OCTOX

ID kaardiga Windows domeeni logimine

Tehniline ülevaade

Urmas Vanem

2012

SERTIFITSEERIMISKESKUS / MICROSOFT

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 haldustarkvara.

Kindlasti on ID kaardiga sisselogimine teenus, mis lähitulevikus järjest enam ja enam Eesti ettevõtetes hakkab levima. 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 autoriseerimis-sertifikaatidega.

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

1) Domeeni kontrollerid peavad omama endi tuvastamiseks sertifikaati, mida usaldavad ka kliendid (tavaliselt on see konfiguratsioon vaikimisi juba korras).
2) Domeeni kontrollerid peavad usaldama sertifitseerimiskeskuse juur- ja kesktaseme sertifikaate.
3) Klientarvutitel peab olema installeeritud ID kaardi haldustarkvara, tänase seisuga soovitavalt vähemalt versioon 3.5.
4) Klientarvutid peavad toetama sertifikaate, millistel puudub spetsiaalne kiipkaardiga logimise toe atribuut.
5) Domeenis peab ID kaardi ja/või Digi-ID autentimissertifikaat olema seotud konkreetse kasutajaga.

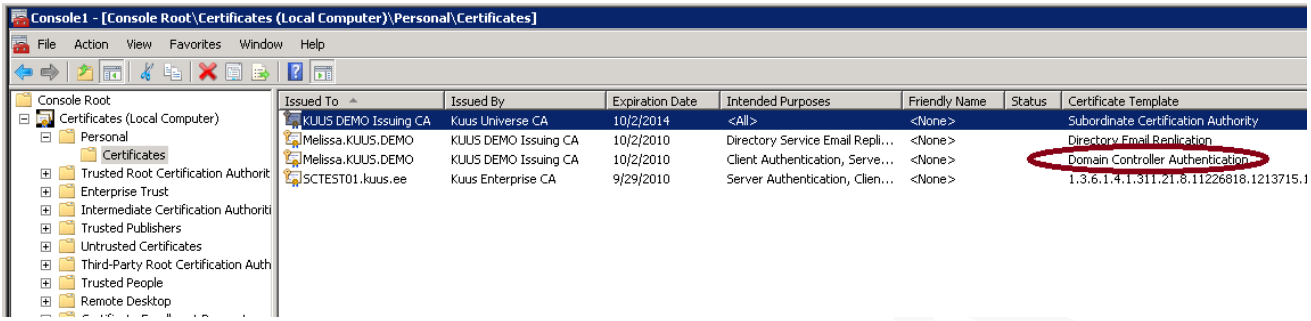
Täpsemalt käsitleme konfiguratsiooni ettevalmistust järgmistes alampunktides.

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 ka klientarvutitele endi identiteeti tõestada. Kõige mõistlikum tundub need sertifikaadid küsida lokaalse PKI lahendus käest[1]. Vaikimisi Windows *Enterprise* CA konfiguratsioonis on publitseeritud „*Domain Controller Authentication*“ sertifikaat[2], mida peavadki omama 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:



JOONIS 1. DOMEENI KONTROLLERI SERTIFIKAAT

Nagu ka eelnevalt juba mainitud, on see konfiguratsioon PKI lahendusega domeenides tavapäraselt juba korras!

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:

1) Juur-SK – usaldusväärne juursertifikaat
2) EE Certification Centre Root CA – usaldusväärne juursertifikaat
3) ESTEID-SK 2007 - usaldusväärne kesktaseme sertifikaat
4) ESTEID-SK 2011 - usaldusväärne kesktaseme sertifikaat

Kui domeeni kontrolleritele ei ole installeeritud ID kaardi tarkvara ja soovime nendel sertifikaate publitseerida automaatselt, siis soovitame modifitseerida *Default Domain Controllers* või mõnda teist

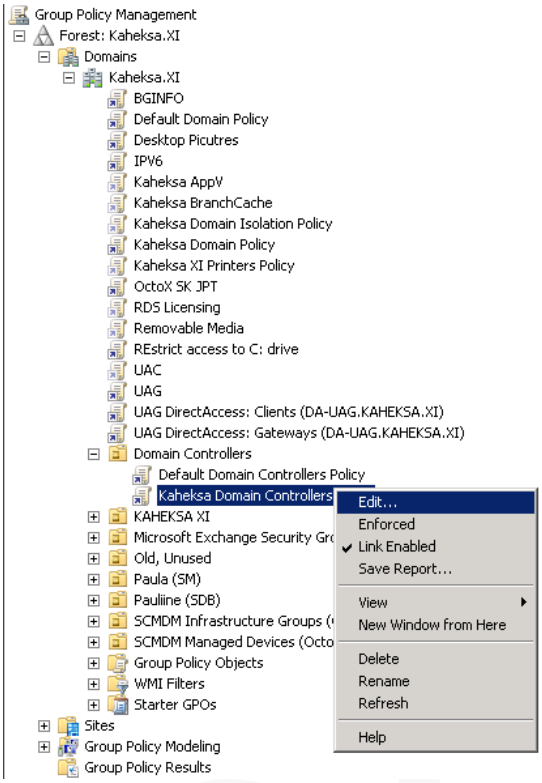
[1] Kui see muidugi olemas on, vastasel juhul tuleb sertifikaat hankida muid teid pidi.

[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.

domeeni kontrollerite CN tasemelt rakenduvat poliitikat. Sertifikaadid tuleb paigutada konteineritesse vastavalt ülaltoodud loendile ja tüübile.

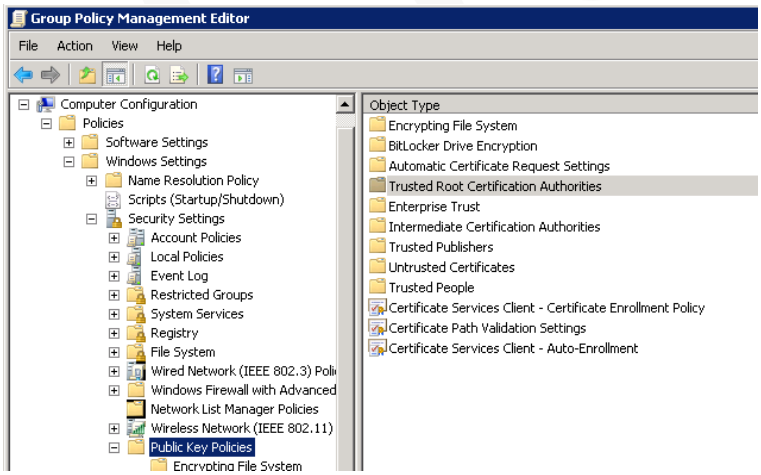
Järgnev on näide, kuidas publitseerida juurtaseme ning kesktaseme sertifikaate. Sertifikaatide publitseerimiseks usaldatud ja kesktaseme sertifikaatide kaustades:

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



JOONIS 2. SOBIVA GPO VALIK

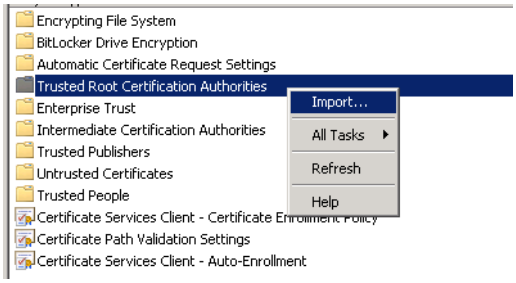
2) Vali kaust „*Computer Configuration/Policies/Windows Settings/Security Setting/Public Key Policies*“



JOONIS 3. GPO KAUSTA VALIK

3) Juur-SK sertifikaadi lisamiseks:

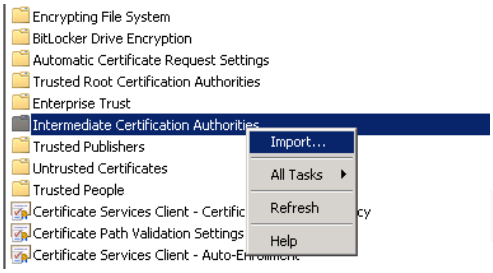
a. Paremkliki kaustal *Trusted Root Certification Authorities* ja kliki *Import*



JOONIS 4. JUUR-SK SERTIFIKAADI IMPORT

b. Kliki *Next*, vali Juur-SK sertifikaat ja impordi see.
c. Korda tegevusi a ja b sertifikaadi „EE Certification Centre Root CA“ lisamiseks publitseeritud juurtaseme sertifikaatide hulka.

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



JOONIS 5. KESKTASEME SERTIFIKAATIDE IMPORT

b. Kliki *Next*, vali sertifikaat ESTEID-SK 2007 ja impordi see.
c. Korda tegevusi a ja b sertifikaadi „ESTEID-SK 2011“ lisamiseks publitseeritud kesktaseme sertifikaatide hulka.

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*.

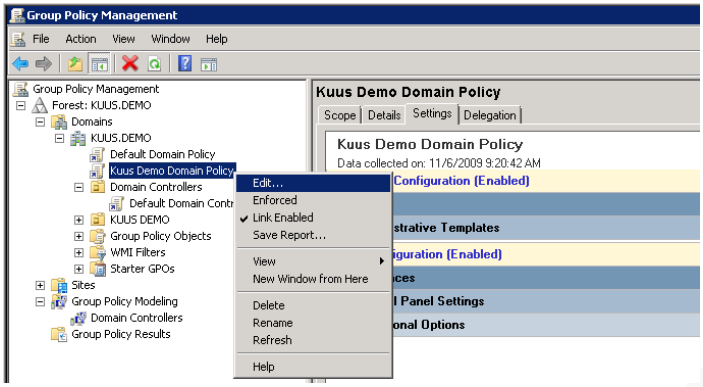
Antud näite varal publitseerime sertifikaadid automaatselt kõikidel domeeni kontrolleritel. Samal viisil võib vajalikud sertifikaadid publitseerida ka kõikidele muudele Windows tööjaamadele ja serveritele. Kuna aga klientidel publitseeritakse sertifikaadid koos ID kaardi utiliidi installatsiooniga, siis vähemalt klientide puhul selline vajadus puudub. Konkreetne lahendus sõltub konkreetsest olukorrast.

Märkus. Kui SK loob uue kesktaseme sertifikaadi ID kaartide sertifikaatide väljastamiseks tuleb vastav sertifikaat ID-logini toetamiseks siin uute ja/või uuendatud sertifikaatidetoetamiseks ka publitseerida. Ja muidugi tuleb vajadusel uuendada ka juurtaseme sertifikaati – seda siis, kui kesktaseme sertifikaat allkirjastatakse uue juursertifikaadiga.

TARGA KAARDI OMADUSTE HÄÄLESTUS

Toetamaks ID kaardi logimist keskselt kõikidel võimalikel klientarvutitel kasutame domeeni taseme poliitikat[3]:

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



JOONIS 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*

Peale muudatuste sisseviimist peavad omadused väljenduma järgmisel visuaalsel kujul:

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

JOONIS 7. *SMART CARD* OMADUSED GPOS

ID KAARDI TOETAMINE ÜKSIKARVUTITEL

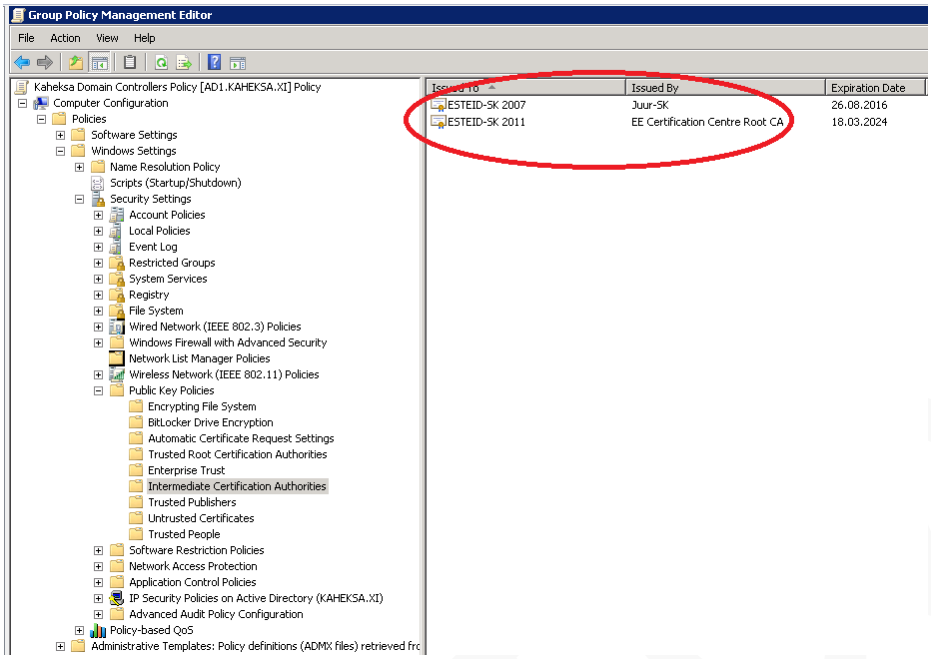
Juhul, kui ID kaardiga tahetakse logida näiteks domeenivälisest koduarvutist domeeni serverisse üle RDP ühenduse, tuleb koduarvuti häälestada toetama ID kaarti (logimise vaates). Selleks tuleb koduarvutil administraatori õigustes käivitada lokaalne poliitikate haldur käsuga *gpedit.msc*. Poliitikate 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"*! Peale kirjeldatud muudatuse sisseviimist tuleb uuendada poliitikaid käsuga *gpupdate /force* või restartida arvuti, ja ID kaardiga logimine osutubki võimalikuks.

OCSP SERTIFIKAADIKONTROLLI MEETODI KEHTESTAMINE

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

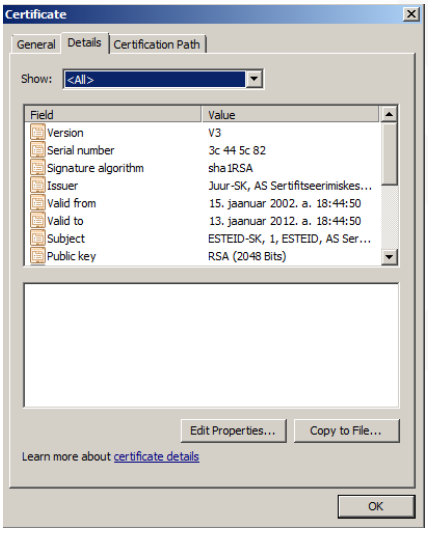
Kasutamaks OCSP-põhist sertifikaadi kehtivuse kontrolli tuleb häälestada publitseeritud kesktaseme sertifikaatide omadused järgmiselt:

1) Ava poliitika kesktaseme sertifikaatide publitseerimine alamosast „Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Intermediate Certification Authorities“:



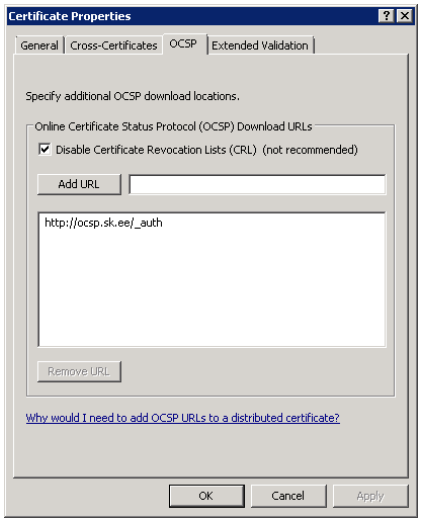
JOONIS 8. KESKTASEME PUBLITSEERITUD SERTIFIKAADID

2) Ava publitseeritud sertifikaat „ESTEID-SK 2007“ topeltklõpsuga ja vali leht *Details*:



JOONIS 9. SERTIFIKAADI OMADISED, DETAILIDE LEHT

3) Kliki nupul „Edit Properties...“ ja avanevas aknas vali OCSP ja lisa tee http://ocsp.sk.ee/_auth [4] SK OCSP teenuse juurde[5]. Puhta OCSP lahenduse kasutuseks keela CRL-põhine kontroll. Vaata joonist[6]:



4) Kliki OK konfiguratsiooni kinnistamiseks
5) Korda samme 2-4 sertifikaadiga ESTEID-SK 2011

Lisaks eeltoodud kesktaseme sertifikaatide konfiguratsioonile tuleb domeeni kontrolleritel usaldada ka SK OCSP autentimise *responder* sertifikaati! Selleks:

1) Lae alla SK OCSP *responder* sertifikaat aadressilt http://www.sk.ee/certs, vali sertifikaat AUTHENTICATION OCSP RESPONDER.
2) Lisa allalaetud sertifikaat domeeni Trusted Root Certification Authorities teeki (vt. peatükki Sertifikaatide publitseerimine).

Eelkirjeldatud, OCSP-põhine kontroll on Sertifitseerimiskeskuse poolt toetatud variant ID-logini rakendamiseks domeenides. OCSP kasutamise eeliseks CRL[7]-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 (seisuga 18.06.2010 on esteid2007.crl 9,66 MB ja esteid2011.crl 942 KB suur). Samas võib kasutaja sisse logida kuni 12 tundi sertifikaadi abil mis enam ei kehti (CRL nimekirjade uuenduste vaheline tsükkel). OCSP-põhise kontrolli puhul küsitakse sertifitseerimiskeskuse OCSP teenuselt kindlal ajahetkel sertifikaadi kehtivuse info, mis on efektiivsem ja turvalisem.

---

[4] http://ocsp.sk.ee/_auth

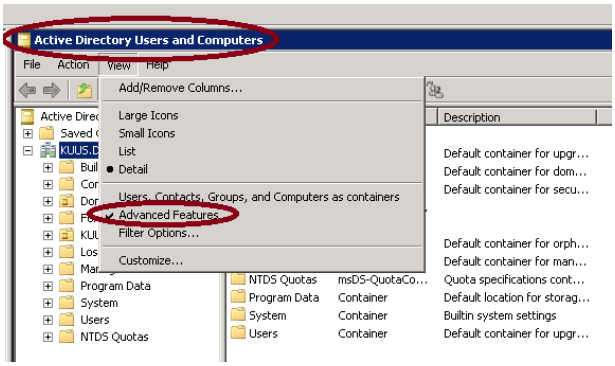
[5] Sertifitseerimiskeskuse OCSP teenus on tasuline ja selle kasutamine tuleb eraldi kokku leppida. Võimalikud on IP aadresside põhised ja sertifikaatidele toetuvad variandid.

[6] Juhul, kui OCSP on kirjeldatud, eelistatakse uuemate Microsofti klientoperatsioonisüsteemide poolt alati vaikimisi seda meetodit. Kui OCSP-põhine kontroll ei õnnestu katsutakse sertifikaadi kehtivust kontrollida CRL-meetodil.

[7] *Certificate revocation list* elik sertifikaatide tühistusnimekiri

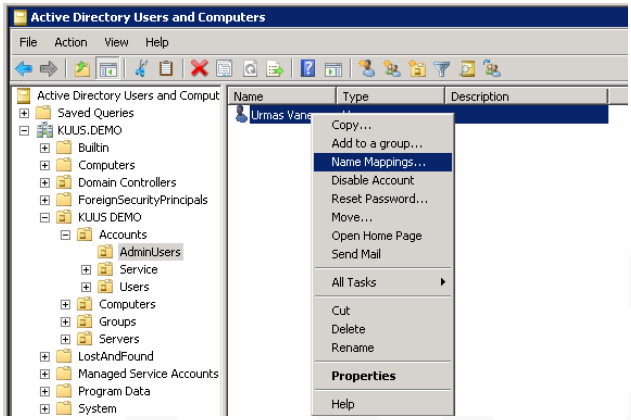
Kasutaja sidumiseks konkreetse ID kaardi sertifikaadiga tuleb:

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



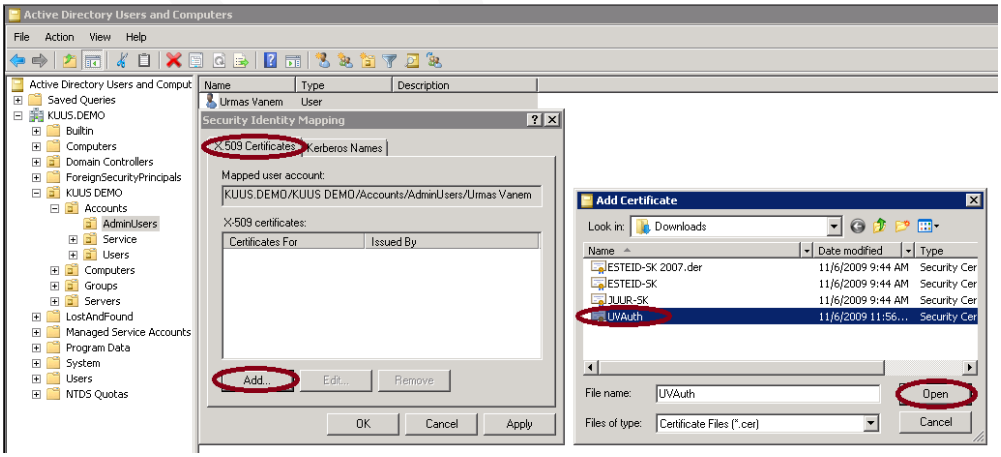
JOONIS 10. ADUC LAIENDATUD VAATE SISSE LÜLITAMINE

2) Paremklikkida soovitaval kasutajal ja valida *Name Mappings*



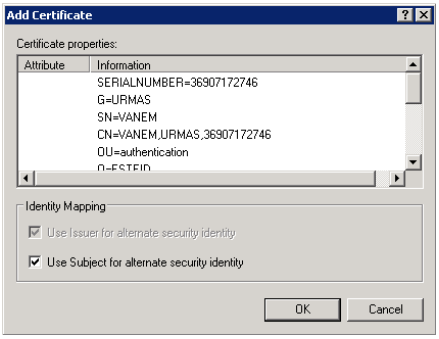
JOONIS 11. *NAME MAPPINGS*

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



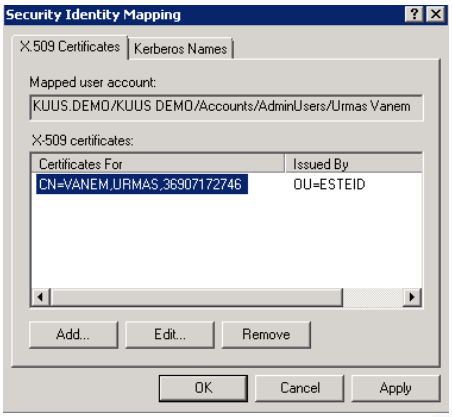
JOONIS 12. KASUTAJASERTIFIKAADI VALIK

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



JOONIS 13. *ADD CERTIFICATE* AKEN

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



JOONIS 14. *SECURITY IDENTITY MAPPING* AKEN

Märkus. Kasutaja sertifikaadi saamiseks on võimlikud erinevad meetodid:

1) Küsida kasutaja sertifikaat isikukoodi põhjal SK LDAP andmebaasist päringuga ldap://ldap.sk.ee:389/c=EE??sub?(serialNumber=ISIKUKOOD), kus ISIKUKOOD on otsitava isiku isikukood
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* (IE8))
3) Käsuga „certutil.exe –scinfo“ kui ID kaart on lugejas
4) Kasutada kohandatud automaatikaid[8]:
    a. Kõikide kasutajate sertifikaatide automaatne uuendus
    b. Sertifikaatide uuendus ADUC konsooli täienduse abil

KLIENTARVUTITE ETTEVALMISTUS

TARKVARA

[8] Vt. peatükk „Kohandatud automaatikad“

Klientarvutitele tuleb installeerida ID kaardi haldustarkvara. Toetame domeeni logimist alates versioonist 3.5.

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!

KOHANDATUD AUTOMAATIKAD

Koostöös „Number Kuus Konsultatsioonid OÜ-ga“ on võimalik tellida kataloogiteenustes sertifikaatide haldust lihtsustav tööriist, mis võimaldab:

1) Laadida kasutajate sertifikaadid isikukoodi alusel alla ning siduda need domeeni kasutajakontoga[9].
2) Luua ajastatud uuendusi – näiteks uuendatakse puuduvaid või aegunud sertifikaate igal ööl.
3) Siduda kasutajatega nii ID-kaardi kui Digi-ID sertifikaadid.
4) Teostada sertifikaatide sidumine kasutajakontoga grupi ja/või OU põhiselt.

VÕIMALIKUD PROBLEEMID

ESIMENE LOGIN JA CSP

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 „valedelt“ kasutajatelt.

KOKKUVÕTVALT

ID-kaardi põhine logimine on hea võimalus lihtsustada kasutajate sisselogimist tõstes samaaegselt süsteemide turvalisust. Kuna täna on paljud ettevõtted juba liikunud Windows 7 platvormile siis muutub see järjest populaarsemaks domeeni logimise viisiks.

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

[9] Isikukoodid peavad eelnevalt olema kataloogiteenustes kirjeldatud.

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!