 ahela sertifikaadi sees on kirjeldatud nii OCSP kui CRL teed. Ülaltoodud konfiguratsioon 2015 ahela sertifikaadi osas on mõttekas vaid siis, kui soovime keelata CRL kasutamist.
- Juhendis on kirjeldatud nö. tasuta OCSP aadressid. Kui teil on vajadus kõrgkäideldava OCSP järele, siis saate rohkem infot lehelt https://sk.ee/teenused/kehtivuskinnituse-teenus/. Kui teil see teenus aga juba tellitud on, saate nii 2018- kui 2015 ahelate puhul kasutada OCSP teenuse aadressi http://ocsp.sk.ee.

- OCSP nõude kehtestamise korral vii end kurssi ka mõistega OCSP maagiline number[3].

OCSP kasutamise eeliseks CRL[4]-põhise lahenduse ees on suurem turvalisus, sertifikaadi kehtivust kontrollitakse „rohkem“ reaalajas. Värskendatud CRL-id genereeritakse kaks korda päevas ja kaks korda päevas tuleb need siis ka alla laadida. Samas võib kasutaja CRL kontrollimeetodi puhul sisse logida kuni pea 12 tundi sertifikaadi abil mis enam ei kehti (12 tundi on CRL nimekirjade uuenduste vaheline tsükkel). OCSP-põhise kontrolli puhul küsitakse sertifitseerimiskeskuse OCSP teenuselt domeeni logimisel sertifikaadi kehtivuse infot ja tehakse selle põhjal otsus, mis võib olla efektiivsem ja on kindlasti ajalises vaates turvalisem.

Kasutajate sidumine sertifikaatidega

Seoses Microsoft tarkvara uuendustega, mis on kirjeldatud artiklis KB5014754, ei ole enam soovituslik kasutada AD GUI'd kasutaja ja sertifikaadi sidumiseks (seisuga 05.09.2022). Põhjuseks on see, et GUI abil seotakse kasutaja sertifikaadis olevate väljadega *issuer* ja *subject*. Nüüdsest aga peetakse seda meetodit ebaturvaliseks ja soovitatakse kasutaja siduda sertifikaadi väljadega *issuer* ja *serialnumber*.



Pilt 11 - AD GUI näide

Kasutaja sertifikaadi hankimiseks vajaliku informatsiooni saamiseks on järgmised võimalused:

1) Küsida kasutaja sertifikaat kesksest LDAP andmebaasist isikukoodi alusel.

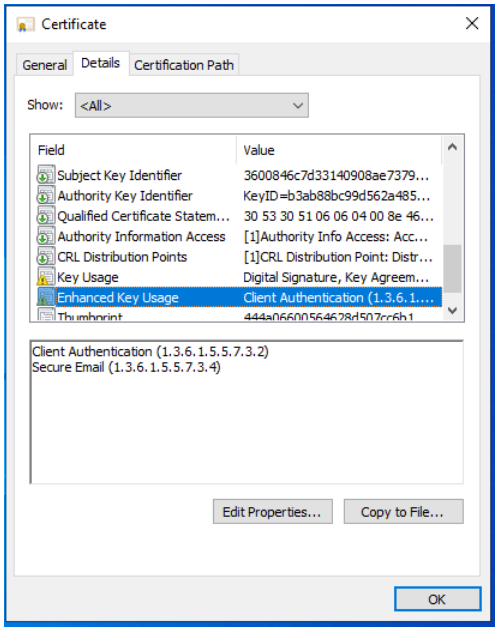
---

[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* elik sertifikaatide tühistusnimekiri.

2) Juhul kui eID kaart on eelnevalt arvutis registreeritud saab sertifikaadi ka kasutajate sertifikaatide hoidlast MMC abil (*Certificates , Personal/Certificates*).
3) Käsuga „certutil.exe –scinfo“ kui eID kaart on lugejas.
4) ...

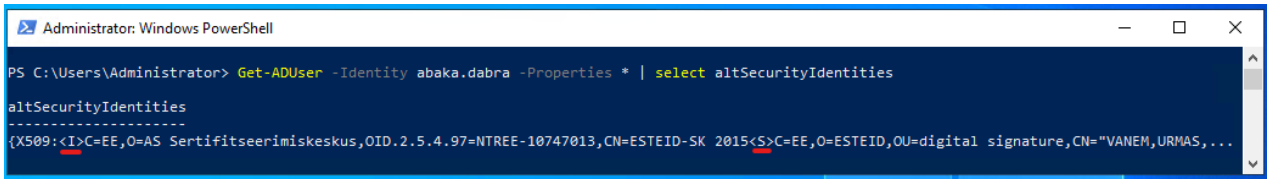
Juhin tähelepanu ka asjaolule, et eID kaartidel on kaks sertifikaati. Domeeni logimiseks eID kaardiga peame kasutama sertifikaati, millisel on EKU all kirjeldatud *Client Authentication.*



Pilt 12 – EKU osaks on Client Authentication

Kasutaja sertifikaadiga sidumise kirjeldus

Nagu juba öeldud, siis kasutades AD GUI-d seotakse sertifikaat kasutajaga väljade *Issuer* ja *Subject* abil ja see kombinatsiooni ei ole Microsoft'i poolt enam soovituslik. Lisaks on Eesti eID kaartide puhul *issuer* väli vähemalt ID- ja Digi-Id kaardi puhul identne.

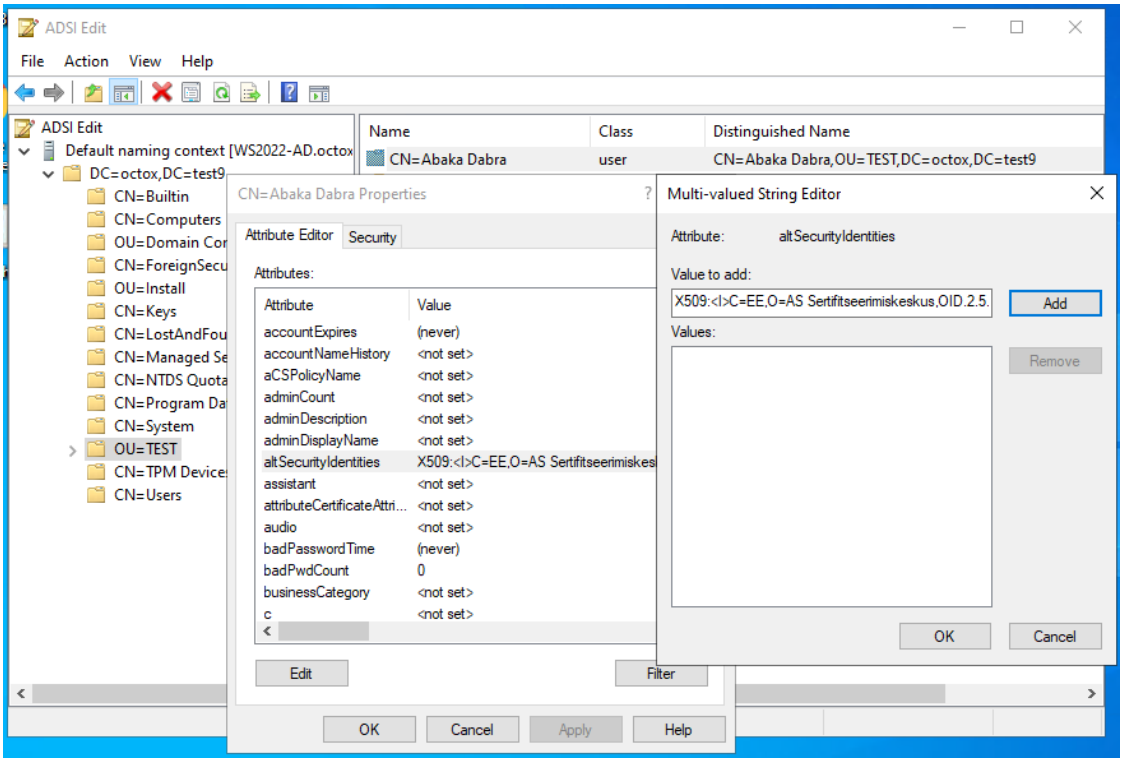


Pilt 13 - <I> ja <S> viitavad sertifikaadi väljadele Issuer ja Subject.

Seega on ilmselt mõistlik järgida Microsofti soovitust ja siduda sertifikaat kasutajaga väljade *issuer* ja *serialnumber* abil. Seda saame üle GUI teha kasutades näiteks *ADSI Edit* võimalusi. Tuleb märkida, et nii issuer'i kui seerianumbri stringid tuleb sidumisel ümber keerata! See tähendab, et kui:

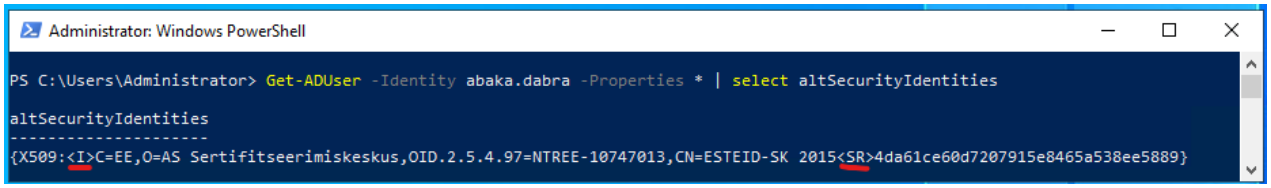
1) Issuer on kirjeldatud sertifikaadis kui „CN = ESTEID-SK 2015 / 2.5.4.97 = NTREE-10747013 / O = AS Sertifitseerimiskeskus / C = EE“, AD-s peab see olema „<I>C=EE,O=AS Sertifitseerimiskeskus,OID.2.5.4.97=NTREE-10747013,CN=ESTEID-SK 2015“;
2) Seerianumber on kirjeldatud sertifikaadis kui 8958ee38a565845e9107720de61ca64d, siis AD-s peab see olema 4da61ce60d7207915e8465a538ee5889. Palun siin pöörata tähelepanu ka asjaolule, et ümberpööramine käib kahe sümboli kaupa!

Korrektne kasutaja ja sertifikaadi sidumise string *ADSI Edit* utiliidis näeb 2015 ahela puhul välja järgmine: „X509:<I>C=EE,O=AS Sertifitseerimiskeskus,OID.2.5.4.97=NTREE-10747013,CN=ESTEID-SK 2015<SR>4da61ce60d7207915e8465a538ee5889".[5]



Pilt 14 - lisame altSecurityIdentities väärtuse ADSI Edit abil

[5] Kui *issuer* on meil reeglina konstant (ahela lõikes), siis *serialnumber* tuleb ümber pöörata kõikidel kasutajatel. Kindlasti on siin mitmeid automatiseerimise meetmeid, ent näitena toon siia Exceli võimaluse selle muudatuse tegemiseks: =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)), kus B4 on siis lahtriks, kus algne seerianumber paikneb.



Pilt 15 - <I> ja <SR> viitavad sertifikaadi väljadele Issuer ja SerialNumber.

Suuremate keskkondade ja kasutajate arvu puhul tuleb kindlasti mõelda eelkirjeldatud tegevuste automatiseerimisele!

Klientarvutite ettevalmistus

Tarkvara

Klientarvutitele tuleb installeerida eID kaardi haldustarkvara (täna, 02.09.2022 soovitame versiooni 22.6.0.1930) ja/või tuleb veenduda minidraiverite korrektses toimimises tööjaamas.

Omadused

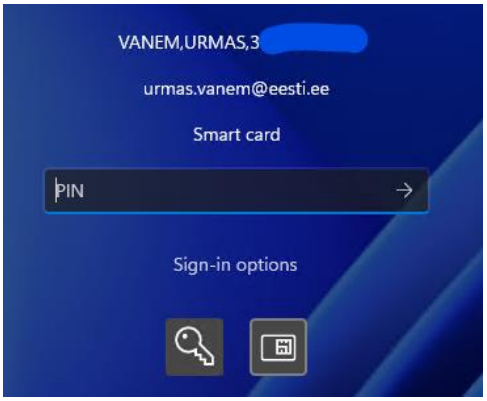
Vajalikud omadused rakenduvad klientarvutitele domeeni tasemelt eelkirjeldatud etteantavate kesksete poliitikatega.

Lõplik rakendamine

ID logini reaalseks rakendamiseks tuleb lihtsalt teha nagu eelnevalt kirjeldatud. Loomulikeks eeldusteks on:

1) Lahenduse testimine test ja/või arenduskeskkonnas;
2) Lahenduse rakendamine töökeskkonnas;
3) Administraatorite koolitus;
4) Kasutajate koolitus.

Peale konfiguratsiooni jõustumist klientarvutis saame logimise aknas valida logimise viisiks kiipkaardi  .

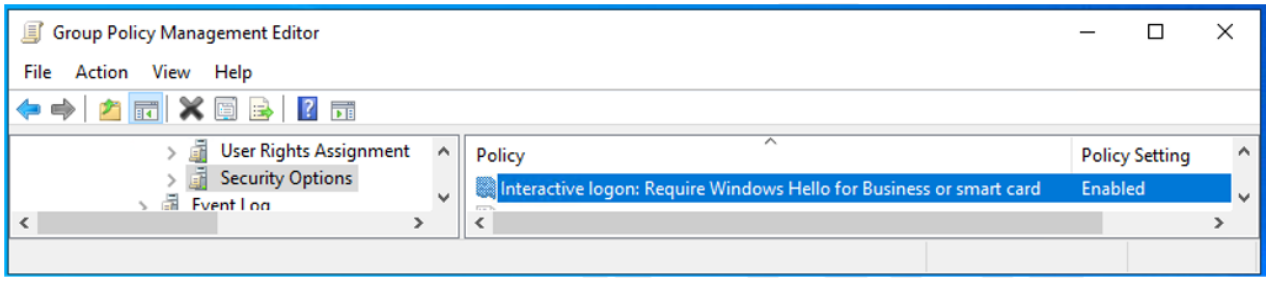


Pilt 16 – eID kaardiga domeeni sisselogimine aken, ootab PIN-ni sisestamist

eID kaardiga domeeni logimise nõue

Mõnikord võime soovida, et kasutajad saaksidki ainult eID kaardiga süsteemidesse sisse logida (teisisõnu keelame parooli kasutamise). See võib puudutada nii tavalisi või spetsiifilisi tööjaamu ja/või RDP servereid. Nõude kehtestamiseks tuleb soovitud arvutitele rakendada järgmine poliitika:

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



Pilt 17 – arvutisse või serverisse logimiseks ei piisa enam kasutajanimest ja paroolist!

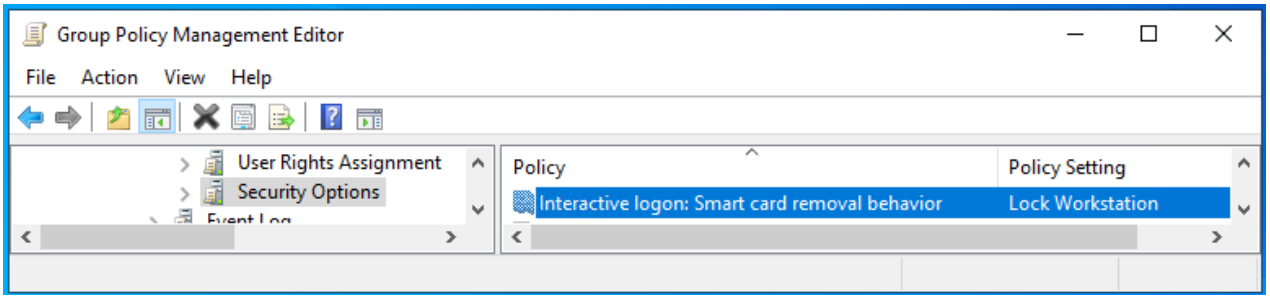
Pilt 18 – veateade juhul, kui kasutaja proovib nime ja parooliga domeeni logida, ent kaardiga logimine on nõutud

Arvuti käitumise juhtimine kiipkaardi eemaldamisel

Võime konfigureerida ka arvuti või arvutite grupi käitumise kiipkaardi eemaldamisel. (Muidugi töötab see poliitika vaid juhul, kui oleme arvutisse/domeeni kiipkaardiga loginud.) Valikutes on:

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

Muudatuse rakendamiseks tuleb määrata üks ülaltoodud väärtustest poliitikale „Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Security Options : Interactive logon: Smart card removal behavior“.



Pilt 19 – selles näites, peale poliitika rakendamist, kiipkaardi eemaldamisel lugejast arvuti lukustatakse

Võimalikud probleemid

Proxy

Kui domeenis on välistele HTTP aadressidele ligipääsuks häälestatud *proxy* ja see poliitika kehtib ka domeeni kontrollerite süsteemikontole, ei õnnestu sertifikaadi kehtivuse kontroll ja seoses sellega ka login.

Mis teha: tuleb domeeni kontrolleritele vastav *proxy* häälestus luua. Vt. näiteks netsh.exe võimalusi.

Sertifikaat mitmel kasutajal

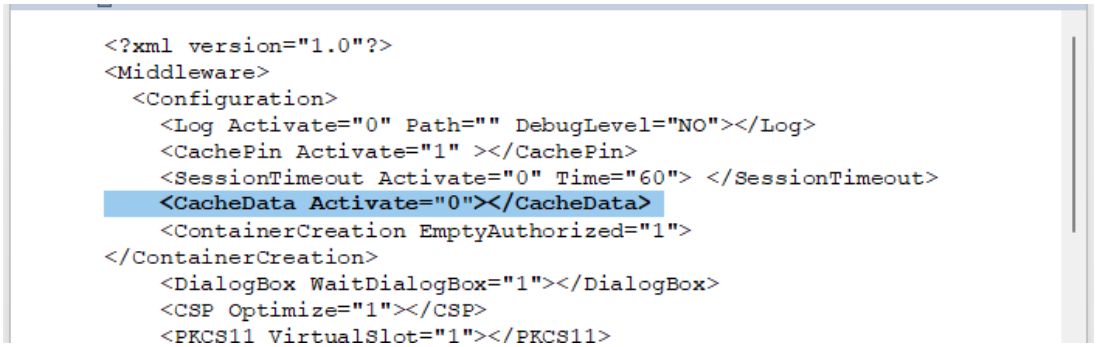
Kui üks autentimissertifikaat on seotud rohkem kui ühe kasutajaga domeenis, siis logimine ei õnnestu.

Mis teha: eemaldada sertifikaat sidumine „vale(de)lt“ kasutaja(te)lt.

Segadus 2018 sertifikaatidega RDP login puhul

Esimeste 2018 ahelast väljastatud sertifikaatide puhul võib esineda „sertifikaatide sassi mineku“ probleemi. Kindlatel tingimustel ei suudeta sertifikaati korrektse kasuajaga siduda ja kasutajale võidakse näidata mõne teise sisse logitud kasutaja kirjeldust. Peamiselt on seda probleemi tuvastatud RDP (terminal) serveritel.

Probleemist ülesaamiseks tuleb keelata Idemia tarkvara poolne vahemälu kasutamine. Selleks tuleb RDP serveril või probleemsel tööjaamal modifitseerida konfiguratsioonifaili OCSMiddlewareConf.xml asukohas „C:\Program Files (x86)\IDEMIA\AWP“ või „C:\Program Files\IDEMIA\AWP“ ja määrata seal „CacheData Activate“ väärtuseks 0! Muudatuse jõustumiseks tuleb seejärel arvuti või server restartida.



```
<?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>
```

Pilt 20 - vahemälu keelamine Idemia tarkvaras

Kokkuvõte

eID kaartidel baseeruv domeeni logimine on hea võimalus lihtsustada kasutajate domeeni sisselogimist tõstes samaaegselt süsteemide turvalisust.

Kasutajate vaates on kindlasti mugavaks omaduseks parooli unustamise vältimine – meeles tuleb pidada vaid autoriseerimise PIN koodi (mis eID kaartide kasutajatel on tõenäoliselt nagunii teada).

Administraatorite ja kasutajatoe vaade on arvatavasti samuti positiivne, kuna lisaks turvalisuse kasvule esineb vähem probleeme paroolide unustamisega kasutajate poolt. Samuti on vastava konfiguratsiooni loomine küllaltki lihtne. Ja huvitav :)