EID KAARDIGA WINDOWS DOMEENI LOGIMINE

Tehniline ülevaade

Dokumendi info	
Loomise aeg	21.01.2019
Tellija	RIA
Autor	Urmas Vanem, OctoX
Versioon	1901

Versiooni info		
Kuupäev	**Versioon**	**Muutused/märkused**
21.01.2019	1901	Avalik versioon, baseerub 1812 tarkvaral

Taust

Alates Windows Server 2008 SP2 ja Windows Vista SP2 sümbioosist on võimalik kasutada ID-kaarti domeeni sisselogimiseks. See teema on olnud aktuaalne juba 2008 aasta sügisest, mil tehti ka vastavad esimesed katsetused (tol ajal tuli operatsioonisüsteemide lisana küll kasutada kindlaid *hotfix*'e, katsetused tehti Microsoft Eesti meeskonnas). Käesolev dokument kirjeldab platvormid ja konfiguratsioonid, millised täna meil ID logimise funktsionaalsust lihtsalt ja edukalt võimaldavad rakendada - kasutusel on vaid Microsofti operatsioonisüsteemid ja ID-kaardi tarkvara.

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

Platvorm

ID login on täna toetatud ja testitud järgmistel platvormidel:

Serverid:

1. Windows Server 2008 SP2 ja uuem

Kliendid:

1. Windows Vista SP2 ja uuem
2. Windows Server 2008 SP2 ja uuem

Rakendamine

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

Kõige lihtsama lahenduse puhul tuleb teha vaid mõni liigutus ja ID-kaardiga logimine hakkabki tööle:

- Domeeni kontrollerid peavad omama endi tuvastamiseks sertifikaati, mida usaldavad ka kliendid.
- Domeeni kontrollerid peavad usaldama sertifitseerimiskeskuse juur- ja kesktasemete sertifikaate.
- Klientarvutitel peab olema installeeritud ID-kaardi haldustarkvara, toetamaks kõiki kaarte peab see olema vähemalt 1812.
- Klientarvutid peavad toetama sertifikaate, millistel puudub spetsiaalne kiipkaardiga logimise toe atribuut (*Smart Card Logon EKU*).
- Domeenis peab ID-kaardi ja/või Digi-ID autentimissertifikaat olema seotud ühe konkreetse kasutajaga.

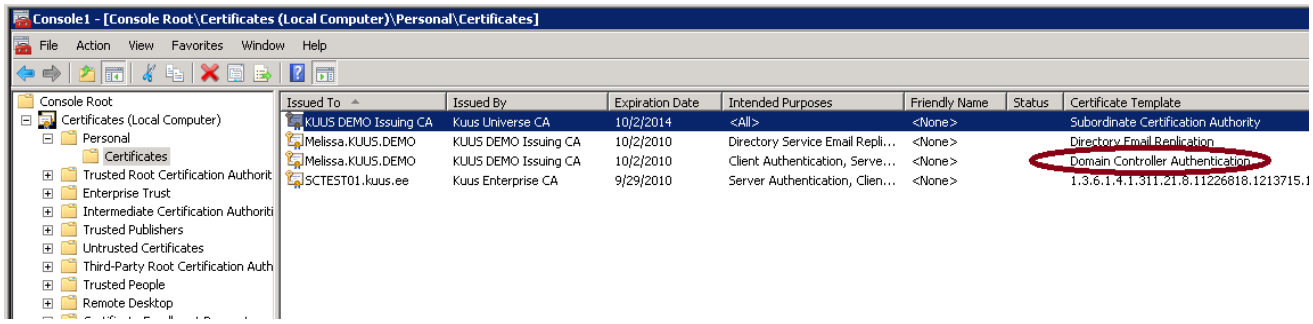
Täpsemalt käsitleme konfiguratsiooni ettevalmistust järgmistes alampunktides.

Domeenist

Domeeni ettevalmistuse osadeks on poliitikate häälestus domeeni kontrolleritele ja töökohtadele. Eelduseks on toimiv PKI lahendus ja vastava sertifikaadi olemasolu domeeni kontrolleritel.

Ettevõtte PKI lahendus

Domeeni kontrollerid vajavad ID-logini toimimiseks sertifikaate, millistega nad suudavad klientarvutitele endi identiteeti tõestada. Kõige mõistlikum tundub need sertifikaadid küsida lokaalse PKI lahenduse käest[1]. Vaikimisi Windows *Enterprise* CA konfiguratsioonis on publitseeritud „*Domain Controller Authentication*“ sertifikaat[2], mida reeglina omavad kõik logimisprotsessis osalevad domeeni kontrollerid. Juhul kui domeeni kontrolleritel *autoenrollment* ei ole lubatud, tuleb nimetatud sertifikaadid küsida “käsitsi”. Piltlikult väljendub nõutav domeeni kontrollerite sertifikaatide konfiguratsioon järgmisel joonisel:



Pilt 1 - Domeeni kontrolleri sertifikaat

Poliitikad

Sertifikaatide publitseerimine

ID-kaardi sertifikaadi kasutamiseks peavad domeeni kontrollerid usaldama ID-kaardil olevaid sertifikaate. Usaldusväärsed peavad olema nii juur- kui kesktaseme sertifikaadid. Sertifikaatide kehtivuse kontrolliks peab olema ligipääs SK OCSP teenusele ja/või sertifikaatide tühistusnimekirjadele (CRL).

Soovitav on nii SK juur kui kesktaseme sertifikaadid publitseerida domeenis kesksete poliitikate abil. Sertifikaadid on allalaetavad lehelt http://www.sk.ee/certs. Tänase seisuga vajame järgmiseid sertifikaate kahest puust:

---

[1] Kui see muidugi olemas on, vastasel juhul tuleb sertifikaat hankida muid teid pidi.

[2] Pakutakse vaikimisi/automaatselt alates *Server 2003 Enterprise*, *Server 2008 Enterprise* ja *Server 2008 R2 Standard* tasemete CA-dest. Vanemat tüüpi CA puhul võib kasutada *Domain Controller* sertifikaati mis teatud juhtudel tuleb „käsitsi“ kõikidele domeeni kontrolleritele küsida. Oluline on sel sertifikaadil *Server Authentication EKU* olemasolu.

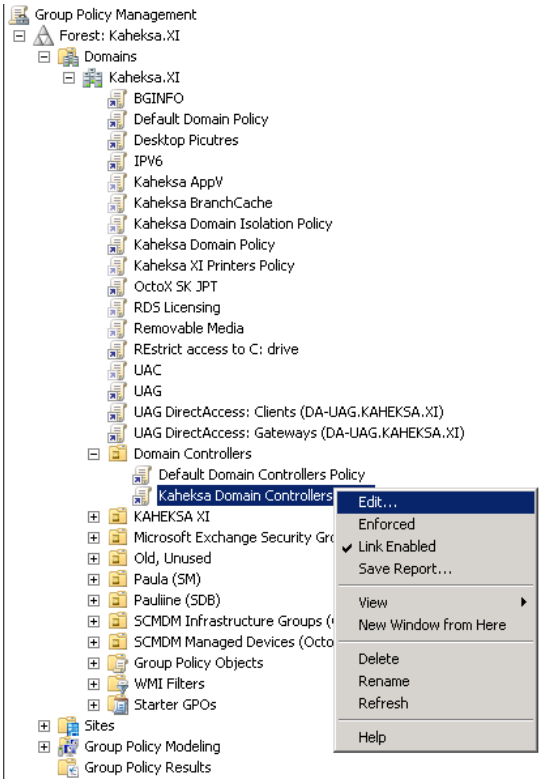
- „Vana“ puu: EE Certification Centre Root CA – usaldusväärne juursertifikaat
    a. ESTEID-SK 2011 - usaldusväärne kesktaseme sertifikaat
    b. ESTEID-SK 2015 - usaldusväärne kesktaseme sertifikaat

- „Uus puu“: EE-GovCA2018 – usaldusväärne juursertifikaat
    a. ESTEID2018 - usaldusväärne kesktaseme sertifikaat

Kui soovime publitseerida sertifikaate domeeni kontrolleritel automaatselt, siis soovitame modifitseerida *Default Domain Controllers* või mõnda teist domeeni kontrollerite CN tasemelt rakenduvat poliitikat. Sertifikaadid tuleb paigutada konteineritesse vastavalt ülaltoodud loendile ja tüübile.

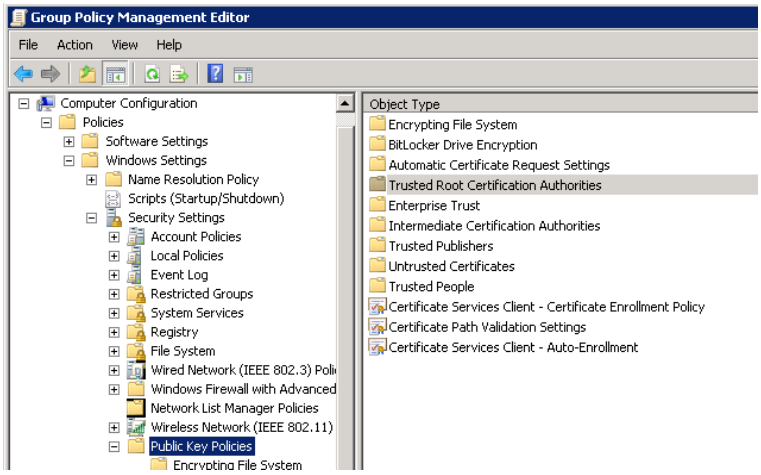
Järgnev on näide, kuidas publitseerida juurtaseme ning kesktaseme sertifikaate. Sertifikaatide publitseerimiseks usaldatud ja kesktaseme sertifikaatide kaustades:

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



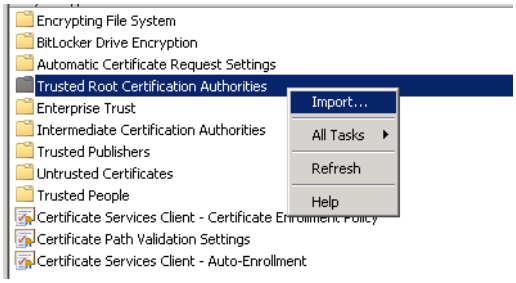
Pilt 2 - Sobiva GPO valik

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



Pilt 3 - GPO kausta valik

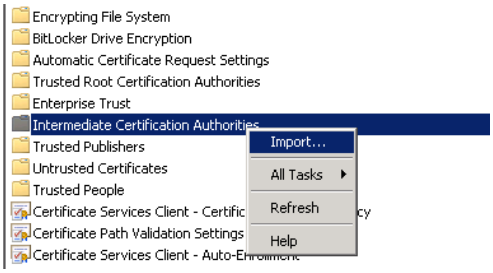
3) „EE Certification Centre Root CA“ ja EE-GovCA2018 sertifikaatide lisamiseks:
    a. Paremkliki kaustal *Trusted Root Certification Authorities* ja kliki *Import*



Pilt 4- „EE Certification Centre Root CA“ sertifikaadi import

    b. Kliki *Next*, vali „EE Certification Centre Root CA“ sertifikaat ja impordi see.
    c. Kliki *Next*, vali „EE-GovCA2018“ sertifikaat ja impordi see.

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



Pilt 5 - Kesktaseme sertifikaatide import

b. Kliki *Next*, vali sertifikaat „ESTEID-SK 2011“ ja impordi see.
c. Kliki *Next*, vali sertifikaat „ESTEID-SK 2015“ ja impordi see.
d. Kliki *Next*, vali sertifikaat „ESTEID2018“ ja impordi see.

Peale sertifikaatide importi on need nähtavad vastavalt *Trusted Root Certification Authorities* ja *Intermediate Certificate Authorities* kaustades. Kuna tegemist on kesksete poliitikatega siis rakenduvad kirjeldatud omadused järgmise poliitikate uuendustsükli ajal kõikidele poliitika alla kuuluvatel töökohtadel. Poliitikate rakendumise kiirendamiseks võib kasutada käsku *gpupdate*.[3]

Antud näite varal publitseerime sertifikaadid automaatselt kõikidel domeeni kontrolleritel. Samal viisil võib vajalikud sertifikaadid publitseerida ka kõikidele muudele Windows tööjaamadele ja serveritele.

Märkus. Kui SK loob uue juur- ja/või kesktaseme sertifikaadi digitaalsete kaartide sertifikaatide väljastamiseks, tuleb vastav sertifikaat ID-logini toetamiseks siin uute ja/või uuendatud sertifikaatide toetamiseks ka publitseerida.

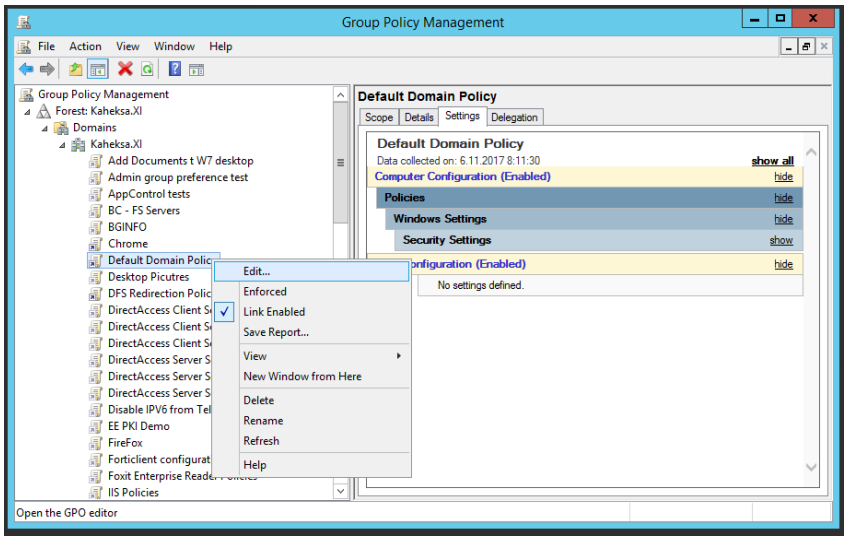
Targa kaardi omaduste häälestus

Toetamaks ID-kaardiga domeeni logimist keskselt kõikidel võimalikel klientarvutitel kasutame domeeni taseme poliitikat[4]:

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

[3] Alternatiivina võime nimetatud sertifikaadid publitseerida AD LDAP-pi, kust neid samuti kõik domeeni liikmed automaatselt usaldama hakkavad. Vt. käsku „certutil -dspublish“.

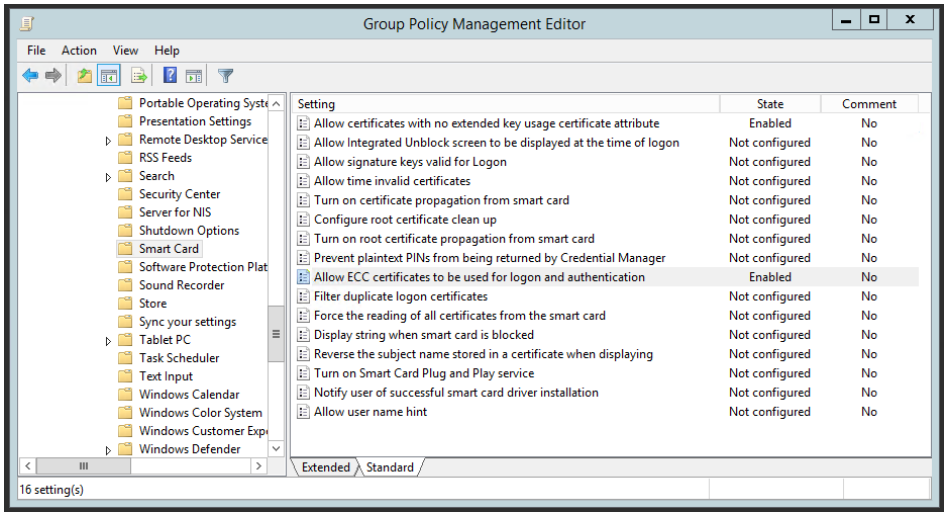
[4] Muidugi võime vastava poliitika rakendada ka ainult klientarvutite OU baasilt.



Pilt 6 - 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 peavad omadused väljenduma järgmisel visuaalsel kujul:



Pilt 7 - *Smart Card* omadused GPOs

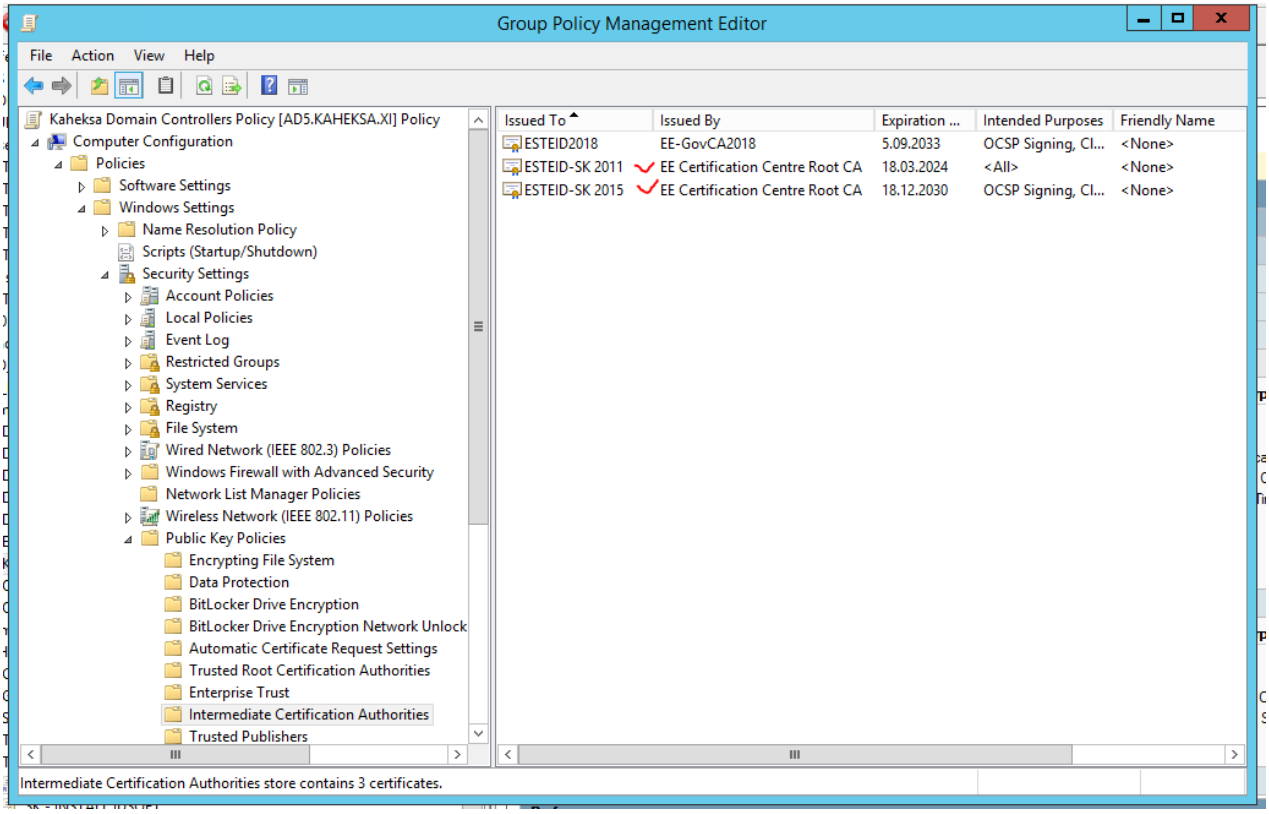
ID-kaardi toetamine üksikarvutitel

Juhul, kui ID-kaardiga tahetakse logida näiteks domeenivälisest koduarvutist domeeni serverisse üle RDP ühenduse, tuleb koduarvuti häälestada toetama ID-kaarti (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 (Targa 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 uuendada poliitikaid käsuga *gpupdate /force* või restartida arvuti, ja ID-kaardiga logimine osutubki võimalikuks.

OCSP sertifikaadikontrolli meetodi kehtestamine „vanadele“ sertifikaatidele

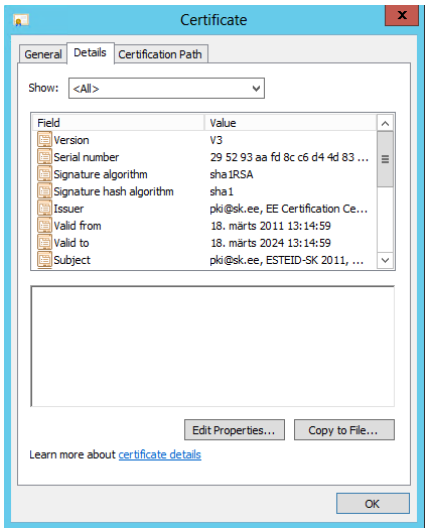
Kasutamaks OCSP-põhist sertifikaadi kehtivuse kontrolli tuleb häälestada publitseeritud kesktaseme sertifikaatide omadused järgmiselt:

- Ava domeeni kontrolleritele suunatud poliitika kesktaseme sertifikaatide publitseerimine alamosast „Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Intermediate Certification Authorities“:



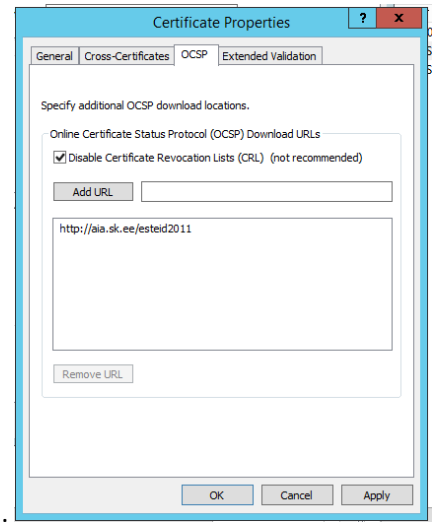
Pilt 8 - Kesktaseme publitseeritud sertifikaadid

- Ava publitseeritud sertifikaat „ESTEID-SK 2011“ hiire topeltklõpsuga ja vali leht *Details*:



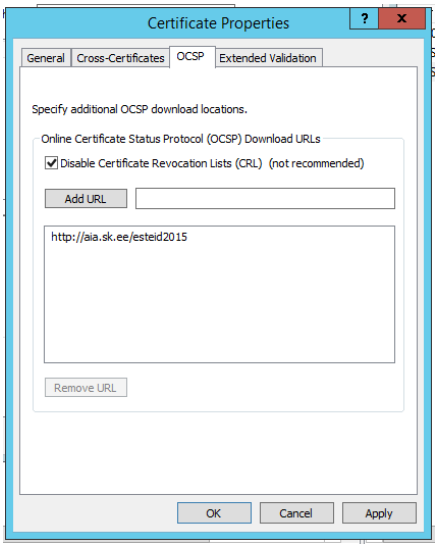
Pilt 9 - Sertifikaadi omadused, detailide leht

- Kliki nupul „Edit Properties...“ ja avanevas aknas vali OCSP ja lisa tee http://aia.sk.ee/esteid2011 SK OCSP teenuse juurde. Puhta OCSP lahenduse kasutuseks keela CRL-põhine kontroll:



Pilt 10 - OCSP nõude häälestus 2011 sertifikaadil

- Kliki OK konfiguratsiooni kinnistamiseks
- Korda samme 2-4 sertifikaadiga ESTEID-SK 2015, ent OCSP teeks määra selle sertifikaadi puhul http://aia.sk.ee/esteid2015:



Pilt 11 - OCSP nõude häälestus 2015 sertifikaadil

Märkuseid

- 2018 aasta lõpust väljastatavate sertifikaatide puhul meil ei ole vajalik OCSP teed enam keskselt kirjeldada, kuna see on sertifikaadis juba sees.
- 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/.
- OCSP nõude korral vii end kurssi ka mõistega OCSP maagiline number[5].

Eelkirjeldatud, OCSP-põhine kontroll on Sertifitseerimiskeskuse poolt toetatud variant ID-logini rakendamiseks domeenides. OCSP kasutamise eeliseks CRL[6]-põhise lahenduse ees on suurem turvalisus ja optimeeritus. Värskendatud CRL-id genereeritakse kaks korda päevas ja kaks korda päevas tuleb need siis ka alla laadida. Samas võib kasutaja sisse logida kuni 12 tundi sertifikaadi abil mis enam ei kehti (CRL nimekirjade uuenduste vaheline tsükkel)[7]. OCSP-põhise kontrolli puhul küsitakse sertifitseerimiskeskuse OCSP teenuselt kindlal ajahetkel sertifikaadi kehtivuse info, mis on efektiivsem ja turvalisem.

---

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

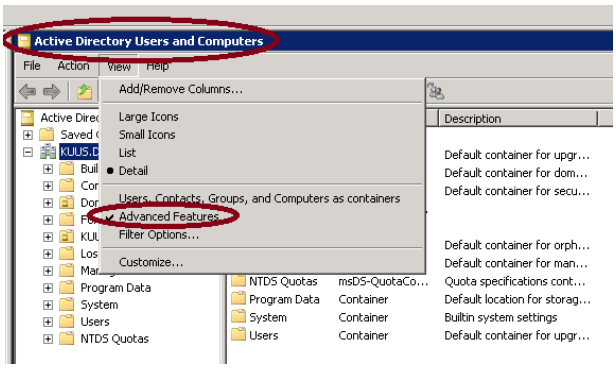
[6] *Certificate revocation list* elik sertifikaatide tühistusnimekiri

[7] See mure on meil ainult vanemate, Gemalto kaartidel olevate sertifikaatide puhul, millistes ei ole OCSP tee kirjeldatud.

Kasutajate sidumine sertifikaatidega

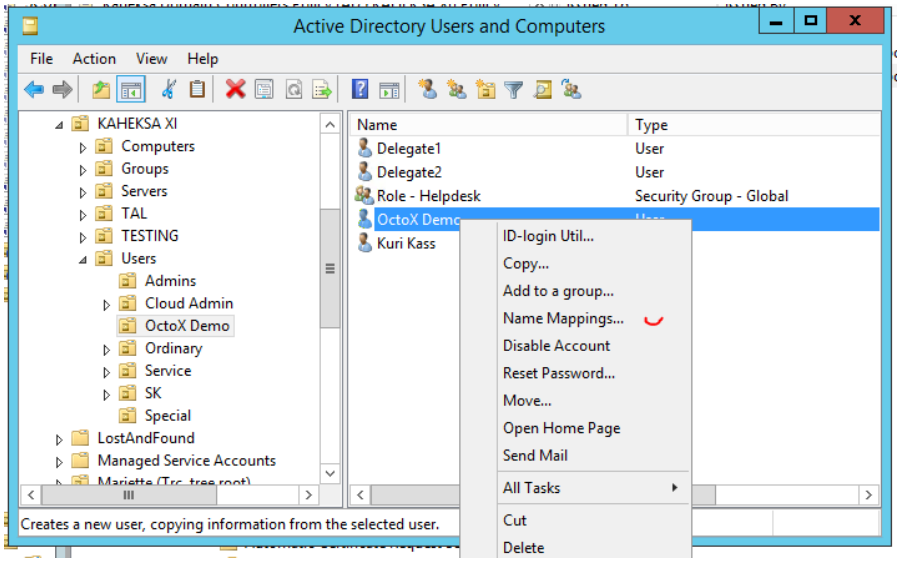
Kasutaja sidumiseks konkreetse ID-kaardi sertifikaadiga tuleb:

1) Avada ADUC konsool ja lülitada sisse *Advanced View*



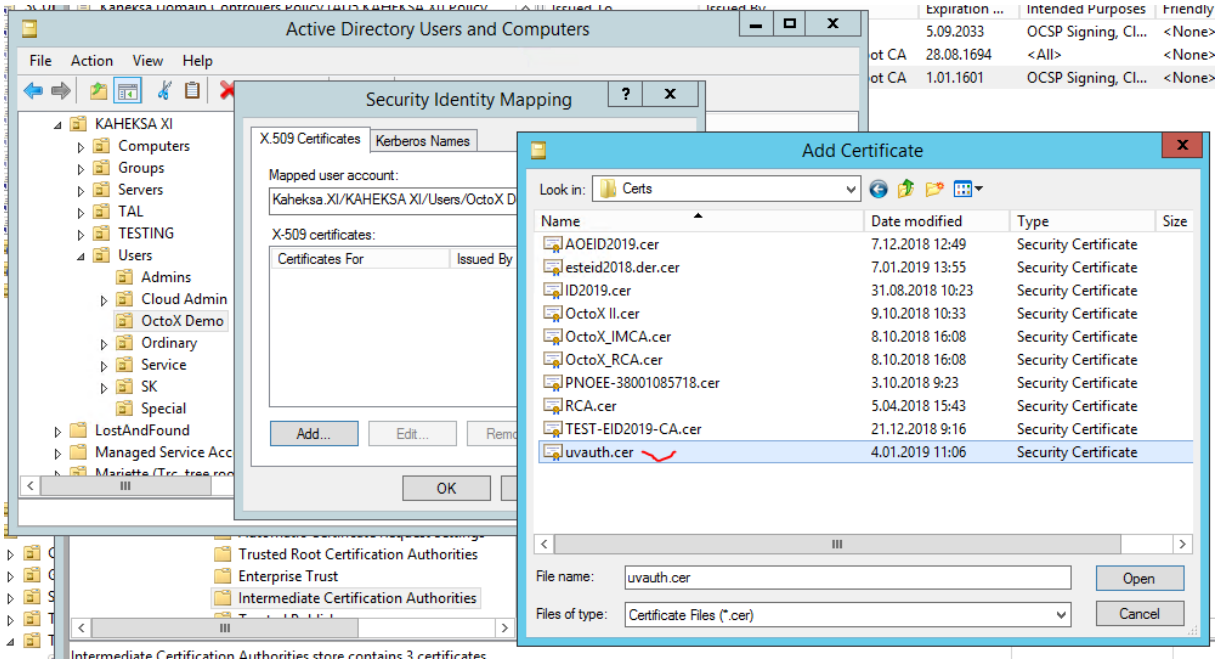
Pilt 12 - ADUC laiendatud vaate sisse lülitamine

2) Paremklikkida soovitaval kasutajal ja valida *Name Mappings:*



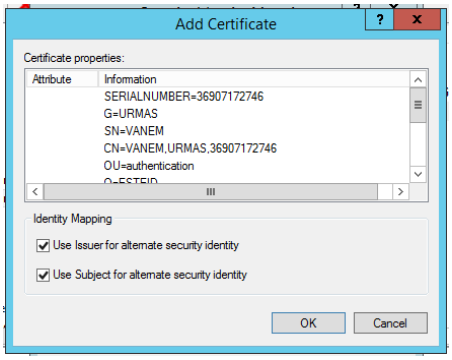
Pilt 13 - *Name Mappings*

3) Jääda X.509 sertifikaadi nupule ja valida *Add*, seejärel valida kasutaja autoriseerimissertifikaat:



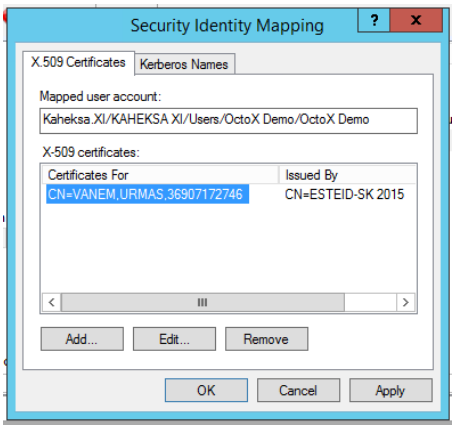
Pilt 14 - Kasutajasertifikaadi valik

4) Klikkida *Open* jätta avanenud *Add Certificate* aknas andmed nagu on ja klikkida OK:



Pilt 15 - *Add Certificate* aken

5) Lõpptulemusena näeb *Security Identity Mapping* aken välja järgmine:



Pilt 16 - *Security Identity Mapping* aken

Kasutaja sertifikaadi saamiseks on võimalikud erinevad meetodid:

1) Küsida kasutaja sertifikaat kesksest LDAP andmebaasist.
2) Juhul kui ID-kaart on eelnevalt arvutis registreeritud saab sertifikaadi ka:
    a. Kasutajate sertifikaatide hoidlast MMC abil (*Certificates snap-in, Personal/Certificates*).
    b. Kasutajate sertifikaatide hoidlast *Internet Explorer (Tools/Content/Certificates*).
3) Käsuga „certutil.exe –scinfo“ kui ID-kaart on lugejas.

Klientarvutite ettevalmistus

Tarkvara

Klientarvutitele tuleb installeerida ID-kaardi haldustarkvara ja/või tuleb veenduda minidraiveri korrektses toimimises tööjaamas. Toetame kõikide EID kaartidega domeeni logimist alates tarkvara versioonist 1812!

Omadused

Vajalikud omadused rakenduvad klientarvutitele domeeni tasemelt etteantavate kesksete poliitikatega.

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

Mõnusat rakendamist!

Võimalikud probleemid

Esimene login ja CRL

Juhul, kui OCSP on häälestamata ja CRL ei ole domeeni kontrolleri vahemälus, võib uue CRI-i allalaadimine kesta nii kaua, et ID-kaardiga login ei õnnestu.

Mis teha: proovida uuesti ja/või minna üle OCSP kasutamisele!

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. netsh.exe võimalusi.

Sertifikaat mitmel kasutajal

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

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

Kokkuvõtvalt

ID-kaardi põhine logimine on hea võimalus lihtsustada kasutajate sisselogimist tõstes samaaegselt süsteemide turvalisust.

Kasutajate vaates on kindlasti mugavaks omaduseks parooli unustamine – meeles tuleb pidada vaid autoriseerimise PIN koodi (mis ID-kaardi kasutajatel on tõenäoliselt nagunii teada).

Süsteemide haldurite vaade on arvatavalt samuti positiivne - kuna esineb vähem probleeme paroolide unustamisega kasutajate poolt. Samuti on vastava konfiguratsiooni loomine küllaltki lihtne. Ja huvitav ☺

Head uute funktsionaalsuste rakendamist!