Haaga-Helia
ammattikorkeakoulu Oy

Active Directory -toimialueelle kirjautuminen terveydenhuollon toimikortilla

Henry Hyttinen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma

2015

Tekijä(t)
Henry Hyttinen

Koulutusohjelma
Tietojenkäsittely

Opinnäytetyön otsikko
Active Directory -toimialueelle kirjautuminen terveydenhuollon toimikortilla

Sivu- ja liitesivumäärä
37 + 3

Opinnäytetyön otsikko englanniksi
Enabling logging on to an Active Directory domain using Finnish healthcare smart card

Työssä mahdollistetaan Active Directory (AD) -toimialueelle kirjautuminen terveydenhuollon toimikorttia käyttäen Windows Server 2012/Windows 7 -ympäristössä. Käydään läpi AD-ympäristöön tehtävät asetukset, jotka vaaditaan toimikorttikirjautumisen mahdollistamiseen, sekä juuri-Certificate Authorityn (CA) asennus ja konfigurointi. Oletetaan, että AD-ympäristö on jo olemassaoleva, eikä täten työssä käydä läpi AD:n asennusta tai määrittelyä niiltä osin, mitkä eivät ole vaadittuja toimikorttikirjautumisen mahdollistamiseen. Työ toteutettiin omassa testiympäristössään.

AD on Microsoftin hakemistopalvelu, joka mahdollistaa organisaation Windows -laitteiden ja niiden käyttäjien keskitetyn hallinnan. AD-toimialueet koostuvat siihen liitetyistä laitteista, joita hallitaan toimialueen Domain Controllereilla.

Asymmetrisen avainparin kryptografiassa käytetään avainparia tiedon salaamiseen ja salauksen avaamiseen. Avainpari koostuu julkisesta ja yksityisestä avaimesta. Ongalmana on se, että julkisen avaimen omistajuudesta ei voida olla täysin varmoja. PKI-hierarkia koostuu laitteista ja ohjelmistoista, jota kolmas osapuoli voi käyttää julkisen avaimen omistajuuden varmistamiseen.

Terveydenhuollon toimikortti on tavallinen sirukortti, jonka Väestörekisterikeskus (VRK) myöntää terveydenhuollon ammattihenkilölle. Se sisältää neljä VRK:n myöntämää varmennetta, joista kaksi ovat VRK:n CA- ja juurivarmenteet, ja henkilön autentikaatio- ja salausvarmenteen sekä allekirjoitusvarmenteen. Autentikaatiovarmenne sisältää AD-ympäristöön kirjautumiseen vaaditun subjectAltName -kentän.

Kortinlukija vaatii toimiakseen ajurit. Kortinlukijaohjelmisto asennetaan toimialueen tietokoneille ryhmäkäytäntöjä hyväksikäyttäen. VRK antaa terveydenhuollon toimikortteja varten käytettäväksi Fujitsun mPollux -ohjelmiston.

Jotta toimikorttikirjautuminen onnistuisi, tulee toimialueen Domain Controllereille jakaa Domain Controller -varmenteet. Tätä varten tulee asentaa ja määritellä toimialueelle oma juuri-CA. Lisäksi VRK:n juuri-CA on lisättävä toimialueen luotettuihin juuriin ryhmäkäytännön avulla.

Jotta korttikirjautuminen onnistuisi VRK:n varmenteita käyttäen, tulee AD-käyttäjien UPN:t muuttaa kortteja vastaaviksi, joka tuottaa ongelmia, mikäli toimialueella on käytössä Office 365-integraatio. Office 365 -integraatio hajoaa mikäli näin tehdään ilman muita toimenpiteitä. Voidaan ottaa käyttöön käyttäjävihjeen syöttö tai Alternate Login ID ongelman väistämiseksi.

Työn tuloksena kirjautuminen AD-toimialueelle terveydenhuollon toimikorttia käyttäen saatiin onnistumaan, ja siihen vaaditut toimialueen asetukset tehtyä oikein. Työ on monivaiheinen, ja siitä haastavan teki se, että siinä mukana olivat VRK:n myöntämät varmenteet, eikä itse myönnetyt. Itse myönnetyillä toimikorttien käyttäjävarmenteilla olisi saanut väistettyä AD-käyttäjien UPN:n vaihdot ja siitä seuraavat ongelmat.

Asiasanat
Active Directory, toimikortit, Windows Server, terveydenhuolto

Author(s)
Henry Hyttinen

Degree programme
Bachelor's Degree in Business Information Technology

Report/thesis title
Enabling logging on to an Active Directory domain using Finnish healthcare smart card

Number of pages and appendix pages
37 + 3

The study looks into the ways to enable logging on to an Active Directory (AD) domain using Finnish healthcare smart card in a Windows Server 2012/Windows 7 environment. The AD settings that are required for smart card login, as well as the installation and configuration of a root Certificate Authority (CA) are explained. It is assumed that the AD environment already exists, and thus this study does not cover any part of AD installation or configuration that is not directly related to enabling smart card logon. Practical part of the study was done in its own testing environment.

The information for the study was gathered out from multiple different web sources, mostly Microsoft's. The study was done by applying the theory to practice in the test environment and creating a working solution.

AD is Microsoft's directory service that allows an organization to administer its Windows devices and users in a centralized way. AD domains consist of the devices joined to it that are administered with the domain's Domain Controllers.

A key pair is used to encode and decode data in asymmetric cryptography. The key pair consists of a public key and a private key. The problem is that normally you can't be completely sure about a public key's ownership. PKI hierarchy consists of devices and software that can be used by a third party to verify the ownership of a public key.

The study reveals that the Finnish healthcare smart card is a normal chip card which is granted by Väestörekisterikeskus (VRK) to healthcare personnel. The card contains four certificates granted by VRK: two of them are VRK's root and CA certificates, and two are the person's authentication and encryption and non-repudiation certificates. The authentication certificate contains the subjectAltName field which is required for AD smart card logon.

The card reader requires drivers for it to work. Group Policies are used to install Fujitsu's mPollux card reader software on the domain's nodes. mPollux is given by VRK for use with healthcare smart cards.

For the smart card logon to work, the domain's Domain Controllers need to be granted Domain Controller certificates. Installing and configuring a root CA for the domain is required for this. In addition, VRK's root CA must be added to the domain's trusted roots using Group Policies.

To enable logon with VRK's certificates, the AD user's UPN must be changed to be the same as on the smart card. This breaks Office 365 integration on domains that use it unless measures are done. User name hints can be enabled or Alternate Login ID used to fix this problem.

To sum it up, the ultimate objective of the study, enabling Finnish healthcare smart card logon on an AD domain was accomplished, and the domain settings required for it were done right. The work consisted of multiple parts, and was made challenging due to using the certificates granted by VRK instead of self-granted certificates. By using self-granted certificates, the AD user UPN changes and problems resulting from it could have been avoided.

Keywords
Active Directory, smart cards, Windows Server, healthcare

Sisällys

1 Johdanto

Sähköisen reseptin (eResepti) käyttö vaatii, että tällaisia reseptejä myöntävä lääkäri käyttää terveydenhuollon toimikorttia tunnistautuessaan eReseptiin. Voidaan myös mahdollistaa terveydenhuollon toimikorteilla kirjautuminen Active Directory (AD) -toimialueeseen. Tässä työssä käydään läpi, miten toimikorteilla kirjautuminen mahdollistetaan AD -ympäristössä. Oletetaan myös, että tässä AD -ympäristössä ei ole olemassaolevaa CA:ta.

Tämä työ käsittelee, miten saadaan mahdollistettua AD -toimialueeseen kirjautuminen terveydenhuollon toimikortilla. Käyttöjärjestelminä toimivat Windows Server 2012 ja Windows 7. Väestörekisterikeskuksen sivuilta aiemmin löytynyt ohjeistus aiheesta oli vuodelta 2004, ja koski vanhaa Windows Server 2003/XP -ympäristöä. Enää kyseistä ohjetta ei Väestörekisterikeskuksen uudistuineilta sivuilta löydy. Tällaiselle dokumentaatiolle on siis tarve.

1.1 Toimeksiantaja

Toimeksiantaja on Plusterveys Oy, joka on suomalainen terveydenhuollon yritys, joka tarjoaa pääosin suun terveydenhuoltopalveluita, mutta myös lääkäri- sekä fysioterapiapalveluita.

1.2 Tavoitteet ja rajaus

Tässä työssä käsitellään terveydenhuollon toimikortteilla AD -ympäristöön kirjautumisen mahdollistavia AD:n asetuksia sekä juuri-Certificate Authorityn (CA) asentamista ja konfiguroimista.
AD -toimialueen pystyttämistä eikä hallintaa käsitellä niiltä osin, mitä ei tarvita toimikorttikirjautumisen käyttöönottoon. Oletetaan, että terveydenhuollon toimikortilla kirjautuminen halutaan mahdollistaa jo olemassaolevaan toimialueeseen.

1.3 Väestörekisterikeskus (VRK)

VRK myöntää ja allekirjoittaa terveydenhuollon toimikorteilla olevat varmenteet. Työssä lisätään VRK:n juurivarmenne osaksi toimialueen luotettuja varmenteita. Lisäksi VRK:lta voidaan saada testikäyttöön tarkoitettu TestiCA -varmenne. Kun työssä puhutaan TestiCA:sta, on siis kyse tästä testitarkoitukseen luodusta VRK:n varmenteesta.

1.4 Opinnäytetyön rakenne

Työssä ensin käydään läpi sen osien teoriataustaa. Aloitetaan Active Directoryllä, minkä jälkeen käydään läpi toimikortti, varmenteet ja PKI -hierarkia. Teoriataustan jälkeen on

käytännön toteutus, jossa käydään läpi, miten ratkaisu toteutettiin. Käytännön toteutuksessa on kuhunkin kohtaan sopivaa taustatietoa sitä tarvittaessa. Käytännön toteutuksen jälkeen käydään läpi ratkaisun testaus sekä lopuksi yhteenveto.

2 Active Directory lyhyesti

Active Directory on Microsoftin hakemistopalvelu, joka on keskeinen osa organisaatioiden Windows -arkkitehtuuria. Se mahdollistaa mm. keskitetyn käyttäjänhallinnan ja tietokoneiden asetusten hallinnan. Active Directoryn rakenne koostuu metsistä (forest), toimialueista (domain) ja organisaatioyksiköistä (organizational unit). Metsä on yksi täysi Active Directory -kokonaisuus, ja se sisältää kaikki kyseisen kokonaisuuden toimialueet, joita voi olla yksi tai useampi. Oletusarvoisesti Active Directory jakaa tietoa ainoastaan metsän sisäisesti. Organisaatioyksiköitä käytetään erilaisten olioiden (kuten tietokoneet tai käyttäjät) organisointiin toimialueiden sisällä niin, että niiden hallinta ja löytäminen onnistuisi. (Microsoft, päivitetty 2014a.)

2.1 Toimialueet

Toimialueet ovat Active Directoryn hallinnan kannalta keskeisin osa. Toimialueet koostuvat yhdestä tai useammasta domain controllerista ja muista laitteista, jotka siihen liitetään. Muut tietokoneet voivat olla työasemia tai palvelimia. Domain controller (tai domain controllerit, mikäli niitä on useampi) nimensä mukaisesti hallitsee toimialuetta ja sen laitteita sekä toimialueen käyttäjätunnuksia. Toimialueeseen luoduilla käyttäjätunnuksilla kirjautuminen onnistuu kaikille saman toimialueen sekä metsän tietokoneille. Käyttäjätunnuksille voidaan antaa eritasoisia oikeuksia ryhmien kautta, kuten esimerkiksi järjestelmänvalvojan oikeudet. (Microsoft, päivitetty 2014a.)

2.2 Organisaatioyksiköt

Organisaatioyksiköt ovat Active Directoryn rakenteen ”alin” osa. Niitä käytetään eri olioiden organisointiin toimialueen sisällä toimialueen hallinnan helpottamiseksi. Olioita ovat esimerkiksi toimialueeseen liitetyt tietokoneet ja toimialueen käyttäjät. (Microsoft, päivitetty 2014a). Tässä työssä saadaan kortinlukijaohjelmiston asennus -ryhmäkäytäntö vaikuttamaan vain haluttuihin koneisiin organisaatioyksiköiden avulla.

2.3 Ryhmäkäytännöt

Ryhmäkäytännöillä (Group Policy) hallitaan toimialueen laitteiden asetuksia. Niillä voidaan esimerkiksi asentaa ohjelmia, tehdä rekisteriin muutoksia tai yhdistää jaettuihin verkkolevyihin. Ryhmäkäytännölle valitaan ”alue”, johon se vaikuttaa. Se voi vaikuttaa koko toimialueeseen, tai yhteen tai useampaan organisaatioyksikköön. Esimerkiksi ryhmäkäytäntö, jolla asennetaan kortinlukijaohjelmisto, voidaan haluta laittaa vaikuttamaan ainoastaan työasemiin, eikä mihinkään muuhun, kuten tässä työssä tehdään. (Microsoft, päivitetty 2013.)

3 PKI (Public Key Infrastructure) -hierarkia

Asymmetristen avainten kryptografiassa käytetään avainparia tiedon (esim. sähköpostin sisältö) salaamiseen ja salauksen avaamiseen. Avainpari koostuu julkisesta että yksityisestä avaimesta, ja parin avaimella salatun tiedon saa avattua ainoastaan saman avainparin toisella avaimella. Käyttäjän on pidettävä yksityinen avaimensa salassa, mutta jaettava julkinen avain kaikille, joiden kanssa hän aikoo vaihtaa tietoa salattuna. Tässä ongelmana on se, että ei ole täyttä varmuutta siitä, kuuluuko jaettu julkinen avain todellakin sille henkilölle, jolle sen väitetään kuuluvan. PKI -hierarkian tarkoituksena on auttaa tässä ongelmassa. (Microsoft, ei julkaisupäivämäärää A.)

PKI -hierarkia koostuu laitteistosta ja ohjelmistosta, jota luotettu kolmas osapuoli voi käyttää julkisen avaimen omistajuuden määrittämiseen. Tätä luotettua kolmatta osapuolta kutsutaan CA:ksi (Certification authority). CA on luotettu taho, joka myöntää varmenteita (sertifikaatteja), joilla taataan julkisen avaimen omistajan identiteetti. (Microsoft, ei julkaisupäivämäärää B.) Se myöntää allekirjoitettuja varmenteita, jotka vahvistavat sen omistajan identiteetin, ja sitovat sen varmenteessa olevaan julkiseen avaimeen. Nämä varmenteet allekirjoitetaan CA:n omalla yksityisellä avaimella, ja CA myöntää vastaavan julkisen avaimen kaikille liittyville osapuolille CA -varmenteessa. Varmenteiden allekirjoitusprosessin tarkoituksena on varmistaa, että julkiseen avaimeen ei ole tehty ulkopuolisia muutoksia, tai että se olisi korruptoitunut tiedonsiirron aikana. (Microsoft, ei julkaisupäivämäärää A.)

PKI -hierarkia koostuu usein CA:sta, Registration Authoritystä, varmennetietokannasta (Certificate Database), varmennesäiliöstä (Certificate Store) sekä avainten arkistointipalvelimesta (Key Archival Server). Registration Authority jakaa tiettyjä varmenteita CA:n myöntämällä varmenteella. Varmennetietokantaan tallennetaan varmennepyynnöt, jaetut ja perutut varmenteet, ja varmennesäiliöön tallennetaan paikalliselle tietokoneelle myönnetyt ja odottavat tai hylätyt varmennepyynnöt. Arkistointipalvelin toimii varmuuskopiona. (Microsoft, ei julkaisupäivämäärää A.)

Tässä työssä luotava PKI -hierarkia on yksinkertainen: se koostuu ainoastaan toimialueen juuri-CA:sta, jonka tehtävänä on lähinnä jakaa Domain Controllereille Domain Controller -varmenteet. Varsinaiset toimikortteihin liittyvät varmenteet saadaan VRK:lta. VRK:n juuri-CA kuitenkin joudutaan lisäämään toimialueen luotettuihin juuriin.

4 Toimikortti ja varmenteet

Väestörekisterikeskus myöntää terveydenhuollon toimikortit ja niillä olevat varmenteet. Terveydenhuollon toimikortti on malliltaan tavallinen sirukortti, joka on kansainvälisen standardin ISO/IEC 7816 mukainen. Standardi määrittelee kortin ominaisuudet, kuten koon ja käytettävän kommunikaatioprotokollan. Kortti koostuu mikropiiristä, joka sisältää tietoa, kontaktipinnasta, jolla tapahtuu kommunikaatio kortin ja kortinlukijan välillä sekä kortin muoviosasta. (Smart Card Alliance, ei julkaisupäivämäärää A.)

Terveydenhuollon toimikortin käyttö tulee lähes pakolliseksi kaikille terveydenhuollon ammattilaisille asteittain Kelan KanTa -palvelujen myötä. Kanta -palvelut sisältävät mm. eReseptin, joka on sähköinen reseptijärjestelmä sekä potilastiedon arkiston. Kaikkien KanTa -palveluiden käyttö vaatii terveydenhuollon ammattilaiselta toimikortin käyttöä niihin tunnistautumisessa. (Kansallinen Terveysarkisto (Kanta) 2015.)

4.1 Toimikortilla olevat varmenteet ja niiden sisältö

Terveydenhuollon toimikortin siru sisältää Root- ja CA-varmenteet sekä kaksi loppukäyttäjän varmennetta, jotka ovat autentikaatioon ja salaukseen käytettävä sekä allerkirjoitusvarmenne (non-repudiation). VRK myöntää nämä kaikki varmenteet, ja ne ovat standardin X.509 v3 mukaisia. (Partanen, Pohjolainen, Toriseva, 2013, 3.) Allekirjoitusvarmenne toimii tiedon eheyden ja alkuperän todisteena. (Adrian McCullagh, William Caelli, 2000.)

Tervedeydenhuollon ammattilaiselle myönnetyt varmenteet sisältävät suuren määrän eri kenttiä, jotka sisältävät erilaista tietoa varmenteesta ja/tai varmenteen haltijasta. Tämän työn kannalta oleellisin kenttä on subjectAltName, joka on osa autentikaatioon ja salaukseen käytettävää varmennetta. Tämä kenttä vaaditaan, jotta toimikorttikirjautuminen Active Directory -ympäristöön olisi mahdollinen. (Partanen, 2013, 8-30.) Alla on selitettynä tämä subjectAltName -kenttä, ja lisäksi varmenteen loput kentät löytyvät liitteestä 1 – VRK:n myöntämän autentikaatio/salausvarmenteen kentät.

4.2 subjectAltName -kenttä

Mahdollistaa useiden identiteettien sitomisen varmenteen subjektiin, kuten esimerkiksi sähköpostiosoitteen. Microsoftin toimikortilla kirjautumisominaisuuksien tukemiseksi tämä sisältää myös UPN:n varmenteen subjektille. UPN:llä identifioidaan käyttäjiä Active Directoryssä, ja se on usein sähköpostiosoite. Esimerkiksi UPN voi olla etunimi.sukunimi@firma.fi tai kuten VRK:n korteille myöntämillä varmenteilla, mallia 123456789@teonet.fi. (Partanen, 2013, 24-25.)

4.3 Kortilla kirjautuminen

Jotta toimialueelle kirjautuminen toimikortilla onnistuisi, tulee kortilla olevan varmenteen täyttää tietyt vaatimukset. Kortilla olevan KDC -juurivarmenteen tulee sisältää HTTP CRL (Certificate Revocation List) -jakopisteen. Kortin kirjautumisvarmenteessa tulee myös olla HTTP CRL -jakopiste. CRL -jakopisteellä tarkoitetaan polkua tai osoitetta, josta kumottujen varmenteiden lista löytyy. CRL -jakopisteen tulee sisältää pätevä julkaistu CRL ja delta-CRL, mikäli mahdollista. Tämän lisäksi toimikortin varmenteessa tulee olla jompikumpi seuraavista: kenttä, joka sisältää toimialueen DNS -nimen tai UPN, jonka toimialueosa vastaa todellista toimialueen nimeä. Esimerkiksi mikäli toimialueen nimi on ont.henryh.local, tulee UPN:n olla mallia kayttaja@ont.henryh.local. (Microsoft, päivitetty 2011.) Koska käytämme kolmannen osapuolen myöntämiä varmenteita, joiden UPN ei ole oikeaa mallia, joudutaan tekemään myöhemmin toimenpiteitä kirjautumisen mahdollistamiseksi.

KDC (Key Distribution Center) on Kerberos -protokollan implementaatio. Tämä protokolla määrittää, miten asiakaskoneet toimivat verkkoautentikointipalvelun kanssa. Asiakaskoneet saavat KDC:ltä tikettejä, jotka kuvaavat käyttäjän verkkotunnuksia (tässä tapauksessa Active Directory -tunnuksia). Nämä asiakaskoneet esittävät sitten palvelimelle tiketit yhteyden muodostamisen jälkeen. (Microsoft, ei julkaisupäivämäärää C). Se toimii yhtenä prosessina, joka vastaa kahdesta palvelusta: Autentikointipalvelu (AS, Authentication Service) ja tikettejä myöntävästä palvelusta (TGS, Ticket-Granting Service). Toimialueen KDC sijaitsee domain controllerilla. Palvelun käynnistää domain controllerin LSA (Local Security Authority). Mikäli KDC tulee saavuttamattomaksi sen asiakkaille (toimialueen tietokoneet), tulee myös Active Directorystä niille saavuttamaton. (Microsoft, ei julkaisupäivämäärää D.)

LSA (Local Security Authority) on suojattu järjestelmä, joka autentikoi ja kirjaa käyttäjät sisään tietokoneelle, ja ylläpitää tietoa kaikista paikallisen järjestelmän turvallisuuden osa-alueista. (Microsoft, ei julkaisupäivämäärää E.)

Kun käyttäjä haluaa päästä tietokoneelle, ottaa tietokone yhteyden tikettejä myöntävään palveluun kyseisen tietokoneen toimialueella, antavat sille TGT:n ja pyytävät tikettiä tälle tietokoneelle. KDC:n tikettejä myöntävä palvelu myöntää tikettejä omassa toimialueessaan oleviin tietokoneisiin yhdistämistä varten. Tikettiä voidaan käyttää kunnes se vanhenee. (Microsoft, ei julkaisupäivämäärää D.)

KDC:n autentikaatiopalvelu myöntää tikettejä myöntäviä tikettejä (ticket-granting ticket, TGT) käytettäväksi toimialueelle yhdistämisessä. Ennen kuin asiakas voi pyytää tikettiä

koneelle, sen tulee pyytää TGT toimialueen autentikaatiopalvelulta. TGT:tä voidaan uudelleenkäyttää kunnes se vanhenee. (Microsoft, ei julkaisupäivämäärää D.)

CRL:n tarkoitus on jakaa tietoa kumotuista varmenteista tahoille, jotka pyrkivät vahvistamaan varmenteiden oikeellisuuden. Kumoamislistat sisältävät kumottujen varmenteiden sarjanumerot ja kumoamispäivämäärän. (Microsoft, ei julkaisupäivämäärää F.) CRL -jakopisteen tarkoituksena on määrittää sijainti, josta tämän kumoamislistan löytää.

4.3.1 Kirjautumistapahtuma toimikorttia käyttäen

Loppukäyttäjälle kirjautumisprosessista näkyy hyvin vähän. Loppukäyttäjä laittaa kortin lukijaan, valitsee kirjautumisikoninsa ja syöttää PIN -koodinsa. Mikäli kaikki menee oikein, niin kirjautuminen onnistuu ja käyttäjä pääsee kirjautumaan tietokoneelle. Mikäli jokin epäonnistuu, tulee tästä virheilmoitus eikä kirjautuminen onnistu.

Kortilla kirjautuminen toimialueen tietokoneelle alkaa sillä, että laitetaan toimikortti kortinlukijaan Windowsin kirjautumisikkunassa. Kun kortti on kortinlukijassa, Windowsin älykorttitunnustenhakija hakee kortilta tunnustetiedot, listan tunnetuista tunnuksista tai mikäli niitä ei kortilla ole, Windowsin löytämät kortinlukijan tiedot. Tämän jälkeen se hakee listan koneeseen liitetyistä kortinlukijoista ja niihin liitetyistä korteista. Sitten se käy läpi jokaisen kortin varmistaakseen, että ryhmäkäytännön hallitsema kirjautumisvarmenne löytyy. Tämä varmenne tallennetaan tietokoneelle turvalliseen välimuistiin. Näiden vaiheiden jälkeen älykorttitunnustenhakija ilmoittaa Windowsin sisäänkirjautumiskäyttöliittymälle, että se on löytänyt uudet tunnukset. (Microsoft, päivitetty 2011.)

Seuraavaksi sisäänkirjautumiskäyttöliittymä pyytää nämä uudet tunnukset älykorttitunnustenhakijalta, joka sitten tarjoaa käyttöliittymälle jokaisen löydetyn kirjautumisvarmenteen. Käyttöliittymään tämän jälkeen ilmestyy kirjautumisikoni jokaiselle näille varmenteelle. Terveydenhuollon toimikortit sisältävät vain yhden kirjautumisvarmenteen, eikä koneisiin normitilanteessa yhdistetä samanaikaisesti useampaa toimikorttia tai kortinlukijaa, joten tässä vaiheessa yleensä ilmestyy ainoastaan yksi kirjautumisikoni, jonka käyttäjä valitsee, ja näkyviin ilmestyy PIN -syöttörivi. Kun käyttäjä syöttää PIN:insä, ja painaa Enter:iä tai käyttöliittymän nuolipainiketta, älykorttitunnustenhakija koodaa sen. (Microsoft, päivitetty 2011.)

Windowsin LogonUI -prosessissa oleva tunnustenhakija kerää syötetyn PIN -tunnuksen. Tiedot pakataan KERB_CERTIFICATE_LOGON -rakenteeseen älykorttitunnustenhakijassa. KERB_CERTIFICATE_LOGON -rakenteen tärkein sisältö on älykortin PIN, käyttäjätunnuksen nimi, toimialueen nimi sekä cspdata (lukijan nimi jne.). Tunnustenhakija käärii

nämä tiedot ja lähettää ne kirjautumiskäyttöliittymälle, josta Winlogon (Windowsin kirjautumisenhallinta) antaa nämä tiedot LSA:lle LSALogonUser:in avulla. (Microsoft, päivitetty 2011.)

LSA pyytää Kerberos SSP:tä (Kerberos -autentikointipaketti) tekemään Kerberos -autentikointipalvelupyynnön, johon kuuluu ennakkoautentikaattori. Tämän ennakkoautentikaattorin sisältämä tieto riippuu siitä, millainen käyttötarkoitus kirjautumiseen käytettävällä varmenteella on. Mikäli varmenteen käyttötarkoitus on digitaalinen allekirjoitus, sisältää se käyttäjän julkisen varmenteen ja vastaavalla yksityisellä avaimella allekirjoitetun varmenteen. Jos varmenteen käyttötarkoitus on salaus, sisältää ennakkoautentikaattori käyttäjän julkisen varmenteen ja vastaavalla yksityisellä avaimella salatun varmenteen. (Microsoft, päivitetty 2011.)

Seuraavaksi pyyntö allekirjoitetaan digitaalisesti. Se tapahtuu siten, että vastaavalle CSP:lle tehdään pyyntö yksityisen avaimen toimenpiteestä. Yksityinen avain on tallennettu tässä tapauksessa toimikortille, joten tämä tapahtuu toimikortilla. Toimenpiteen tulos lähetetään jälleen Kerberos SSP:lle, joka lähettää autentikaatiopyynnön domain controllerilla olevalle KDC:lle. KDC hakee käyttäjän tunnuksen Active Directorystä, ja vahvistaa allekirjoituksen käyttäjän varmenteella. (Microsoft, päivitetty 2011.)

Tämän jälkeen KDC vahvistaa käyttäjän varmenteen, jotta se voisi varmistua siitä, että varmenne on luotetusta lähteestä. Varmenteesta tarkastetaan mm. aika ja ettei sitä ole kumottu. Sitten KDC käyttää CryptoAPI:a rakentaakseen varmennepolun käyttäjän varmenteesta CA -varmenteeseen, joka sijaitsee domain controllerilla. KDC käyttää CryptoAPI:a vahvistaakseen ennakkoautentikaattorissa olleen digitaalisen allekirjoituksen. Domain controller vahvistaa allekirjoituksen ja käyttää käyttäjän julkista avainta varmistaakseen, että pyyntö tuli julkista avainta vastaavan yksityisen avaimen omistajalta. Tässä vaiheessa KDC myös varmistaa, että varmenteen myöntäjä on luotettu, ja että se löytyy NTAuth -varmennesäiliöstä. (Microsoft, päivitetty 2011.)

KDC saa käyttäjätunnuksen tiedot AD DS:ltä, minkä jälkeen KDC rakentaa haettuun käyttäjätunnukseen pohjautuvan TGT:n. TGT sisältää käyttäjän turvallisuustunnisteen (eli SID:n, security identifier), universaalien ja globaalien toimialueryhmien, joihin käyttäjä kuuluu, SID:t sekä sellaisten universaalien ryhmien SID:t, joissa käyttäjä on jäsen. Domain controller lähettää TGT:n osana KRB_AS_REP -vastausta. KRB_AS_REP koostuu seuraavista osista: oikeusattribuuttivarmenne (Privilege attribute certificate, PAC), käyttäjän SID, ryhmien, joissa käyttäjä on jäsenenä, SID:t, pyynnön tikettejä myöntävälle palvelulle sekä ennakkoautentikointitiedot. (Microsoft, päivitetty 2011.)

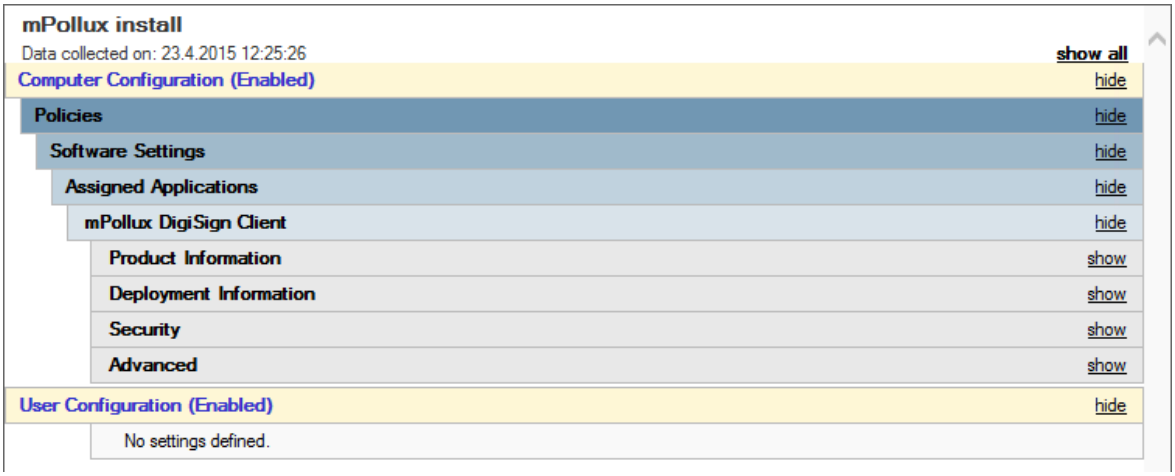
Seuraavaksi asiakaskone varmistaa KDC:n antaman vastauksen ensin KDC:n varmenteesta luotettuun juuri-CA:han johtavalla varmennepolun rakentamisella minkä jälkeen se käyttää KDC:n julkista avainta vastausallekirjoituksen vahvistamiseen. TGT on nyt saatu, ja asiakaskone saa palvelutiketin, jota käytetään tietokoneelle kirjautumiseen. Mikäli tämä onnistuu, niin LSA säilöö tiketit ja palauttaa LSALogonUser:ille onnistumisviestin, minkä jälkeen mm. käyttäjäprofiili ladataan ja ryhmäkäytännöt suoritetaan. Kun käyttäjäprofiili on ladattu, Windowsin palvelu CertPropSvc lukee varmenteet kortilta ja tallentaa ne käyttäjän varmennesäiliöön. Kun kortti poistetaan lukijasta, välimuistissa olleet varmenteet poistetaan. Ne eivät ole enää saatavilla kirjautumiseen. (Microsoft, päivitetty 2011.)

5 Kortinlukijaohjelmiston asennus

Jotta toimikortilla kirjautuminen voisi onnistua, tarvitaan toimialueen työasemiin kortinlukijan ohjelmisto ja ajurit. Tässä tapauksessa ohjelmistona toimii Fujitsu OY:n mPollux DigiSign Client, jonka VRK tarjoaa käyttöön ilmaiseksi niille, jotka käyttävät VRK:n myöntämää kansalais- tai organisaatiovarmennetta. (Väestörekisterikeskus). Asennusohjelmisto löytyy osoitteesta https://eevertti.vrk.fi/Default.aspx?id=307, ja vaihtoehtoina on sekä .exe -että .msi -versiot 32- ja 64-bittisinä. Valitaan haluttu .msi -versio, sillä .msi -pakettien asennus onnistuu ryhmäkäytäntöjen kautta automatisoidusti. Tallennetaan valittu .msi -paketti Domain Controllerille. Tämän jälkeen luodaan ryhmäkäytäntö, jolla paketti asentuu toimialueen työasemille.

5.1 Ryhmäkäytännön luonti

Avataan Group Policy Management, valitaan haluttu metsä ja toimialue, minkä jälkeen avataan Group Policy Objects. Luodaan Group Policy Objects -kansion alle uusi ryhmäkäytäntö. Kun ryhmäkäytäntö on luotu, ja se näkyy Group Policy Objects:in alla, muokataan sitä (hiiren oikea painike-> Edit). Group Policy Management Editor aukeaa. Valitaan Computer Configuration → Policies → Software Settings → Software Installation. Painetaan tyhjää aluetta hiiren oikealla painikkeella, ja valitaan New → Package. Asennuspaketin tulee olla verkkoon jaetussa kansiossa, jonka käyttöoikeudet on määritelty oikein. Tämän jälkeen valitaan oikea .msi -paketti, ja annetaan seuraavaan valintakohtaan ”Assigned”, mikäli ei ole tarvetta tehdä muutoksia asennusasetuksiin. Asennuspaketin sijainniksi tulee antaa sen verkkosijainti (muotoa \\share\folder\installer.msi), tai asennus ei onnistu (Kragh, 2012). Kun tämä on tehty, voidaan Group Policy Management Editor sulkea, ja linkittää luotu ryhmäkäytäntö vaikuttamaan haluttuun osaan toimialuetta, kuten tiettyyn OU:n. Luodun ryhmäkäytännön Settings -välilehden tulisi näyttää tämän jälkeen kuvan 1 mukaiselta.



Kuva 1 Kortinlukijaohjelmiston asennus -ryhmäkäytäntö

6 Root CA:n asennus

Palvelimesta tehdään enterprise root CA. Ennen Active Directory Certificate Services (AD CS) -roolin asennusta varmista, että palvelin, jolle sitä ollaan asentamassa, on liitetty oikeaan AD -toimialueeseen. AD CS -rooli tulisi asentaa sellaiselle palvelimelle, joka ei toimi Domain Controllerina palvelinten hyökkäyspinta-alan minimoimiseksi. (Adare, 2010.)

6.1 CAPolicy.inf -tiedoston valmistelu

CAPolicy.inf -tiedosto on valmisteltava ennen AD CS -roolin asentamista. Koska tiedostoa ei ole luotu automaattisesti, on se luotava polkuun c:\Windows\CAPolicy.inf. Kun tiedosto on luotu, avataan se Notepadilla, ja syötetään sen sisällöksi seuraavaa:

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID=Organisaation oma
Notice="Legal Policy Statement"
URL=http://pki.corp.contoso.com/pki/cps.txt
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=5
CRLPeriod=weeks
CRLPeriodUnits=1
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=1
[CRLDistributionPoint]
[AuthorityInformationAccess]
```

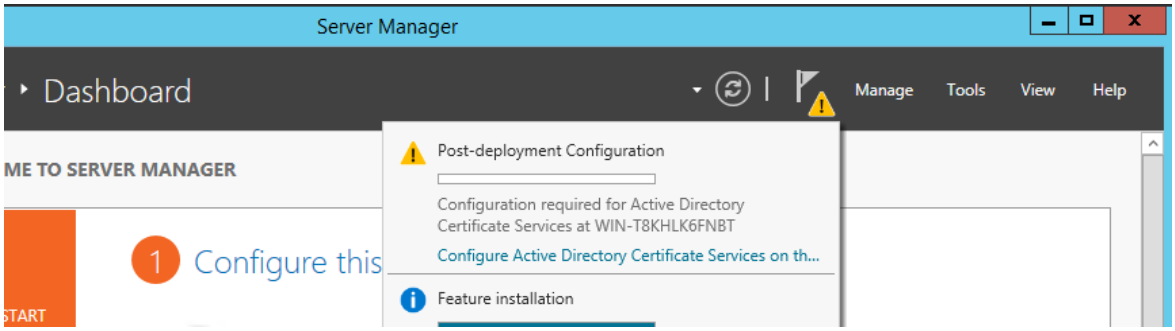
Riville ”URL=http://pki.corp.contoso.com/pki/cps.txt” määritellään certificate practice statementin (CPS) sijainti, ja riville ”OID=” syötetään organisaation oma OID. Kun yllä olevat tiedot on syötetty, tallennetaan tiedosto. Varmista, että tiedostopäätteenä on .inf, ja että merkistönä on ANSI. (Microsoft 2012a, Microsoft 2012b.)

6.2 Roolin asennus

AD CS -roolin asennus aloitetaan avaamalla Add Roles and Features Server Managerista. ”Before you begin” -ikkunassa valitaan Next, minkä jälkeen avautuvassa ”Installation type” -ikkunassa varmistetaan, että ”Role-based or feature-based installation” -kohta on valittuna, minkä jälkeen valitaan jälleen Next. ”Select destination server” -kohdassa varmistetaan, että tämä oikea palvelin on valittuna. ”Select server roles” -ikkunassa valitaan Active Directory Domain Services. Kun kysytään, asennetaanko AD CS:n vaatimat ominaisuudet, valitaan Add Features. Tämän jälkeen painetaan Next. ”Select features” -ikkunassa valitaan Next. Active Directory Certificate Services -ikkunassa valitaan Next. ”Select role services” -ikkunassa varmistetaan, että kohta ”Certification Authority” on valittuna, eikä muuta, sillä muille näille palveluille ei ole tarvetta nyt. ”Confirm installation selections” -ikkunassa varmistetaan, että on tehty oikeat valinnat. Kun ollaan tästä varmoja, valitaan Install. Kun asennus on valmis, voidaan tämä ikkuna sulkea. (Microsoft 2012a.)

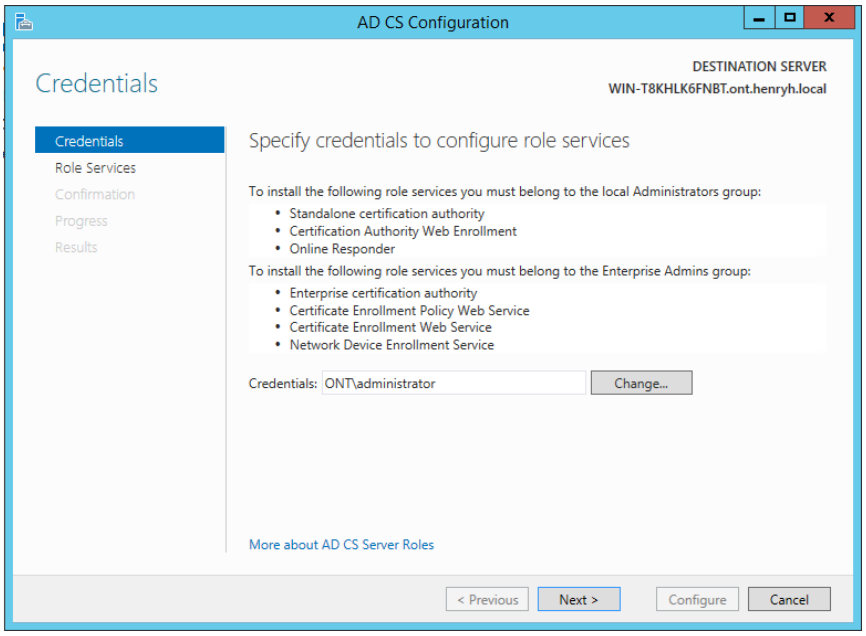
6.3 AD CS:n perusmäärittely

Kun rooli on asennettu ja asennusvelho suljettu, voidaan AD CS:n määrittely aloittaa Server Managerista kuvassa 2 näkyvästä, huutomerkillä merkitystä paikasta.



Kuva 2 Määrittelyn aloitus

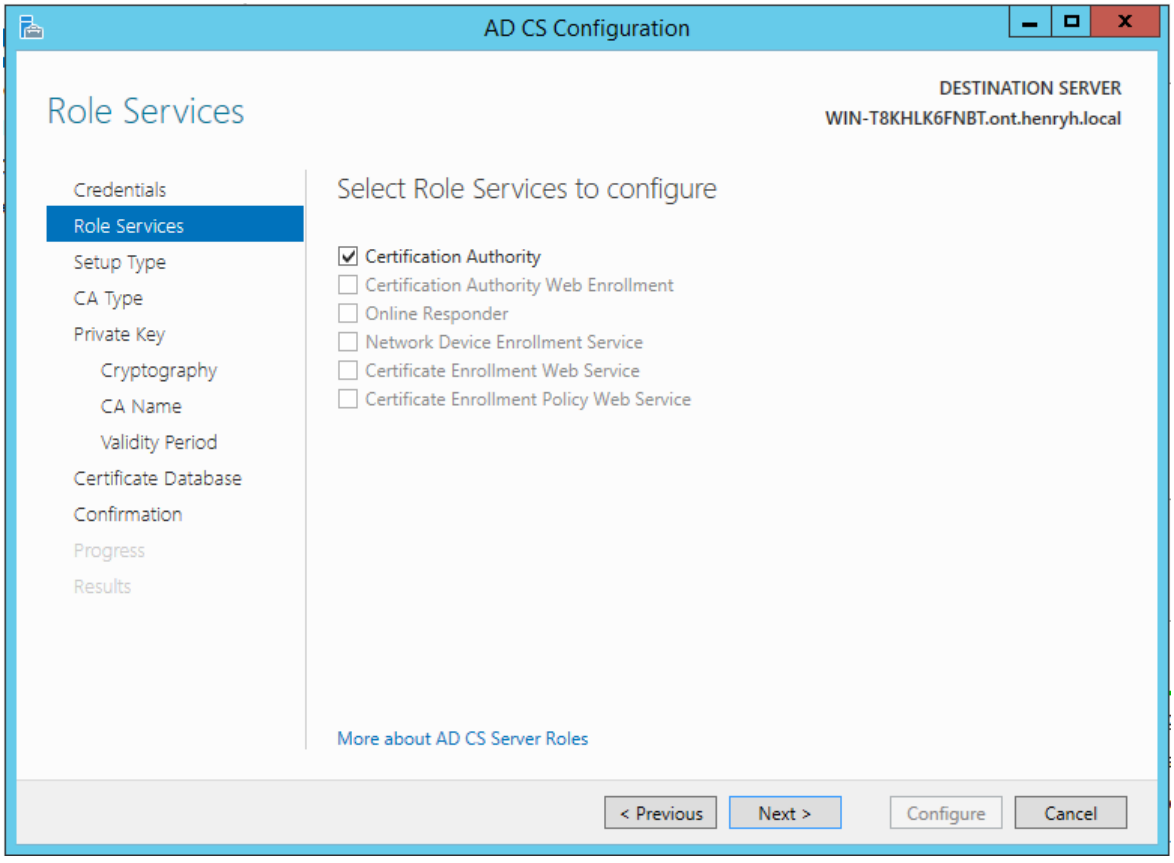
Kun määrittely aloitetaan, pyytää määrittelyvelho tunnukset, joilla palvelut määritellään. Koska halutaan luoda Enterprise certification authority, tulee käyttää sellaisia tunnuksia, jotka kuuluvat AD:n Enterprise Admins -ryhmään. (Microsoft 2012a.)



Kuva 3 Tunnusten antaminen

Käyttäjätunnus valitaan kuvassa 3 näkyvästä ”Change...” -painikkeesta. Kun tarvittavilla oikeuksilla varustettu käyttäjätunnus on valittu, mennään eteenpäin Next -painikkeesta.

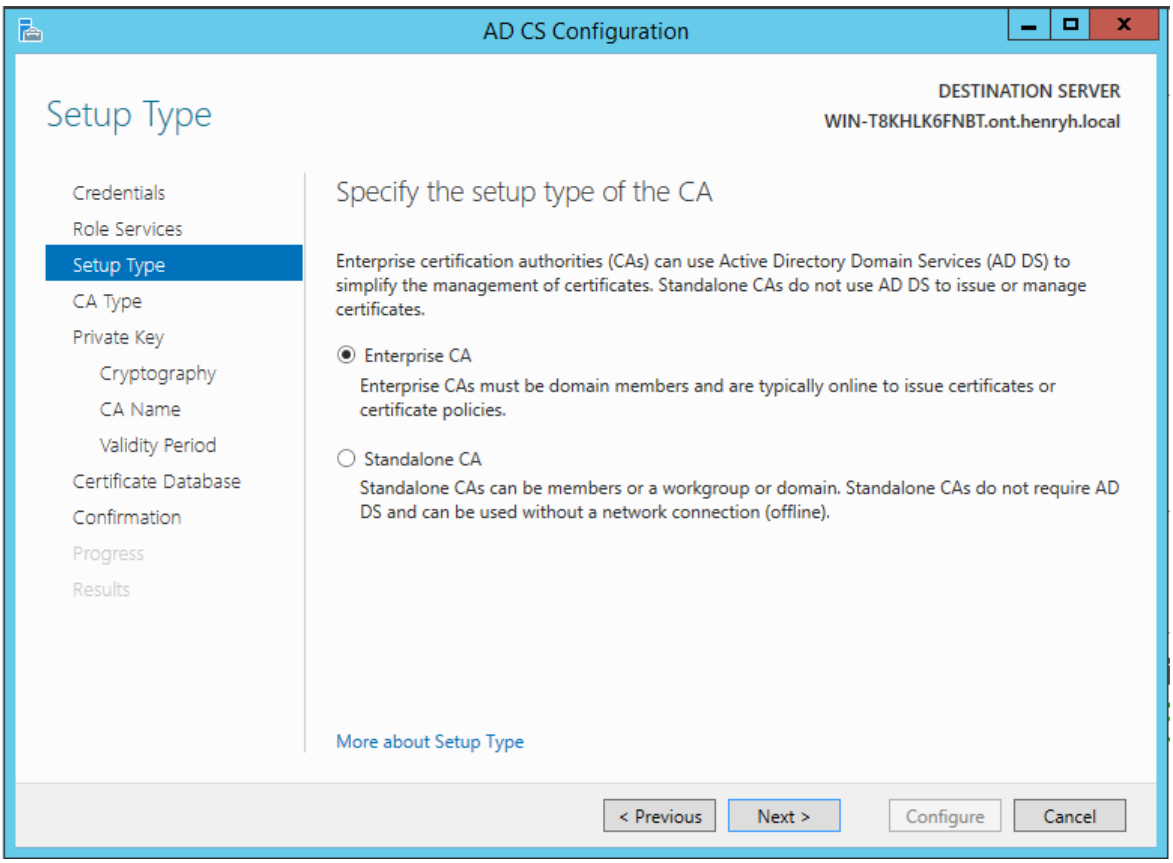
Seuraavaksi aukeaa kuvan 4 mukainen Select Role Services to Configure -ikkuna:



Kuva 4 Select Role Services to Configure

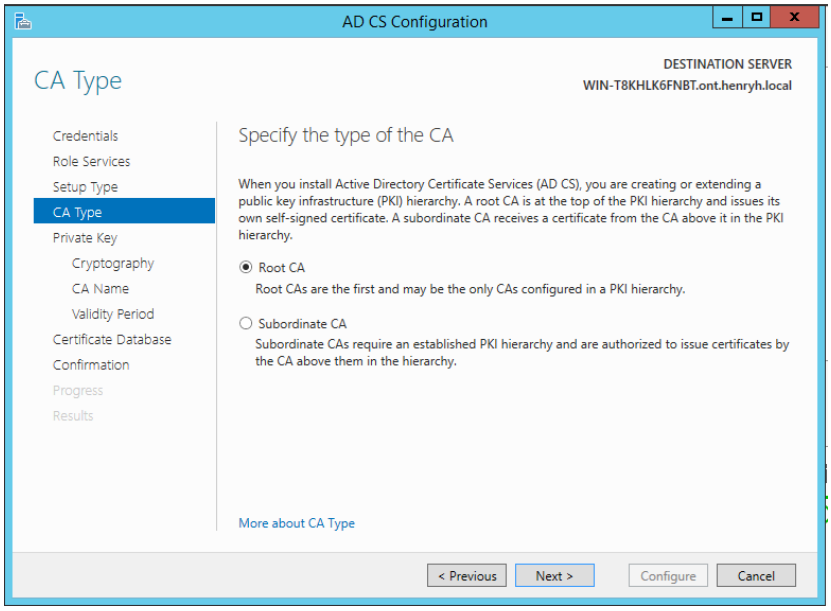
Aluksi tässä ikkunassa ei ole valittu mitään. Valitaan siis kuvan mukaisesti Certification Authority, ja painetaan Next -painiketta.

Seuraavassa ikkunassa valitaan, halutaanko tehdä Enterprise CA vai Standalone CA. Näiden eroina on se, että Enterprise CA:n tulee olla toimialueen jäsen, ja on tyypillisesti verkossa jakaakseen sertifikaatteja ja sertifikaattikäytäntöjä, kun taas Standalone CA:n ei ole pakko olla toimialueen jäsen, ja niitä voidaan käyttää ilman verkkoyhteyttä. Teemme Enterprise CA:n, joten valitaan se, ja painetaan Next -painiketta. Kuvassa 4 näkyy kyseinen ikkuna. Mikäli Enterprise CA:n valinta ei ole mahdollista, varmista, että olet antanut aikaisemmin sellaiset tunnukset, jotka kuuluvat Enterprise Admins -ryhmään.



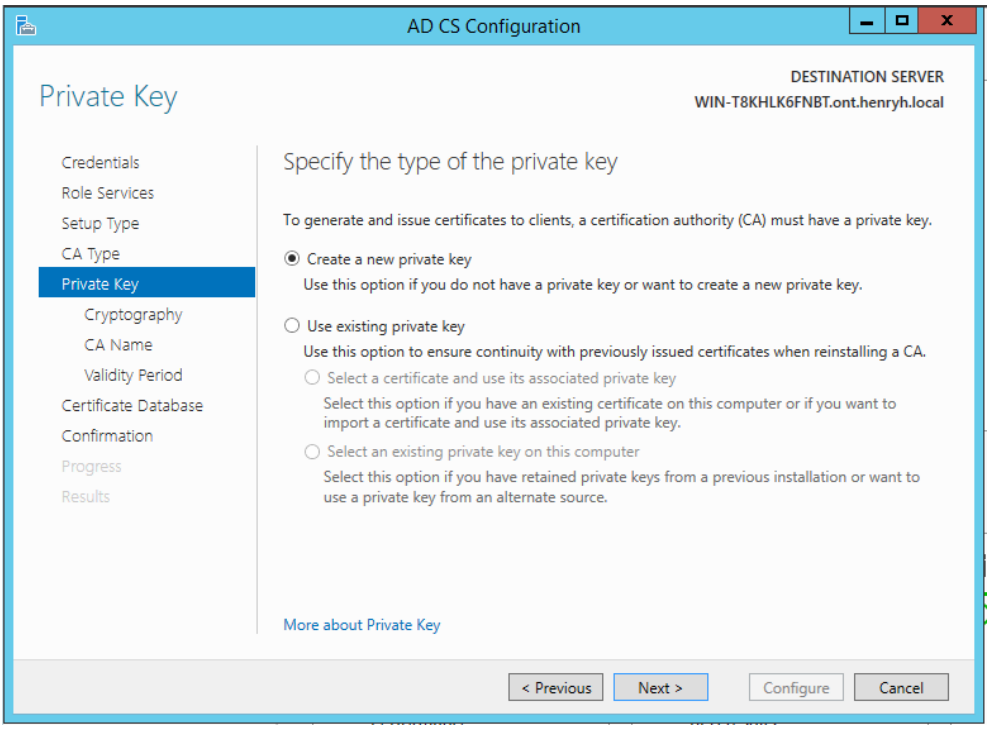
Kuva 5 CA:n asennustyypin valinta

Seuraavaksi määritellään CA:n tyyppi. Vaihtoehtoja on kaksi: Root CA tai Subordinate CA.



Kuva 6 CA:n tyypin valinta

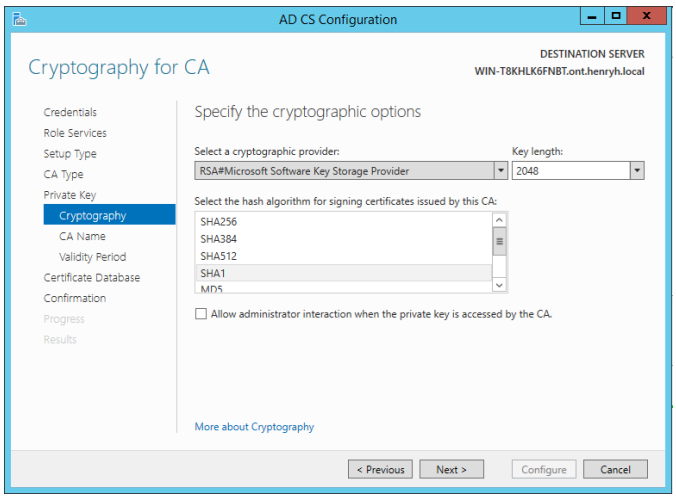
Root CA on PKI -hierarkian huipulla, ja jakaa oman itse-allerkirjoitetun sertifikaattinsa, ja ne ovat aina ensimmäinen, ja voivat olla myös ainoa, hierarkiaan määritelty CA. Subordinate CA puolestaan vastaanottaa sertifikaatit hierarkiassa itsensä yläpuolella olevalta CA:lta, ja niiden käyttäminen vaatii jo luotua PKI -hierarkiaa. (Microsoft, 2014.) Koska olemme luomassa ensimmäistä ja ainoata CA:ta tähän hierarkiaan, valitaan Root CA, ja painetaan Next -painiketta.



Kuva 7 Yksityisen avaimen tyypin valinta

Seuraavaksi valitaan yksityisen avaimen tyyppi. CA:lla on oltava yksityinen avain luodakseen ja jakaakseen sertifikaatteja asiakkaille.
Vaihtoehtoja on jälleen kaksi: uuden yksityisen avaimen luonti ja jo olemassaolevan avaimen käyttö. Valitaan uuden avaimen luonti (Create a new private key), koska palvelimella ei ole vielä mitään yksityistä avainta. Olemassaolevaa yksityistä avainta käytetään, kun halutaan varmistaa jatkuvuus aikaisemmin jaettujen sertifikaattien kanssa kun CA:ta uudelleenasennetaan. Kun on valittu, että luodaan uusi avain, painetaan Next -painiketta.

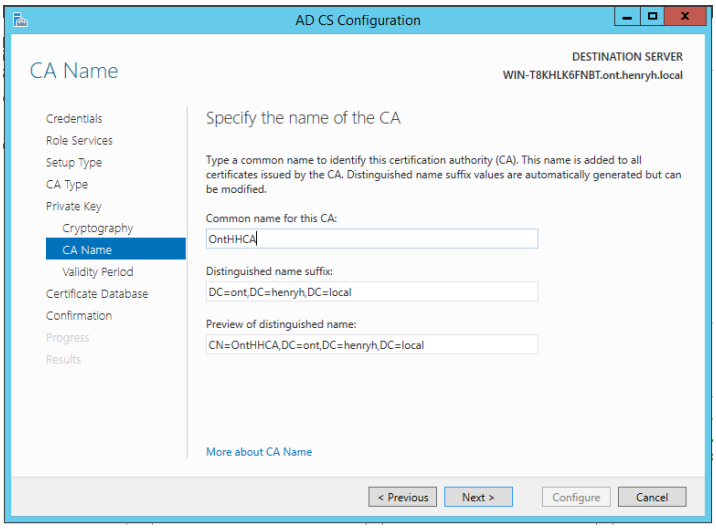
Seuraavaksi määritellään käytettävän kryptografian asetukset.



Kuva 8 Kryptografian asetukset

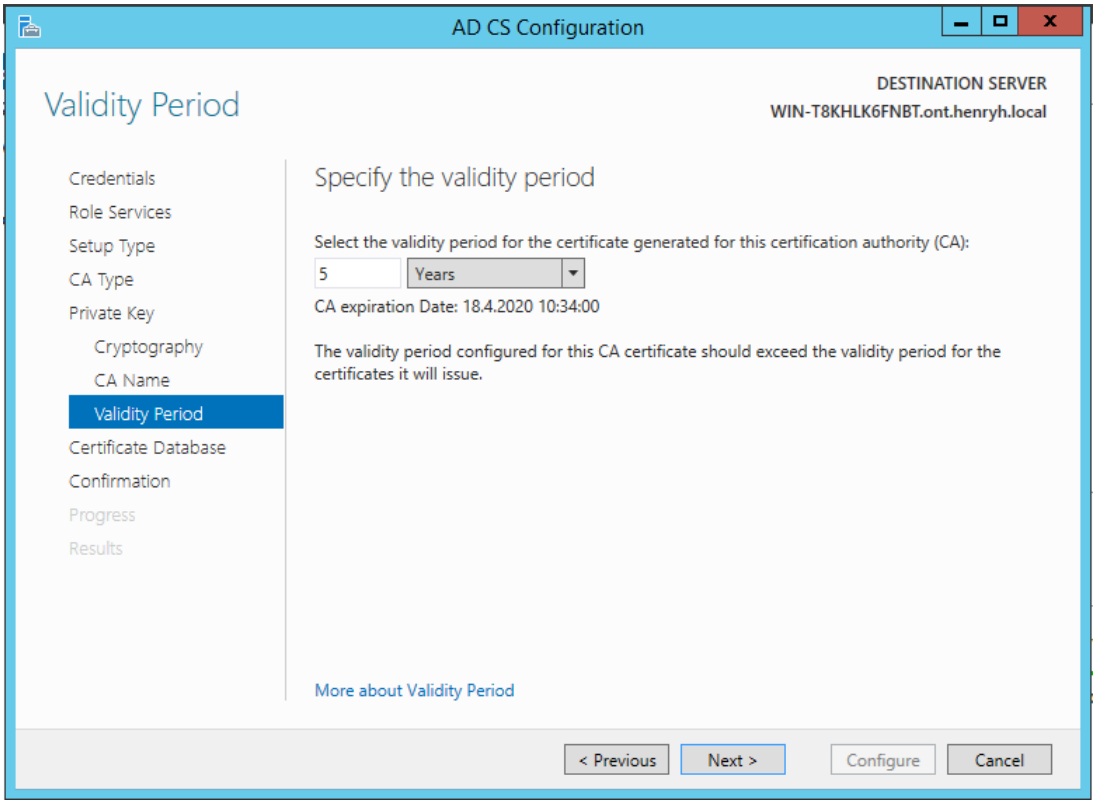
Varmista, että ”Select a cryptographic provider:” -alasvetovalikosta on valittu ”RSA#Microsoft Software Key Storage Provider”, Key Length on 2048 ja että tämän CA:n jakamat sertifikaatit allekirjoitetaan SHA1 -algoritmillä. Jätetään ”Allow administrator interaction when the private key is accessed by the CA” -valinta tyhjäksi, ja painetaan Next -painiketta. (Microsoft, 2012a.)

Seuraavassa ikkunassa määritellään CA:lle nimi. Syötetään haluttu nimi ”Common name for this CA” -kenttään, ja jätetään muut kentät koskemattomiksi (Microsoft, 2012a). Tämän jälkeen jatketaan eteenpäin.



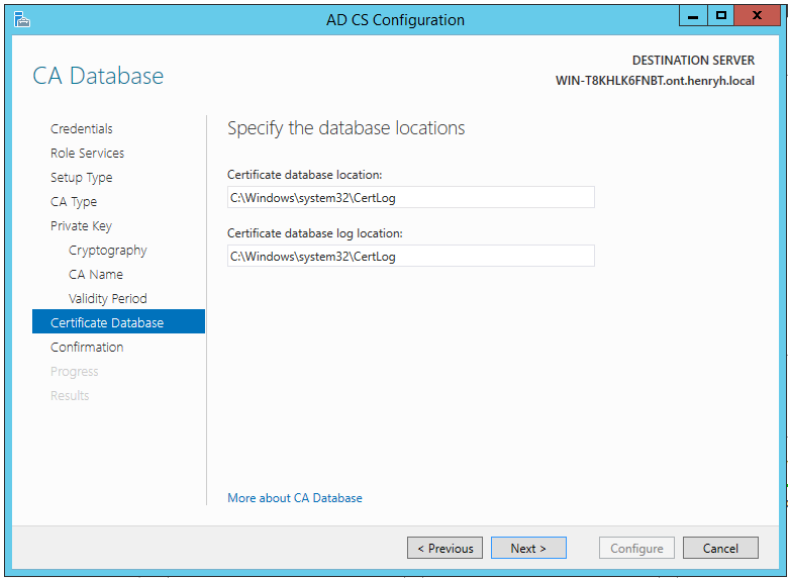
Kuva 9 CA:n nimeäminen

CA:n nimeämisen jälkeen määritellään, kuinka pitkän aikaa CA:lle luotu sertifikaatti on voimassa. Tässä määriteltävän pituuden tulisi olla pidempi, kuin sertifikaatit, joita se jakaa.



Kuva 10 Sertifikaatin voimassaoloajan määrittely

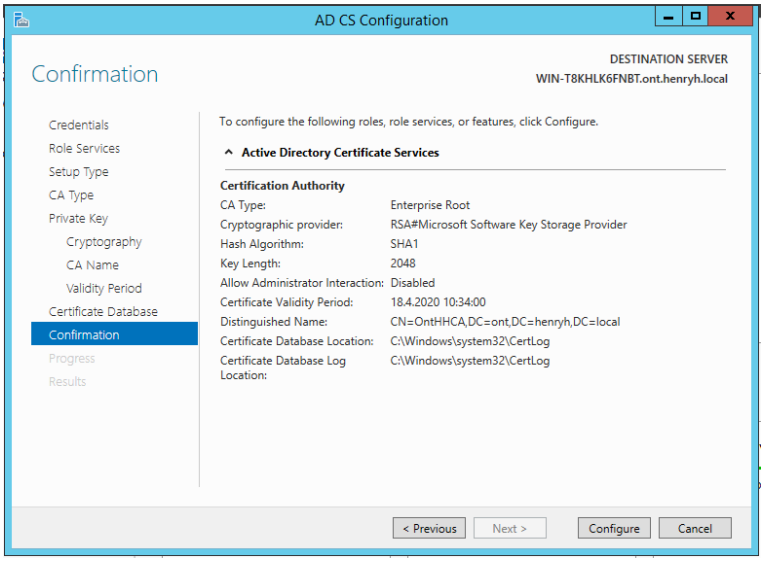
Valitaan kullekin sopiva pituus, ja jatketaan eteenpäin ”Next” -painikkeella. Seuraavassa ikkunassa määritellään tietokantojen sijainnit.



Kuva 11 Tietokantojen sijainnit

Mikäli ei ole erityistä tarvetta antaa sijainneiksi jotain tiettyä, jätetään ne oletusarvoihinsa, ja painetaan Next -painiketta.

Seuraava ikkuna on vahvistusikkuna:



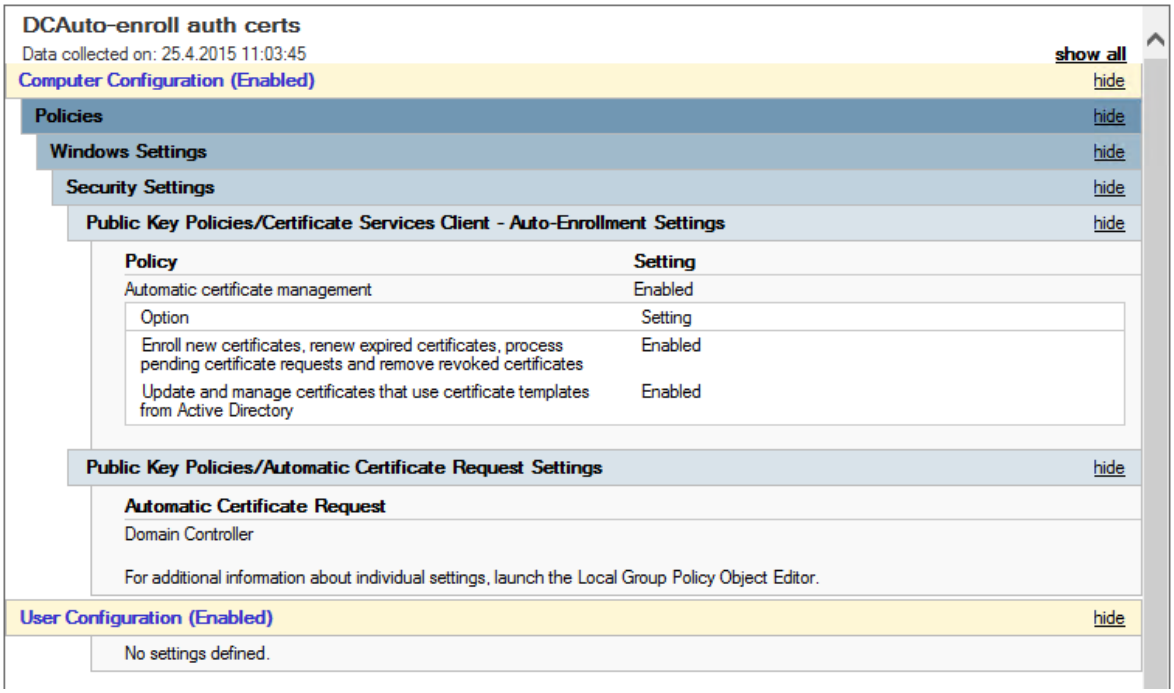
Kuva 12 Vahvistusikkuna

Varmistetaan, että asetukset on annettu oikein, minkä jälkeen voidaan painaa Configure -painikkeesta määrittelyn käytäntöönpanemiseksi. Kun määrittelyt on suoritettu, tulee vielä ikkuna, jossa tästä kerrotaan. Tämä ikkuna voidaan sulkea.

6.4 Domain Controller -sertifikaattien luonti ja jakaminen

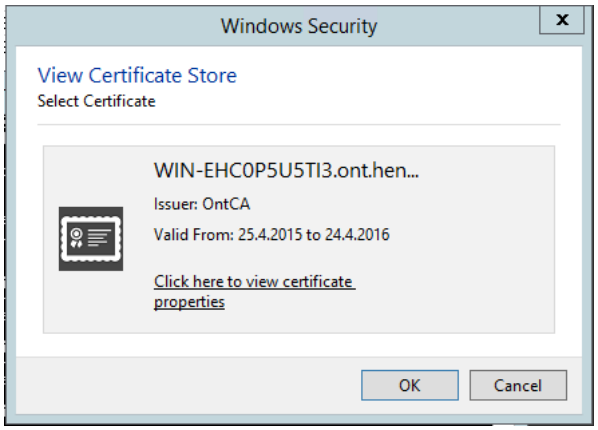
Jokaisella Domain Controllerilla, jota käytetään toimikorttikirjautumisen autentikointiin, tulee olla Domain Controller -sertifikaatti (Microsoft, ei julkaisupäivämäärää G). Avataan CA -koneelta Certification Authority -työkalu. Valitaan ikkunassa kohta Certificate Templates, jonka pitäisi olla tyhjä. Valitaan se hiiren oikealla painikkeella, ja aukeavasta valikosta valitaan New → Certificate Template to Issue. Valitaan aukeavasta ikkunasta ”Kerberos Authentication”, ja painetaan ”OK” -painikkeesta. Nyt sertifikaattipohja on luotu, ja Certificate Templates -kansion ollessa valittuna pitäisi ikkunan oikeassa osassa näkyä kohta ”Kerberos Authentication”. ”Kerberos Authentication” -templaatti on uusin Domain Controller -sertifikaattitemplaatti, ja sen käyttöä suositellaan Windows Server 2008 (tai uudemmille) Domain Controllereille. (Simonsen, 2013.)

Siirrytään Domain Controllerille. Luodaan ryhmäkäytäntö, jolla laitetaan päälle sertifikaattien automaattinen hakeminen ja pyytäminen Domain Controllereille. Luodaan siis uusi ryhmäkäytäntö, ja tehdään siihen seuraavat asetukset: Computer Configuration → Policies → Windows Settings → Security Settings → Public Key Policies → Certificate Services Client – Auto-Enrollment. Asetetaan kohtaan ”Configuration Model” valinta ”Enabled. Lisäksi valitaan sekä ”Renew expired certificates, update pending certificates, and remove revoked certificates” että ”Update certificates that use certificate templates”. Tämän jälkeen painetaan ”Apply” -painikkeesta, minkä jälkeen ikkunan voi sulkea. Public Key Policies -kohdan alta löytyy myös kohta ”Automatic Certificate Request”. Avataan se, minkä jälkeen painetaan hiiren oikealla painikkeella, ja otetaan avautuvasta valikosta New → Automatic Certificate Request. Tällöin aukeaa velho, jonka toisessa kohdassa valitaan ”Domain Controller”, ja jatketaan eteenpäin. Lopputuloksena pitäisi olla kuvan 13 mukainen ryhmäkäytäntö. (Simonsen, 2013.)

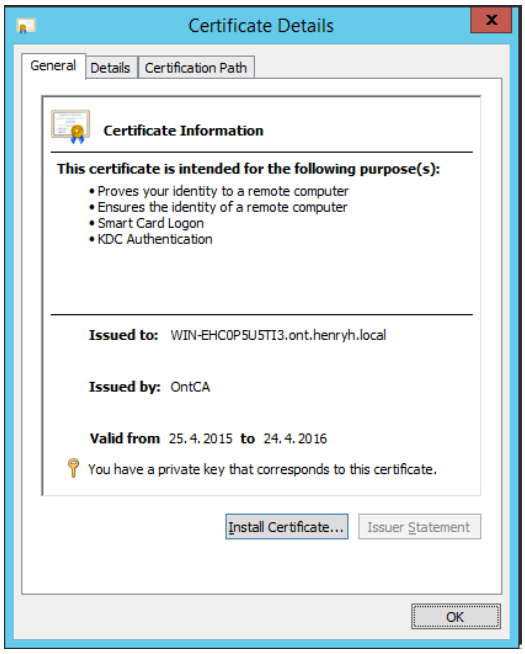


Kuva 13 Domain Controller –sertifikaattikäytäntö

Tämän jälkeen linkitetään luotu ryhmäkäytäntö vaikuttamaan Domain Controllereihin. Muutokset saadaan voimaan välittömästi komennolla *gpupdate /force.* Kun tämä on tehty, voidaan vielä tarkastaa, onko sertifikaatti otettu vastaan komennolla *certutil -viewstore my.* (Microsoft, 2012c.) Mikäli on, aukeaa kuvan 14 kaltainen ikkuna, josta sertifikaatin ominaisuuksia tarkastellessa aukeaa kuvan 15 kaltainen ikkuna, jossa näkyvät samat sertifikaatin tarkoitukset.



Kuva 14 Sertifikaatti löytyy



Kuva 15 Sertifikaatin tiedot

7 VRK:n sertifikaatin kanssa tehtävät toimenpiteet

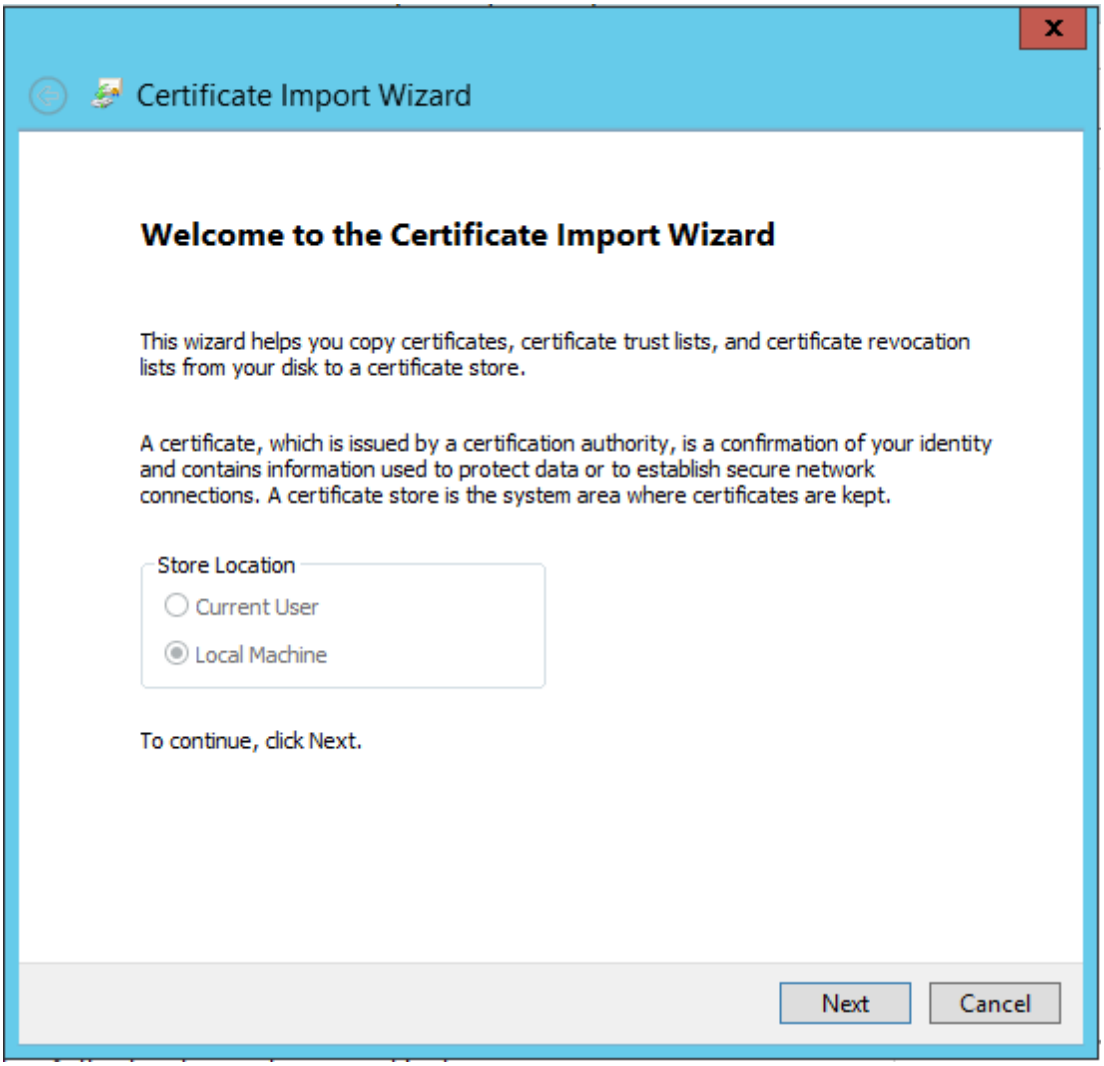
Korttikirjautumisessa voidaan valita, käytetäänkö VRK:n niille jo kirjoittamia sertifikaatteja, vai kirjoitetaanko niille omat kirjautumista varten. Käytetään ainoastaan VRK:n jo toimikorteille kirjoittamia, sillä omien käytössä on muutamia käytännön ongelmia, kuten mm. se, että tällöin jokaiselle kortille tarvitsee erikseen kirjoittaa sertifikaatit, joka tuottaa hyötyyn nähden liikaa työtä, ja se, että tällöin kirjautuessa käyttäjä joutuisi valitsemaan, kumpaa sertifikaattia hän käyttää, mikä ei ole loppukäyttäjän kannalta hyvä asia. Kun käytetään pelkkiä VRK:n sertifikaatteja, joudutaan tekemään joitakin toimenpiteitä asian saamiseksi toimintakuntoon.

7.1 VRK:n juurisertifikaatin tuonti ja lisäys luotettuihin juuriin

CA jakaa Domain Controllerille CA:n allekirjoittamat ja domainin luottamat sertifikaatit. VRK:n sertifikaatit on lisättävä luotettujen listaan, minkä seurauksena terveydenhuollon toimikortti (VRK:n sertifikaatti) ja Domain Controller (CA:n sertifikaatti) luottavat toisiinsa. Nyt käydään läpi, miten VRK:n sertifikaatit lisätään luotettujen listaan.

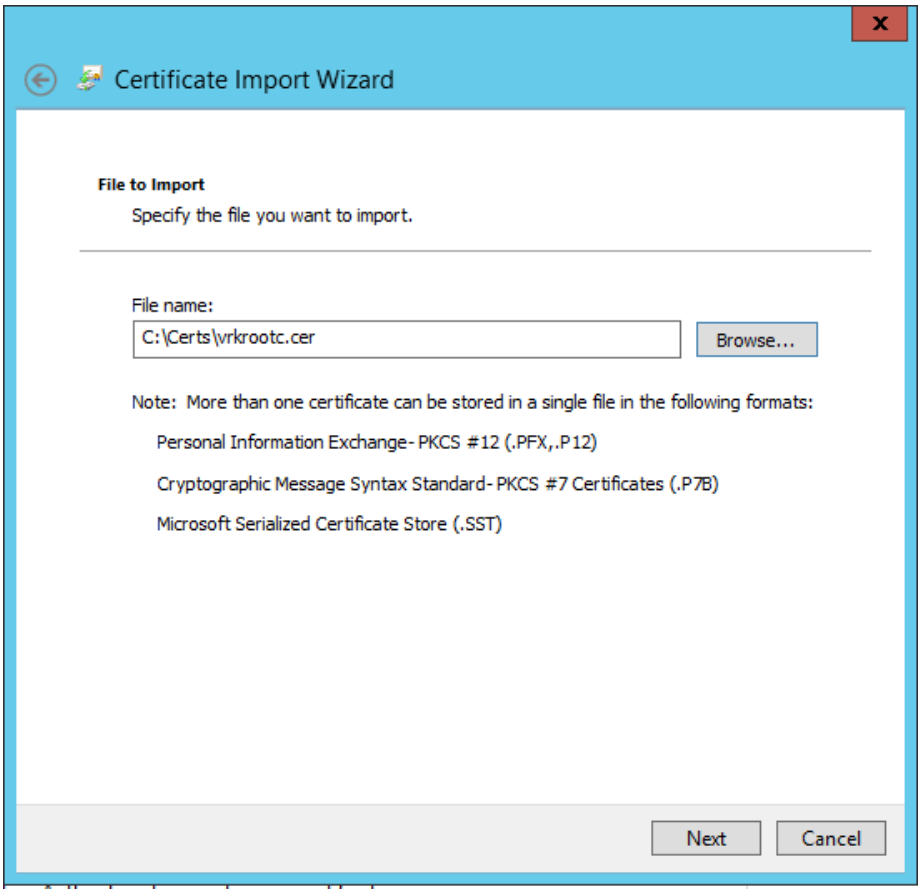
Aloitetaan tallentamalla VRK:n juurisertifikaatti Domain Controllerille (Microsoft, ei julkaisupäivämäärää G). Sertifikaatti löytyy osoitteesta http://vrk.fineid.fi/certs/vrkrootc.crt.

Tämän jälkeen lisätään VRK:n juuri-CA luotettuihin juuriin ryhmäkäytännöllä. Avataan ensin Group Policy Management. Valitaan ensin oikea toimialue, ja luodaan uusi ryhmäkäytäntö tätä varten. Aletaan tekemään ryhmäkäytäntöön muutoksia. Aukeavassa Group Policy Management Editorissa valitaan Computer Configuration → Policies → Windows Settings → Security Settings → Public Key Policies. Valitaan Trusted Root Certification Authorities hiiren oikealla painikkeella, ja valitaan valikosta kohta ”Import”. (Microsoft, ei julkaisupäivämäärää G.) Aukeaa kuvan 16 mukainen sertifikaatin tuontivelho.



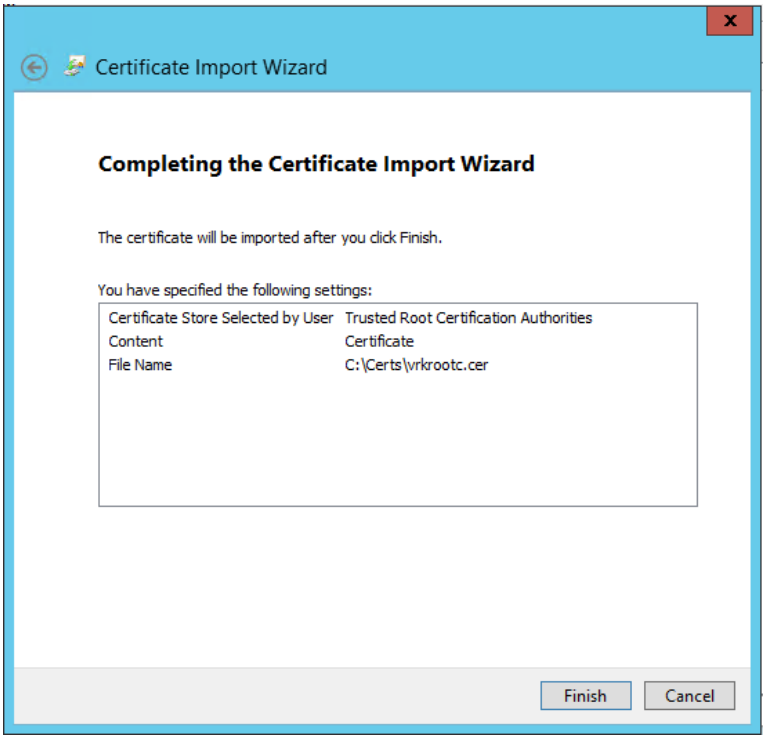
Kuva 16 Sertifikaatin tuontivelho

Tässä vaiheessa ei voida vielä tehdä muuta kuin edetä. Seuraavassa ikkunassa valitaan, mikä sertifikaattitiedosto halutaan tuoda. Valitaan ”Browse”, ja navigoidaan siihen paikkaan, johon VRK:n juurisertifikaatti aiemmin tallennettiin. Kun sertifikaatti on valittu, näyttää ikkuna kuvan 17 kaltaiselta, ja voidaan jatkaa eteenpäin.



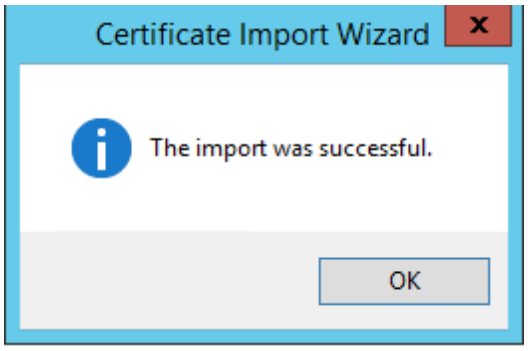
Kuva 17 Sertifikaatin valinta

Seuraavassa ikkunassa valitaan sertifikaatille tallennuspaikka. Valitsimme jo aikaisemmin Trusted Root Certification Authorities:in, joten tässä vaiheessa ei voi tehdä muutoksia, vaan jatketaan eteenpäin. Seuraava ikkuna on vahvistusikkuna. Varmistetaan, että tiedot ovat oikein, ja painetaan ”Finish” -painiketta.



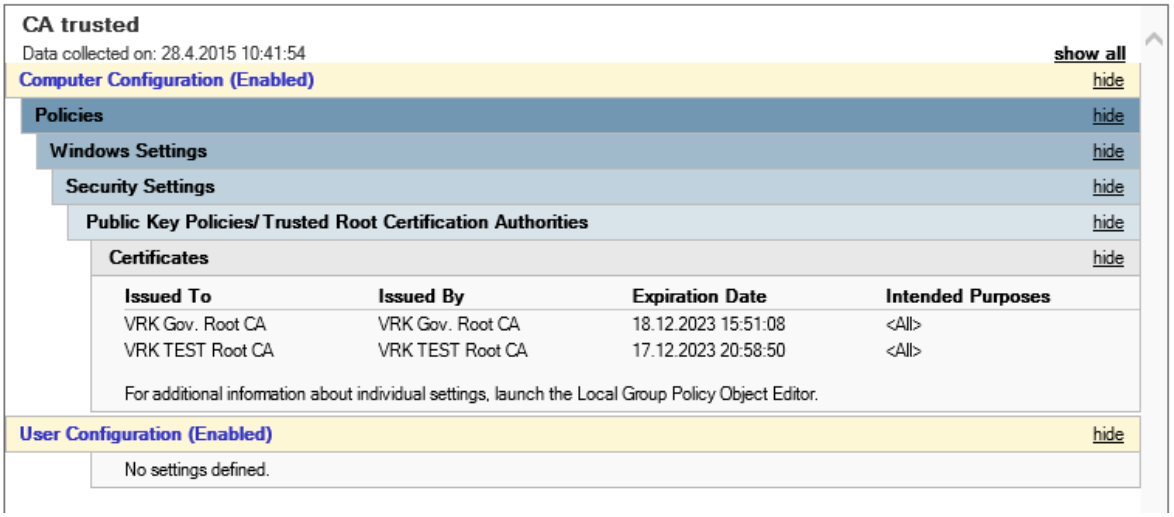
Kuva 18 Sertifikaatin tuontivelhon vahvistusikkuna

Tämän jälkeen odotetaan hetki. Mikäli tuonti onnistui, ilmestyy tästä ruudulle ilmoitus. Painetaan tästä OK.



Kuva 19 Tuonti onnistui –ilmoitus

Nyt Group Policy Management Editorin voi sulkea. Näiden toimenpiteiden jälkeen luodun ryhmäkäytännön Settings -välilehden pitäisi olla kuvan 20 näköinen. VRK:n TEST Root CA:ta ei tarvitse lisätä luotettuihin juuriin, mikäli toimintaa ei ole tarkoituksena testata käyttämällä puhtaasti testitarkoituksiin luotuja toimikortteja. Linkitetään luotu ryhmäkäytäntö vaikuttamaan koko toimialueeseen.



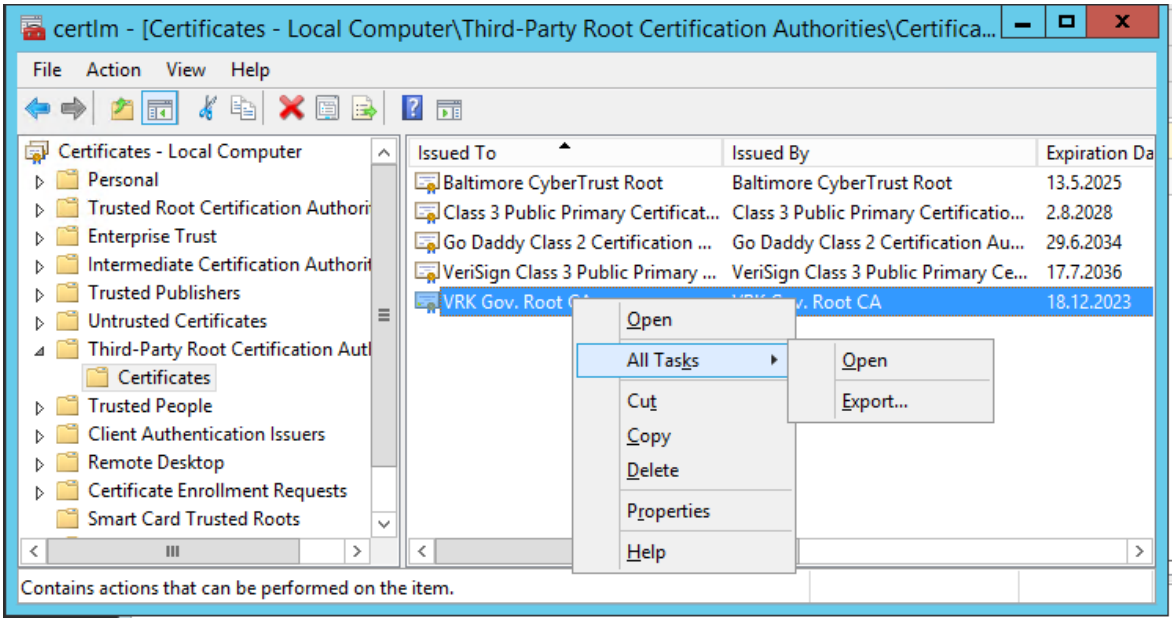
Kuva 20 Luotu ryhmäkäytäntö

7.2 VRK:n CA:n lisääminen NTAuth -säiliöön

Toimikortilla kirjautumiseen käytettävän sertifikaatin tulee olla sellaisen CA:n jakama, joka löytyy NTAuthCertificates -säiliöstä. Mikäli CA ei löyty NTAuthCertificates -säiliöstä, niin kirjautuminen toimikortilla ei onnistu, ja saadaan virheilmoitus ”Unable to verify the credentials”. Tämä säiliö luodaan automaattisesti, kun Enterprise CA asennetaan. Enterprise CA:t lisätään oletusarvoisesti automaattisesti NTAuthCertificates -säiliöön. (Microsoft, ei julkaisupäivämäärää G.)

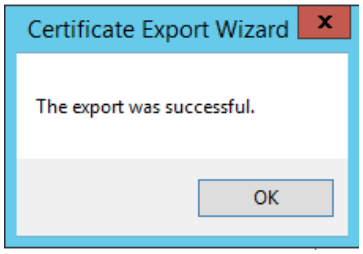
7.2.1 Juurisertifikaatin vienti oikeaan muotoon

Mikäli haluttu juurisertifikaatti on jo .cer -muodossa, tätä vaihetta ei tarvitse tehdä. Aloitetaan NTAuthCertificates -säilöön lisääminen viemällä VRK:n juuri-CA:n sertifikaatti .cer -tiedostomuotoon, joka tukee joko DER -koodattua binäärimuotoa tai base-64 -koodattua X.509 -muotoa. Avataan sertifikaattien hallintaikkuna. Avataan kansio, josta sertifikaatti löytyy. Se on ”Third-Party Root Certification Authorities”, jonka alta ”Certificates”. Valitaan VRK:n sertifikaatti hiiren oikealla painikkeella, ja valitaan All Tasks → Export. (Microsoft, ei julkaisupäivämäärää H.)



Kuva 21 Sertifikaattien hallintaikkuna

Tällöin aukeaa sertifikaatin vientivelho. Valitaan ”No, do not export the private key”, mikäli tällainen valinta tulee jossain vaiheessa vientiä. Painetaan ensimmäisessä ikkunassa ”Next”, minkä jälkeen aukeaa ikkuna, jossa valitaan tiedostomuoto. Valitaan muodoksi ”DER encoded binary X.509 (.CER)”, minkä jälkeen painetaan ”Next” -painiketta. Seuraavaksi valitaan, mihin vietävä tiedosto tallennetaan, ja minkä nimiseksi. Annetaan kuvaava nimi ja tallennetaan se sellaiseen paikkaan, josta se löytyy. (Microsoft, ei julkaisupäivämäärää H.) Tämän jälkeen jatketaan eteenpäin seuraavaan kohtaan, jolloin aukeaa vahvistusikkuna.
Varmistetaan, että tiedot ovat oikein, ja painetaan ”Finish”. Mikäli vienti onnistuu, ilmestyy kuvan 22 mukainen ilmoitus. Sitten sertifikaattien hallintaikkuna voidaan sulkea.



Kuva 22 Vienti onnistui -ilmoitus

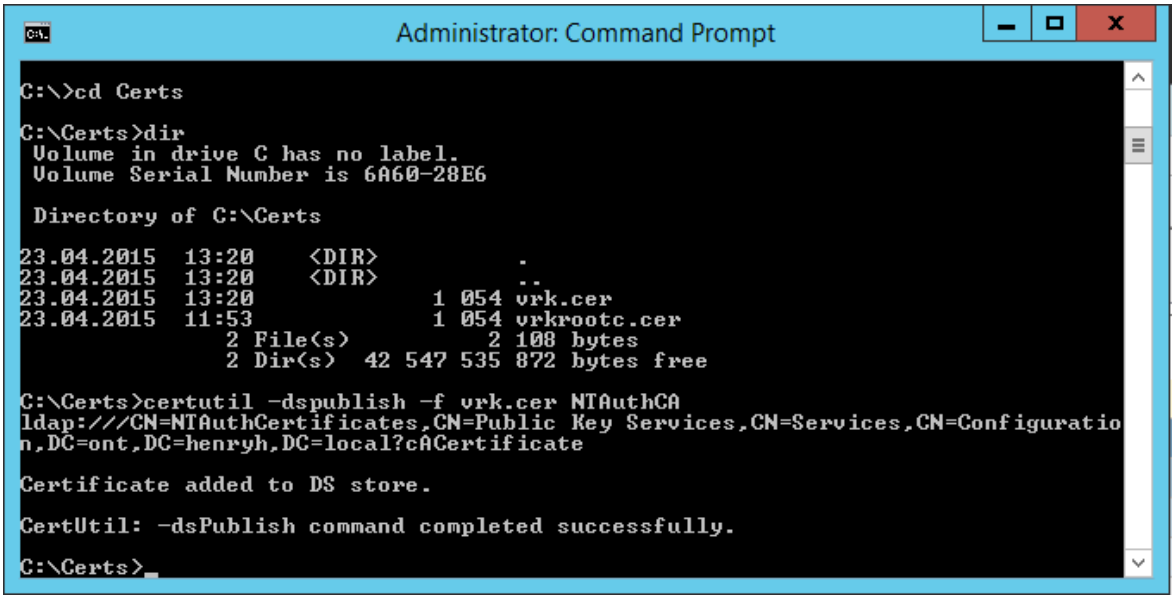
7.2.2 Viedyn sertifikaatin lisäys NTAuthCertificates -säiliöön

Seuraavaksi lisätään sertifikaatti NTAuthCertificates -säiliöön. Avataan komentorivi, ja navigoidaan sillä kansioon, johon sertifikaatti vietiin. Kun ollaan oikeassa kansiossa, annetaan syötetään komento

certutil -dspublish -f FILENAME NTAuthCA

(Microsoft, ei julkaisupäivämäärää l).

Mikäli lisäys onnistuu, saadaan tästä komentoriville ilmoitus. Kuvassa 23 näkyy tehty toimenpide.



Kuva 23 Sertifikaatin lisäys NTAuthCertificates -säiliöön

8 Lopputoimenpiteet

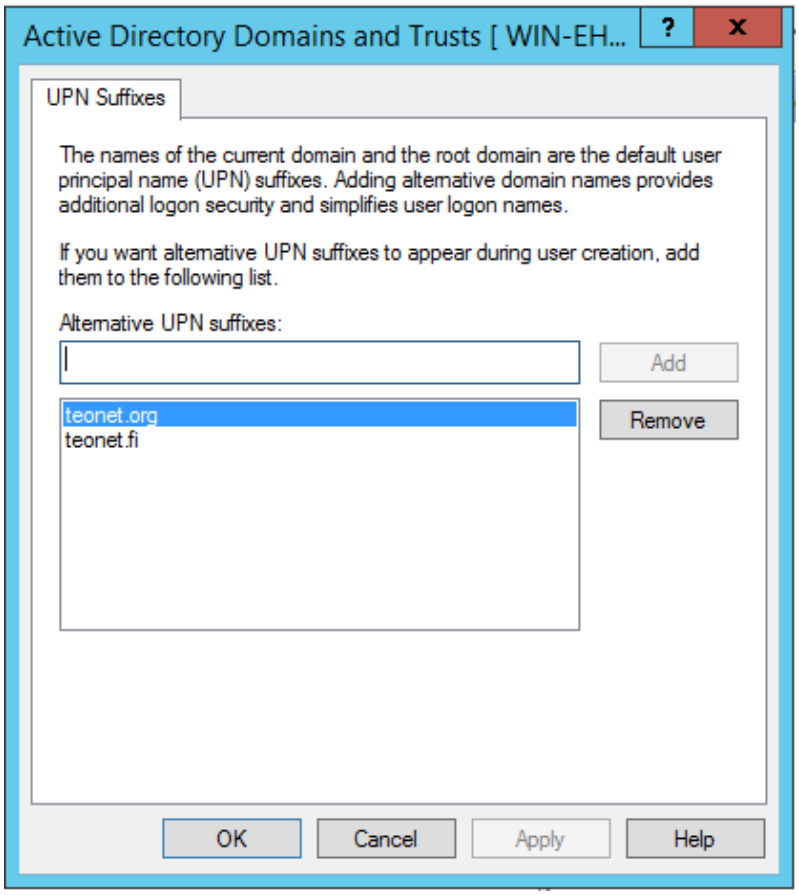
Koska ei käytetä kirjautumisessa itse korteille myönnettyjä sertifikaatteja, tulee vielä tehdä yksi toimenpide, jotta korttikirjautuminen onnistuu. Vaihtoehtoja on kaksi: käyttäjän AD:sta löytyvä User Principal Name (UPN) pitää vaihtaa samaksi kuin mikä kortilta löytyy. Tässä ongelmana on se, että mikäli toimialueella on Office 365 -integraatio, ei tätä voida käyttää, sillä se rikkoisi Office 365 -toiminnallisuuden käyttäjältä (Kallioniemi, 2014). Tähän on AD FS -pohjainen ratkaisu. On myös toinen vaihtoehto, jonka kanssa Office 365 ei aiheuta ongelmia, mutta käyttäjä joutuu syöttämään vihjeen käyttäjästä (Patrick, 2010). Käydään läpi nämä eri ratkaisut ja niiden toteutus.

8.1.1 Office 365 -integraatio

Office 365 on mahdollista integroida jo olemassaolevan AD -kokonaisuuden kanssa. Tällöin voidaan synkronoida olemassaolevan AD -kokonaisuuden käyttäjätunnukset Office 365:n, joka mahdollistaa molempien ympäristöjen käyttäjätunnusten hallinnan sekä ns. single sign-on:in, jolloin käyttäjät voivat kirjautua sekä AD-metsän laitteille että Office 365:n samoilla tunnuksilla. Hyötynä tässä on myös se, että tätä käyttäjäsynkronointia käytettäessä ei tarvitse uudelleenluoda jokaiselle käyttäjälle tunnuksia Office 365:n, vaan jo olemassaolevat AD -tunnukset riittävät. (Microsoft, ei julkaisupäivämäärää J.)

8.2 Käyttäjän UPN:n vaihtaminen

Aloitetaan lisäämällä metsään uusi UPN -jälkiliite. Avataan Active Directory Domains and Trusts. Valitaan vasemman reunan palkista kohta ”Active Directory Domains and Trusts” hiiren oikealla painikkeella ja avataan valikosta ”Properties”. Lisätään ikkunan kautta halutut jälkiliitteet. (Microsoft, päivitetty 2012.) VRK:n todellisten käyttäjien UPN -jälkiliitteet ovat teonet.org, ja testi-CA:n käyttäjien jälkiliitteet teonet.fi. Lisätään nämä siis jälkiliitteisiin.



Kuva 24 Jälkiliitteiden lisäys

Kun jälkiliitteet on lisätty, voidan ikkuna sulkea ”OK” -painikkeella. Nyt on mahdollista käyttäjää luodessa antaa jälkiliitteeksi muukin, kuin toimialueen oletusliite. Käyttäjätunnuksen jälkiliitteen voi nyt myös vaihtaa suoraan käyttäjän tiedoista. Toimikorteilla olevat UPN:t ovat mallia 11223344556@teonet.org. Nyt voidaan avata käyttäjä normaalisti Active Directory Users and Computers:ista, ja vaihtaa sisäänkirjautumisnimi vastaamaan kortilta löytyvää UPN:ää. Kun käyttäjän AD:ssa oleva UPN vastaa toimikortilla olevaa UPN:ää, onnistuu työasemalle kirjautuminen toimikortilla pelkkää toimikortin PIN -tunnusta käyttäen. (Microsoft, ei julkaisupäivämäärää G.)

8.2.1 Office 365 -ongelma ja Alternate Login ID

Mikäli toimikorteilla kirjautuminen mahdollistetaan muuttamalla käyttäjien UPN:t vastaamaan korteilta löytyviä, AD FS:ää käyttäviin ohjelmistoihin (kuten Office 365) kirjautuminen ei enää onnistu, kun UPN ei vastaa enää käyttäjän sähköpostiosoitetta. Ratkaisuna ongelmaan voi olla AlternateLoginId. AlternateLoginId:llä saadaan mahdollistettua näihin AD FS:ää käyttäviin ohjelmistoihin kirjautuminen jollain muulla tunnuksen attribuutilla, kuin UPN:llä. Microsoft suosittelee ”mail” -attribuutin käyttöä. Lisätietoa Alternate Login ID:stä

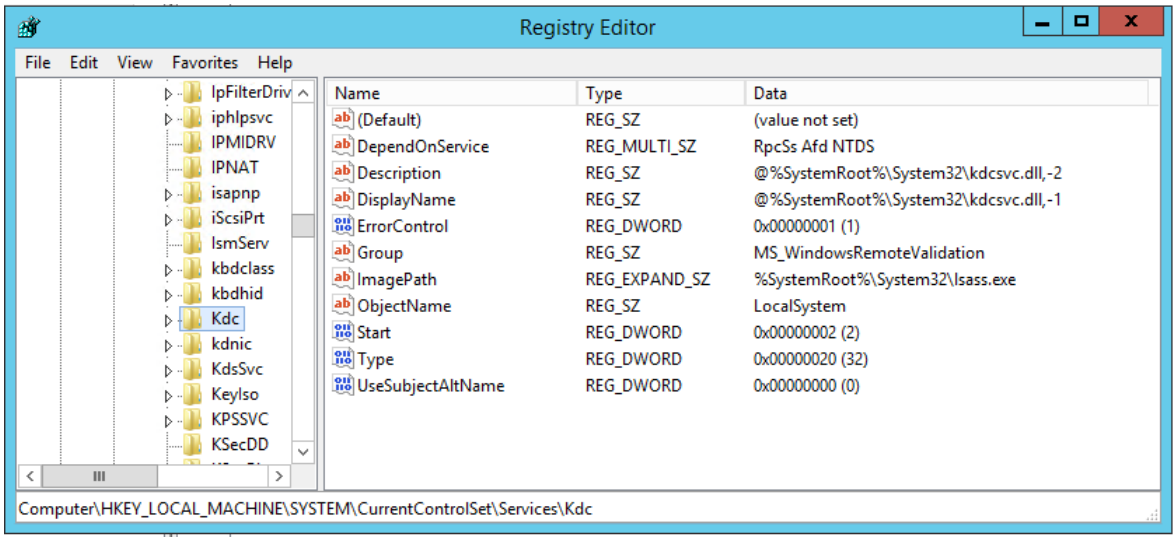
löytyy osoitteesta https://technet.microsoft.com/en-us/library/dn659436.aspx. (Microsoft, päivitetty 2014b.)

8.3 UPN -mappauksen käytöstäpoistaminen

Toimikortilla kirjautuminen saadaan myös toimimaan ottamalla toimialueen UPN -mappaus pois käytöstä. Kun UPN -mappaus on käytössä, korttikirjautumisessa AD:sta haetaan kortin Subject Alternative Name -kentästä löytyvää UPN:a vastaavaa tunnusta. Mikäli kortilla olevaa UPN:a vastaavaa tunnusta ei AD:sta löydy, epäonnistuu kirjautuminen. Kun UPN -mappaus otetaan pois käytöstä, saadaan kirjautuminen toimikortilla mahdollistettua vaikkei AD:sta löytyisikään toimikortin varmenteesta löytyvää UPN:aa vastaavaa käyttäjää. (Patrick, 14.6.2010.) Tämän ratkaisun hyvinä puolina käyttäjätunnusten UPN:ää ei tarvitse muuttaa, ja AD FS:ää käyttäviin ohjelmiin sisäänkirjautuminen onnistuu ilman erillisiä toimenpiteitä. Huonona puolena käyttäjä joutuu syöttämään käyttäjätunnuksensa kirjautumisen onnistumiseksi toimikortin PIN -numeron lisäksi, ja toteutus on työläs.

8.3.1 Subject Alternative Namen poistaminen käytöstä

Ensiksi tulee ottaa oletus-UPN -mappaus pois käytöstä. Tämä onnistuu tekemällä rekisterimuutos, joka tulee tehdä jokaiselle Domain Controllerille. Rekisterin kansioon HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc tulee lisätä avain ”UseSubjectAltName”, joka on tyypiltään DWORD, ja jonka arvo on 0. (Patrick, 2010; Microsoft 2010.) Tämä onnistuu rekisterieditorin kautta. Kun avain on lisätty, näyttää rekisterieditorissa avattu Kdc -kansio kuvan 25 mukaiselta.

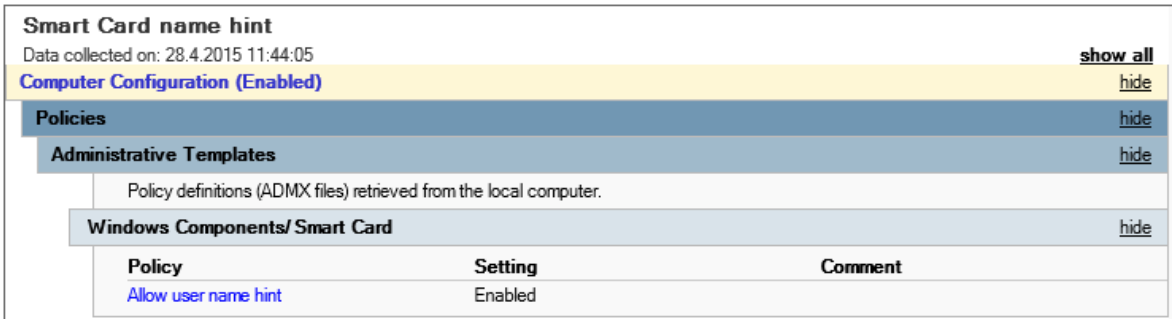


Kuva 25 UseSubjectAltName lisättynä rekisteriin

Kun tämä avain on lisätty jokaiselle Domain Controllerille, on aiemmin kuvattu toimikorttikirjautumisessa oletusarvoisesti käytettävä UPN -mappaus otettu pois käytöstä. Seuraavaksi tulee mahdollistaa käyttäjävihjeen antaminen korttikirjautumisessa.

8.3.2 Käyttäjävihjeen mahdollistaminen

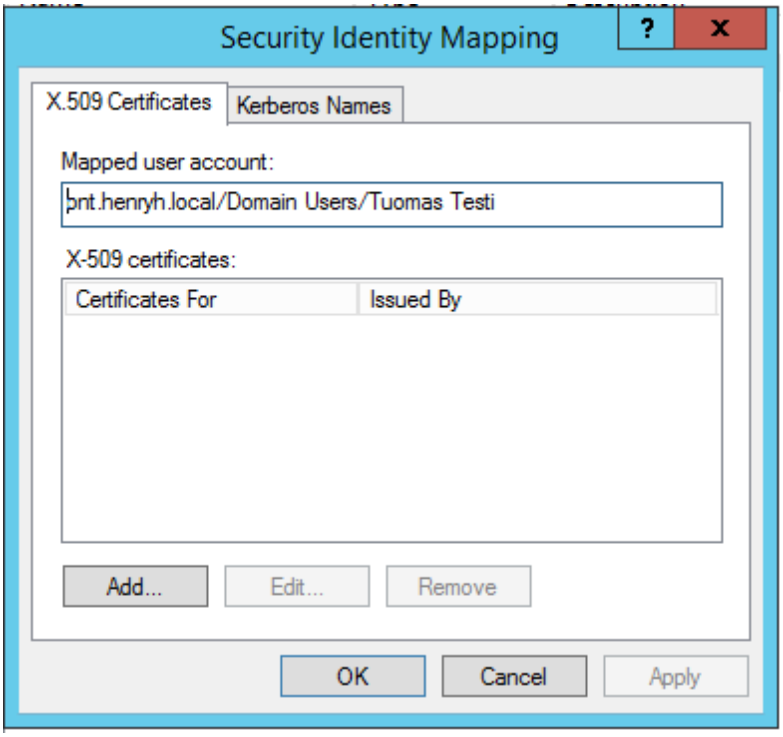
Kun UPN -mappaus on otettu pois käytöstä, tulee käyttäjän antaa vihje käyttäjätunnuksesta, eli käytännössä syöttää se. Mahdollistetaan tämä ryhmäkäytännöllä. Luodaan uusi ryhmäkäytäntö. Mennään ryhmäkäytäntöeditorissa Computer Configuration → Policies → Administrative Templates → Windows Components → Smart Card → Allow user name hint. Annetaan ”Allow user name hint” -kohdan arvoksi ”Enabled”. Linkitetään ryhmäkäytäntö vaikuttamaan haluttuihin organisaatioyksiköihin. (Patrick 2010.)



Kuva 26 Ryhmäkäytäntö, jolla mahdollistetaan käyttäjävihje

8.3.3 Korttisertifikaatin mappaus AD -käyttäjään

Jotta kirjautuminen nimivihjeen kanssa onnistuisi, tulee vielä mapata kortin käyttäjäsertifikaatti AD:n käyttäjään (Patrick, 14.6.2010). Ensiksi tulee viedä sertifikaatti kortista. Tämä onnistuu helposti mPolluxin kautta. Kun sertifikaatti on viety kortilta, tulee se siirtää sille Domain Controllerille, jonka kautta se halutaan mapata käyttäjään. Kun tämä on tehty, avataan kyseisellä Domain Controllerilla Active Directory Users and Computers, ja navigoidaan halutun käyttäjän kohdalle. ”Advanced Features” tulee olla valittuna ”View” -valikosta. Valitaan käyttäjä hiiren oikealla painikkeella, ja otetaan aukeavasta valikosta kohta ”Name Mappings...”. (Microsoft, päivitetty 2008.) Aukeaa kuvan 27 kaltainen ikkuna.



Kuva 27 Korttisertifikaatin yhdistäminen AD-käyttäjään

Valitaan ”X.509 Certificates” -välilehdellä ”Add...”. Aukeavassa tiedostonhakijassa haetaan oikea sertifikaatti, ja tämän jälkeen aukeavassa ikkunassa jätetään sekä ”Use Issuer for alternate security identity” että ”Use Subject for alternate security identity” valituiksi, ja painetaan ”OK”. (Microsoft, päivitetty 2008.) Tämän jälkeen sertifikaatti löytyy kuvan 27 ikkunasta, ja voidaan sulkea ikkuna ”OK” -painikkeella. Nyt kortin sertifikaatti on mapattu käyttäjään, ja korttikirjautuminen onnistuu antamalla sekä kortin PIN -koodi että käyttäjätunnus.

9 Ratkaisun testaus

Ratkaisu testattiin liittämällä yksittäinen tietokone luotuun testiympäristö-toimialueeseen. Ennen siihen liittämistä varmistettiin, että kyseisellä tietokoneella ei ole mitään sellaisia ohjelmia tai asetuksia, jotka haittaisivat testausta, eli tarkastettiin, ettei mitään kortinlukija-ohjelmistoa kyseiseltä tietokoneelta löydy asennnettuna. Testauksen aikana testattiin sekä käyttäjätunnuksen UPN:n vaihtaminen kortilta löytyväksi että käyttäjävihjeen syöttäminen. Alternate Login ID -ratkaisua ei voitu testata, sillä testitoimialueella ei ollut mitään Office 365 -integraatiota. Testaus tehtiin selkeästi osissa: ensin testattiin kortinlukijaohjelmiston asentaminen ryhmäkäytännöllä, jonka jälkeen testattiin kumpaakin eri kirjautumistapaa. Testaus tehtiin osissa, jotta saataisi varmuus jokaisen vaiheen toimivuudesta.

Ennen toimikortilla kirjautumisen testaamista varmistettiin, että kortinlukijaohjelmisto oli asentunut ryhmäkäytännöllä. Tämä testattiin liittämällä tietokone toimialueeseen, uudelleenkäynnistämällä se ja kirjautumalla sille sisään normaalisti toimialueen käyttäjätunnusta ja salasanaa käyttäen. Kirjautumisen jälkeen varmistettiin, että mPollux -ohjelma löytyy asennetuista ohjelmista.

Seuraavaksi toimialueelle luotiin testauksessa käytettyä korttia vastaava käyttäjä. Koska ensin testattiin käyttäjätunnuksen UPN:n vaihtamista korttia vastaavaksi, käyttäjätunnukselle tehtiin näin. Kun käyttäjätunnus oli luotu, testattiin kortilla kirjautumista. Kun kortti asetettiin lukijaan, löytyi toimialueelta vastaava tunnus, ja kirjautuminen tietokoneelle kortin PIN-tunnusta käyttäen onnistui.

Lopuksi testattiin käyttäjävihjeellä kirjautumista. Käyttäjään ja toimialueelle tehtiin sen mahdollistavat muutokset. Kun ne oli tehty, asetettiin kortti lukijaan. Syötettiin käyttäjävihje ja kortin PIN-tunnus. Kirjautuminen onnistui näillä toimenpiteillä. Terveydenhuollon toimikortilla kirjautuminen AD-toimialueelle siis onnistui.

10 Yhteenveto

Työssä saatiin rakennettua toimiva ratkaisu. Toimikorttikirjautumista koskeva dokumentaatio ja erilaiset ohjeet löytyivät helposti, ja vaikka osa niistä olikin suunnattu vanhemmille järjestelmille, onnistui niiden käyttö uudempien järjestelmien kanssa vähällä vaivalla. Suurin haaste tulikin siitä, että dokumentaatiossa ja eri ohjeissa melkolailla oletettiin, että käytetään korteille itse myönnettyjä varmenteita, kun työssä taas haluttiin käyttää korteille VRK:n myöntämiä varmenteita. Tämä toi työhön muutaman lisävaiheen, joita ei olisi muuten tarvinnut tehdä, kuten VRK:n juurivarmenteen lisääminen toimialueen luotettuihin juuriin sekä AD-käyttäjien UPN -muutokset, jotka puolestaan aiheuttivat uusia haasteita.

Toimialueen Office 365 -integraatio tuotti ongelmia UPN -muutosten kanssa, sillä tämä integraatio hajoaa, mikäli käyttäjien UPN:t vaihtaa kortteja vastaavaksi eikä tee muita toimenpiteitä. Tähän löytyi parikin ratkaisua – käyttäjävihje sekä Alternate Login ID. Käyttäjävihjeratkaisu saatiin testattua ja todettua toimivaksi, muttei se ole kuitenkaan täydellinen. Alternate Login ID -ratkaisua taas ei päästy testaamaan, koska testitoimialueella, jolla työ toteutettiin, ei Office 365 -integraatiota ollut. Kehitysehdotuksena työhön onkin Alternate Login ID -ratkaisun testaaminen ja käyttöönottaminen ja sen ohjeistus.

10.1 Oma oppiminen

Työ laajensi osaamista Windows Server- ja Active Directory -alueilla. Toimialueen pystytys ja hallinta olivat jo aiempaa osaamista. CA:n asennus ja määrittely olivat puolestaan uusia asioita, jotka tulivat nyt tutuiksi. Koko CA:n toiminta osana AD:ta olivat myös uutta opittua, kuten myös muutkin varmenteisiin liittyvät asiat AD:n liittyen. Työn aikana tuli myös toimikorttien rakenne ja käyttötapa tutuksi sekä AD-kirjautumisen tekninen toiminta. Office 365 -integraation toimintaan tuli myös tehtyä lyhyt katsaus. Lyhyesti tiivistettynä voikin sanoa, että koko toimialueelle toimikortilla kirjautumisen mahdollistaminen ja siihen liittyvät asiat olivat uutta asiaa. Työn alkuperäinen aikataulutus oli liian tiukka, ja se näkyikin siinä, etten siinä kykenyt pysymään.

Lähteet

Adare, P. 6.9.2010. Certificate Services, install on domain controller? Luettavissa: https://social.technet.microsoft.com/Forums/windowsserver/en-US/66cd9712-b44a-406b-b77f-07ee945bf80f/certificate-services-install-on-domain-controller Luettu 19.3.2015.

Timo Kallioniemi, keskustelupalstaviesti. 25.4.2014. Luettavissa: https://social.technet.microsoft.com/Forums/office/en-US/4357a73c-bdaa-44ce-9f00-c53528ac720c/smart-card-logon-with-third-party-ca-combined-with-adfs-to-office-365?forum=winserversecurity Luettu: 14.4.2015.

Kansallinen Terveysarkisto (Kanta) 2015. Tietoturvallisuus. Luettavissa: http://www.kanta.fi/tietoturvallisuus Luettu 17.8.2015.

Kragh, J. O. 30.5.2012. GPO Software Installation Problem. Luettavissa: https://social.technet.microsoft.com/Forums/windowsserver/en-US/8570d268-7777-4140-969c-22a52f980599/gpo-software-installation-problem Luettu 19.3.2015.

Adrian McCullagh, William Caelli, 8.2000. Non-Repudiation in the Digital Environment. Luettavissa: http://firstmonday.org/ojs/index.php/fm/article/view/778/687 Luettu 28.8.2015.

Microsoft, päivitetty 19.11.2014a. What Are Domains and Forests? Luettavissa: https://technet.microsoft.com/en-us/library/cc759073%28v=ws.10%29.aspx Luettu 3.8.2015.

Microsoft, päivitetty 24.6.2013. Group Policy Overview. Luettavissa: https://technet.microsoft.com/library/hh831791 Luettu 3.8.2015.

Microsoft, ei julkaisupäivämäärää A. Public Key Infrastructure. Luettavissa: https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432%28v=vs.85%29.aspx Luettu 7.8.2015.

Microsoft, ei julkaisupäivämäärää B. Security Glossary (C). Luettavissa: https://msdn.microsoft.com/en-us/library/windows/desktop/ms721572%28v=vs.85%29.aspx#_security_certification_authority_gly Luettu 7.8.2015.

Microsoft, ei julkaisupäivämäärää C. Security Glossary (K). Luettavissa : https://msdn.microsoft.com/en-us/library/windows/desktop/ms721590%28v=vs.85%29.aspx#_security_kerberos_protocol_gly Luettu 30.8.2015.

Microsoft, päivitetty 15.6.2011. Certificate Enumeration. Luettavissa: https://technet.microsoft.com/en-us/library/92aea8c5-c617-4a04-9356-e0ad8dd4cea9%28v=ws.10%29#BKMK_SmartCardLogonFlowVista Luettu 30.8.2015.

Microsoft, ei julkaisupäivämäärää D. Key Distribution Center. Luettavissa: https://msdn.microsoft.com/en-us/library/windows/desktop/aa378170%28v=vs.85%29.aspx Luettu 30.8.2015.

Microsoft, ei julkaisupäivämäärää E. Security Glossary (L). Luettavissa: https://msdn.microsoft.com/en-us/library/windows/desktop/ms721592%28v=vs.85%29.aspx#_security_local_security_authority_gly Luettu 31.8.2015.

Microsoft, ei julkaisupäivämäärää F. View Certificate Revocation List Details. Luettavissa: https://technet.microsoft.com/en-us/library/cc730795.aspx Luettu 30.8.2015.

Microsoft, 2012a. Päivitetty 24.6.2013. Test Lab Guide: Deploying an AD CS Two-Tier Hierarchy. Luettavissa: https://technet.microsoft.com/library/hh831348.aspx Luettu 19.3.2015.

Microsoft, 2012b. Prepare the CAPolicy.inf File. Luettavissa: https://technet.microsoft.com/en-us/library/jj125373.aspx Luettu 19.3.2015.

Microsoft, 2014. Securing PKI: Planning a CA hierarchy. Luettavissa: https://technet.microsoft.com/en-us/library/dn786436.aspx Luettu 10.4.2015.

Microsoft, 2012c. Päivitetty 14.11.2012. Certutil. Luettavissa: https://technet.microsoft.com/en-us/library/cc732443.aspx Luettu 24.4.2015.

Microsoft, ei julkaisupäivämäärää G. Viimeksi tarkastettu 7.5.2009. Guidelines for enabling smart card logon with third-party certification authorities Luettavissa: https://support.microsoft.com/en-us/kb/281245 Luettu 13.4.2015.

Microsoft, ei julkaisupäivämäärää H. Export a Certificate. Luettavissa:

https://technet.microsoft.com/en-us/library/cc730988.aspx Luettu 23.4.2015.

Microsoft, ei julkaisupäivämäärää I. Add Published Certificates to Active Directory Containers. Luettavissa:
https://technet.microsoft.com/en-us/library/cc731612.aspx Luettu 23.4.2015.

Microsoft, ei julkaisupäivämäärää J. Office 365 integration with on-premises environments. Luettavissa: https://support.office.com/en-au/article/Office-365-integration-with-on-premises-environments-263faf8d-aa21-428b-aed3-2021837a4b65 Luettu 29.8.2015.

Microsoft, päivitetty 2012. Add User Principal Name Suffixes. Luettavissa:
https://technet.microsoft.com/en-us/library/cc772007.aspx Luettu 23.4.2015.

Microsoft, päivitetty 10.4.2014b. Configuring Alternate Login ID. Luettavissa:
https://technet.microsoft.com/en-us/library/dn659436.aspx Luettu 27.4.2015.

Microsoft 2010. How to disable the Subject Alternative Name for UPN mapping. Luettavissa:
https://technet.microsoft.com/en-us/library/ff520074%28WS.10%29.aspx Luettu 24.4.2015.

Microsoft, päivitetty 2008. Map a Certificate to a User Account. Luettavissa:
https://technet.microsoft.com/en-us/library/cc754866.aspx Luettu 24.4.2015.

Partanen, 18.12.2013. FINEID – S2 VRK (PRC) CA-model and certificate contents v2.4. Sivut 3, 6-30. Luettavissa:
https://eevertti.vrk.fi/Default.aspx?id=0&docid=951&action=Publish Luettu 28.8.2015.

Patrick, S. 14.6.2010. HowTo: Disable UPN mapping for SmartCard logon. Luettavissa:
http://blogs.msdn.com/b/spatdsg/archive/2010/06/14/howto_3a00_-disable-upn-mapping-for-smartcard-logon.aspx Luettu 24.4.2015.

Simonsen, M. 25.6.2013. Active Directory Domain Controllers and Certificate Auto-enrollment. Luettavissa:
https://morgansimonsen.wordpress.com/2013/06/25/active-directory-domain-controllers-and-certificate-auto-enrollment/ Luettu 24.4.2015.

Smart Card Alliance, ei julkaisupäivämäärää A. About Smart Cards: Frequently Asked Questions. Luettavissa: http://www.smartcardalliance.org/smart-cards-faq/ Luettu 17.8.2015.

Väestörekisterikeskus, ei julkaisupäivämäärää. Kortinlukijaohjelmisto ja varmenteen testaus. Luettavissa: https://eevertti.vrk.fi/Default.aspx?id=247 Luettu 17.3.2015.

Liitteet

Liite 1 – VRK:n myöntämän autentikaatio/salausvarmenteen kentät

Certificate
Varmenne koostuu kolmesta vaaditusta kentästä, jotka ovat tbsCertificate, signatureAlgorithm ja signatureValue. Nämä käydään läpi seuraavaksi. (Partanen, 2013, 9.)

signatureAlgorithm
Sisältää CA:n tämän varmenteen allekirjoittamiseen käyttämän salausalgoritmin tunnisteen. Käytetty algoritmi on joko SHA-1 tai sha256. (Partanen, 2013, 9.)

signatureValue
Sisältää ASN.1 DER -koodattua tbsCertificatea vastaan lasketun digitaalisen allekirjoituksen. Tällä allekirjoituksella CA varmentaa tbsCertificate -kentän tietojen oikeellisuuden. (Partanen, 2013, 9-10.)

TBSCertificate
Sisältää varmenteen myöntäjän sekä varmenteen subjektin nimet, subjektiin liittyvän julkisen avaimen, versionumeron, varmenteen voimassaoloajan sekä sarjanumeron. Sisältää myös laajennukset. Käydään läpi TBSCertificaten kentät. (Partanen, 2013, 10.)

Version
Kertoo varmenteen standardin version. Tässä tapauksessa se siis on 3. (Partanen, 2013, 10.)

serialNumber
Sisältää varmenteen sarjanumeron. Jokaisella saman CA:n myöntämällä varmenteella on oma, uniikki sarjanumeronsa. (Partanen, 2013, 10.)

issuer
Sisältää tiedot varmenteen allekirjoittaneesta ja myöntäneestä tahosta, jota kuvataan usealla eri ominaisuudella. Nämä ominaisuudet ovat commonName (kuvaava CA:n nimi), organizationName (joka on myöntävän organisaation nimi), organizationalUnitName (myöntävän organisaatioyksikön kuvaava nimi, näissä varmenteissa tätä käytetään ylimääräisenä suomenkielisenä varmenteen tyypin kuvauksena), stateOrProvinceName (myöntäjän valtio) sekä countryName (myöntäjän valtion lyhenne). Kaikilla VRK:n CA -varmenteilla on sama myöntäjä: Väestörekisterikeskus CA. (Partanen, 2013, 11-12.)

validity

Sisältää ajanjakson, jonka ajan CA takaa säilyttävänsä tietoa varmenteen tilasta. (Partanen, 2013, 12-13.)

subject

Tunnistaa tahon, joka liittyy subject public key -kenttään tallennettuun julkiseen avaimeen. Kun kyseessä on terveydenhuollon ammattilaiselle myönnetty varmenne, sisältää se attribuutit title (subjektin ammattinimike suomeksi ja ruotsiksi) ja pseudonym (subjektin tunnistamiseen käytetty koodi). (Partanen, 2013, 13, 15.)

subjectPublicKeyInfo

Sisältää julkisen avaimen ja tällä tunnistetaan algoritmi, jolla avainta käytetään. Kaikissa VRK:n myöntämissä varmenteissa käytetään RSA-algoritmia. (Partanen, 2013, 19.)

Varmennelaajennukset

X.509 v3:lle määritellyt laajennukset mahdollistavat lisäattribuuttien käyttämisen käyttäjien ja julkisten avainten kanssa. X.509 v3 myös antaa mahdollisuuden määritellä yksityisiä laajennuksia, joita käytetään kyseiselle organisaatiolle uniikin tiedon sisältämiseen. Jokainen laajennus on joko kriittinen tai ei-kriittinen. Varmennetta käyttävän järjestelmän on pakko hylätä varmenne, mikäli siinä on kriittinen laajennus, jota järjestelmä ei tunnista. Ei-kriittiset voidaan puolestaan jättää huomiotta vaikka niitä ei tunnistettaisikaan. (Partanen, 2013, 19.) Käydään läpi VRK:n myöntämissä varmenteissa käytettäviä laajennuksia.

authorityKeyIdentifier

Mahdollistaa varmenteen allekirjoitukseen käytetyn julkisen avaimen tunnistamisen. (Partanen, 2013, 20.)

subjectKeyIdentifier

Mahdollistaa tietyn julkisen avaimen sisältävien varmenteiden tunnistamisen. (Partanen, 2013, 21.)

keyUsage

Määrittää varmenteessa olevan avaimen tarkoituksen (esim. allekirjoitus, varmenteen allekirjoitus). Tätä laajennusta on käytettävä sellaisissa varmenteissa, jotka sisältävät julkisia avaimia, joita käytetään muissa julkisen avaimen varmenteissa olevien digitaalisten allekirjoitusten vahvistamiseen. (Partanen, 2013, 21-22.)

certificatePolicies

Sisältää tietoa yhdestä tai useammasta käytäntöinformaatioehdosta, joista jokainen koostuu OID:sta (Object identifier) ja vapaavalintaisista määreistä. (Partanen, 2013, 22.)

subjectAltName
Mahdollistaa useiden identiteettien sitomisen varmenteen subjektiin, kuten esimerkiksi sähköpostiosoitteen. Microsoftin toimikortilla kirjautumisominaisuuksien tukemiseksi tämä sisältää myös UPN:n varmenteen subjektille. UPN:llä identifioidaan käyttäjiä Active Directoryssä, ja se on usein sähköpostiosoite. Esimerkiksi UPN voi olla etunimi.sukunimi@firma.fi tai kuten VRK:n korteille myöntämillä varmenteilla, mallia 123456789@teonet.fi. (Partanen, 2013, 24-25.)

Basic Constraints
Tunnistaa, onko varmenteen subjekti CA. (Partanen, 2013, 25.)

extendedKeyUsage
Määrittelee, mihin varmenteen julkista avainta voidaan käyttää. (Partanen, 2013, 26.)

cRLDistributionPoints
Määrittelee, miten CRL (Certificate Revocation List, varmenteiden kumoamislista) -tietoa saadaan haettua. (Partanen, 2013, 27.)

Näiden laajennusten lisäksi varmenteissa on enintään kolme yksityistä laajennusta. Uudemmissa varmenteissa ei näistä yhtä, netscape-cert-type, ole, sillä se on vanhentunut eikä enää käytössä.