Topias Alvinen

PKI-INFRASTRUKTUURIN JA VAHVAN TUNNISTAUTUMISEN SUUNNITTELU JA TOTEUTUS

Tietotekniikan koulutusohjelma
2016

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

PKI-INFRASTRUKTUURIN JA VAHVAN TUNNISTAUTUMISEN SUUNNITTELU JA TOTEUTUS

Alvinen, Topias
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Huhtikuu 2016
Ohjaaja: Hentunen, Ilmari
Sivumäärä: 49
Liitteitä: -

Asiasanat: Toimikortti, PKI, Vahva tunnistautuminen, Sertifikaatti

---

Opinnäytetyön aihe on PKI-infrastruktuurin ja vahvan tunnistautumisen suunnittelu ja toteutus. Työn toimeksiantajana toimi yritys nimeltä AGCO Power ja työ toteutettiin tavoitekeskeisenä projektina. Projekti toteutettiin yrityksen tiloissa, jolloin työ saatiin suunniteltua ja testattua siinä ympäristössä, jossa se lopulta otettiin käyttöön.

Projektin tavoitteena oli käyttöönottaa yrityksen henkilöstölle identiteettikortti, mahdollistaa kortilla kulunvalvonta yrityksen tiloissa, sekä mahdollisuus kertakirjautumiseen tietokoneille. Lisäksi opinnäytetyössä tutustutaan vahvaan tunnistatumiseen sekä teoriaosuudessa toimikorttien yleisiin toimintoihin sekä standardeihin. Tavoitteen saavuttamiseksi tutustuttiin toimikorttien toimintaan sekä julkisen avaimen infrastruktuuriin. Tämä infrastruktuuri pitää sisällään toimikortin varmentamiseen liittyvän ympäristön eli varmenteiden hallintaan keskittyvät palvelimet ja palvelut. Kyseisen ympäristön toteuttamiseen ja tavoitteisiin pääsemiseksi oli olennaista löytää laadukas palveluntarjoaja yhteistyökumppaniksi projektiin.

Projektin alussa tutkimusongelmaksi muodostettiin seuraavat kaksi kysymystä: Mitä etuja on vahvan tunnistautumisen käytössä kevyen tunnistautumisen sijaan? Onko AGCO Powerilla tarvetta vaihtaa tunnistusmenetelmä kevyestä vahvaan? Asetettuihin kysymyksiin lähdettiin etsimään vastauksi perehtymällä aihetta käsitteleviin tieteellisiin artikkeleihin, tunnistautumiseen liittyviin yleisiin ohjeistuksiin ja hyödyntämällä asiantuntijoilta saatuja lausuntoja sekä mielipiteitä aiheesta.

Projektin lopputuloksena oli henkilön nimellä ja yrityksen logolla varustettu toimikortti, joka on varmennettu niin, että henkilö pystyy käyttämään korttia kulunvalvonnassa sekä tietokoneelle kirjautuessa. Toimikortin käyttöönotto sujui hyvin ja korttien varmentamisessa ei ilmennyt ongelmia. Toiminta testattiin ja toimikortit todettiin käyttöominaisuuksiltaan hyväksi sekä hyödylliseksi tietoturvan osalta.

DESIGNING AND IMPLEMENTING PUBLIC KEY INFRASTRUCTURE AND STRONG AUTHENTICATION

Alvinen Topias
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Technology
April 2016
Supervisor: Hentunen, Ilmari
Number of pages: 49
Appendices: -
Keywords: Smart card, PKI, Strong Authentication, Certificate

The subject of this thesis is designing and implementing public key infrastructure and strong authentication. The task of the thesis was assigned by AGCO Power and it was carried out as a goal focused project. The project was executed in the company's premises which enabled the planning and the testing to take place in the same environment where it was later taken in to use.

The goals for this project were the identity card implementation for personnel, the access control enabling with smart card in the company´s property and the providing of the possibility for single sign-on. In the theory part of the thesis strong authentication and common functions and standards of the smart card are introduced. To achieve the goals the functions of the smart card and the infrastructure of the public key were explored. The infrastructure contains environment associated with the smart card enrollment, meaning servers and services focusing on controlling certificates. To carry out the environment in question and to reach the goals it was essential to find a quality service provider as a cooperation partner for the project.

In the beginning of the project two questions formed the research problem: What benefits does strong authentication provide in comparison to a basic authentication? Does the AGCO Power have the need for replacing basic access authentication with a strong authentication? The answers for these questions were found by looking into the scientific articles as well as the common instructions around the subject and utilizing the given expert statements and views of the matter.

Conclusion of the project was smart card supplied with owner’s name and company´s logo. Smart card is secured in a way that allows owner to use card in access control and while logging in on a computer. Introduction of smart card ran well and no problems occurred during smart card enrollment. Functionally was tested and smart cards were found to both have good fixed assets and beneficial concerning information security.

SISÄLLYS

1 JOHDANTO

Nykyhetken trendi tuntuu olevan se, että yritysten kaikki tärkeä ja olennainen informaatio löytyy verkosta. Tämä luo tietoturvalle entistä tärkeämmän merkityksen. Aiemmin tärkeiden kansioiden varastamiseen tarvittiin moninumeroinen numerokoodi. Nykyään tietokoneelle ja verkkoon pääsee, jos tietää henkilön käyttäjätunnuksen ja salasanan. Helpon salasanan hakkeri murtaa jo muutamassa tunnissa. Edellä mainituista syistä johtuen monien yritysten on tärkeää päivittää tietoturvakäytäntönsä nykyaikaisemmaksi. Tässä opinnäytetyöprojektissa päätavoitteena oli parantaa AGCO Powerin tietoturvaa käyttäen vahvennettua tunnistamista, jossa kirjautumiseen käytetään toimikorttia ja PIN-koodia.

Opinäytetyössä tutustutaan projektin tavoitteisiin, tarpeisiin, toteutukseen ja lopputulokseen. Käyn opinnäytetyössä läpi myös kaikki projektin käyttöönoton työvaiheet eli toimikorttikirjautumiseen vaadittavien palvelinten asennukset ja määritysten tekemiset sekä toimikortin myöntämisen loppukäyttäjälle.

Opinnäytetyössä tutustutaan lisäksi tutkimuksen kautta vahvaan tunnistamiseen sekä kirjallisessa osuudessa toimikorttien yleisiin toimintoihin ja standardeihin. Opinnäytetyö projektin tavoitteisiin kuului mahdollistaa kirjautuminen Thin Client-laitteisiin, joita AGCO Power käyttää tuotantoympäristössä. Projektin tavoitteena oli myös hankkia ja käyttöönottaa kulunvalvontaan sekä kertakirjautumiseen käytettävät sirulliset henkilökortit.

Käyttöönottoa varten perustettuun projektiin nimettiin projektiryhmä, jonka vastuulla oli määritellä ja toteuttaa projekti. Toimin ryhmän projektipäällikkönä.

2 YRITYSKUVAUS

Merkittävänä ja uusia sekä innovatiivisempia tuotteita kehittelevänä yrityksenä AGCO Powerilla on intressinä parantaa jatkuvasti tietoturvaansa ja tuotesuojaustaan.

Opinnäytetyön laatiminen lähti liikkeelle AGCO Powerin tarpeesta saada henkilökunnalle käyttöön henkilökortit, joilla onnistuu kulunvalvonnan lisäksi kirjautuminen toimihenkilöiden tietokoneille sekä kaikille yleisessä käytössä oleville kioski-PC:lle.

AGCO Power on 70 vuotta Nokialla toiminut dieselmoottoritehdas. AGCO Power on ollut yksi maailman isoimmista dieselmoottoreiden valmistajista siitä lähtien, kun entinen Sisu Diesel yhdistyi amerikkalaiseen AGCO-konserniin vuonna 2008.
Tehdas sijaitsee Nokian Linnavuoressa ja se valmistaa vuosittain n. 30 000 dieselmoottoria ja henkilöstön määrä on n. 700. ACGO Powerin dieselmoottori löytyy useimmista maailman johtavista traktoreista sekä maatalouskoneista. Valmistettavia moottoreita ovat 3-, 4-, 6-, 7- ja 12-sylintereiset moottorit. Linnavuoressa myös huolletaan käytettyjä ja viallisia moottoreita. Dieselmoottoreiden lisäksi AGCO Power valmistaa hammaspyöriä, akseleita ja vaihteistoja. AGCO Power kuuluu AGCO-konserniin, joka on maailman kolmanneksi suurin maatalouskoneiden kehittäjä ja valmistaja. AGCO:n maailmankuuluja merkkejä ovat traktorivalmistaja Massey Ferguson, Suomessa toimiva traktorivalmistaja Valtra sekä Cleaner puimurit. AGCO tuotteita myydään yli 140 maassa.

3 TERMIT JA KÄSITTEET

ASM	Tekninen integraatio työasemaan. Käyttäjän PIN-koodin hallinta.
CA	Certificate Authoritylla tarkoitetaan varmentajaa, jonka tarkoitus on jakaa sertifikaatteja eli varmenteita tunnistamista varten.
EEPROM	Ohjelmamuisti, joka säilyttää tietonsa vaikka virta katkaistaan.
Flexim	Asiantuntijayritys, jota AGCO Power on käyttänyt jo kymmeniä vuosia kulunvalvontaan liittyvissä ratkaisuissa.
HR	Human Resources, henkilöstöosasto.

Hybridikortti	Kortti, joka sisältää kaksi eritaajuista sirua. Tässä projektissa toinen siru oli työasemakirjautumista varten ja Rfid-siru kulunvalvontaa varten.
Intranet	Sisäverkko tai lähiverkko, joka on eristetty vain tietylle joukolle.
MMC	Microsoft Management Console. Windowsin työkalu, jolla hallitaan verkon osia, ohjelmia ja laitteita.
Minidriver	Minidriver tarjoaa base CSP/KSP rajapinnan, jonka avulla toimikorttia voi käyttää suoraan Microsoft CA-järjestelmän kanssa mm varmenteiden myöntämisen ja hallintaan.
POC	Proof of concept eli projektin vaihe, jossa todetaan idea käytännössä toimivaksi.
Private Key	Private key eli yksityinen avain on julkisen avaimen menetelmässä salauksen purkamiseen ja sähköiseen allekirjoittamiseen käytetty puolisko avainparista.
RAM	Työmuisti. Sitä tarvitaan laskemiseen ja vastaamiseen. Kun kone suljetaan työmuisti katkeaa.
ROM	Laitteen pysyvämuisti, johon ei voi tehdä muutoksia normaalikäytön aikana.
RFID-siru	Radio FrequencyIDentification eli radiotaajuinen etätunnistus.
Thin Client	Tietokone, joka saa kaiken palvelupohjaisen sisällön pilvipalvelusta tai verkosta.
Varmenne	Sähköisesti allekirjoitettu dokumentti. Se sisältyy omistajan tiedoista, julkisesta ja salatusta avaimesta. Varmenne suojataan PIN-koodilla.

4 TOIMIKORTIT

4.1 Yleistä tietoa toimikorteista ja niiden toiminnoista

Toimikortti eli älykortti tunnetaan yleisesti luottokortin kokoisena muovikorttina, jonka sisään on rakennettu mikropiiri. Standardikoosta poikkeavia toimikortteja ovat esimerkiksi matkapuhelimissa käytettävät sim-kortit sekä muistikortit. Toimikortit voidaan jakaa neljään ryhmään: muistikortit, kontaktilliset kortit, etäluettavat kortit sekä hybridikortit.

Muistikorttia käytetään usein tiedon varastoimiseen, sillä kortissa ei ole tietojenkäsittelyominaisuuksia. Kortin muistisirussa on ohjelmamuisti EEPROM, joka on haihtumatonta puolijohdemuistia. Se voidaan kirjoittaa uudelleen 10 000-100 000 kertaa.

Kontaktillinen kortti on muistikorttia kehittyneempi kortti. Sen lisäksi että kortti voi varastoida tietoa, se voi suorittaa tietojenkäsittelyä sekä laskutoimituksia. Kontaktikortin yleisin tunnusmerkki on ulkopinnassa oleva metallisiru, jonka kautta kortti kytkeytyy lukijaan. Kontaktilliselle toimikortille virtalähteen ja kellosignaalin tuottaa kortinlukija. Kun kortti asetetaan lukijaan, päätelaite avaa tiedonsiirtoa varten tietoliikennekanavan laitteen sovellusohjelman ja kortin käyttöjärjestelmän välillä. Järjestelmä on vuorosuuntainen eli tällöin järjestelmässä dataa lähettäviä osapuolia voi olla vain yksi kerrallaan. Toimikortin sirulta vastaanotetut paketit tai kortille lähetetty data varastoidaan kortin työmuistiin. Toimikortin ja päätelaitteen pitää tunnistaa toisensa ennen kuin korttitapahtuma voi alkaa. Kortti luo ensiksi satunnaisluvun, jonka se lähettää päätelaitteelle. Tämän jälkeen päätelaite salaa luvun yhteisellä salausavaimella ja lähettää salatun luvun takasin kortille. Kortti vertaa saamaansa lukua omaan salaukseensa ja jos yhteys on varmistettu ja tiedonsiirto voi alkaa. Jokainen sanoma joka lähetetään, varmistetaan ja vahvistetaan vahvistuskoodilla.

Kontaktiton eli etäluettava kortti toimii korttiin asennetun RFID-antennin avulla, joka kommunikoi radiovastaanottaminen kanssa. Tällainen kortti sopii hyvin käytettäväksi esimerkiksi joukkoliikenteen maksuvälineenä tai kulunvalvonnassa. Kontaktittoman toimikortin lähe-

tin/vastaanotin saa virtansa RFID-lukijasta tiedonsiirron aikana. Jotta kortin lukija ja kortin lähetin voisivat kommunikoida, niiden pitää käyttää samaa radiotaajuutta. Kaikkia toimikortteja luetaan päätelaitteella tai kortinlukijalla. Kortin käyttö vaihtelee siihen ohjelmoitujen toimintojen mukaan. Sähköinen allekirjoitus edellyttää salausprosessorin sisältävää sirukorttia.

Toimikortit ovat olleet käytössä Suomessa 1990-luvun alusta asti, mutta silti niitä on hyödynnetty korttien potentiaaliin nähden yllättävän vähän. Yleisenä tietoturvavälineenä tietojenkäsittelyssä vasta kymmeniä vuosia vuotta. Älyllistä korttitekniikkaa on käytetty aikaisemmin laajamittaisesti matkapuhelimien SIM-korteissa, maksuvälineenä sekä julkisessa liikenteessä. (Rinne 2002, 13)

4.2 Projektissa käytettäväksi valitun toimikortin fyysiset ominaisuudet

Toimikorttien fyysisiä standardeja ja sähköisiä ominaisuuksia on standardoitu. ISO 7816-standardiperhettä pidetään kaikkien toimikorttistandardien perustana. Muut toimikorttistandardit pohjautuvat ISO 7816-standardiin ja ovat siihen yhteensopivia. ISO 7816-1-standardi määrittelee toimikortin fyysiset mitat ja toimikorttipiirin sijoittumisen runkoon. Standardi myös kuvaa rungon valmistusmateriaalin ominaisuudet ja toimikortille tehtävät fyysiset rasitustestit.

Tämä standardi jakaa toimikortit fyysisten mittojen mukaan eri luokkiin. Niistä yleisimmät ovat ID-1, niin sanottu luottokorttikoko (Kuva1) sekä ID-000, joka on toteutus SIM-kortista. (Rinne 2002, 21)

Kuva 1. AGCO Power toimikortti (ID-1)

4.3 Projektissa käytettäväksi valitun toimikortin tekniset ominaisuudet

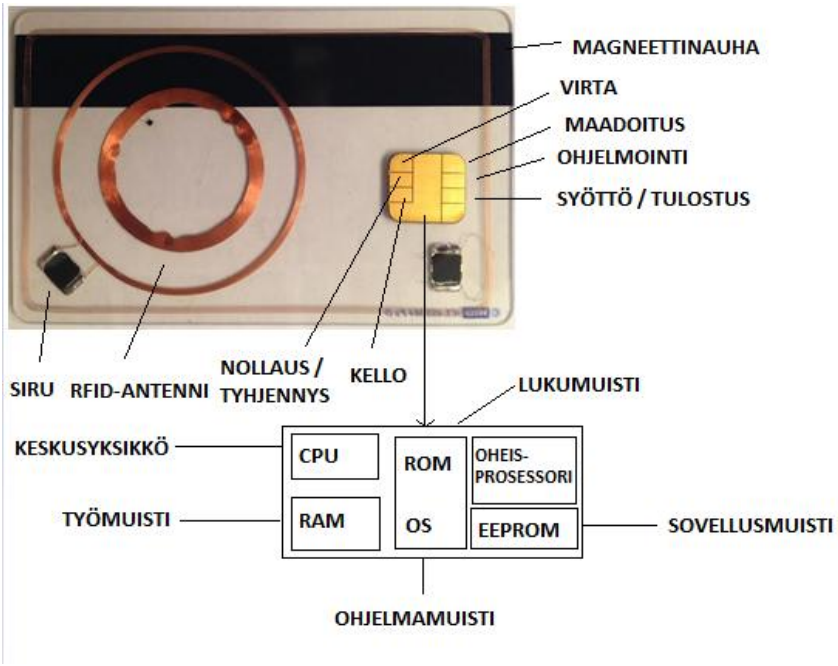
Kontaktillisen toimikortin tekniikka on kortin sirussa. Kortin siru sijaitsee kortin pinnalla olevan kultaisen kontaktimoduulin alla, jonka kautta toimikortti on yhteydessä päätelaitteeseen tai kortinlukijaan.

Kontaktimoduulissa on kahdeksan kontaktia. Yksi niistä tarjoaa tarvittavan virran kortille ja vastakkainen tuottaa maadoituksen. Kolmas kontakti on tyhjennystä varten ja neljäs kellosignaalille. Viides on syöttö-/tulostusportti ja kuudes on ohjelmointiportti. Kaksi tyhjää porttia on varattu tulevaa käyttöä varten. (Kuva 2)

Kontaktillinen prosessikortti sisältää muistijärjestelmän, prosessorin sekä syöttö- ja lähetysportin. Muistijärjestelmä sisältää lukumuistia ROM:ia, johon on sijoitettu kortin tiedostojärjestelmän ylläpito, käyttöjärjestelmä sekä muut perusohjelmat. ROM on kooltaan korteissa 8-32 kilotavua ja sitä voi vain lukea.
Muistijärjestelmän työmuisti RAM toimii väliaikaisena muistina. Sitä tarvitaan laskemiseen ja vastaamiseen. Työmuisti katkeaa, kun virta katkaistaan. RAM on noin kilotavun kokoinen. Muistiin voi kirjoittaa ja sitä voi lukea. Kortin ohjelmamuisti eli EEPROM säilyttää tietonsa vaikka virta katkaistaan. EEPROM-muistiin tallentuvat

kaikki muuttuvat tiedot kuten rahan määrä. Sovellusohjelmat voivat sekä lukea että kirjoittaa EEPROM:iin, joka 1-24 kilotavun kokoinen.

Toimikortin ydin on ROM:ssa sijaitseva käyttöjärjestelmä, jota voidaan verrata tietokoneen vastaavaan järjestelmään sillä erolla, että toimikortin sirussa on vähemmän muistia kuin tietokoneessa. Toimikortin käyttöjärjestelmä hallinnoi kortin ominaisuuksia, valvoo kortille pääsyä ja huolehtii datan siirrosta kortille.
Mikroprosessori on toimikortin aivoina toimiva keskusyksikkö, joka toteuttaa konekäskyt sekä ohjaa muistin jakamista eri toiminnoille. Mikroprosessori kontrolloi kortin syöttö –ja lähetysporttia, jonka kautta kortti kytkeytyy päätelaitteisiin sekä kortinlukijoihin. (Lerssi-Lahdenvesi 2006, 8)



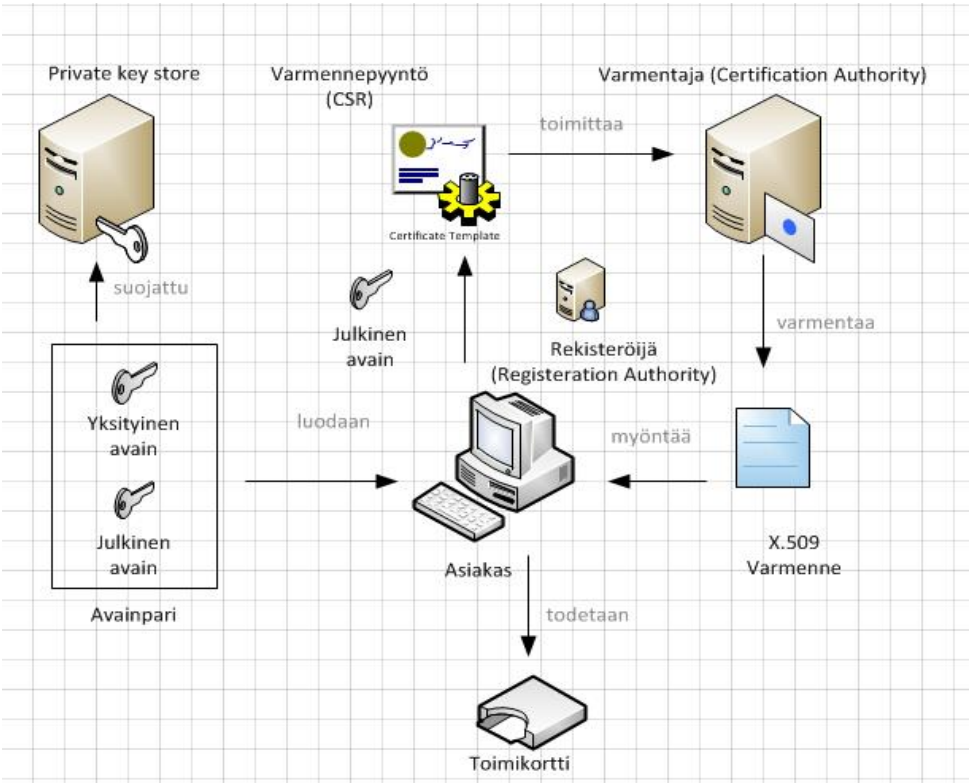
Kuva 2. Toimikortin tekniset ominaisuudet

5 JULKISEN AVAIMEN INFRASTRUKTUURI ELI PKI

Julkisen avaimen infrastruktuuri (Kuva 4) sisältää palvelimia ja palveluita, joiden avulla hallitaan varmenteita. Ympäristö koostuu yhdestä tai useammasta varmenteita hallitsevasta palvelimesta, joita kutsutaan Certification Authority –palvelimiksi. Yleensä palvelimia on ainakin kaksi: yksi ylemmän tason Juuri-Ca sekä varmenteita jakava Certification Authority –palvelin. Julkisen avaimen infrastruktuurin on tarkoi-

tus yhdistää varmenteet, salaus ja varmenneviranomaiset yhdeksi kokonaiseksi tietoturva-arkkitehtuuriksi. Tässä menetelmässä luotettava taho eli varmentaja sitoo julkisen avaimen käyttäjään. Tämän jälkeen käyttäjä rekisteröityy järjestelmään ja hänelle myönnetään varmenne. Tämän tekee rekisteröijä eli RA.

Mikäli julkisen avaimen infrastruktuurissa on tarkoituksena hyödyntää toimikorttia, tällöin lisätään julkinen avain eli varmenne toimikorttiin. Varmennetta pystyy käyttämään sen jälkeen, kun toimikortti on todentanut käyttäjän PIN-koodin avulla. Avain parin luomisen jälkeen varmentaja varmentaa toimikortin ja allekirjoittaa luodun julkisen avaimen ja varmennettavan käyttäjän tiedot omalla yksityisellä avaimellaan.



Kuva 4. Julkisen avaimen infrastruktuuri

6 AGCO POWER PROJEKTI - TOIMIKORTIN KÄYTTÖÖNOTTO

Toimikortin suunnittelun ja yhteiskumppanin eli palveluntarjoajan valinnan jälkeen projektin seuraava vaihe oli toimikortin käyttöönottaminen yrityksen tiloissa. Käyttöönotto oli projektin sisäinen oma prosessinsa, jonka toteutus suunniteltiin ja testat-

tiin huolellisesti ennen varsinaista käyttöönottoa. Käyttöönottoon liittyi eri vaiheita, joista kerrotaan tulevissa kappaleissa tarkemmin.

6.1 Projektin tutkimusongelma ja tutkimusmenetelmät

Ennen projektin aloittamista oli tarpeellista selvittää tutkimusongelma: Onko AGCO Powerille tarpeellista toteuttaa vahva tunnistautuminen vai riittääkö nykyinen kevyt tunnistautuminen yrityksen tietokoneille, joista on pääsy järjestelmiin ja arkaluontoisiin tietoihin. Tutkimus rajattiin niin, että vahva tunnistatutuminen tapahtuisi toimikortilla ja PIN-koodilla ja kevyt tunnistautuminen tapahtuisi perinteisesti käyttäjätunnuksen ja salasanan avulla. Tutkimusongelma oli tarpeellista selvittää heti projektin alkuvaiheessa, koska se oli lähtökohta ja motivaatio koko opinnäytetyöprojektille.

6.2 Projektin tutkimusongelman menetelmien selvitys ja pohdinta

Tunnistautuminen on menetelmä, jossa tunnistetaan järjestelmän käyttäjä salasanan tai avaimen avulla. (Simula 2014, 2)
Tunnistautumista sanotaan kevyeksi tunnistautumiseksi, jos se nojautuu vain yhteen todentamistapaan. Esimerkkejä kevyestä tunnistautumisesta:

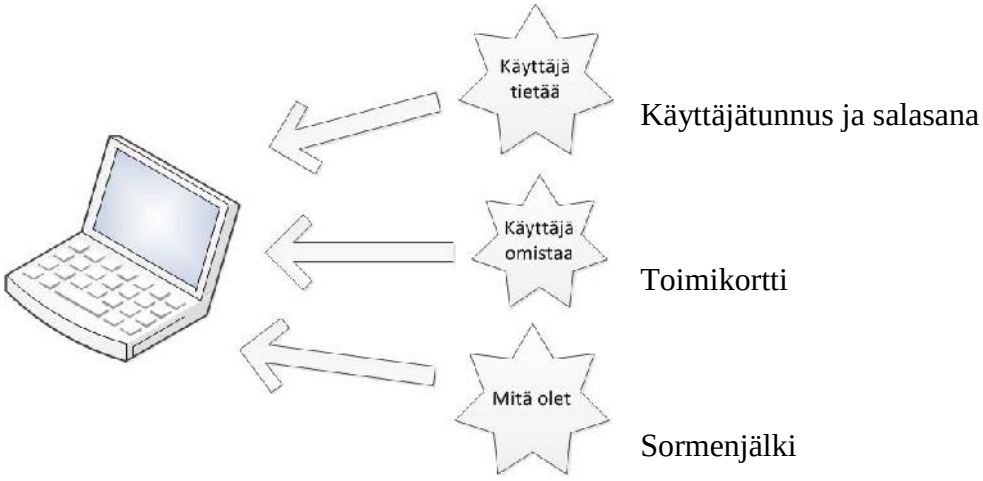
- käyttäjätunnus + salasana

(Valtiovarainministeriön hallinnon kehittämisosasto 2012, 20)
Vahva tunnistautuminen (Kuva 3) nojautuu kahteen tai useampaan todentamistapaan. Tämän tyylisiä tunnistamismenetelmiä ovat esimerkiksi:

- verkkopankkitunnuksiin ja vaihtuviin salasanalistoihin perustuva TUPAS-tunnistus
- varmenteellinen sirukortti + PIN-koodi

(Valtiovarainministeriön hallinnon kehittämisosasto 2012, 27)

AGCO Powerille suunnittelussa tunnistusmenetelmässä käyttäjällä on kaksi todistetta käyttäjän tunnistautumiseen. Käyttäjällä on toimikortti, jonka hän omistaa sekä vain hänen itsensä tietämä PIN-koodi.



Kuva 3. Vahvennettu tunnistautuminen

Vahva tunnistautuminen on tarpeen silloin kun nähdään, että mahdolliset väärinkäytökset aiheuttavat merkittävää haittaa ja riski väärinkäytökselle on suuri.
(Valtiovarainministeriön hallinnon kehittämisosasto 2012, 27)
Tutustuessani menetelmään tarkemmin vahvistui nopeasti ajatus siitä, että tämä on tunnistusmenetelmä, jota pitäisi käyttää aina yrityksissä, jossa halutaan varmistaa, etteivät ulkopuoliset pääse sisään tietokoneeseen ja arkaluonteiseen tietoon. Kevyt tunnistautuminen riittää mielestäni moneen järjestelmään, kuten esimerkiksi sosiaaliseen mediaan kirjautuessa. Mikäli yrityksen liikesalaisuuksiin ja muuhun arkaluontoiseen materiaaliin päästään kevyellä tunnistatumisella kirjautumaan, se on yritykselle iso riski. Tämä tulos ja pohdinta riitti siihen, että on tarpeellista aloittaa projekti ja sen myötä lisätä AGCO Powerin tietoturvallisuutta merkittävästi vahvan tunnistatumisen avulla.

6.3 Projektin toiminnalliset ja liiketoiminnalliset tavoitteet ja tarkoitukset

Projektille määriteltiin aluksi tavoitteet eli mitä asioita toimikortilla pitäisi pystyä konkreettisesti tekemään tulevaisuudessa yrityksen eri tunnistautumistilanteissa. Projektin aloituspalaverissa jaoimme tavoitteet kahteen kategoriaan: toiminnallisiin ja liiketoiminallisiin tavoitteisiin.

Projektin toiminnallisiin tavoitteisiin kuului sirullisten henkilökorttien hankkiminen kulunvalvontaan, hyödyntäen jo aiemmin yrityksessä käytössä olevaa Flexim-pääsynhallintajärjestelmää. Tämän lisäksi tavoitteena oli mahdollistaa teknisesti toimikortilla kertakirjautuminen AGCO Powerin Windows-tietokoneisiin. Projektin tavoitteisiin kuului myös mahdollistaa kirjautuminen Thin Client-laitteisiin eli kevytpäätteisiin, joita AGCO Power käyttää tuotantoympäristössä.

Projektin liiketoiminnallinen tavoite oli hankkia AGCO Powerin henkilökunnalle identiteettikortit ja toimikorttikirjautumisen helppouden avulla muuttaa henkilöstön kioski-pc:lle kirjautuminen aiempaa sujuvammaksi.

Yhteenvetona tavoitteista voisi sanoa, että projektilla oli kaksi keskeistä tarkoitusta. Ensimmäinen niistä oli toimikortin mahdollistama vahvennettu tunnistautuminen. Tässä tapauksessa työntekijä käyttää perinteisen menetelmän eli näppäimistöllä tietokoneelle kirjautumisen sijaan toimikorttia, joka sisältää omistajansa henkilökohtaisen varmenteen ja PIN-koodin.

Toinen olennainen tarkoitus oli flexim-kulunvalvontaan kirjautuminen samalla toimikortilla, kuin koneille. Tällaista toimikorttia kutsutaan nimellä hybridikortti. Tämä tarkoittaa käytettävän toimikortin olevan teknisiltä ominaisuuksiltaan sellainen, että varmenteen lisäksi siihen liitetään RFID-tunniste eli radiotaajuustunniste, jolla kulunvalvontaan vaadittava leimaus onnistuu.

6.4 Toimikortin määrittely ja suunnittelu

Ennen kun aloin kartoittamaan toimikortin toimittajaa oli toimikortille mietittävä ja sovittava kortin sisältö. Oli suunniteltava mitä teemme toimikortilla ja mitä se pitää sisällään. Tavoitteiden kautta pääpiirteet toimikortille oli selvät, mutta kortin tekniikka ja yhteensopivuus ennalta mietittyjen ratkaisujen kanssa oli määriteltävä tarkkaan. Perehdyin pääpiirteittäin erilaisiin toimikorttiratkaisuihin, joilla saisimme tavoitteemme ja yrityksen tarpeet täytettyä. Mietimme toimikortille valintakriteerit. Kortin oli oltava tehdasympäristöön soveltuva eli materiaaliltaan kestävä. Toimikorttiin oli pystyttävä tallentamaan sertifikaatti eli varmenne, jotta tietokoneelle kirjautuminen

mahdollistuisi. Tämän lisäksi toimikortin oli oltava visuaalinen tunnistusväline, joten sovimme alustavasti kulunvalvontaan liittyen, että käytetty Flexim-kulunvalvonta prosessi täytyy käydä läpi tarkasti toimittajan kanssa sekä varmentaa käytetty RFID-teknologia, jotta kortit voidaan varustaa oikealla tekniikalla. Tämän avulla voisimme korvata aikaisemmin käytössä olleet avaimet toimikorteilla.

Edellä mainittujen seikkojen lisäksi toimikorttiin halutuiksi ominaisuuksiksi määriteltiin fyysinen ja looginen tunnistautuminen. Fyysisellä tunnistamisella tarkoitetaan kulun ja- pääsynvalvontaa tiloihin ja rakennuksiin. Tämän tunnistusmenetelmän avulla varmistutaan siitä, että vain oikeutetut henkilöt voivat liikkua yrityksen tiloissa. Loogisella tunnistamisella tarkoitetaan pääsynvalvontaa eri tietojärjestelmiin. Tämän tunnistamismuodon avulla varmistutaan siitä, että vain oikeutetut henkilöt voivat päästä sisään yrityksen tietoverkkoihin ja järjestelmiin.

6.5 Toimikortin toimittajien vertailu ja valinta

Projektin seuraava askel oli selvittää ja valita yritykselle toimikorttien toimittaja, joka tarjoaisi parhaan korttiratkaisun budjettiin sopivaan hintaan. Tarkoituksena oli löytää ja valita toimittaja, joka pystyisi auttamaan AGCO Poweria löytämään oikeat ratkaisut tietoturvan, käytettävyyden ja kustannusten mukaan. Pyysin tarjousta toimikorttiratkaisusta kahdelta eri toimittajalta. Tarkoituksena oli löytää tarjousten joukosta vaatimukset täyttävä toimikorttiratkaisu.

Näistä kahdesta toimittajasta SecureLink pystyi tarjoamaan meille paremman toimikorttiratkaisun. Yritys tarjosi fyysisen tunnistuksen osalta ratkaisua, jossa käyttäjän tunnistus toteutetaan jo AGCO Powerissa käytössä olevalla teknologialla. Kyseinen tekniikka on Fleximin toimittama HID Prox II-tunnistusteknologia, joka liitetään kortin sisään. Loogisen tunnistuksen osalta SecureLink tarjosi ratkaisua, joka ei edellytä erillisen työasemasovelluksen asentamista vaan tietokone tunnistaa kortin Windowsin laitehallinnassa Microsoftin allekirjoittaman Minidriver-korttiajurin avulla. Sujuvan ja huolellisesti rakennetun toimikorttiratkaisun lisäksi SecureLink tarjosi

pakettia huomattavasti edullisemmalla hinnalla kuin toinen vaihtoehtomme, joten päätimme hyväksyä Secure Linkin tarjouksen sähköisistä henkilövarmennekorteista.

6.5.1 HID Crescendo C1150

SecureLink tarjosi HID Crescendo C1150 toimikorttiratkaisua. Tämän toimikortin luvattiin tarjoavan tehokkaan turvaratkaisun, kun AGCO Powerin tarpeena oli yhdenmukainen kokonaisratkaisu vahvan tunnistuksen tilanteisiin ja vaatimuksiin. Kortin tarjoaman vahvan turvallisuuden lisäksi kortti oli AGCO Powerille monipuolisuudellaan ja helppoudellaan paras yhdistelmä. Tämä oli näistä toisiinsa verratuista ratkaisuista meille sopivin sillä C1150-kortti mahdollisti loogisen tietojärjestelmäkirjautumiseen työasemilla sekä fyysisen kuluvalvonnan samalla kortilla. Microsoft BaseCSP Minidriver ajurin ansiosta C1150-korttia pystyi hyödyntämään Microsoft ympäristössä ilman erillistä sovellusta.

6.6 Toimikorttien käyttöönoton Proof of Concept-toteutus

Projektin onnistumisen kannalta oli hyvä vaatia toimittajalta Proof of Concept – vaihe. Käytännössä tämä vaihe tarkoittaa sitä, että tuoteidean toteutettavuus varmistetaan. Tuote ja sen toteutus esitellään tilaajalle, joka halutessaan hyväksyy lopputuloksen ja on valmis ostamaan tuotteen ja lopullisen käyttöönoton. Proof of conceptin toteutusvaiheessa Secure Linkin asiantuntija tuli Linnavuoreen AGCO Powerin tiloihin esittämään Microsoft CA-järjestelmän tukemaa korttien hallinnan konfigurointia. Toteutuksen tavoitteena oli, että toimikortteja voisi myöntää ja hallinnoida itsenäisesti AGCO Powerin henkilöstöosasto.

Ennen Proof of concept-vaihetta olimme päättäneet toimikortin käyttötarkoituksen eli mitä kortilla tehdään ja mitä se pitää sisällään. AGCO Powerin tarpeita huomioiden päädyimme malliin, jossa toimikortilla kertakirjaudutaan sisään Windowsiin. Tämä toimintamalli mahdollistaa vahvan tunnistautumisen kirjautumisvaiheessa. Yrityksen sovellukset tulevat käyttämään jatkossakin käyttöjärjestelmätunnistusta. Proof of concept piti sisällään:

- Microsoft CA-hierarkian suunnittelu ja luominen
- Microsoft CA:n käyttöönotto ja asetusten varmistus hyvien turvallisuus-käytäntöjen mukaisesti
- MS Certificate Templatien tekeminen: Enrolment ja Smartcard User
- Windows Smart Card –palvelujen käyttöönotto korttien myöntämiseen MMC:n kautta

6.6.1 Microsoft CA-hierarkian suunnittelu ja luominen

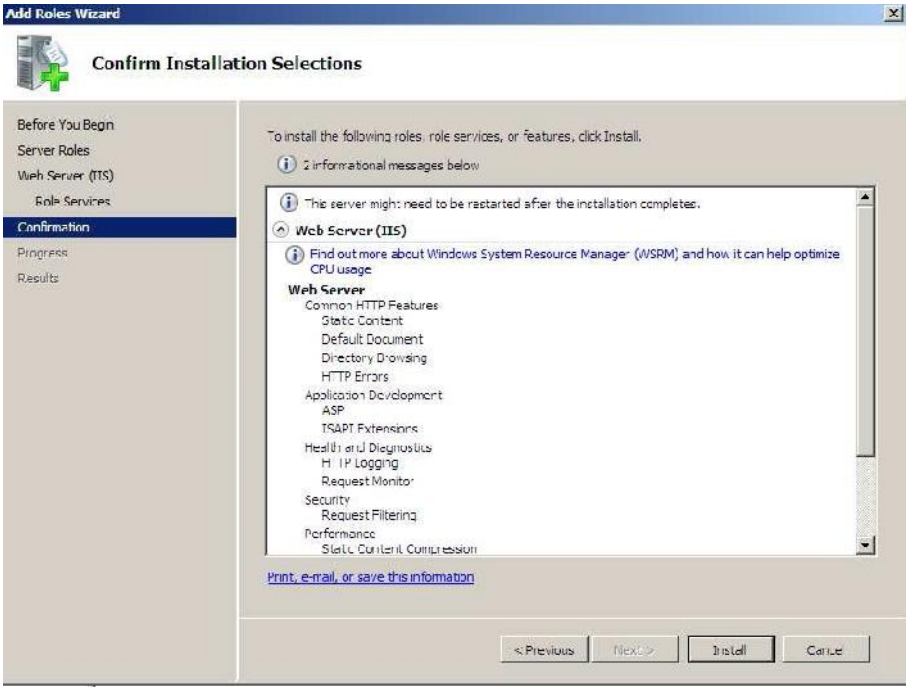
Ennen kun pystyimme aloittamaan CA-palvelimien asennuksen ja käyttöönoton, oli mietittävä tulevaa CA-hierarkiaa, joka muodostuu varmenteita myöntävistä palvelimista. AGCO-konserni käyttää toimintamallina kaksitasoista CA-hierarkiaa eri toimipisteissään. Tämä tarkoittaa sitä, että tässä toimintamallissa tietoturvatasoa on nostettu kytkemällä AGCO-konsernin Juuri-CA- palvelin offline -tilaan, jolloin se ei ole alttiina hyökkäyksille. Juuri-CA voi olla offline-tilassa, koska se myöntää sertifikaatteja ja julkaisee sulkulistoja vain harvoin. Juuri-CA:n rooliksi jää usein vain myöntää sertifikaatit toisen tason palvelimille. Tämä palvelin ei ole liitetty yrityksen Active directory – palvelimeen.
PKI:n asentaminen aloitetaan yleensä Juuri-CA:n asennuksella ja tämän jälkeen asennetaan Juuri-CA:n alapuolelle tarvittavat CA-palvelimet, mutta tässä tapauksessa asensimme vain toisen tason CA-palvelimet, jotka myöntävät sertifikaatit AGCO Powerin käyttäjille.

Tiivistetty malli AGCO Powerin CA:n rakenteesta:

1. Offline Juuri CA (AGCO Inc.)
   1.1 Standalone CA (AGCO Power)
      1.1.1 Enterprise Subordinate CA (AGCO Power)

Lähdimme luomaan AGCO Powerin CA-hierarkiaa niin, että pyysimme aluksi AGCO Powerin palvelinpuolen järjestelmänasiantuntijaa asentamaan meille kaksi virtuaalista Windows 2008 R2 Enterprise Server 64 bittistä palvelininstanssia toisen tason CA-palvelimia varten. AGCO Powerilla on omat palvelinsäännöt, jotka määrit-

tävät esimerkiksi palvelimien nimeämiskäytännöt. Sertifikaattipalvelimet nimettiin kyseisten sääntöjen mukaan nimillä Palvelin1 ja Palvelin2. Tarkoituksena oli, että koneissa olisi asennettuna vain varmennepalvelu eikä niitä asennettaisi AGCO Powerin toimialueen ohjauskoneiksi. Näihin sertifikaattipalvelimiin oli asennettava Web Server IIS-palvelu, jossa on ASP-ohjelmointimenetelmän tuki (Kuva 5). IIS on Microsoftin kehittämä Windows pohjaisissa palvelimissa käytettävä palvelinohjelmistokokonaisuus. Asennus tehtiin Domain Admin-tunnuksilla *XXX*.



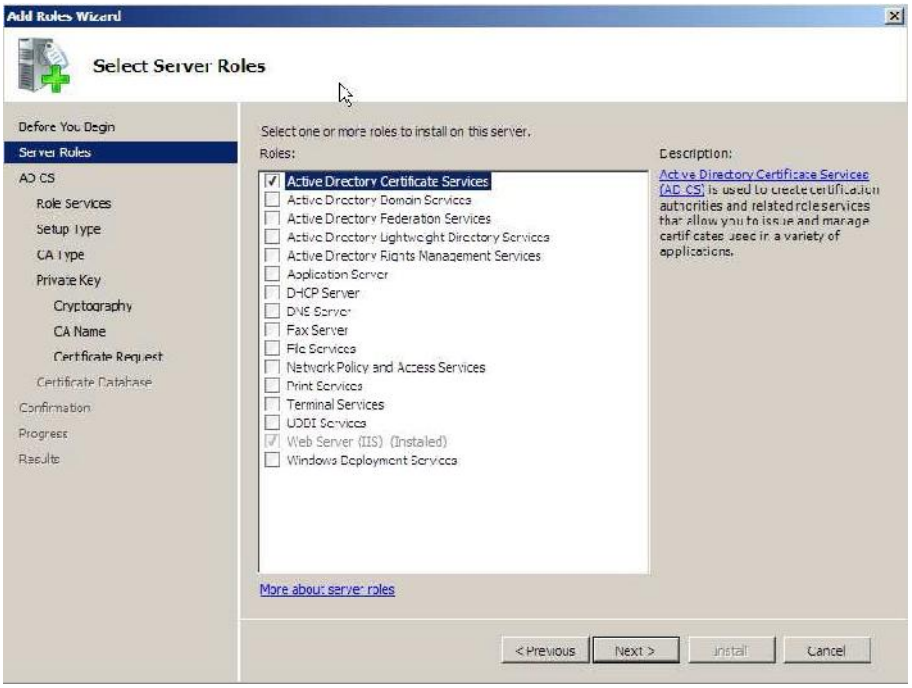
Kuva 5. IIS- palvelun asennus

6.6.2 Standalone Root CA palvelimen asennus

Päätimme perustaa käytäntö-CA eli Standalone Root CA:n sen jälkeen kun virtuaalipalvelimet olivat asennettu Palvelin1:lle. Kyseinen palvelin tulisi jakamaan sertifikaatit myöntäjä-CA:lle AGCO:n Root CA:lta.

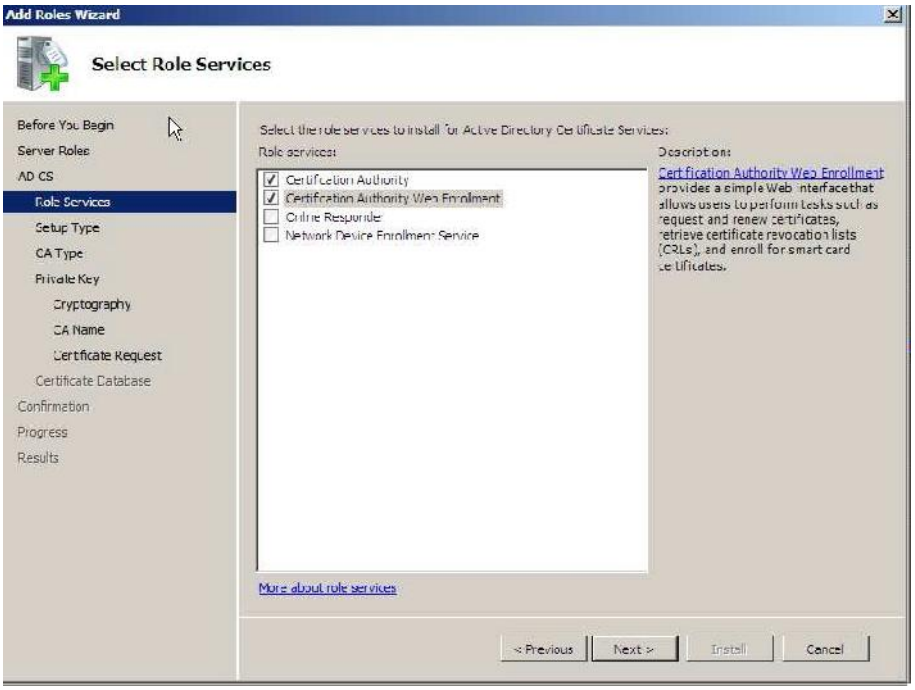
Standalone Root CA:n asennuksen alkaessa tuli Palvelin1:lle kirjautua Enterprise Admin tunnuksella, jolla on pääsy aktiivihakemiston configuration-osioon. Standalone Root CA asennuksessa oli 9 asennusvaihetta, joiden jälkeen itse Standalone Root

CA oli asennettu käyttövalmiiksi. Ensimmäisessä asennusvaiheessa (Kuva 6) lisäsimme Palvelin1:lle roolin Active Directory Certificate Services.



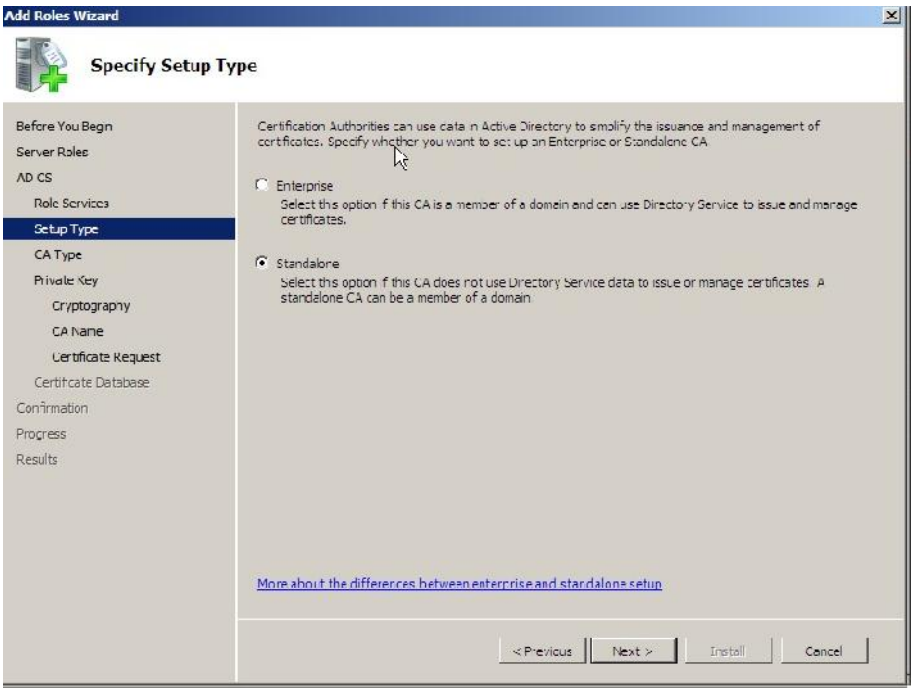
Kuva 6. Palvelin1 roolien valinta

Toisessa asennusvaiheessa (Kuva 7) lisäsimme Active Directory Certificate Services roolille roolipalveluita eli toiminnallisuuksia. Active Directory Certificate Services rooliin sisältyvät neljä roolipalvelua, josta valitsimme kaksi: Certification Authority – palvelu, jota käytetään varmenteiden hallitsemiseen ja Certification Authority Web Enrollment –palvelu. Jälkimäinen palvelu tarjoaa käyttöliittymän, jonka avulla voidaan muun muassa lisätä ja uusia varmenteita.



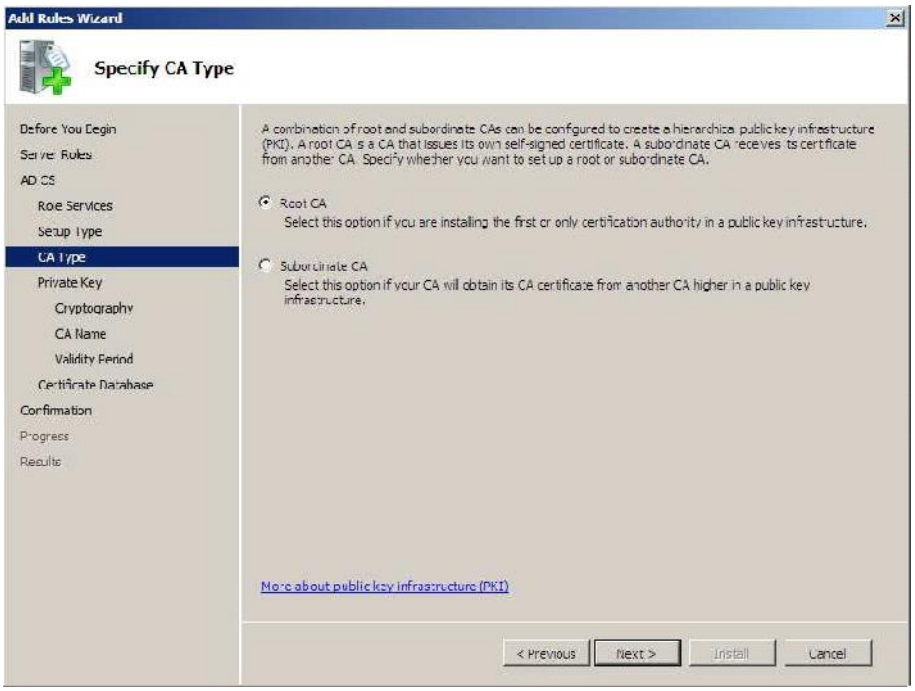
Kuva 7. Palvelin1 roolienpalvelujen valinta

Kolmannessa vaiheessa (Kuva 8) asennus jatkui CA-palvelityypin valitsemisella. Palvelin 1:stä olimme päättäneet tehdä Standalone Root CA:n, joka tulisi jakamaan varmenteet myöntäjä-CA:lle, joten valitsemme kohdan Standalone. Standalone CA:n tarkoitus on myöntää varmenteita korteille.



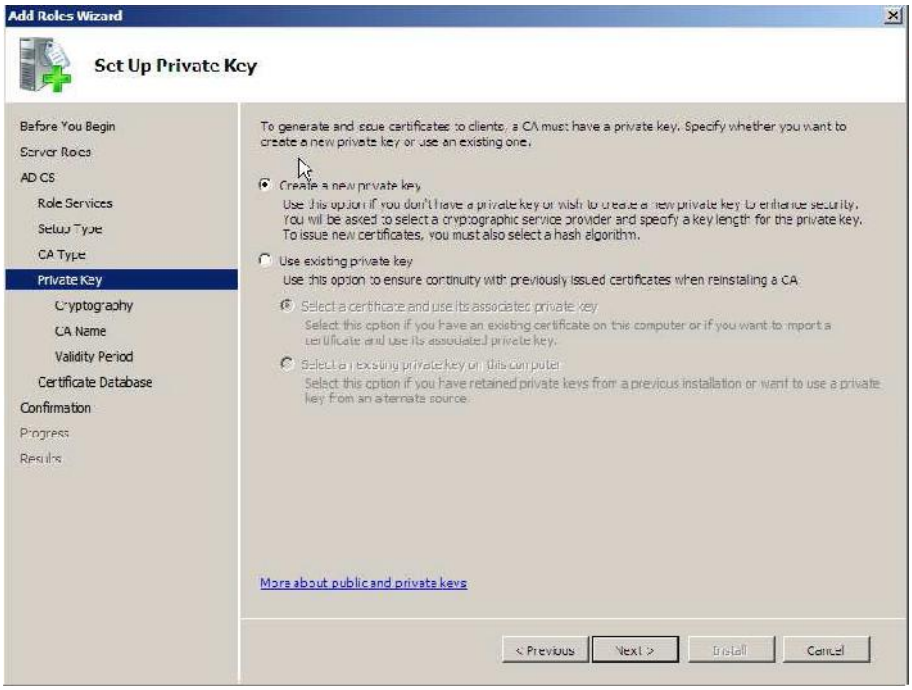
Kuva 8. Palvelin1:en CA-palvelintyypin valinta

Neljännessä vaiheessa (Kuva 9) valitsimme Certification Authority tyypin. Valittavana oli Root CA sekä Subordinate CA. Suunnitelman mukaan valitsimme Palvelin 1:en Root CA:ksi ja jätimme Subordinate CA:n valinnan seuraavalle palvelimelle nimeltä Palvelin2.



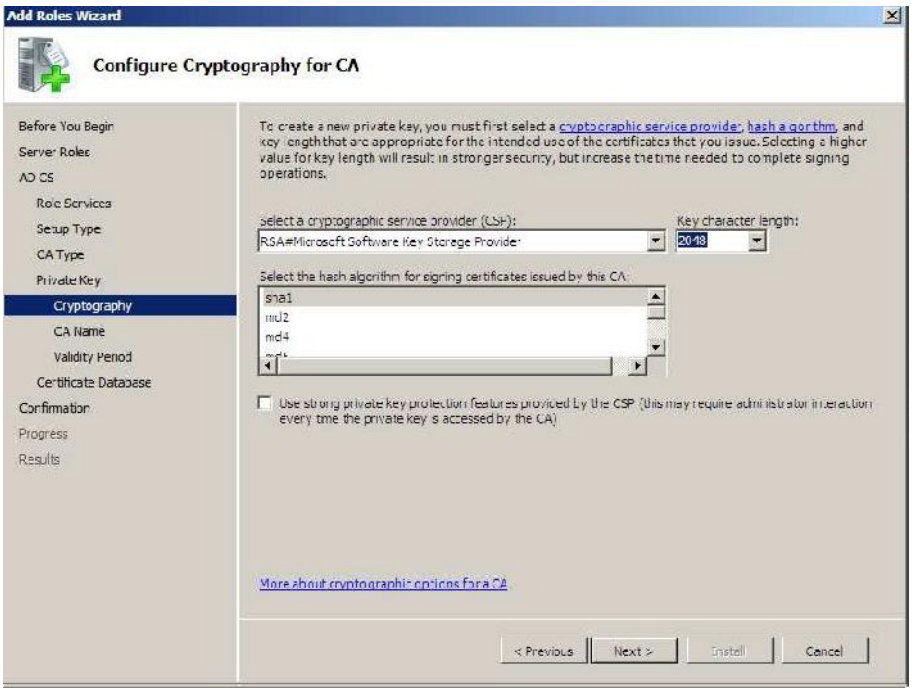
Kuva 9. Palvelin1 CA-tyypin valinta

Viidennessä vaiheessa (Kuva 10) luotiin palvelimelle uusi private key eli yksityinen avain. Yksityistä avainta käytetään julkisen avaimen menetelmässä salauksen purkamiseen ja sähköiseen allekirjoittamiseen. Julkisen avaimen menetelmä tarkoittaa menetelmää, jossa viesti salataan eri avaimella kuin se puretaan. Viesti puretaan yksityisellä avaimella sen jälkeen, kun se on salattu julkisella avaimella.



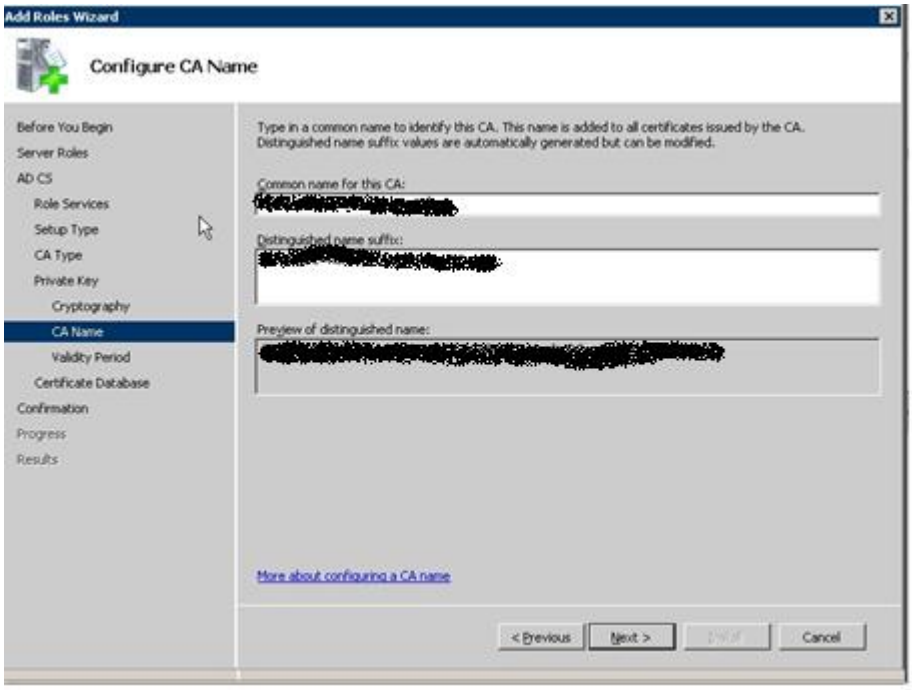
Kuva 10. Palvelin1 Private Keyn luonti

Kuudennessa vaiheessa (Kuva 11) määritellään käytettävät salaustekniikat. Ne on hyvä jättää oletusasetuksille. On tärkeää tarkistaa, että CA:n sertifikaatin avaimen pituus on 2048 merkkiä ja että Cryptographic service provider kohdassa on valittuna Microsoft Software Key Storage Provider.



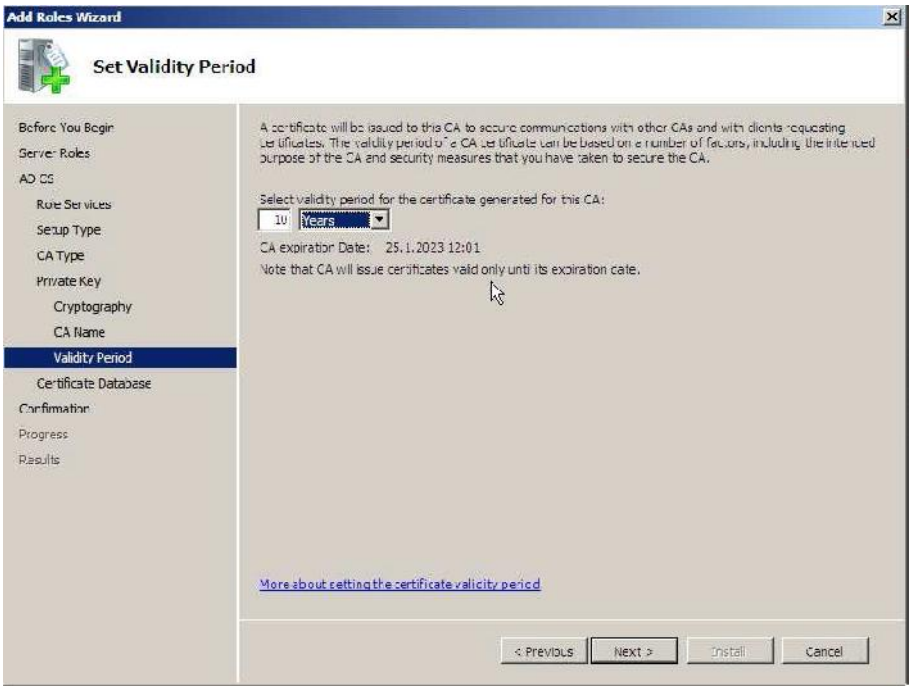
Kuva 11. Palvelin1:en salaustekniikat.

Seitsemännessä vaiheessa lisätään (Kuva 12) CA:lle nimi. CA:n nimen tulee olla kuvaava, jotta palvelimet erottaa toisistaan. Päätimme antaa CA:lle nimen AGCO-StandaloneRoot-CA. Active Directory eli käyttäjä-ja tietokonetietokanta antoi asentamallemme CA Enterpriselle automaattisesti nimeksi *DC=X, DC=X, DC=X, DC=X*. Tämä nimi on on aktiivihakemistonimeä vastaava LDAP-nimi.



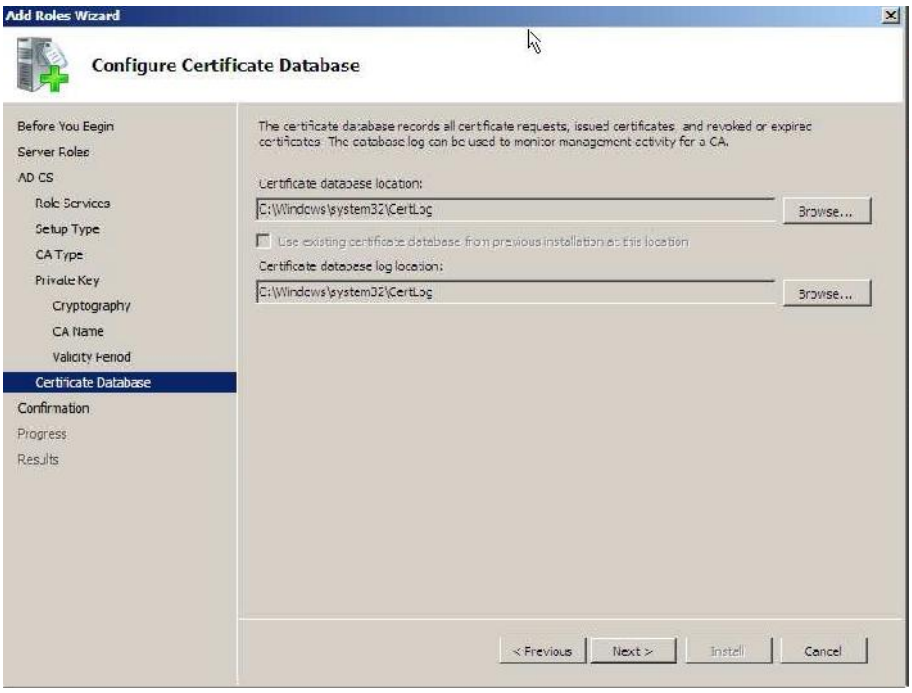
Kuva 12. Palvelin1:en CA:n nimen lisääminen

Kahdeksannessa vaiheessa (Kuva 13) asetettiin AGCO--Standalone-ROOT CA:n sertifikaatin voimassaoloaika. Yhteistyökumppani suositteli ajaksi kymmenen vuotta eli sertifikaatti vanhenisi vuonna 2023. Sertifikaatin uusiminen vuosittain ei tuo käytölle varsinaisia hyötyjä joten voimassaoloaikaa ei ollut tarvetta määrittää lyhyemmäksi.



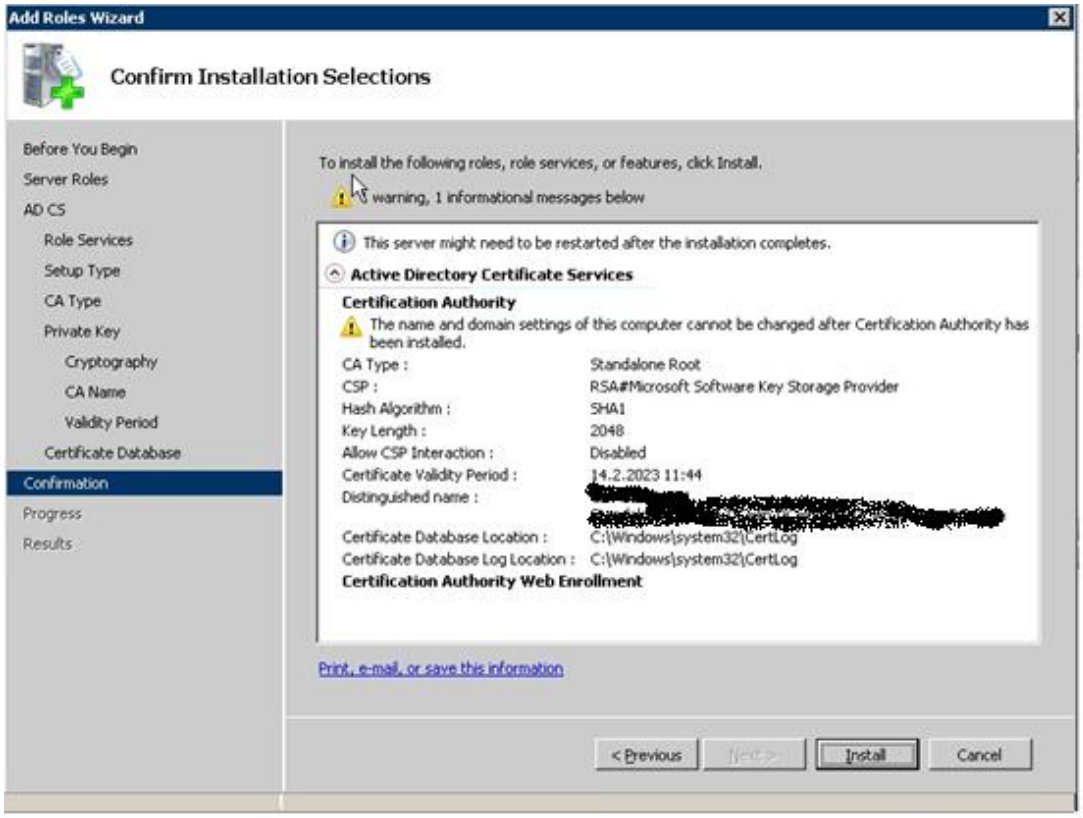
Kuva 13. Palvelin1:sen CA:n voimassaolojan asettaminen

Yhdeksännessä vaiheessa (Kuva 14) määritimme tietokannan sekä log-tiedoston tallennussijainnin. Tallennussijainnin tulee sijaita paikallisella levyllä. Päädyimme molemmissa oletussijaintiin, joka oli Certificate database location: C:\Windows\system32\Certlog.

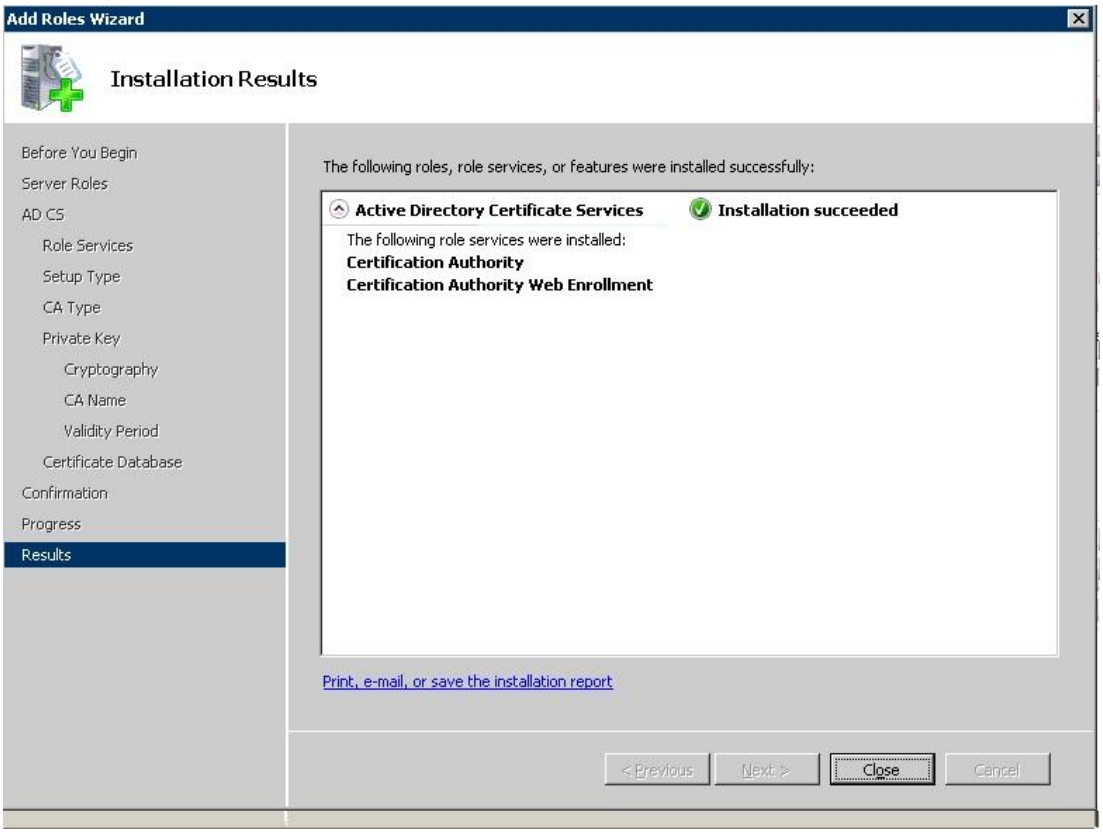


KUVA 14. Palvelin1:en tallennussijaintien määritys

Lopuksi (Kuva 15) tarkistimme määritetyt asetukset ja asensimme CA:n. Asennuksen valmistuttua saimme vahvistuksen, että asennus oli onnistunut (Kuva 16). Tämän jälkeen jatkoimme seuraavaan vaiheeseen eli myöntäjä-CA:n asennukseen.



Kuva 15. Palvelin2:en asetusten tarkastus ja hyväksyntä



Kuva 16. Palvelin1:en Standalone Root Ca onnistunut asennus

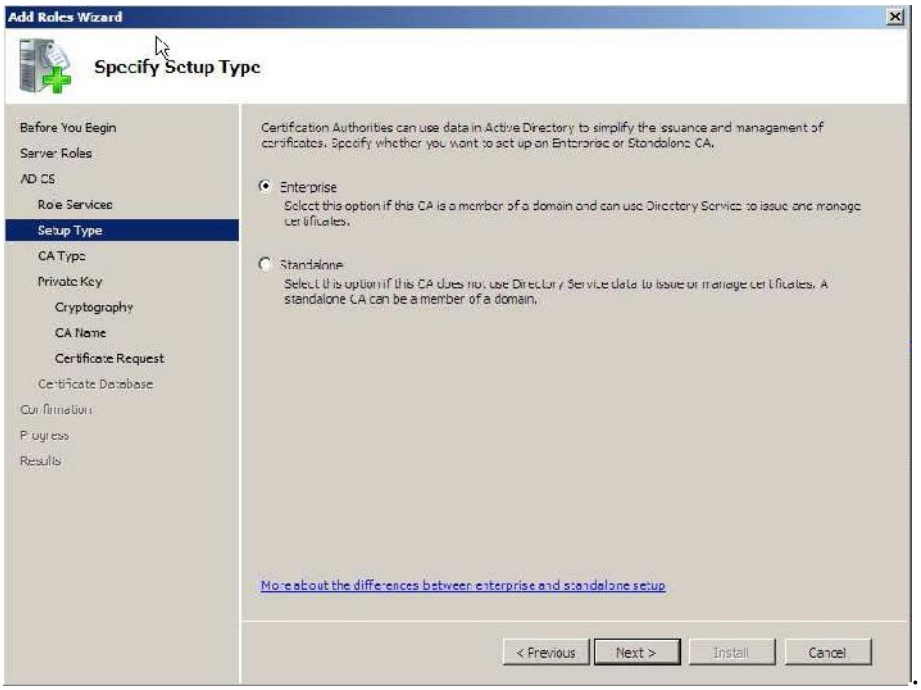
6.6.3 Enterprise Subordinate CA palvelimien asennus

Käytäntö-CA:n alapuolelle Palvelin2:lle perustimme myöntäjä-CA:n eli Enterprise Subordinate CA, joka jakaa sertifikaatit AGCO Powerin loppukäyttäjille. Myös Palvelin2:lle tuli asennuksen alkaessa kirjauduttua Enterprise Admin tunnuksilla. Enterprise Subordinate CA asennuksessa oli 9 asennusvaihetta, joiden jälkeen Enterprise Subordinate CA oli asennettu käyttövalmiiksi.

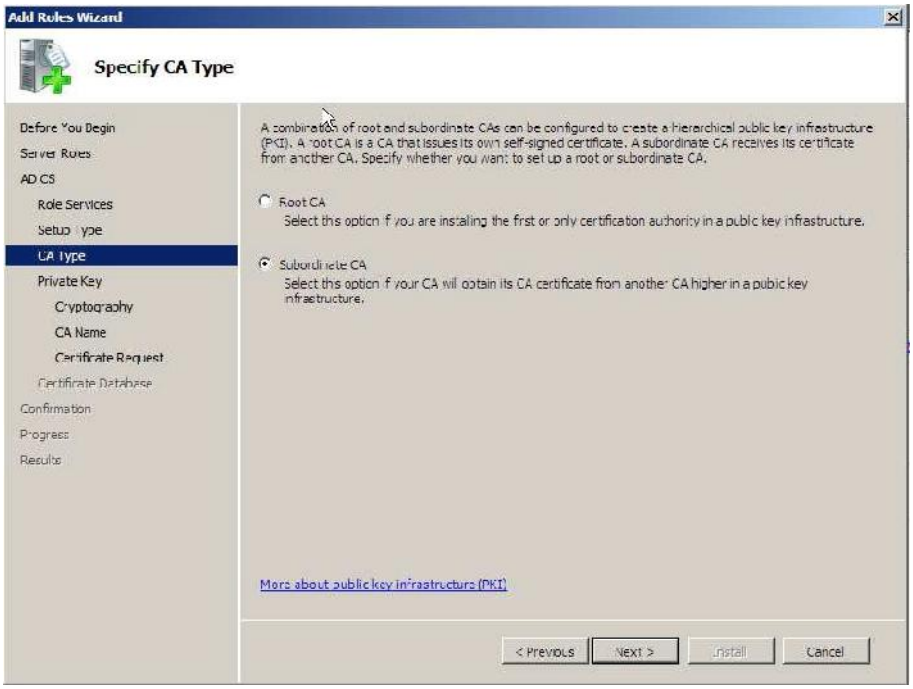
Ensimmäiset asennusvaiheet teimme saman kaavan mukaan kuin aikaisemmassa asennuksessa. Ensimmäiseksi lisäsimme Palvelin 2:lle roolin Active Directory Certificate Services. Tämän jälkeen lisäsimme Active Directory Certificate Services roolille roolipalveluita. Roolipalvelut olivat samat kuin aikaisemmassa eli Certification Authority Certification ja Authority Web Enrollment -palvelut.

Samoin kuin aikaisemmassa asennuksessa, seuraavaksi oli vuorossa CA-palvelintyypin valitseminen. Olimme päättäneet tehdä Palvelin2:sta loppukäyttäjille varmenteet myöntävän Enterprise Subordinate CA:n joten valitsemme kohdan Enter-

prise. Neljännessä vaiheessa (Kuva 17) valitsimme taas Certification Authority-tyypin. Tälle palvelimelle vuorostaan valitsimme Subordinate CA (Kuva 18).

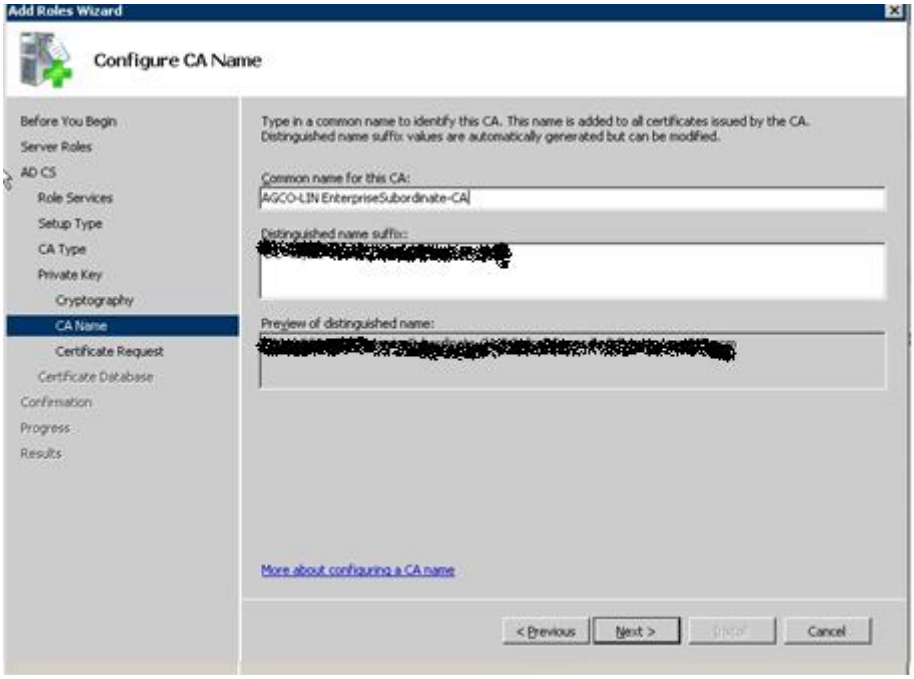


Kuva 17. Palvelin2 CA-palvelintyypin valinta



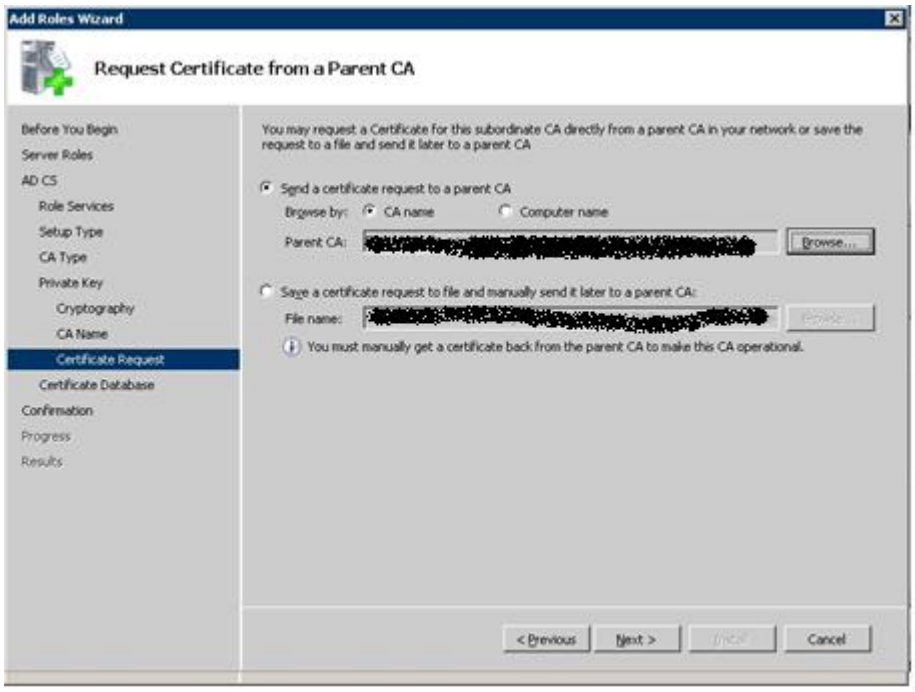
Kuva 18. Palvelin2 CA-tyypin valinta

Seuraavat vaiheet menivät taas kuten edellisessä asennuksessa, jossa loimme uuden private key:n ja määritimme käytettävät salaustekniikat. Tämän jälkeen tuli asennusvaihe (Kuva 19), jossa lisäsimme CA:lle nimen. Päätimme laittaa toiselle CA:lle nimen AGCO- EnterpriseSubordinate-CA, aikaisemman nimistandardin mukaan.



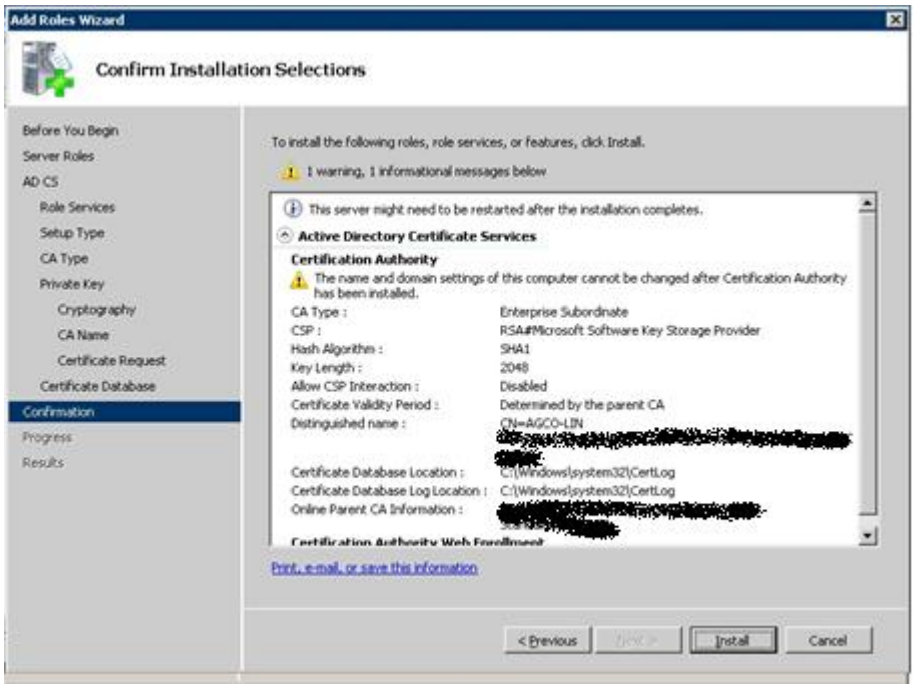
Kuva 19. Palvelin2 CA:n nimen lisääminen

Seuraavassa asennusvaiheessa (Kuva 20) generoimme CA-varmennepyynnön aikaisemmin asennetulle StandaloneRoot CA –palvelimelle, josta muodostui niin sanottu isäntäpalvelin. Aikaisemmin asennettu StandaloneRoot CA:n tuli olla verkossa, jotta sille pystyi generoimaan varmennepyynnön. Parent CA -kohtaan täytyi aluksi kirjoittaa palvelimen nimi, jossa StandaloneRoot CA sijaitsee. Tämän perään kirjoitettiin kauttaviivalla eroteltuna StandaloneRoot CA:n nimi. Tässä tapauksessa nimeksi muodostui Palvelin1.XXX.XXX.XXX\AGCO-StansaloneRoot-CA.

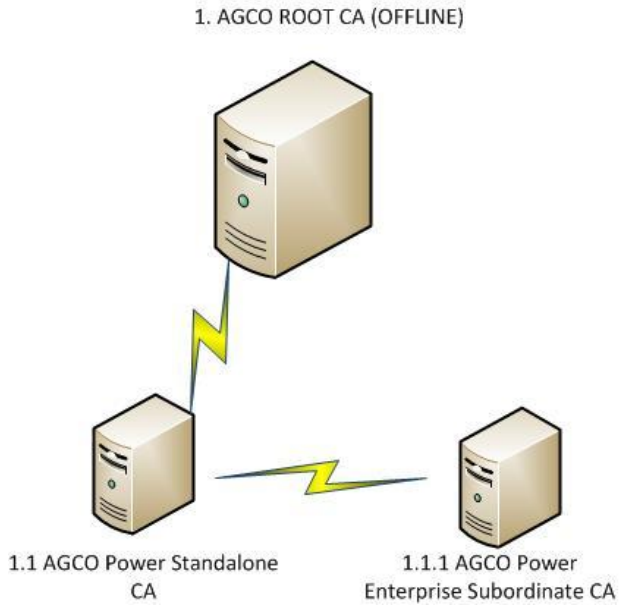


Kuva 20. Palvelin2:en varmennepyynnön generoiminen isäntä CA:lle

Asennuksen lopuksi (Kuva 21) määritimme tietokannan sekä log-tiedoston tallennussijainnin samalla tavalla ja samaan paikkaan kuin aikaisemmassakin asennuksessa. Tämän jälkeen tarkistimme vielä määritetyt asetukset ja vahvistimme CA:n asennuksen. Seuraavaksi palautimme mieleen mitä olimme asentaneet aiemmin projektin vastaavassa vaiheessa. Havainnointiin auttoi kuva, jonka piirsimme uudistuneesta PKI-rakenteesta (Kuva 22).



Kuva 21. Palvelin2:en CA asennuksen hyväksyntä

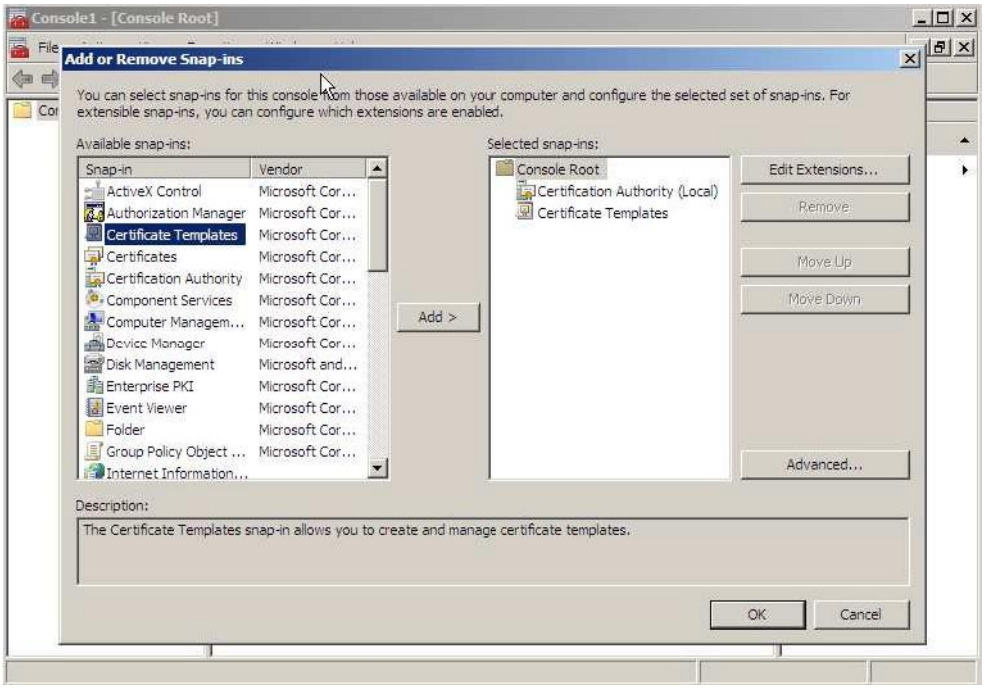


Kuva 22. AGCO Powerin päivitetty PKI-rakenne

6.6.4 Varmenteen julkaisu

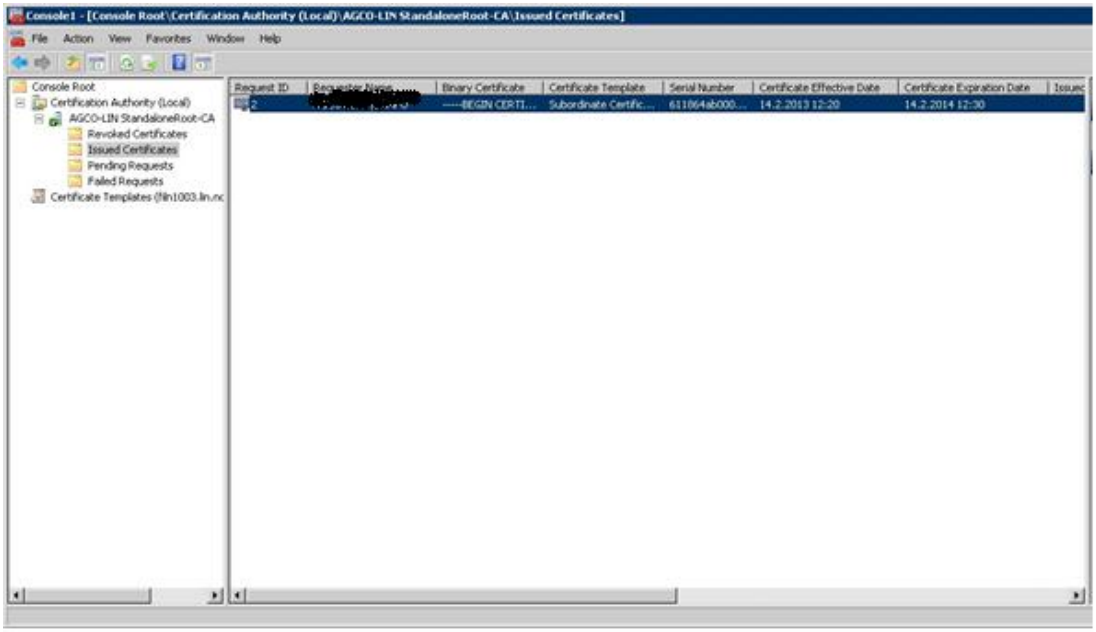
Enterprise Subordinate CA asennuksen jälkeen asennuksessa tuotettu varmennepyyntö toimitettiin Palvelin1 Standalone CA:lle. Kirjauduimme Palvelin1:een, josta löytyi työkalu nimeltä Certification Authority eli sertifikaatin myöntäjä, jonka sai auki kir-

joittamalla run-ikkunaan mmc-komennon. Työkalun auettaessa valitsimme File → Add/Remove Snap-In ja avoinna olevasta valikosta valitsimme Certificates Templates → Add. Tämän laajennuksen avulla voitiin luoda ja hallita templateja (Kuva 23).



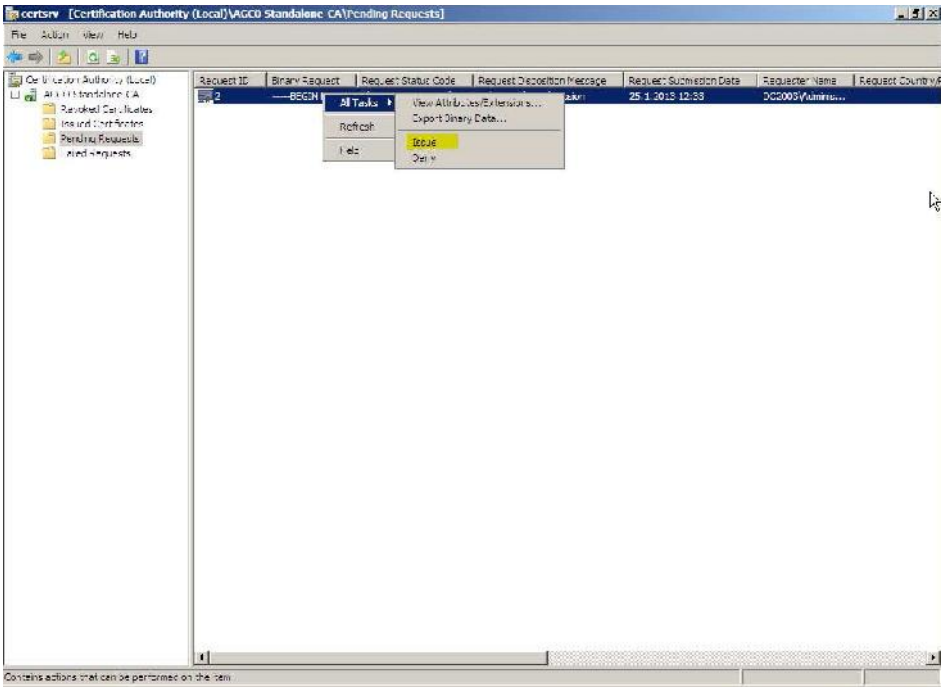
Kuva 23. Certificate templates lisäys

Tämän jälkeen (Kuva 24) Certification authority työkalu näytti yhden julkaistun varmenteen.Requested ID = 2, Requester name = XXX, sama enterprise administrator tunnus, jolla asensimme palvelimet. Varmenteessa näkyy myös voimassaolopäivä ja varmenteen vanhentumispäivämäärä.



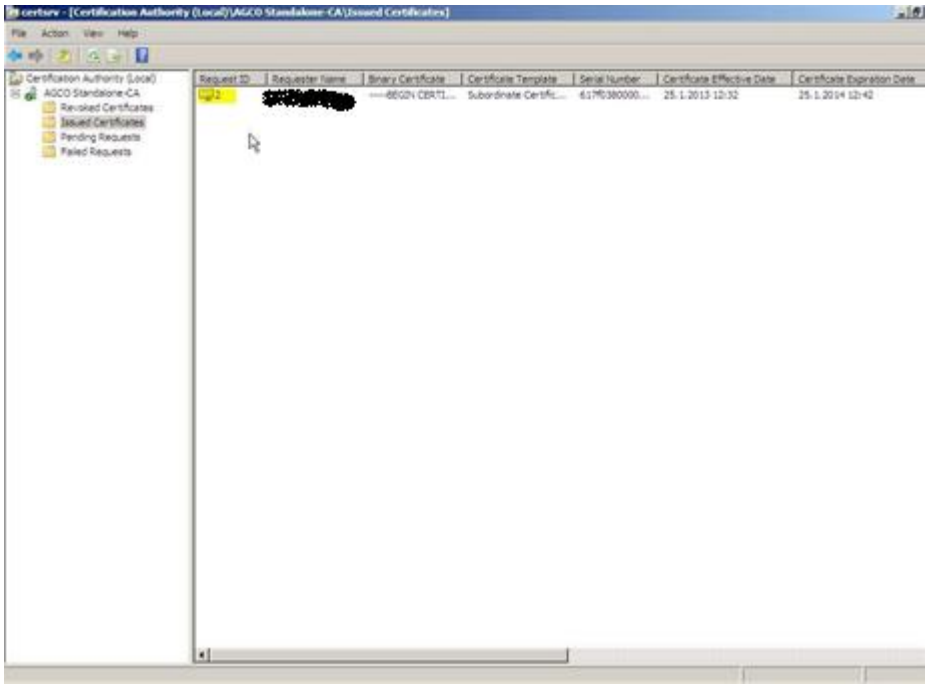
Kuva 24. Julkaistu varmenne

Tämän jälkeen (Kuva 25) katsoimme samasta työkalusta kohdan Pending request – säiliön kuvakkeen alle, jossa löytyi avoin pyyntö. Valitsimme valikosta kyseisen pyynnön myöntääksemme varmenteen. Valitsimme valikosta käskyn All task → Issue.



Kuva 25. Varmenteen myöntäminen Palvelin1:llä

Edellisen vaiheen jälkeen (Kuva 26) avasimme Issued Certificates –kuvakkeen ja näimme siellä myönnetyn varmenteen. Valitsemalla haluamansa varmenteen kuvakkeen ja sen avaamalla voi tarkistaa, että sen sisältämä informaatio on validia. Erityisesti voimassaoloaika on tärkeä tarkistaa. Requester name on XXXX joka tarkoittaa sitä, että käyttöönottoa tehtäessä pyytäjä on AGCO Powerin AD-palvelimen Administrator.

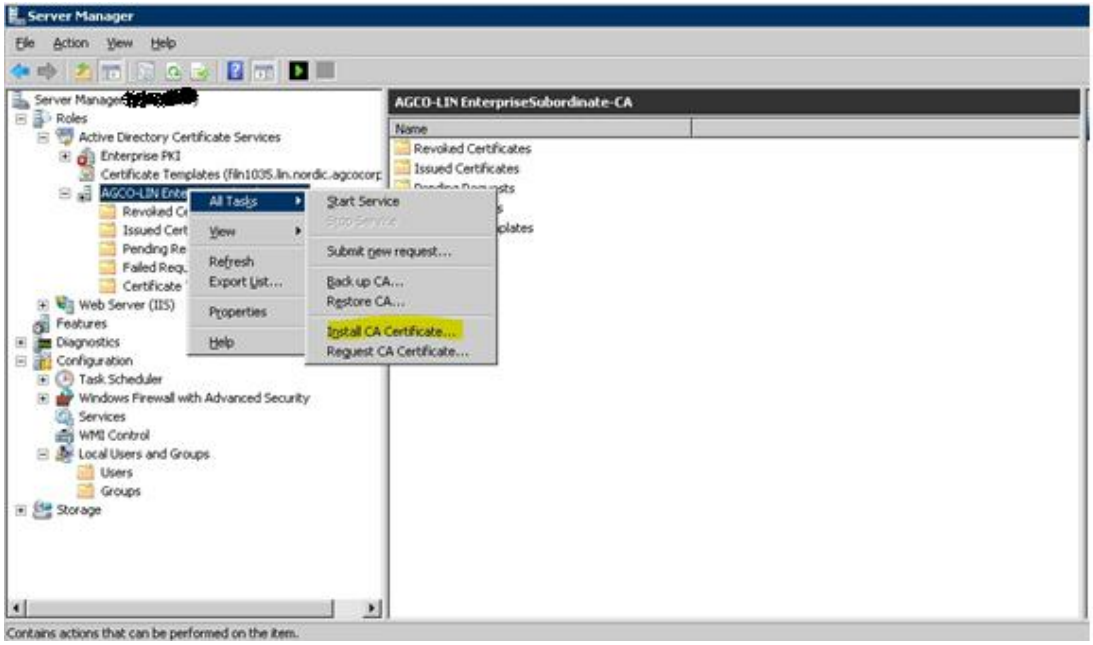


Kuva 26. Myönnetty varmenne

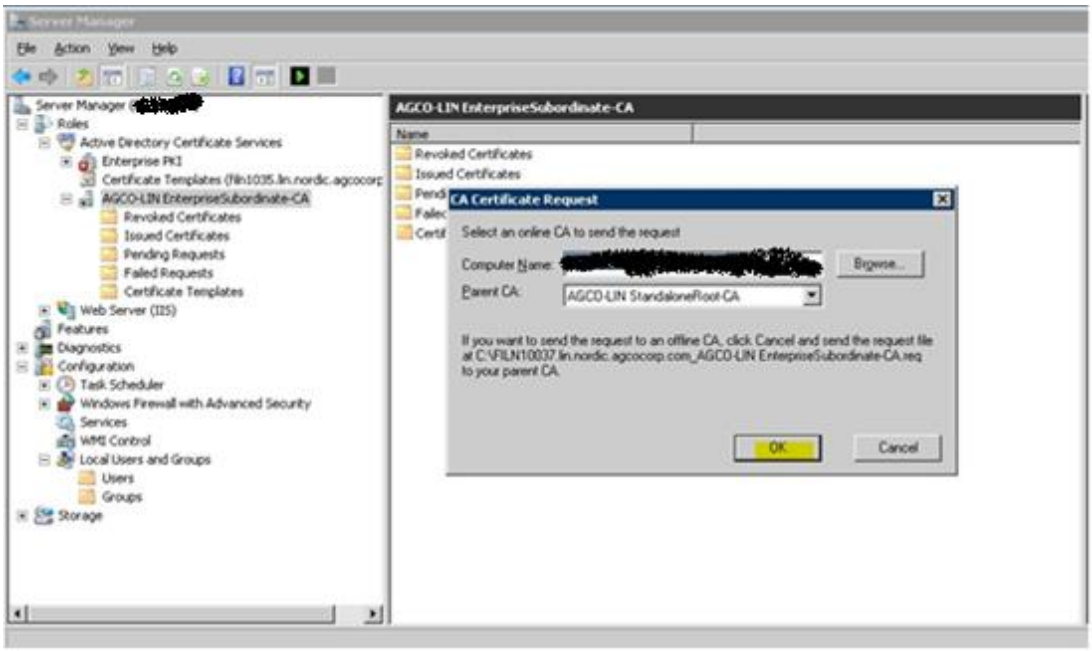
Seuraavassa vaiheessa vaihdoimme Palvelin1:en toiseen asennettuun Palvelin2:een sulkematta kuitenkaan Palvelin1:stä. Palvelin2:lta löytyi Server manager-työkalu ja Roles-valikon alta aukesi rooliksi määritetty Active Directory Certificates Services eli Windows – pohjainen varmennepalvelu. Sen avaamalla saimme esiin aiemmin asennetun AGCO- Enterprise Subordinate CA:n. Valitsemalla CA-palvelimen valikosta pystyimme asentamaan CA-varmenteen seuraavanlaisesti: All Tasks → Install CA Certificate (Kuva 27).

Tämän jälkeen avautui CA Certificate Request-ikkuna, jonka tarkoituksena on hakea automaattisesti yrityksen verkossa oleva StandaloneRoot CA–palvelimen eli aikaisemmin asennettuun AGCO- StandaloneRoot-CA:n. (Kuva 28) Mikäli palvelin ei olisi verkossa, täytyisi varmennepyyntö viedä palvelimelle esimerkiksi muistitikulla. Tämän toimenpiteen jälkeen pystyimme käynnistämään palvelun valitsemalla Start

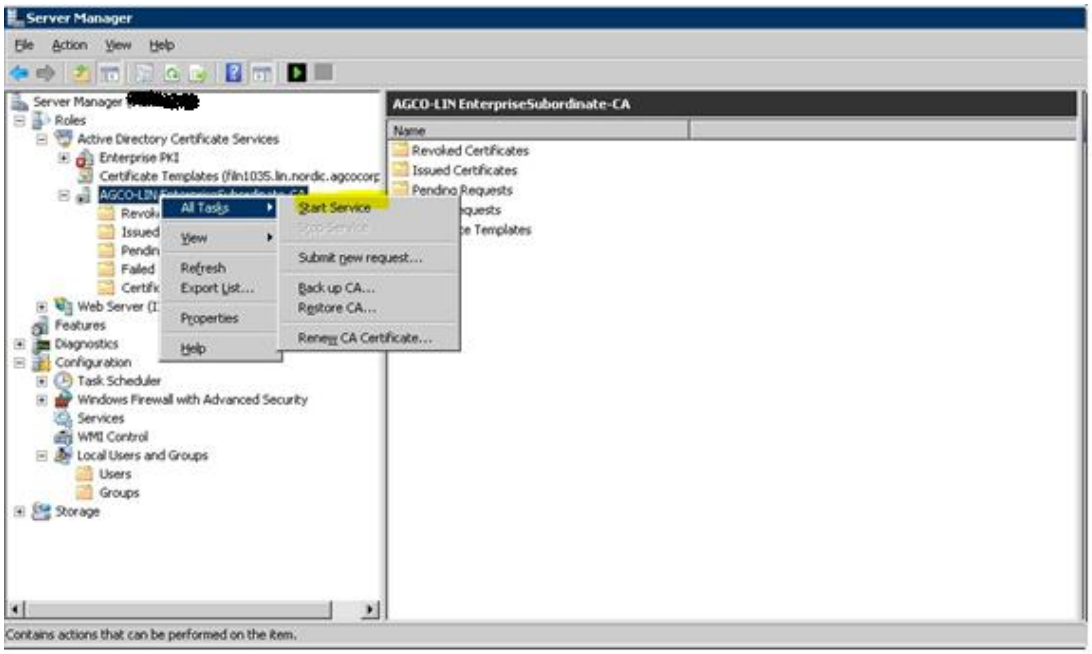
Service-käskyn (Kuva 29). Viimeisessä vaiheessa tarkistimme mmc-komennolla, että AGCO Enterprise subordinate-CA on päällä eli että palvelu antaa signaalin vihreällä valolla. Signaali merkitsee kommunikoinnin onnistuvan palvelimien välillä (Kuva 30).



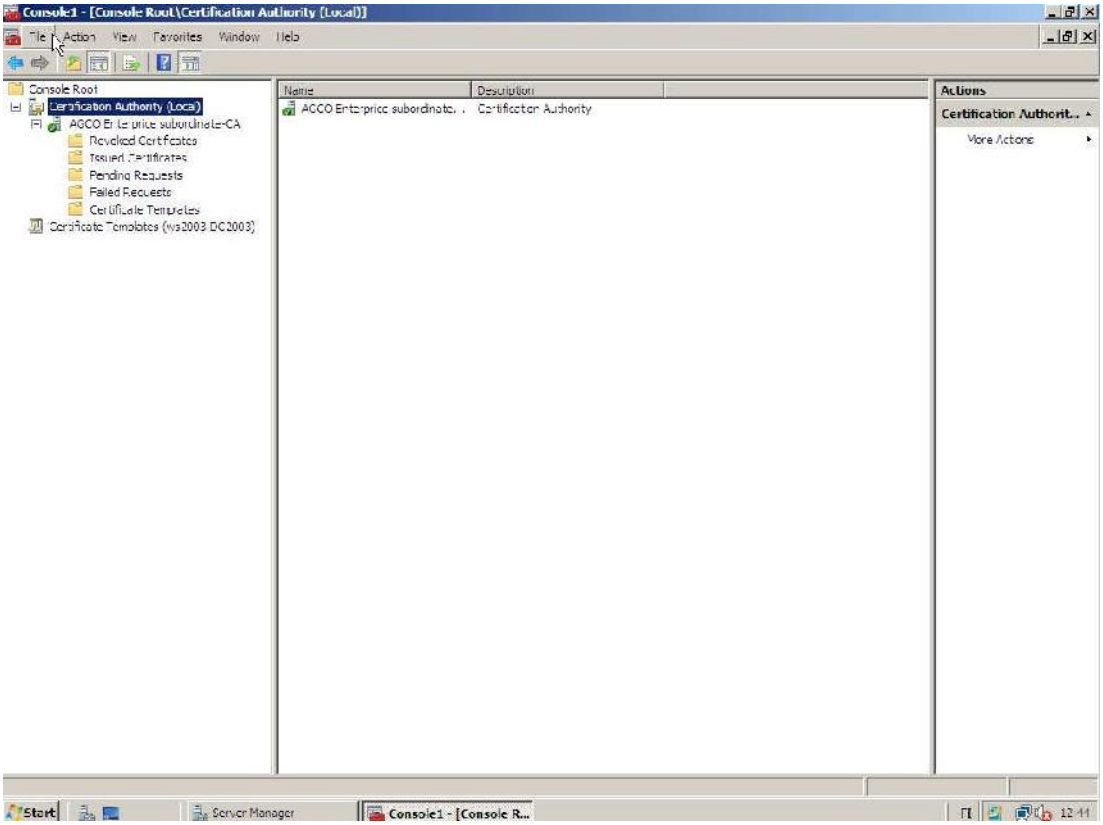
Kuva 27. CA varmenteen asennus Palvelin2:lla



Kuva 28. Varmennepyynnön lähettäminen



Kuva 29. AGCO- Enterprise Subordinate-CA käynnistäminen



Kuva 30. AGCO Enterprise subordinate-CA päällä

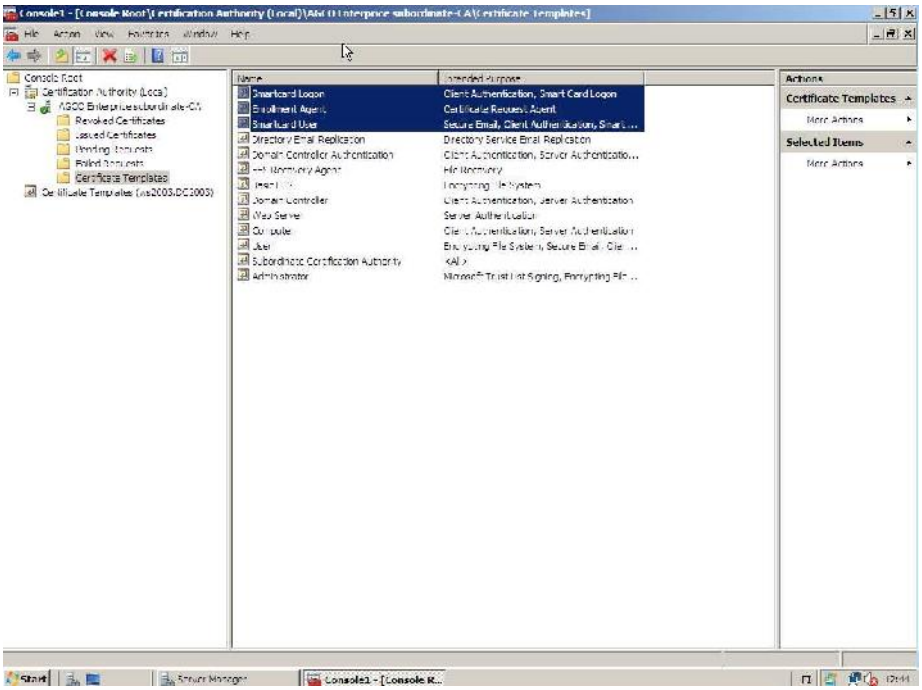
6.6.5 Microsoft varmennemallien konfigurointi

Ennen korttien varsinaista myöntämistä oli luotava varmennemallit varmenteille, joita myönnämme käyttäjille. Varmennemallien tehtävä on sujuvoittaa varmenteiden myöntämistä automaattisesti valmiiksi laaditun käytännön mukaisesti. Varmennemallit haettiin aikaisemmin käynnistetyn AGCO Enterprise subordinate-CA:n juurikansiosta, joka löytyi nimellä Certificate Template. Valitsimme kuvakkeen New → Certificate Template to Issue (Kuva 31). Seuraavaksi valikosta oli valittava seuraavat kolme varmennemallia:

Smartcard Logon – Varmennemalliin lisätään käyttäjät, jotka kirjautuvat koneelle verkon kautta toimivalla AD-tunnuksella, joka lisätään toimikorttiin.

Smartcard user – Tämä varmennemalli on samanlainen kuin Smartcard logon, mutta monipuolisempi käyttömahdollisuuksiltaan. Kyseistä mallia voidaan käyttää allekirjoituksiin ja sähköpostin salaukseen. AGCO Powerin käyttäjille on annettu oikeudet tähän ryhmään.

Enrollment Agent – Varmennemalliin lisätään käyttäjä, jolla on valtuudet luoda varmenteita toisten käyttäjien toimikorteille. Ryhmän jäsenien tulee lisätä varmenne omalle myöntökoneelle ennen kuin he voivat luoda varmenteita toimikorteille. AGCO Powerissa oikeudet on annettu osalle henkilöstöosaston työntekijöille, jotka luovat varmenteita toimikortteihin.

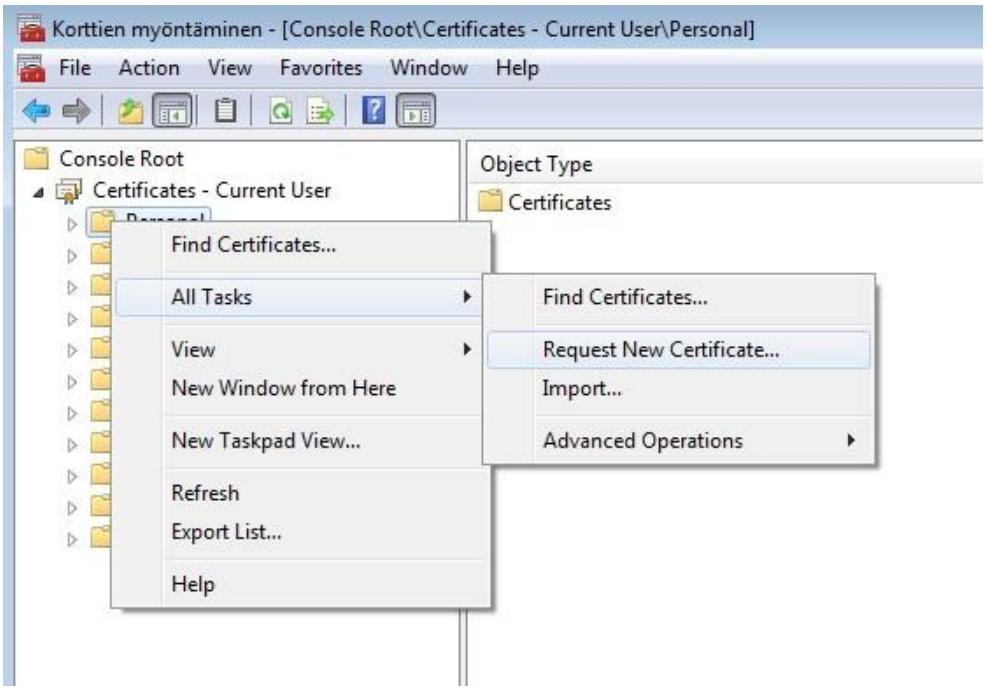


Kuva 31. Varmennemallien lisäys

6.6.6 Enrollment Agentin käyttöönotto ja toimikortin varmenteen jakaminen

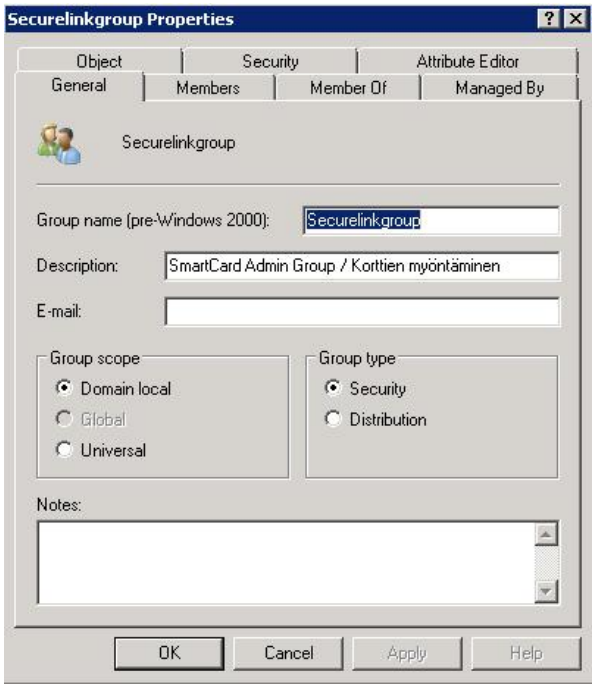
Proof of conceptin viimeiseen vaiheeseen sisältyi Windows Smart Card –palvelujen käyttöönotto ja toimikorttien myöntäminen Microsoft Management Consolen kautta (MMC). Olimme sopineet puhelimitse, että asennan valmiiksi myöntökoneen ACGO Powerin henkilöstöosastolle toimikorttien varmenteiden lataamista varten. Tällä samaisella koneella voisimme toteuttaa Proof of conceptin toimikorttien varmenteiden myöntämisharjoituksen. Teimme toteutusharjoituksen omalla Active Directory-tunnuksellani *alvinto*.

Myöntökoneella aukaistiin ensimmäisellä kerralla Microsoft management console, jossa luotiin certificates-työkalu. Saadaksemme uuden varmennepyynnön tehtyä (Kuva 33) täytyi meidän avata Certificates – Current user-kuvake, jonka alta löytyi Personel-kansio. Avasimme kansion ja valitsimme listasta toiminnon All Tasks → Request New certificate.

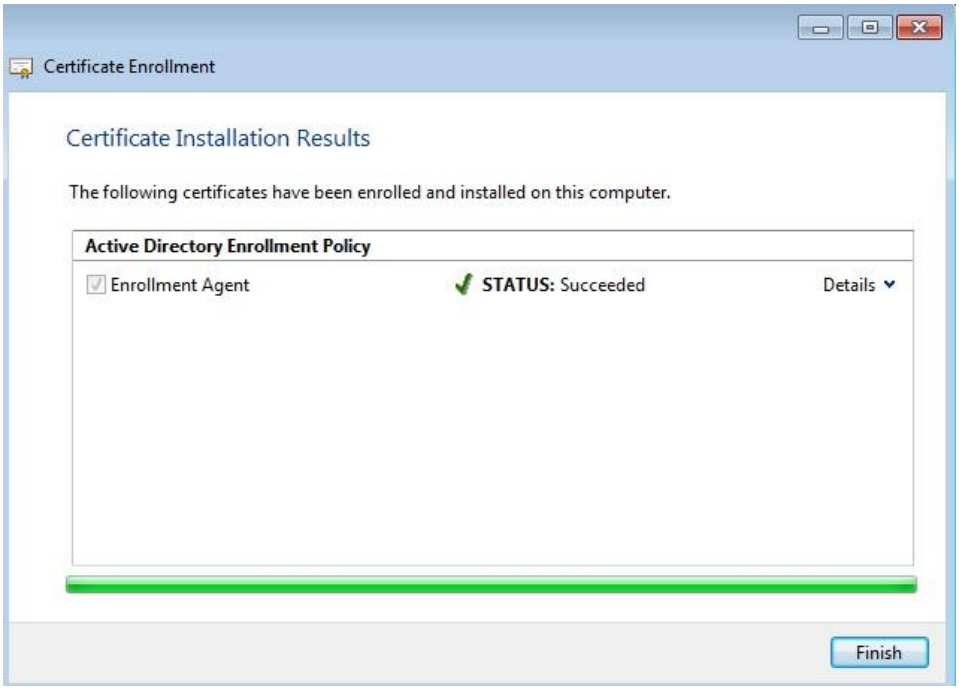


Kuva 33. Uuden varmenteen pyyntö

Seuraavaksi tuli valita Enrollement Agent. Tämän varmenteen avulla oikeutettu käyttäjä voi ladata toimikortteihin myös muiden käyttäjien ad-tunnuksia. Teimme (Kuva 34) Active directoryyn ryhmän nimeltä Securelinkgroup, joka oli SmartCard Admin Group-ryhmä. Tämän ryhmän käyttäjillä oli oikeus Enroll Agent-varmenteen lataamiseen. Next –kuvakkeen valitsemalla asensimme Enrollment Agent-varmenteen myöntökoneelle (Kuva 35). Tulimme siihen tulokseen, että Certificates-työkalun luominen henkilöosaston työntekijöille voi olla haastavaa. Tästä syystä sovimme, että teemme toteutuksen jälkeen yhden myöntötunnuksen *SD* ja yksinkertaiset ohjeet tuleville myöntäjille.



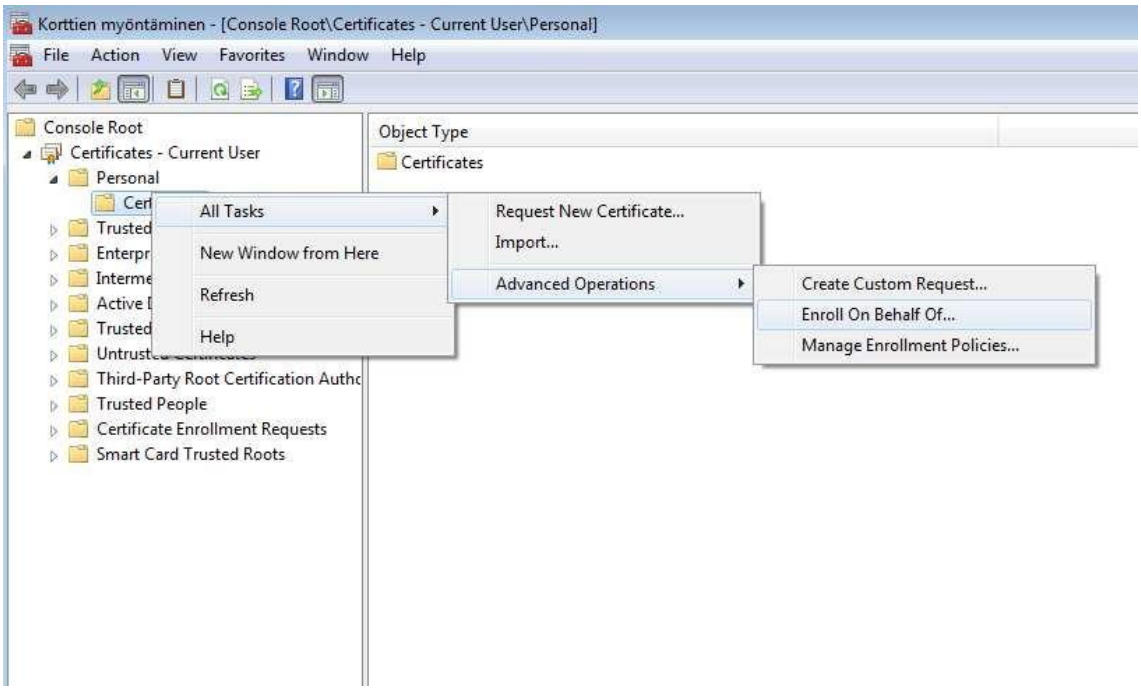
Kuva 34. Secure Admin Group



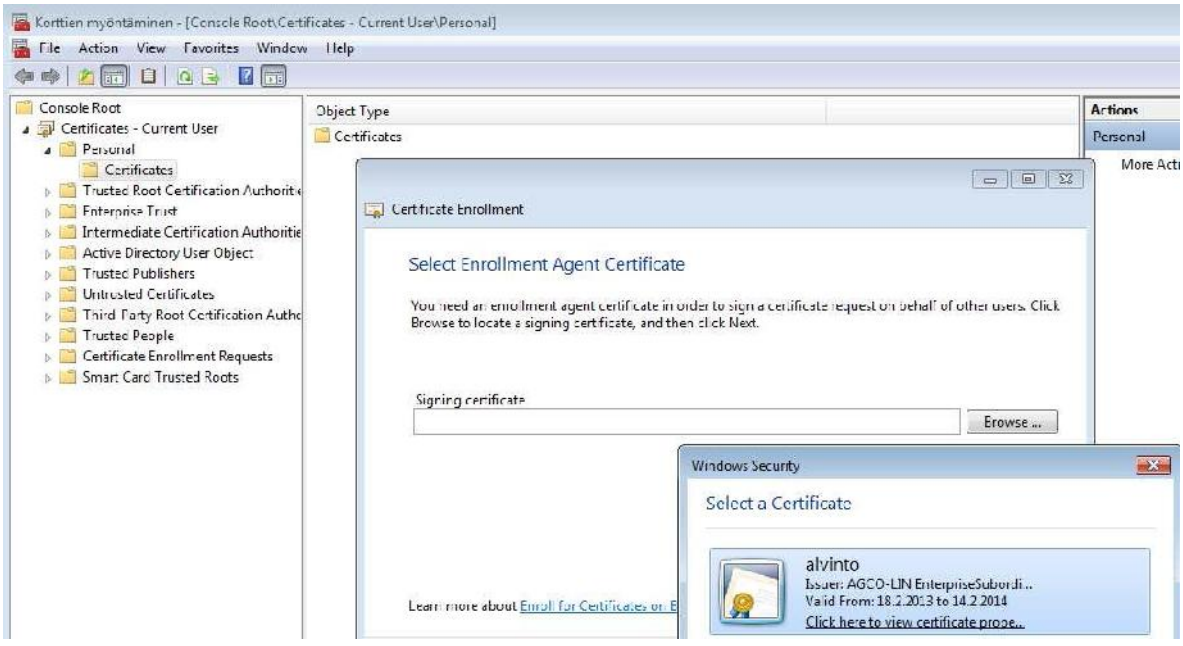
Kuva 35. Enrollment agent –varmenne asennettu

Seuraavaksi (Kuva 36) olimme valmiita testaamaan varmenteen lisäämistä toimikorttiin. Taas avasimme kohdan Certificates – Current User ja hiiren oikealla kohtaa painoimme Personel, jonka jälkeen valitsimme All Tasks. Valikosta valitsimme nyt Ad-

vanced Operations → Enroll On Behalf Of.. –kohdan. Seuraavassa vaiheessa (Kuva 37) haimme äsken myöntökoneelle luodun Enrollment Agent-varmenteen.



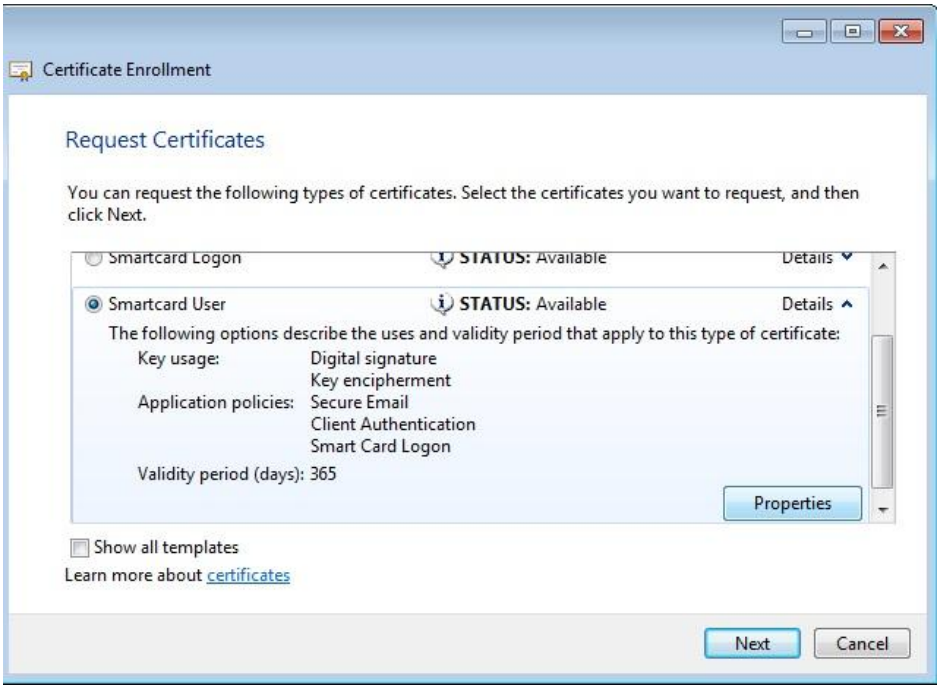
Kuva 36. Enroll Agent varmenne



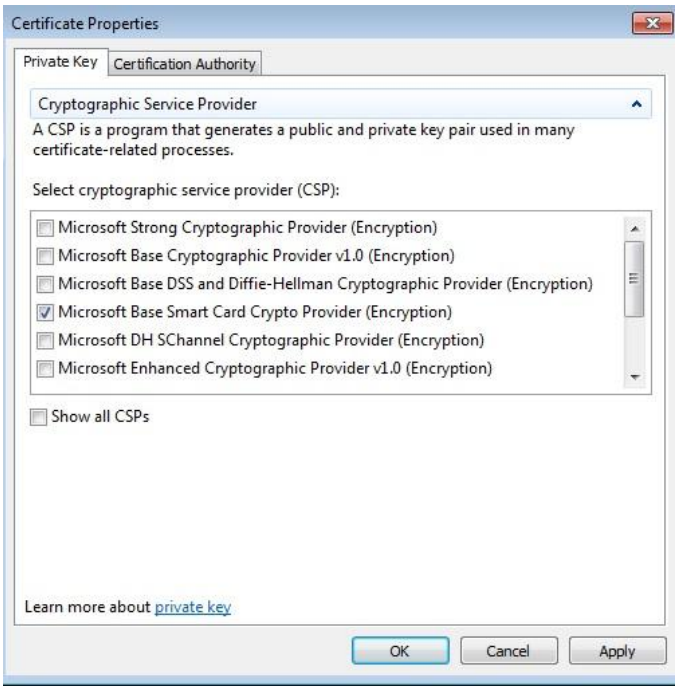
Kuva 37. Enrollment Agent varmenteen lisäys

Request Certificates-kohdassa (Kuva 38) tuli valita aikaisemmin luoduista varmennemalleista monipuolisempi Smartcard user – varmennemalli. Tämän jälkeen valit-

simme properties-kuvakkeen jotta pääsimme valitsemaan haluamamme CSP:n eli Crystographics Service provide–ohjelmiston. Valintana oli Microsoft Base Smart Card Crypto Provider (Kuva 39). CSP:n tehtävänä on tarjota koneen käyttöjärjestelmälle rajapinta toimikorttiin, sekä luoda yksityinen ja julkinen avain kun käyttöjärjestelmä on ensin lähettänyt kyselyn CSP:lle kortin varmenteen myöntövaiheessa. CSP luo avainparin käyttäjän myöntökoneeseen ja tämän jälkeen julkinen avain lähetetään CA:lle muun tiedon mukana. CSP salaa yksityisen avaimen käyttäjän toimikorttiin ja jos CA hyväksyy haun, se luo ja allekirjoittaa varmenteen.

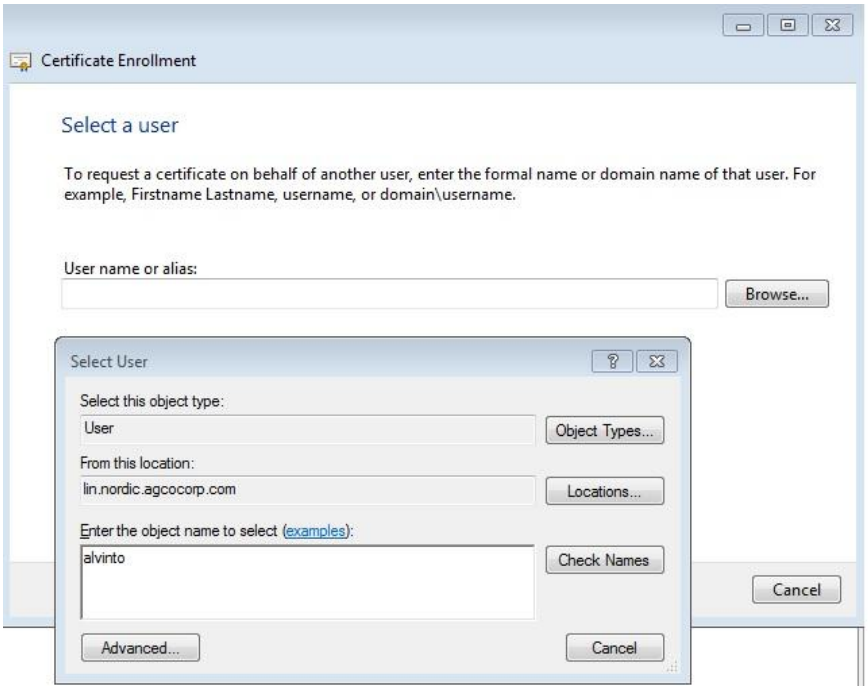


Kuva 38. Smartcard user varmenneallin valinta



Kuva 39. Microsoft Base Smart Card Crypto Provider -valinta

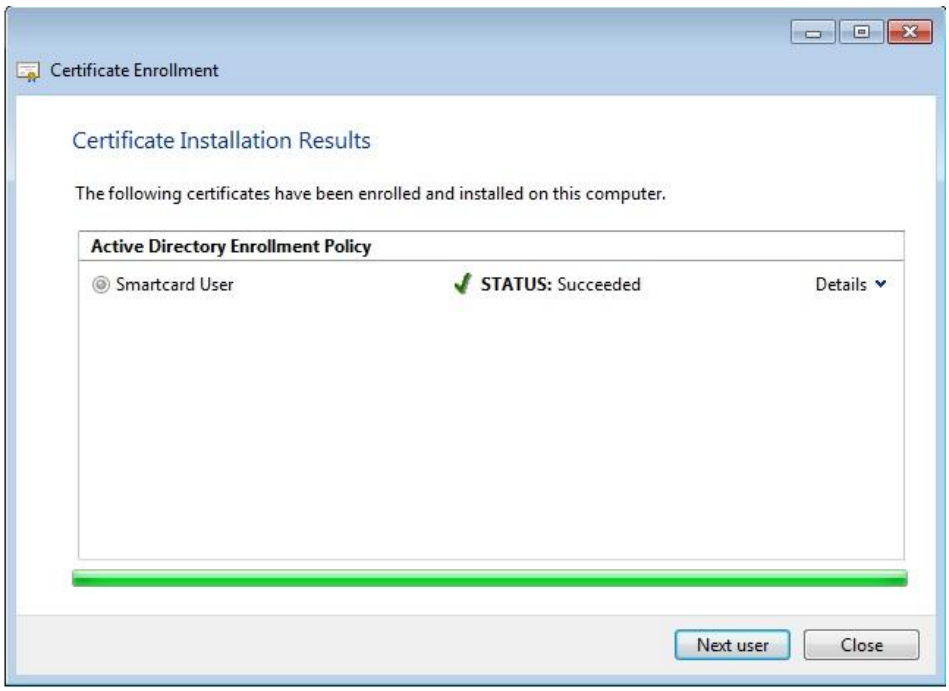
Seuraavassa vaiheessa (Kuva 40) haettiin toimikortille käyttäjä AGCO Powerin domainista lin.nordic.agcocorp.com. Tarkoituksena oli tehdä minulle testikortti, joten haimme käyttäjätunnuksen alvinto. Tämän jälkeen tapahtui itse myöntäminen painamalla Enroll-kuvaketta.



Kuva 40. Käyttäjän haku yrityksen Active directorysta

Tämän jälkeen (Kuva 41) kone pyysi laittamaan toimikortin lukijaan ja syöttämään PIN-koodin. Näissä toimikorteissa oletus PIN-koodi oli kahdeksan nollaa. Lopuksi Certificate Enrollment kertoo tuloksen, että varmenne on lisätty onnistuneesti korttiin (Kuva 42).

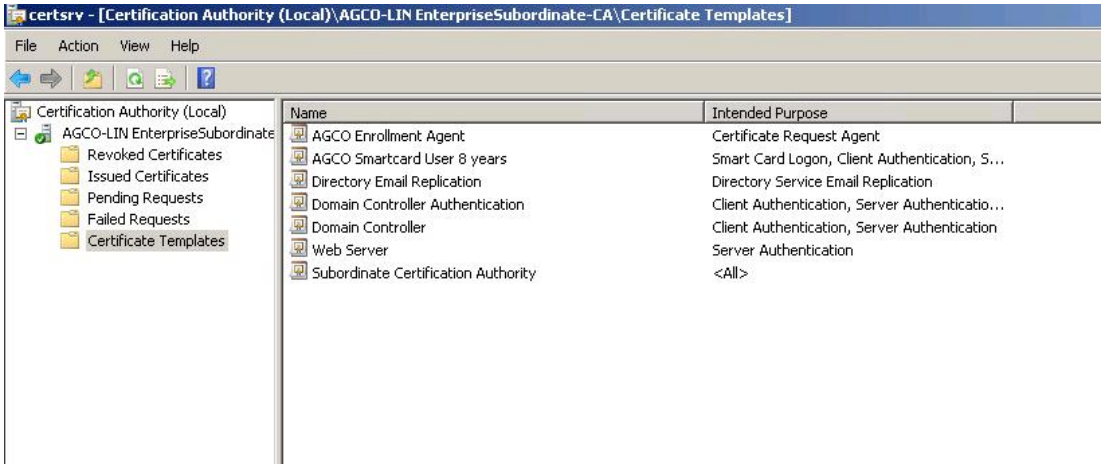
Kuva 41. PIN-koodin syöttö



Kuva 42. Myöntö on onnistunut

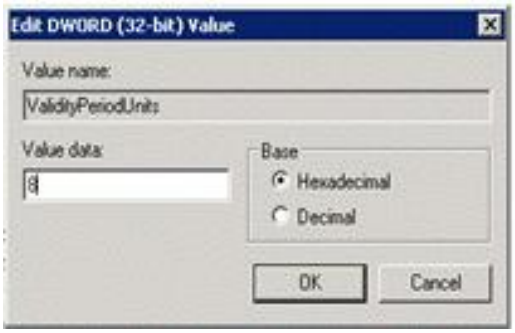
6.6.7 Toimikortin varmenteen voimassaoloajan muokkaaminen

Windowsin suositeltu voimassaoloaika myönnetylle varmenteelle on vain yksi vuosi. Tarkoituksena oli kuitenkin uusia varmenteet suositusaikaa harvemmin, joten muutimme voimassaoloajan kahdeksaksi vuodeksi. Teimme Palvelin2 Standalone CA palvelimelle uuden Smartcard user – varmennemallin, jonka nimesimme AGCO Smartcard user 8year (Kuva 43).



Kuva 43. AGCO Smartard User 8 years -varmennemalli

Palvelimiin Palvelin1:lle ja Palvelin2:lle oli myös tehtävä seuraava rekisterimuutos saadaksemme varmenteen iäksi kahdeksan vuotta yhden sijaan:
Rekisterieditori:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CertSvc\Configuration\< AGCO Enterprise Subordinate CA >
Arvo“ValidityPeriodUnits” muutettiin oletuksesta arvo: “1” arvoon “8” molemmissa palvelimissa (Kuva 44). Muutoksen jälkeen käynnistettiin uudelleen palvelu “certsvc” kummallakin palvelimella. Tämän toimenpiteen jälkeen toivottu kahdeksan vuoden ikä tuli voimaan uusiin AGCO Smartcard user 8year-varmennemallilla varmennettuihin kortteihin.



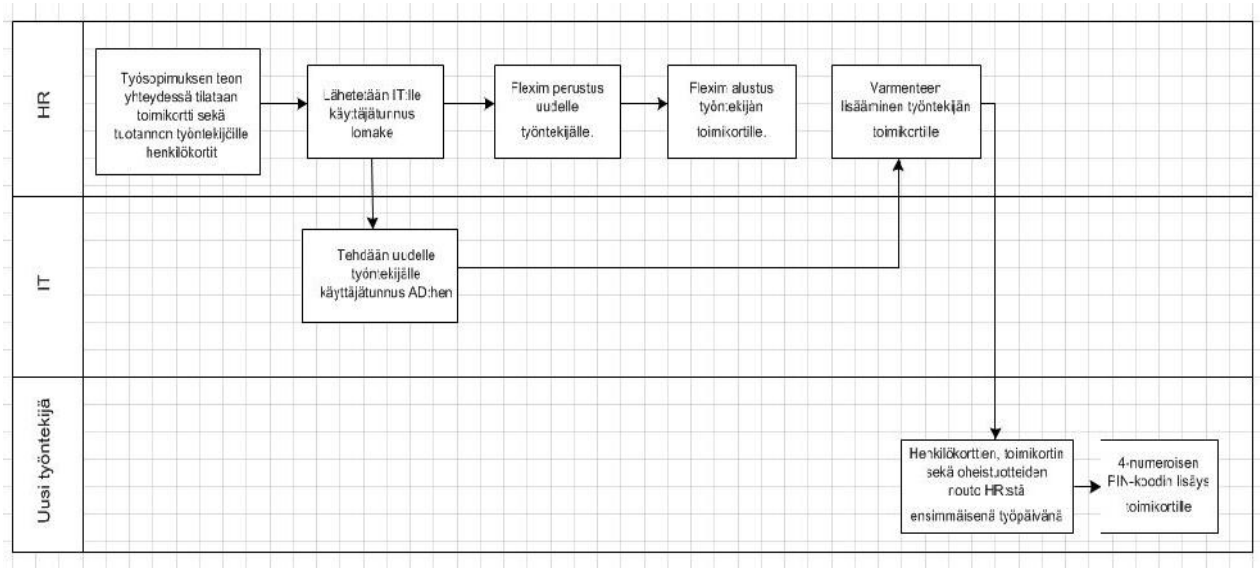
Kuva 44. Rekisterimuutos

6.7 Proof of concept-yhteenveto

Proof of concept-vaiheen lopputulos oli se, että palvelun tarjoaja vakuutti meidät heidän toimikorttiratkaisunsa sopivuudesta määrittelemiimme kriteereihin. Pystyimme myöntämään ja hallinnoimaan toimikortteja. Tämän lisäksi toimikorteilla pystyi kirjautumaan windows-tietokoneisiin sisälle ja toimikorteilla onnistui leimaaminen kulunvalvonnassa. Proof of concept oli hyväksytty ja päätimme tilata tuotteen kyseiseltä tarjoajalta.

6.8 Ohjeistus ja prosessikaavion tekeminen

Tuotteen tilaamisen ja teknisesti toimivaksi toteamisen jälkeen oli aika opastaa ja käydä läpi AGCO Powerin henkilöstöosaston kanssa henkilökortin käyttöönottoprosessi. Aluksi suunnittelimme yhdessä projektissa mukana olevan tiimin kanssa prosessikaavion(Kuva 45) ,jonka mukaan toimimme uuden henkilön tullessa taloon. Sovimme IT-osaston työntekijän tekevän uudelle henkilölle Active Directory-tunnuksen ja HR:n tehtävänä olisi varmentaa kortti uuden prosessikaavion mukaisesti tällä tunnuksella. HR myös asettaa toimikortin RFID-siruun flexim-korttikoodin siihen tarkoitetun RFID-lukijan ja flexim sovelluksen avulla.



Kuva 45. Uusi työntekijä –prosessikaavio

6.9 Projektin arviointi ja yhteenveto

Ennen varsinaisen projektin aloitusta perehdyin tutkimusongelmaan, joka muodostettiin kahdesta seuraavasta jo aiemmin esitellystä kysymyksestä: Mitä etuja on vahvan tunnistautumisen käytössä kevyen tunnistautumisen sijaan? Onko AGCO Powerilla tarvetta vaihtaa tunnistautuminen kevyestä vahvaksi? Tutkimuskysymysten asettamisen tavoitteena oli saada selville projektin mahdollinen kannattavuus. Aiheeseen liittyvään informaatioon perehtymisen myötä totesin yhdessä esimieheni kanssa vahvan tunnistautumisen olevan AGCO Powerille erittäin tarpeellinen tunnistusmenetelmä tietoturvan kannalta. Tähän vastaukseen päädyttyämme pystyin aloittamaan varsinaisen projektin eli toimikorttien suunnitteluun ja käyttöönottoon liittyvien tehtävien johtamisen. Projektin edettyä tiedonhankinnasta, suunnittelusta ja testauksesta lopulliseen käyttöönottoon pääsin toteamaan projektin olleen erittäin onnistunut. Varsinaista palautetta toimikorttien toimivuudesta ja käytettävyydestä ei järjestelmällisesti kerätty, mutta saatu palaute oli ja on ollut pääsääntöisesti positiivista ja toimikorttien käyttö on ollut sujuvaa. Vielä kolme vuotta projektin jälkeen AGCO Powerin henkilöstö käyttää suunnittelemiani tunnistautumiseen tarkoitettuja toimikortteja kulunvalvonnassa ja tuotannon tietokoneille kirjautuessa. Nykyään toimikortteja on otettu käyttöön projektin alussa suunniteltua laajempaan käyttöön esimerkiksi yrityksen sisäisissä maksutapahtumissa.

7 OMA POHDINTA OPINNÄYTETYÖSTÄ

Tämä oli ensimmäinen projekti, jonka johdossa toimin läpi prosessin. Päällimmäisenä jäi mieleen projektista hyvä maku. Mielestäni onnistuin itselleni asettamistani ja henkilökortin käyttöönottoon liittyvistä AGCO Powerilta saaduissa tavoitteisiin pääsyssä hyvin. Pysyin projektin tilaajan kanssa lähes sovitussa aikataulussa ja yritys sai tavoitteen sekä kriteereiden mukaisen tuotteen budjetoidulla summalla. Oli kiinnostavaa kokea projektinvetäjänä toimimista sekä tutustua projektiin liittyviin yllättävän moninaisiin vaiheisiin. Samalla sain tärkeää kokemusta paineen alaisena työskentelystä AGCO Powerin tietoturvallisuuden parantamisesta päävastuussa olevana henkilönä. Paineensietokykyni osoittautui yllättävän hyväksi ja asian havaitseminen oli minulle uusi oppimisen kokemus itsestäni työntekijänä. Haastavaa projektissa oli työn määrä sillä projektin ollessa myös samalla opinnäytetyöni oli luonnollista ettei tehtäviä voinut delegoida juurikaan muille ja vastuu projektin toteuttamisesta, onnistumisesta ja siihen liittyvien töiden tekemisestä kuului minulle. Oma haasteensa olivat myös tilanteet, joissa omat vaikuttamisen mahdollisuudet olivat vähäiset, mutta muiden tahojen merkitys projektin onnistumiseen oli kuitenkin merkittävä. Kaiken kaikkiaan kokemus oli haasteista huolimatta ja ehkä osittain niiden vuoksi antoisa ja uskon, että vastaisuudessa tartun samankaltaisiin työtehtäviin mielenkiinnolla ja uudella osaamisella.

8 LÄHTEET

Rinne, T. 2002. Älykortit, tekniikka, sovellusalueet ja käyttöönotto. Jyväskylä: Talentum

Lerssi-Lahdenvesi, A. 2006. Sirukortti seminaariesitys. Lappeenranta

Simula, T. 2012.Vahva vs. heikko tunnistautuminen Valorin tietoturvaseminaari

Valtiovarainministeriön hallinnon kehittämisosasto. 2012. VAHTI 3/2012 - Teknisen ICT-ympäristön tietoturvaohje. Helsinki.