TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikka, ohjelmistotekniikka
Kimmo Nevalainen

Tutkintotyö

Vahvennettu kirjautuminen Microsoft Windows -toimialueeseen

Työn ohjaaja lehtori Erkki Hietalahti
Työn teettäjä Instasec Oy, valvojana Ville Kuumola
Tampere 2005

Tekijä: Kimmo Nevalainen
Työn nimi: Vahvennettu kirjautuminen Microsoft Windows -toimialueeseen
Päivämäärä: 3.5.2005
Sivumäärä: 22 sivua
Hakusanat: toimikortti, toimialue, kirjautuminen
Koulutusohjelma: Tietotekniikka
Suuntautumisvaihtoehto: Ohjelmistotekniikka

Työn ohjaaja: lehtori Erkki Hietalahti
Työn teettäjä: Instasec Oy, valvojana Ville Kuumola

Nykyisin tietokoneille kirjaudutaan useasti päivässä eri yhteyksissä, myös muiden läsnä ollessa. Kirjautumien voidaan tehdä monilla eri tavoilla. Perinteinen tapa on kirjautua käyttäjätunnuksella ja salasanalla, mutta parempaa tietoturvaa vaativille on olemassa vahvennettuja kirjautumisvaihtoehtoja. Vahvennetussa käyttäjän tunnistamisessa käytetään perinteisen menetelmän sijaan toimikorttia, varmennetta ja pin-koodia. Toimikortti on älysirun sisältävä muovikortti. Sen älysiru sisältää muistia, jonne voidaan tallentaa esimerkiksi varmenteita. Varmenne taas on sähköisesti allekirjoitettu dokumentti. Se koostuu niin julkisesta ja salaisesta avaimesta sekä omistajansa tiedoista. Pin-koodilla suojataan varmennetta toimikortilla ja mahdollistetaan toimikortin käyttö.

Vahvennettuun käyttäjän tunnistamiseen tarvitaan perinteisestä kirjautumisesta poikkeavia ohjelmistoja, kuten Certifier-, Token Master, LDAP- ja CSP -ohjelmistoja. Certifier- ja Token Master -ohjelmistot liittyvät vahvennettuun käyttäjän tunnistamiseen siten, että niillä luodaan tarvittavat varmenteet, toimikortit ja sulkulista. LDAP-ohjelmistoa käytetään sulkulistan julkaisemiseen. CSP-ohjelmistoa taas tarvitsee se käyttäjän työasema, jolla halutaan kirjautua vahvennettua käyttäjän tunnistamista käyttäen. Myös perinteiseen kirjautumiseen käytettäviä ohjelmistoja pitää konfiguroida vahvennetun käyttäjän tunnistamisen käyttöönoton yhteydessä. Toimialueohjain, johon kirjaudutaan, pitää konfiguroida hyväksymään varmennepohjainen kirjautuminen toimikortilla.

Työn kirjallisessa osuudessa esitellään ensin työn toteutuksessa käytetyt uudet ohjelmat ja käsitteet tarkasti. Sen jälkeen kaikki työvaiheet, eli vahvennettuun käyttäjän tunnistamiseen tarvittavien palvelimien ja ohjelmien asennukset ja konfiguroinnit käydään läpi yksityiskohtaisesti. Työn lopputuloksena on itsenäisesti asennettu ja konfiguroitu järjestelmä, jolla voidaan tehdä vahvennettu kirjautuminen Microsoft Windows -toimialueeseen.

Author: Kimmo Nevalainen
Work title: Strong network authentication to Microsoft Windows domain
Date: 3.5.2005
No of pages: 22 pages
Keywords: Smartcard, Domain Logon, Certifier
Programme: Computer systems engineering
Orientation option: Software engineering

Work Supervisor: Lecturer Erkki Hietalahti
Commissioning Company: Instasec Oy, Supervisor Ville Kuumola

Nowadays it is very common, that you log in to computers several times a day in different situations, also in the presence of others. There are many different ways to log in. The most common and traditional way to do it is by using a user identifier and a password, but for those who require for better data security, there is an option called the strong network authentication available. Unlike the traditional way, strong network authentication uses a smart card, a certificate and a pin-code. Smart card is a plastic card that contains a smart chip. Smart chip contains memory, which you can use for storing for example certificates. Certificate is a document that is signed electrically. It consists of two keys, so called public and secret keys, and also of the information of it's owner. Pin-code is used to protect the certificate with a smart card. It also makes it possible to use the smart card.

To make the strong network authentication work, you need to use software that differs from the traditional logging in, such as Certifier-, Token Master, LDAP-, and CSP-software. Certifier and Token Master-software are used in strong network authentication to create the certificates, smart cards and the certificate revocation list that are needed to make it work. LDAP-software is used to publish the certificate revocation list. CSP-software is needed by the specific workstation that is used to log in by using the strong network authentication. The software that is used in the traditional logging in, is also needed to be configured when the strong network authentication is being taken to use. The domain controller that you are logging in to, needs to be configured to accept the certificate based logging in with a smart card.

First in this literary part of the work, there are some new software and concepts that are accurately explained. After that, all the different stages of work are being gone through in detail. As a result, there is an independently installed and configured system, that can be used in stronger network authentication in Microsoft Windows domain.

ALKUSANAT

Tämä opinnäytetyö on tehty Instasec Oy:lle, jossa työskentelin syksyllä 2004 järjestelmäasiantuntijana. Työn aihe sovittiin yhdessä esimieheni Ville Kuumolan kanssa. Kiitokset hänelle ja muille Tampereen Instasec Oy:n Service centerin työntekijöille, jotka auttoivat aiheeseen perehtymisessä. Lisäksi haluan kiittää työn ohjaamisesta ja tarkastamisesta lehtori Erkki Hietalahtea. Kiitokset myös lähipiirille avusta ja tuesta.

Tampereella 3. toukokuuta 2005

_____

Kimmo Nevalainen

SISÄLLYSLUETTELO

KÄYTETYT MERKINNÄT JA TERMIT

CA	Certificate Authority, varmennevarmentaja eli eräänlainen päävarmenne
Certificate Services	Varmennepalveluohjelmisto MS Windows -käyttöjärjestelmään
CSP	Cryptographic Service Provider, rajapintaohjelmisto tietokoneen ja toimikortin välillä
DC	Domain Controller, toimialueohjain, palvelin, jossa on määritelty toimialue
DN	Distinguished Name, DN -nimeämiskäytäntö on varmenteissa käytettävä nimeämiskäytäntö.
Group Policy	Ryhmäoikeudet Microsoft Windows -toimialueessa
HSM	Hardware Security Module, lisälaite suojaamaan varmenteiden salaisia avaimia
IP	Internet Protocol, Internet-protokolla, jota käytetään Internetissä tiedon siirtämiseen
LDAP	Lightweight Directory Access Protocol, kevyt tietokanta tiedolle ja rajapinta siihen, sisältää yleensä henkilöiden tietoja.
PKI	Public Key Infrastructure, julkisen avaimen menetelmä, joka on luotettava tapa todistaa varmenteen omistajan henkilöllisyys
Sulkulista	Lista julkisista avaimista, jotka eivät ole voimassa
Varmenne	Sähköisesti allekirjoitettu dokumentti, joka koostuu julkisesta ja salaisesta avaimesta, ja omistajansa tiedoista. Varmennetta kutsutaan myös sertifikaatiksi.
X.500-standardi	Varmenteita koskeva standardi.
X.509-standardi	Toinen varmenteita koskeva standardi.

1 JOHDANTO

Nykyisin työpaikoilla tulee esimerkiksi työpisteissä ja neuvottelutiloissa asioidessa tilanteita, joissa työtoverisi tai vieraat näkevät salasanasi ja kirjautumisesi tietokoneelle. Teoriassa he voivat silloin kirjautua sinun oikeuksillasi yrityksen tietokoneille ja verkkoon. Tietokoneelle kirjautumiseen on turvallisuudeltaan eri tapoja, esimerkiksi normaalikirjautuminen ja vahvennettu käyttäjän tunnistaminen. Normaalikirjautumisella tarkoitetaan käyttäjätunnuksen ja salasanan syöttämistä niille varattuun sisäänkirjautumisikkunaan. Vahvennettu käyttäjän tunnistaminen taas tarkoittaa sitä, että normaalikirjautumisesta tehdään turvallisempi. Yksi tapa tehdä se esitellään tässä työssä.

Työskentelen tamperelaisessa tietoturvaan erikoistuneessa yrityksessä Instasec Oy:ssä. Työpaikkani osti uudet varmenneohjelmat, SSH Certifier ja SSH Token Master, koska käytössä ollut Secgo Certificate Manager -varmenneohjelma ei ollut riittävä nykyisille vaatimuksille. Se, mitä varmenne ja kyseiset ohjelmistot tarkoittavat, selvitetään työssä myöhemmin. Työpaikallani tarvittiin uusien ohjelmistojen yhteydessä osaamista vahvennetusta käyttäjän tunnistamisesta. Aloitin työn tutustumalla aiheeseen ja uusien ohjelmistojen käyttöohjeisiin. Sen perusteella suunnittelin laboratorioympäristön, jossa asensin, konfiguroin ja käytin järjestelmää, johon sisältyi yhteensä viisi tietokonetta. Jokaisessa tietokoneessa oli oma ohjelmistonsa, joita tarvitaan vahvennetussa käyttäjän tunnistamisessa.

Työssä on tavoitteena tehdä järjestelmä vahvennetulle käyttäjän tunnistamiselle. Työn vaiheet eli ohjelmien asennus, konfigurointi ja käyttö tehdään itsenäisesti. Työn kaikki vaiheet dokumentoidaan käyttöohjeeksi, jonka avulla järjestelmä voidaan asentaa ja konfiguroida.

Aluksi työn kirjallisessa osuudessa selvitetään yleisesti uusia asioita ja termejä. Sen jälkeen käydään tarkasti läpi viiden ohjelmiston asennus, konfigurointi ja käyttö vahvennettuun käyttäjän tunnistamiseen. Lopuksi esitellään työn tuloksia, järjestelmän heikkouksia ja jatkokehitysideoita.

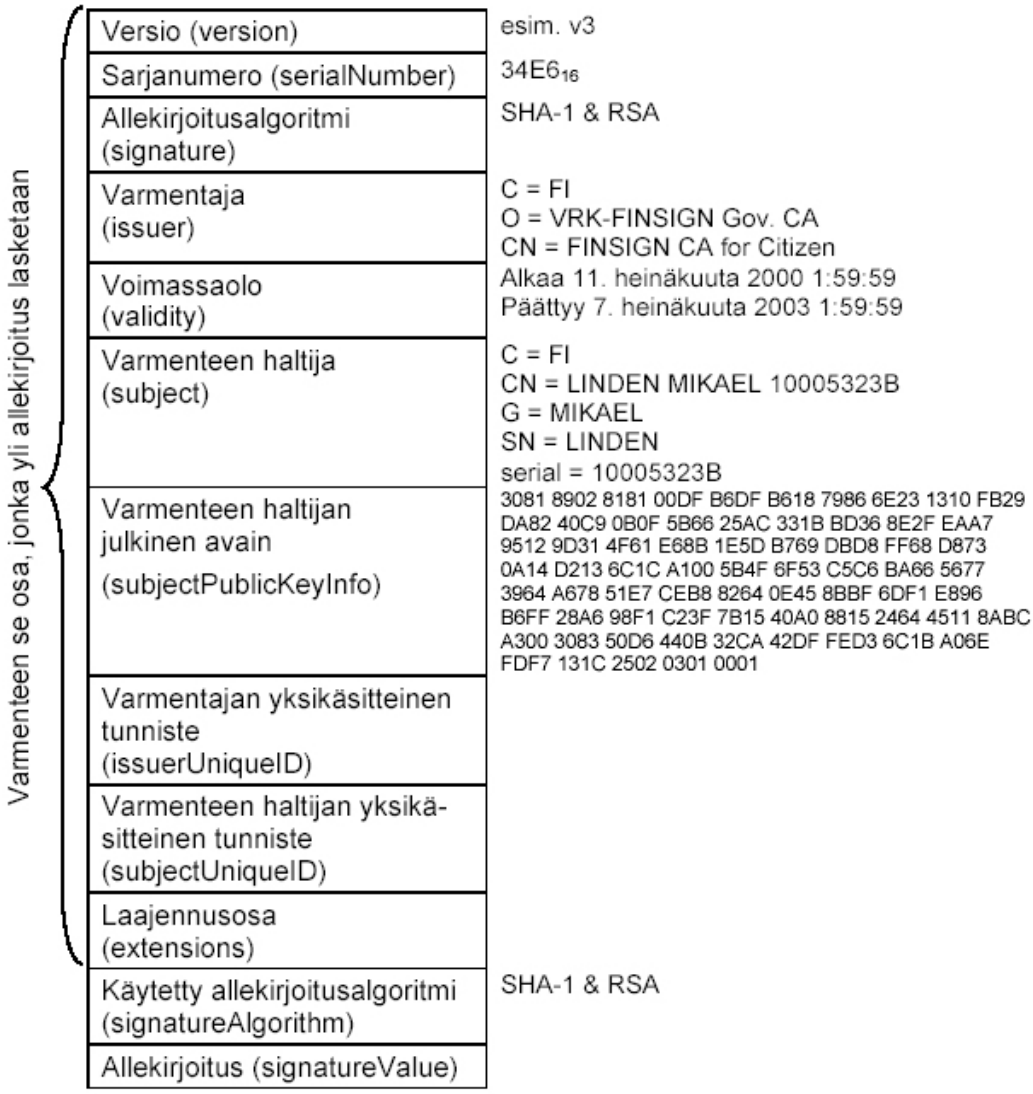
2 VAHVENNETUN KÄYTTÄJÄN TUNNISTAMISEN OHJELMISTOT

Seuraavassa käydään läpi järjestelmän vaatimat ja tarvitsemat ohjelmistot, uudet asiat ja termit yleisesti tarkastelematta vielä tarkemmin, miten niitä on hyödynnetty vahvennetussa käyttäjän tunnistamisessa.

2.1 Certifier-ohjelmisto

Certifier-ohjelmisto on SSH-yrityksen kehittämä kaupallinen ohjelmisto, jolla voidaan tehdä nykyaikaisia varmenteita, CA-varmenteita, varmennepyyntöjä, sulkulistoja ja hallinnoida PKI:tä (Public Key Infrastructure). [1]

Varmenne on sähköisesti allekirjoitettu dokumentti, jota käytetään osoittamaan varmenteen omistajan henkilöllisyys. Varmenne kertoo myös, kuka sen on allekirjoittanut eli varmentanut sekä varmenteen voimassaoloajan. Varmenteeseen voidaan lisätä myös tieto siitä, millaisiin tarkoituksiin sitä voidaan käyttää. Varmenteeseen liittyy oleellisesti niin sanottu julkinen avain, joka liittyy matemaattisesti ainoastaan varmenteen omistajan salaiseen avaimeen. [2] Varmenne koostuu avainparista, joka sisältää julkisen ja salaisen avaimen. Salainen avain on nimensä mukaisesti tarkoitus pitää salaisena, eli sitä ei koskaan saa luovuttaa mihinkään. Vastaavasti julkinen avain on nimensä mukaisesti julkinen siten, että nykyään julkiset avaimet julkaistaan usein Internetissä. Varmennetta kutsutaan myös sertifikaatiksi. Varmenteella on kuvassa 1 esiteltyjä esimerkkitietoja ja rakenne.



Kuva 1. Kuva varmenteen rakenteesta. [10]

Versio -kenttä ilmaisee yksinkertaisesti, mistä varmenteen versiosta on kyse, yleisimmin käytössä on v3. Tällä hetkellä käytössä on versioita v1, v2, v3 ja v4. Sarjanumero on varmentajan kyseiselle varmenteelle antama yksikäsitteinen juokseva numero. Kaikilla yhden varmentajan myöntämillä varmenteilla tulee olla eri sarjanumero. Allekirjoitusalgoritmikenttä kertoo, mitä tiiviste- ja salausalgoritmia varmentaja on käyttänyt allekirjoittaessaan varmennetta. Sama tieto löytyy myös varmenteen lopusta. [10]

Varmentaja -kenttä kertoo kyseessä olevan varmenteen myöntäjän. Varmenne on allekirjoitettu varmentajan salaisella avaimella. Varmenteen haltija on kyseisen varmenteen kohde, eli alivarmentaja tai loppukäyttäjä. Varmenteen oleellisin tehtävä on yhdistää varmenteen haltija -kenttä varmenteen haltijan julkinen avain -kenttään,

joka sisältää itse julkisen avaimen lisäksi myös tunnisteen salausalgoritmille, kuten RSA, johon kyseinen avain sopii. Varmentajalle ja varmenteen haltijalle voidaan antaa vaihtoehtoisia nimiä varmenteen laajennuskentissä. [10]

Varmentaja ja varmenteen haltija, eli organisaatio tai luonnollinen henkilö, yksilöidään X.500-standardin käyttämän DN (distinguished name) -nimeämiskäytännön mukaisesti. DN koostuu hierarkkisista osista, jotka voidaan ajatella omina tasoinaan. Yleisesti käytettyjä hierarkian tasoja ovat maatunnus C (country), organisaatiotunnus O (organization), organisaatioyksikkö OU (organizational unit) ja nimi CN (common name). [10]

Voimassaolo -kenttä ilmaisee varmenteen voimassaoloajan, eli sen, koska varmenteen voimassaolo alkaa ja koska se päättyy. Ajan esityksessä on suositeltavaa käyttää UTC-aikaa. Varmentajan yksikäsitteinen tunniste ja varmenteen haltijan yksikäsitteinen tunniste ovat kenttiä, joita ei suositella käytettävän enää X.509-standardin version 3 tai 4 varmenteissa. [10]

CA-varmenne (Certificate Authority) on eräänlainen päävarmenne. Yleensä CA-varmenne on itse itsensä allekirjoittava. Tämä tarkoittaa sitä, että varmenne on aina jonkun allekirjoittama. Ensimmäisen CA-varmenteen on oltava itse itsensä allekirjoittama, sen jälkeen sillä voidaan allekirjoittaa varmennehierarkiassa alempana olevia varmenteita, CA-varmenteita ja sulkulistoja.

Varmennepyyntö tarkoittaa RSA Security -yrityksen standardoimaa PKCS#10-standardin mukaista varmennepyyntöä, jossa on tarvittavat tiedot varmenteelle, mutta jota ei ole allekirjoitettu varmenteeksi. [3]

Sulkulista tarkoittaa listaa julkisista avaimista, jotka eivät ole voimassa eli joihin ei pidä luottaa. Sulkulista julkaistaan yleensä myös Internetissä, jolloin se on kaikkien saatavilla. Sulkulista suojataan allekirjoittamalla se CA-varmenteella, allekirjoittamattomaan sulkulistaan ei luoteta. Sulkulista voidaan julkaista aina uudelleen, kun listalle tulee uusi varmenteen julkinen avain. Sulkulistalla on yleensä kahden tunnin voimassaoloaika, jonka aikana julkaistaan uusi sulkulista, joka on voimassa taas

kaksi tuntia julkaisemisesta lähtien. Näin mahdolliset pienet tietotekniset häiriöt ja latenssit eivät aiheuta ongelmia.

PKI:llä tarkoitetaan julkisen avaimen menetelmää. Jotta sähköistä allekirjoitusta voitaisiin käyttää avoimessa ympäristössä kuten Internetissä, jossa osapuolet eivät välttämättä tunne toisiaan, tarvitaan tietoa siitä, kuka on allekirjoituksen tehnyt henkilö. Siksi on kehitetty PKI-järjestelmä, jossa luotettava kolmas osapuoli myöntää varmenteen. [9]

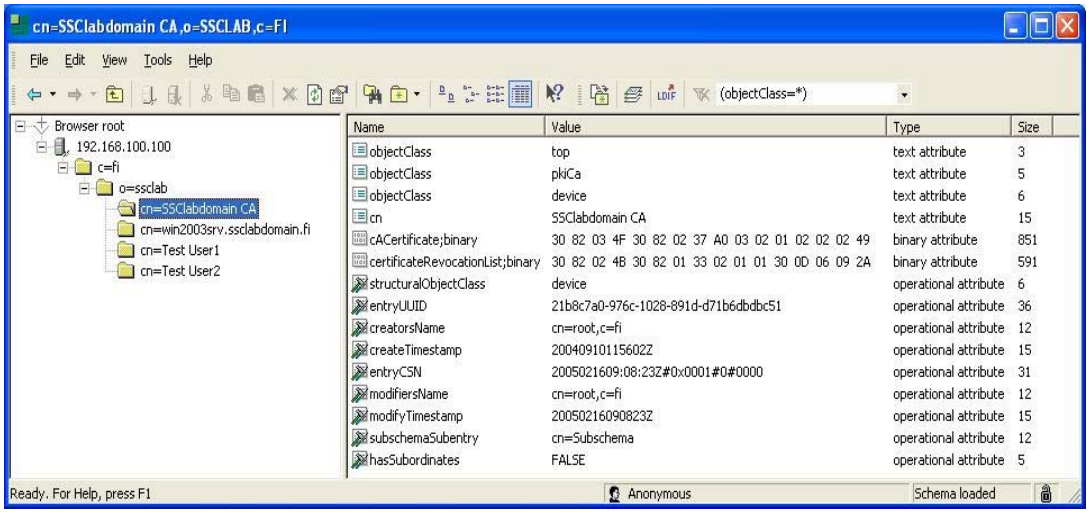
Certifier-ohjelmisto tukee myös HSM-lisälaitetta (Hardware Security Module) tietokoneeseen. HSM-lisälaitteeseen voidaan tallentaa CA-varmenteiden salaisia avaimia talteen. Laite suojaa salaisia avaimia siten, että se estää niiden varastamisen ja kopioimisen ja suojaa niiden käyttöä suojakoodilla. Laite kykenee myös tuhoamaan avaimet tilanteessa, jossa salaiset avaimet ovat vaarassa joutua vääriin käsiin. [4]

2.2 LDAP-ohjelmisto

LDAP-protokollaohjelmisto (Lightweight Directory Access Protocol) tarkoittaa kevyttä rajapintaa tietokantaan. Kevyellä rajapinnalla tarkoitetaan sitä, että rajapinta on optimoitu yksinkertaisten hakujen nopeutta varten. Yleisesti puhuttaessa LDAP-rajapinnasta tarkoitetaan kuitenkin itse tietokantaa rajapinnan takana. LDAP-tietokantaohjelmistoja käytetään julkisina tiedostopalvelimina Internetissä. LDAP-tietokantaan voi tallentaa mitä tahansa tietoa, jota voi tallentaa normaalitietokantaankin. LDAP-ohjelmiston on hyvä olla omassa tietokoneessaan verkkotopologisessa mielessä, koska LDAP-ohjelmisto tulee yleensä Internetiin näkyviin, jolloin on tietoturvallista, ettei sen palomuuriin tarvitse avata kuin yksi portti auki Internetistä päin.

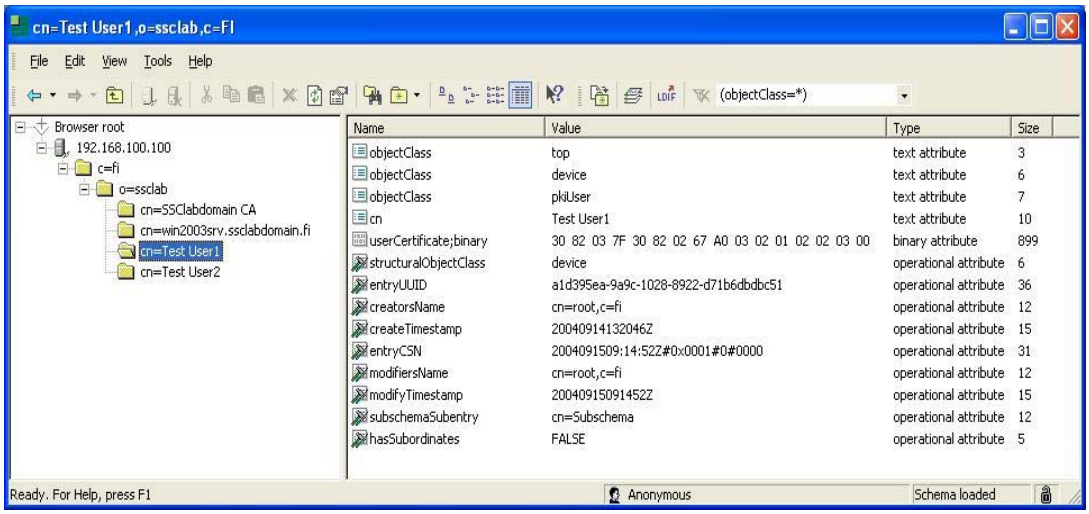
Seuraavassa kuvassa on esimerkki LDAP -tietokannan sisällöstä LDAP -selaimella esitettynä. Vasemman puoleisessa ikkunassa näkyvät X.500-standardin mukaisesti tasot alkaen juuresta, joka on maatunnus C, ja sen jälkeen organisaatiotunnus O.

Organisaatioyksikköä OU ei esimerkkikuvasta löydy, mutta nimi CN löytyy viimeisenä tasona. Oikeanpuoleisessa ikkunassa on avattuna organisaation cn=SSClabdomain CA tiedot, joiden alta löytyy paljon muuta tietokannassa olevaa tietoa. Tärkeimpiä tietoja ovat cACertificate;binary ja certificateRevocationList;binary -tiedot, ne ovat SSClabdomain CA-varmenteen julkinen avain ja sille kuuluva sulkulista.



Kuva 2. LDAP -tietokanta LDAP -selaimella, CA-varmenne avattuna.

Seuraavassa kuvassa on esillä cn=Test User1 -käyttäjän tiedot. Tärkeimmät ovat tietona userCertificate;binary -tieto, joka on käyttäjän varmenteen julkinen avain.

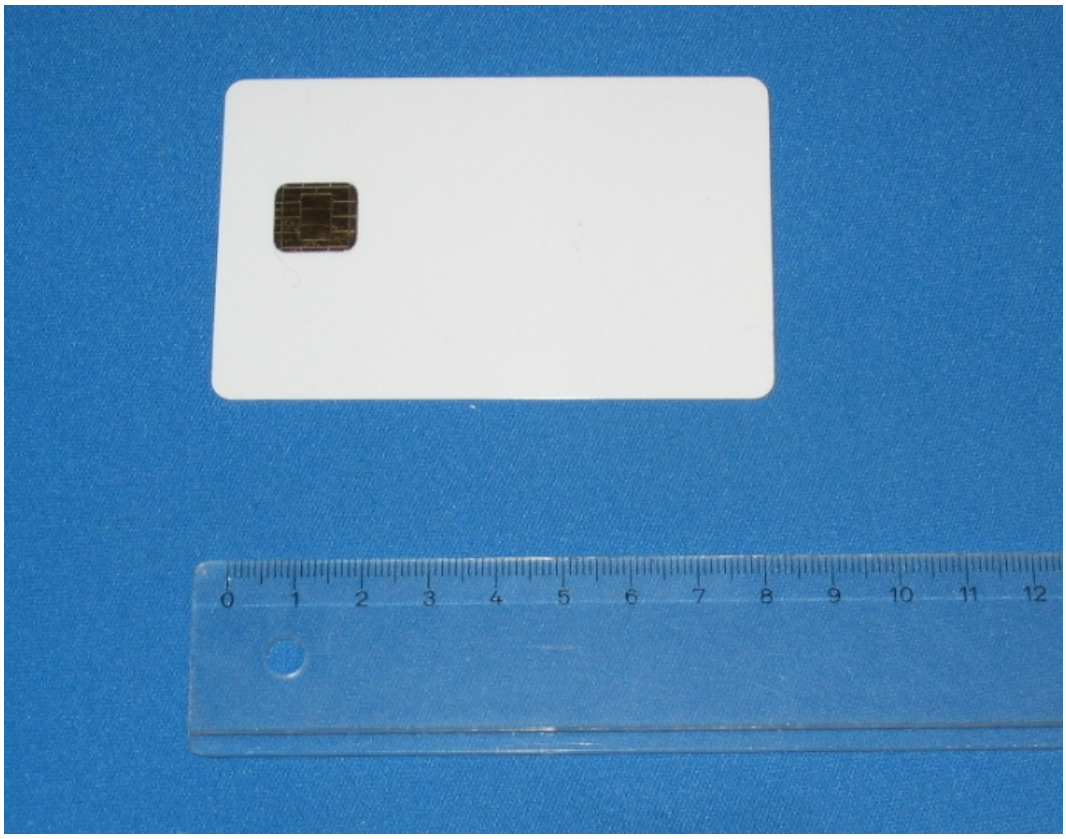


Kuva 3. LDAP -tietokanta LDAP -selaimella, käyttäjän varmenne avattuna.

2.3 Token Master -ohjelmisto

Token Master -ohjelmisto on myöskin SSH-yrityksen kehittämä kaupallinen ohjelmisto. Se on lisäohjelmisto Certifier-ohjelmistoon, ja se nopeuttaa ja helpottaa toimikorttien tekemistä ja tukee myös toimikorttien massatuotantoa. [1]

Toimikortti on tiedonsuojausväline. Toimikortti tarkoittaa luottokortin kokoista muovikorttia, jossa on älysiru ja sen liitin kortin pinnassa näkyvissä (kuva 4). Älysiru on kuten tietokone, se sisältää käyttöjärjestelmän ja tyhjää tilaa tiedolle. Toimikortille varmennetta tehdessä tietoturvallinen ja hyvä tapa on arpoa varmenteen salainen avain toimikortin käyttöjärjestelmällä. Tällöin salainen avain ei koskaan jää mihinkään kopiona, kuten voisi käydä siirrettäessä sitä tietokoneelta toimikorttiin. Koska toimikortin käyttöjärjestelmä estää salaisen avaimen kopioimisen kortilta, toimikortti on todella turvallinen tapa säilyttää varmenteita. Toimikortti suojataan yleensä pin- ja puk-koodeilla vielä käytön yhteydessä. Pin- ja puk-koodit ovat eräänlaisia tunnuslukuja, joilla estetään toimikortin vapaa käyttö. Toimikortti suojataan pin- ja puk-koodeilla esimerkiksi siten, että ensimmäisen varmenteen salaista avainta suojataan pin1-koodilla, ja toisen varmenteen salaista avainta pin2-koodilla. Pin-koodeilla on yleensä rajallinen määrä vääriä yrityksiä, minkä jälkeen pin-koodit lukittuvat ja ne voidaan avata puk-koodeilla. Puk-koodien väärien yritysten määrä voidaan myös rajoittaa, ja sallittujen väärien yritysten jälkeen toimikortti lukitsee itsensä lopullisesti. [5]



Kuva 4. Kuva toimikortista.

2.4 Toimialueohjain

Toimialueohjain tarkoittaa palvelinta, jossa on määritelty toimialue. Paremmin tunnetut käsitteet ovat englanninkielisiltä nimiltään Domain ja Domain Controller eli toimialue ja toimialueohjain. Yleisimmin käytössä oleva toimialue on Microsoft-yrityksen kehittämä Microsoft Windows -toimialue, joka voidaan asentaa käyttöön Microsoft Windows Server -käyttöjärjestelmissä. Toimialuepalvelin tarvitsee Certificate Services -lisäohjelmiston vahvennettua käyttäjän tunnistamista varten. Certificate Services on Microsoft Windows -käyttöjärjestelmän lisäohjelmisto, joka tarkoittaa varmennepalvelua. Se on siis Microsoft-yrityksen kehittämä varmenneohjelmisto Microsoft Windows -käyttöjärjestelmään. Microsoft Windows -varmennepalvelulla voidaan tehdä varmenteita ja sulkulistoja ja julkaista sulkulistoja. Aivan kaikkea haluamaansa ei kuitenkaan voi määritellä tai tehdä. Esimerkiksi tarkkaa voimassaoloaikaa ei voi määritellä tai massatuotannon tuki puuttuu. Tämän

vuoksi Microsoft Windows -varmennepalvelun yleistyminen varmenneohjelmistona on vaikeaa. [6]

2.5 Käyttäjätyöasema

Käyttäjätyöasemalla tarkoitetaan käyttäjän työasemaa, joka on liitetty toimialueeseen ja jolla työntekijä tekee töitä. Yleisimmät käyttöjärjestelmät työasemakäytössä ovat Microsoft Windows NT 4.0, Microsoft Windows 2000 Professional ja Microsoft Windows XP Professional. Uusimpana käyttöjärjestelmänä työhön valittiin Microsoft Windows XP Professional, joka on yleistymässä niin yritys- kuin kotikäytössäkin.

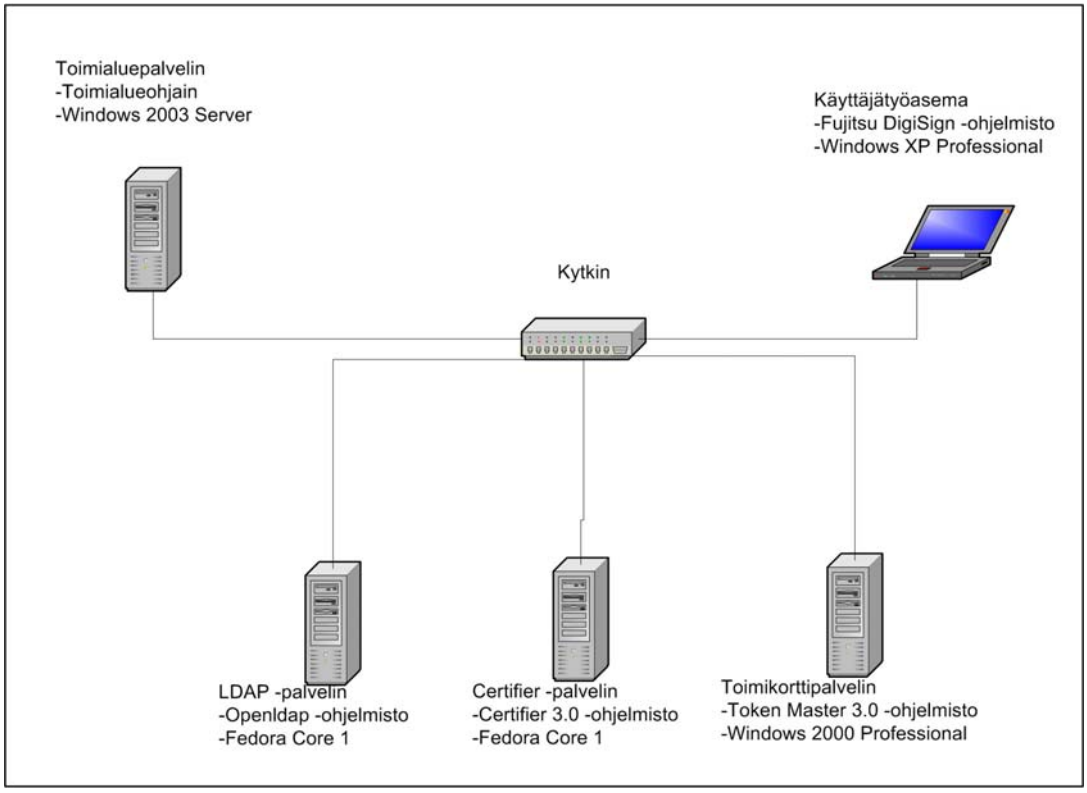
Käyttäjän työasemaan tulee asentaa myös jokin CSP-ohjelmisto (Cryptographic Service Provider). CSP-ohjelmisto tarkoittaa ohjelmistoa toimikortin ja tietokoneen käyttöjärjestelmän väliin. CSP-ohjelmisto tarjoaa tietokoneen käyttöjärjestelmälle rajapinnan toimikorttiin. Ilman CSP-ohjelmistoa Microsoft Windows -käyttöjärjestelmät eivät osaa lukea toimikortteja.

Vahvennetussa käyttäjän tunnistamisessa on kaksi asiaa, joita tarvitaan kirjautumiseen, toimikortti ja pin-koodi. Sen vuoksi ei ole kovin vaarallista, jos vieras henkilö tai työtoverisi näkee sinun syöttävän pin-koodin tai saa haltuunsa sinun toimikorttisi, koska kummallakaan ei tee yksinään mitään. Pin-koodin voi vaihtaa aina halutessaan uudeksi, joten sen näyttäminen ei ole kovin haitallista. Niin kauan kuin toimikortti on hallussasi, kukaan ei tee mitään pelkällä pin-koodilla. Vastaavasti toimikortin häviäminen ei yksinään ole vaarallista, koska ilmoitus varmentajalle riittää estämään toimikortilla kirjautumisen. Varmentaja lisää käyttäjän toimikortilla sijaitsevan varmenteen sulkulistalle ja julkaisee sulkulistan uudelleen. Toimialueohjain tarkistaa joka kirjautumisen yhteydessä sulkulistan. Kun kortin löytymisestä ilmoitetaan, varmentaja poistaa varmenteen sulkulistalta ja julkaisee uuden sulkulistan, minkä jälkeen kirjautuminen onnistuu taas.

Toimikortti rajoittaa myös yhdenaikaisia kirjautumisia. Jos normaali kirjautuminen estetään tai toimikortin poistamista lukijasta ei sallita, käyttäjä ei voi olla kirjautuneena tietokoneelle useammassa paikassa yhtä aikaa kuin mihin käyttäjällä on toimikortteja. Yleensä on järkevää tehdä vain yksi toimikortti ja katoamistilanteessa uusia se. Kortin kopioiminen ei ole mahdollista, sen estää kortin käyttöjärjestelmä. Jos kuitenkin halutaan varmistaa katkoton toiminta, kuten esimerkiksi jossain erikoisjärjestelmissä, muita toimikortteja olisi hyvä säilyttää esimerkiksi kassakaapissa, pankin tallelokerossa tai muussa vartioidussa paikassa. Katoamistilanteessa tehdään tietenkin ilmoitus kadotetusta toimikortista varmentajalle.

3 TYÖN SUORITTAMINEN JA TEHDYT HAVAINNOT

Seuraavassa kuvassa on yksinkertaistettu verkkokuva laboratoriokokonaisuudesta (kuva 5). Kuvassa on esitetty vahvennettuun käyttäjän tunnistamiseen tarvittavat tietokoneet, ohjelmistot ja käyttöjärjestelmät.



Kuva 5. Verkkokuva laboratorioympäristöstä.

3.1 LDAP-palvelin

Työn ensimmäisessä vaiheessa tarvitaan LDAP-palvelua. LDAP-ohjelmistoa käytetään työssä toimialueen käyttäjien ja varmentajan julkisten avainten tallentamiseen ja julkaisemiseen, sekä sulkulistojen tallentamiseen ja julkaisemiseen. Sitä varten asennetaan yhteen tietokoneeseen Linux-käyttöjärjestelmä, ja siihen LDAP-ohjelmisto. LDAP-palvelua tulee käyttämään lähes jokainen työssä käytetty ohjelmisto, joten sen on oltava toiminnassa ensimmäisenä.

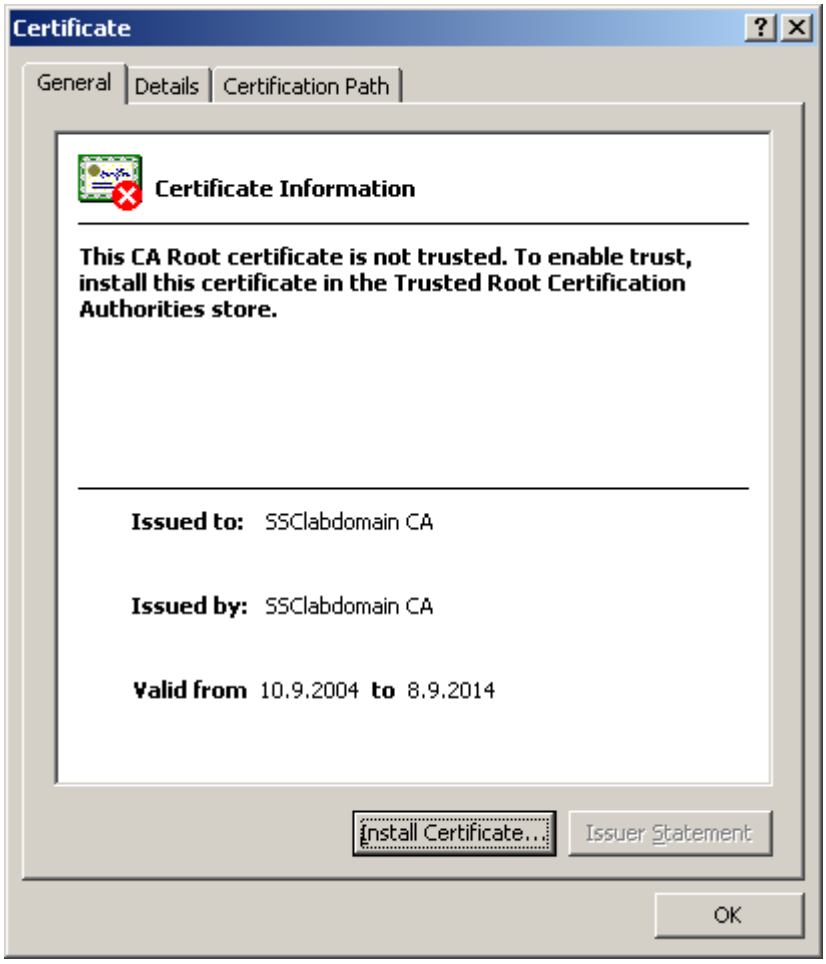
Linux-käyttöjärjestelmäksi valittiin Fedora Core 1 -käyttöjärjestelmä, koska se on lisenssivapaa ja yleisesti käytössä Instasec Oy:ssä ja sitä kautta entuudestaan tuttu. Tarkoitukseen soveltuvat myös muut käyttöjärjestelmät. Koneelle konfiguroitiin kiinteä IP-osoite, jotta muut koneet ja ohjelmistot saisivat siihen yhteyden. LDAP-ohjelmistoksi valittiin OpenLDAP-ohjelmisto, koska sekin on lisenssivapaa, ja jo aiemmin käytössä vakaaksi ja hyväksi todettu. Tarkoitukseen soveltuvat myös muut LDAP-ohjelmistot. Ohjelmistolle konfiguroidaan tietoja, joilla määritellään LDAP-ohjelmiston näkyvyys- ja kirjoitusoikeudet. Näkyvyys määriteltiin niin, että kaikki ohjelmistoon tallennettu tieto näytetään kaikille. Kirjoitusoikeudet valittiin niin, että vain rekisteröity käyttäjä voi tallentaa tietoa LDAP-ohjelmistoon.

3.2 Certifier-palvelin

LDAP-ohjelmiston konfiguroinnin jälkeen vuorossa oli Certifier-palvelimen asentaminen. Certifier-ohjelmistoa käytetään työssä CA-varmenteen luomiseen, käyttäjävarmenteiden allekirjoittamiseen ja sulkulistojen luomiseen. Certifier-ohjelmisto asennettiin myös Fedora Core 1 -käyttöjärjestelmään, ja myös sille annettiin kiinteä IP-osoite. Certifier-ohjelmisto koostuu kahdesta isosta osasta, Certifier server:stä ja Certifier engine:stä, jotka voitaisiin haluttaessa sijoittaa omiin koneisiinsa keventämään koneen prosessorikuormaa. Tässä kokonaisuudessa se ei ole tarpeellista, koska koneen suorituskyky ei ole tärkeää laboratorioympäristössä. Certifier-ohjelmistoon olisi voitu myös asentaa HSM-lisälaite, mutta korkean hintansa vuoksi sitä ei ollut tähän järjestelmään tarvetta liittää. Se ei myöskään vaikuta Certifier-

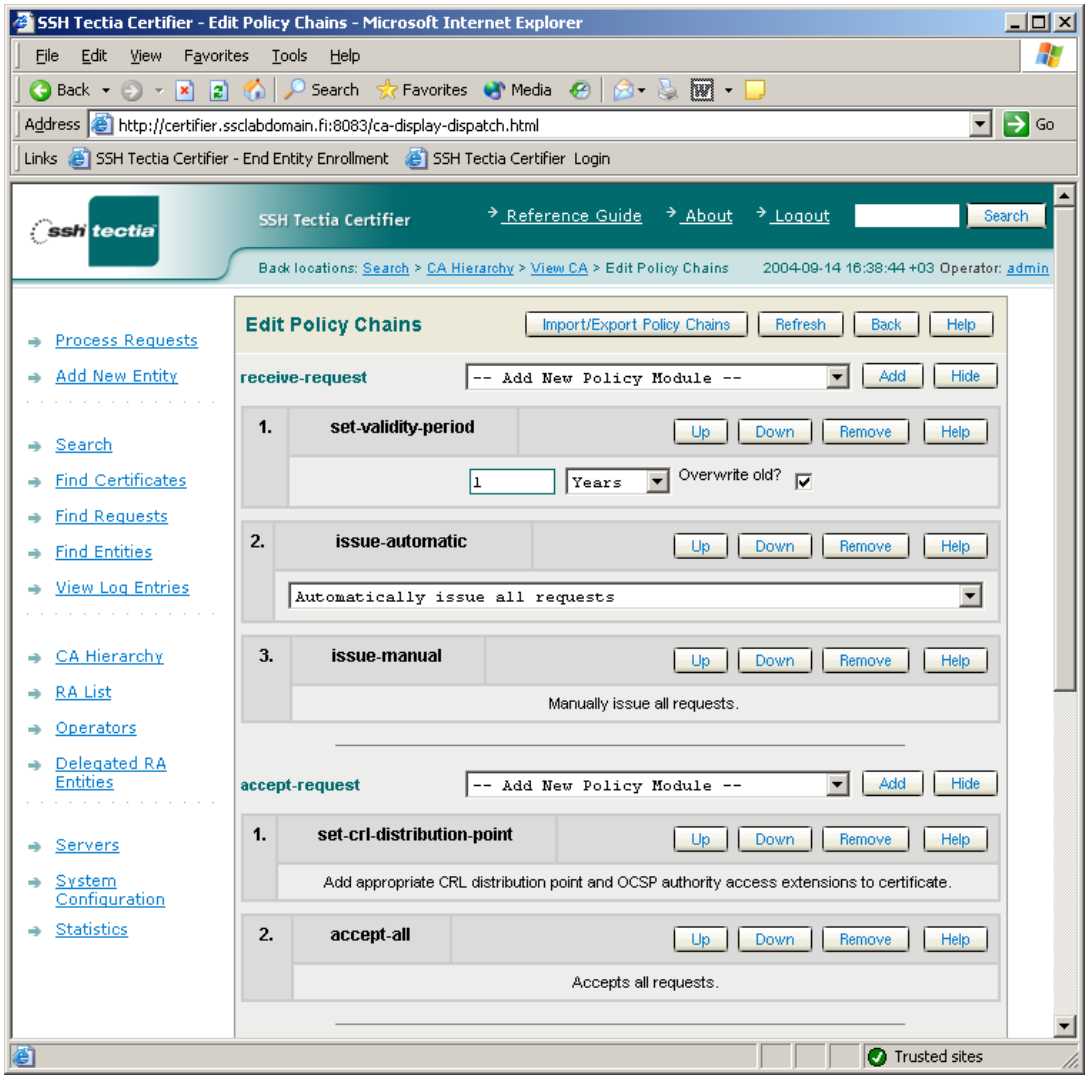
ohjelmiston toimintaan, vaan ainoastaan CA-varmenteiden turvallisuuteen. Tämäkään ei ole tarpeellista laboratorioympäristössä. Certifier-ohjelmiston asennuttua, itse ohjelmassa voidaan konfiguroida kaikkia ohjelmiston toimivuuteen vaikuttavia asetuksia, kuten CA-varmenteita ja niiden politiikkoja. Ohjelmaa käytetään Internet-selaimella.

Certifier-ohjelmistoon luotiin uusi CA-varmenne, joka on itse itsensä allekirjoittava (kuva 6). CA-varmenteelle määriteltiin nimi, organisaatio, maa, voimassaoloaika, salaisen avaimen pituus, sekä avaimen käyttötarkoitukset. Tärkeimpiä tietoja varmenteella ovat voimassaoloaika, salaisen avaimen pituus ja avaimen käyttötarkoitukset. Voimassaoloajaksi valittiin kymmenen vuotta, kuten itse allekirjoittavalle CA-varmenteelle on yleistä. Tämä näkyy myös kuvan 3 varmenteen tietodialogissa. Salaisen avaimen pituudeksi valittiin 2048 bittiä, joka on nykyään suositeltava minimimäärä CA-varmenteelle. Avaimen käyttötarkoitukseksi oli valittava varmenteen ja sulkulistan allekirjoitus, koska muuten niitä ei olisi mahdollista tehdä.



Kuva 6. Varmenteen tietodialogi.

CA-varmenteelle konfiguroitiin Certifier-ohjelmistoon politiikka (kuva 7), jonka mukaan Certifier-ohjelmisto käsittelee automaattisesti kaikki varmennepyynnöt ja sulkulistan julkaisun LDAP-tietokantaan. Sulkulistan voimassaoloajaksi kerrallaan määriteltiin kaksi tuntia. Tämä tarkoittaa sitä, että jokainen sulkulista on julkaisusta lähtien kaksi tuntia voimassa, mutta uusitaan puolessa välissä eli tässä tapauksessa tunnin jälkeen taas kahdeksi tunniksi eteenpäin. Sulkulistan julkaisuun liittyvät LDAP-tietokannan osoite ja käyttäjätiedot konfiguroitiin samalla.



Kuva 7. Osa Certifier -ohjelmiston varmenteen myöntämispolitiikkaa.

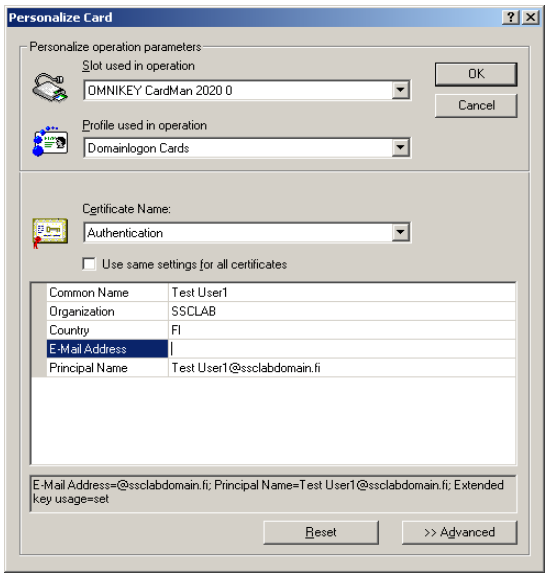
3.3 Toimikorttipalvelin

Seuraavana työvaiheena asennettiin Token Master -ohjelmisto Windows 2000 Professional -käyttöjärjestelmään. Token Master -ohjelmistoa käytetään työssä toimikorttien luomiseen. Käyttöjärjestelmään ladattiin ja asennettiin kaikki tarpeelliset päivitykset, mikä on aina tärkeää kaikille Microsoft Windows -käyttöjärjestelmille tietoturvapäivitysten vuoksi. Kiinteä IP-osoite ei olisi ollut tietokoneelle välttämätön, mutta varmistusten ja selkeyden vuoksi kiinteä IP-osoite annettiin ja tietokone sijoitettiin muiden koneiden kanssa samaan paikkaan verkossa. Tietokoneeseen liitettiin toimikortinlukija, johon käyttöjärjestelmän kehotuksesta asennettiin ajurit.

Myös Token Master -ohjelmistossa voidaan muuttumattomat tiedot tallentaa politiikan kaltaisesti profiileiksi, joiden mukaan Token Master toimii samalla tavalla joka kerta samanlaisissa tilanteissa. Siten käyttäjän tekemää ylimääräistä työtä voidaan vähentää huomattavasti.

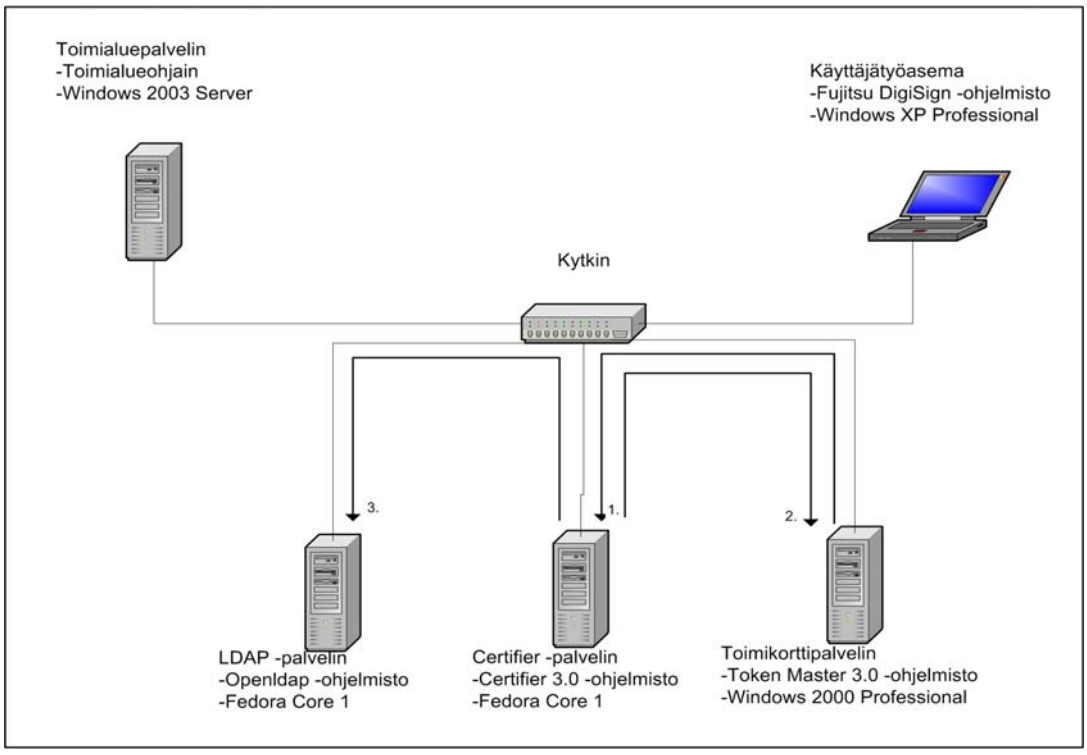
Token Master -ohjelmistoon tehtiin toimikorttikirjautumista varten uusi profiili. Profiiliin konfiguroitiin CA-varmenne, organisaatio ja maa oletuksiksi sekä varmenteen käyttötarkoituksiksi käyttäjän tunnistaminen ja toimikorttikirjautuminen. Nämä ovat välttämättömiä toimikorttikirjautumiseen tarkoitetussa toimikortissa. Token Master -ohjelmistolla voi myös määritellä pin- ja puk-koodien asetukset, jotka myös asetettiin profiiliin. Valittu profiili näkyy kuvassa 8.

Toimikortti tehdään Token Master -ohjelmiston personointiohjelmalla. Valmiiksi määriteltyyn pohjaan tarvitsee vain antaa kuvassa 8 näkyviä määrityksiä. ”Principal Name” -kenttään tulee vahvennetun käyttäjän tunnistamisen kannalta tärkein tieto, siihen kirjoitetaan käyttäjän toimialuetunnus ja ’@’-merkillä erotettuna toimialueen nimi.



Kuva 8. Näkymä Token Master -ohjelmiston toimikortin personointiohjelmasta.

Seuraavassa kuvassa on esitetty tiedon kulku palvelimien välillä toimikortin luontitilanteessa. Ensimmäisessä vaiheessa toimikorttipalvelin lähettää käyttäjän varmenteen allekirjoitettavaksi Certifier-palvelimelle. Varmenne hyväksytään Certifier-palvelimella henkilön toimesta tai ohjelmistoon valmiiksi määritellyn kaavan mukaan. Toisessa vaiheessa Certifier-palvelin lähettää allekirjoitetun varmenteen takaisin. Kolmannessa vaiheessa Certifier-palvelin lähettää käyttäjävarmenteen julkisen avaimen julkaistavaksi LDAP-palvelimelle.



Kuva 9. Tiedon kulku toimikortin luomisen aikana.

3.4 Toimialuepalvelin

Tässä vaiheessa työtä oli asennettu kolme erikoispalvelinta. Seuraavaksi siirryttiin kahden tavallisemman tietokoneen asennukseen, konfigurointiin ja käyttöön. Työhön valittiin toimialueohjaimeksi Microsoft Windows 2003 server -käyttöjärjestelmä, joka asennettiin. Sille annettiin kiinteä IP-osoite, kuten toimialueohjaimelle suositellaan annettavaksi nimipalvelun vuoksi. Käyttöjärjestelmään ladattiin ja asennettiin kaikki tarpeelliset päivitykset. Sen jälkeen käyttöjärjestelmään asennettiin ja konfiguroitiin käyttöön uusi toimialue (ssclabdomain.fi). Normaalisti nämä vaiheet ovat jo valmiiksi tehtyinä, koska yleensä toimialue on jo käytössä, kun siihen lisätään vahvennettu käyttäjän tunnistaminen.

Microsoft Windows -varmennepalvelu asennettiin toimialueohjaimeen. Asennettaessa luodaan itse itsensä allekirjoittava CA-varmenne, ja määritellään siihen perustietoja, kuten julkisen avaimen määrityksiä, salaisen avaimen pituus ja sen salausalgoritmi. Myös CA-varmenteen nimi, toimialueen nimi sekä voimassaoloaika määritellään.

Asennuksen tuloksena Microsoft Windows -varmennepalvelu oli käynnissä, ja toimialueen oma CA-varmenne oli luotu. Toimialueohjaimet pyytävät itselleen automaattisesti omaa varmennetta toimialueen omalta CA-varmenteelta ryhmäoikeuksien päivityksen yhteydessä. Normaalisti tämä tapahtuu kahdeksan tunnin välein. Varmennepyyntöä voi nopeuttaa suorittamalla toimialueohjaimien komentorivillä seuraavan komennon:

```
certutil -pulse.
```

Toimialueohjaimessa on ryhmäoikeudet, joita toimialueohjain jakaa kaikille siihen liitetyille koneille. Ryhmäoikeudet tunnetaan paremmin englanninkielisellä nimellään Group Policy, ja ne tarkoittavat siis kaikille toimialueeseen kuuluville käyttäjille yhteisiä oikeuksia toimialueessa.

Jotta toimialueohjaimet luottaisivat niin sanottuihin kolmannen osapuolen CA-varmenteisiin, Certifier-ohjelmistolla luotu CA-varmenne pitää lisätä toimialueoh-

jaimeen, yhteensä kolmeen paikkaan. CA-varmenne lisätään toimialuepalvelimen ryhmäoikeuksien Root CA -objektiin, NTAuth-objektiin sekä tietokoneen varmennevarastoon. Lisäykset ryhmäoikeuksien Root CA -objektiin ja NTAuth-objektiin voidaan tehdä ajamalla seuraavat komennot komentorivillä:

```
certutil –dspublish –f ca-tiedosto.cer rootca
certutil –dspublish –f ca-tiedosto.cer ntauthca
```

Certifier-ohjelmistolla luotu CA-varmenne pitää asentaa myös palvelimen varmennevarastoon, josta sen voi myös halutessaan kopioida muualle. Varmennevarastossa varmenne on kokonaisuudessaan. Tärkeää on huomioida, että varmennevarasto on jaettu kolmeen osaan: käyttäjän, ohjelmien ja tietokoneen varmennevarastoksi. Oletuksena varmenteen voi asentaa vain käyttäjän varmennevarastoon, josta se pitää kopioida tietokoneen varmennevarastoon. Tämä johtuu siitä, että jos käyttäjä ei ole kirjautuneena koneelle, ei Certifier-ohjelmistolla luotu CA-varmenne ole tarjolla toimialueohjaimelle. Kopiointi tehtiin graafisella Microsoft Windows -käyttöjärjestelmän hallintaan tarkoitetulla Microsoft Management Console -ohjelmalla. Ohjelmassa avattiin ensin sekä käyttäjän että tietokoneen varmennevarasto, sitten varmenteesta otettiin kopio käyttäjän varmennevarastossa ja lopuksi liitettiin se tietokoneen varmennevarastoon.

Koska toimialueohjaimet päivittävät automaattisesti ryhmäoikeudet normaalisti kahdeksan tunnin välein, ei edellinen lisäys tule voimaan ennen kuin ryhmäoikeudet on päivitetty uudelleen. Ryhmäoikeudet voi päivittää astumaan heti voimaan suorittamalla toimialueohjaimissa komentorivillä seuraavan komennon:

```
gpupdate /force.
```

3.5 Käyttäjätyöasema

Työn viimeinen vaihe aloitettiin Microsoft Windows XP Professional -käyttöjärjestelmän asentamisella. Microsoft Windows XP Professional -

käyttöjärjestelmään ladattiin ja asennettiin kaikki viimeisimmät päivitykset, minkä jälkeen työasemaan liitettiin toimikortinlukija. Käyttöjärjestelmä löysi silloin uuden laitteen ja kehotti asentamaan tarvittavat ajurit toimikortinlukijalle, jotta sitä voitaisiin käyttää.

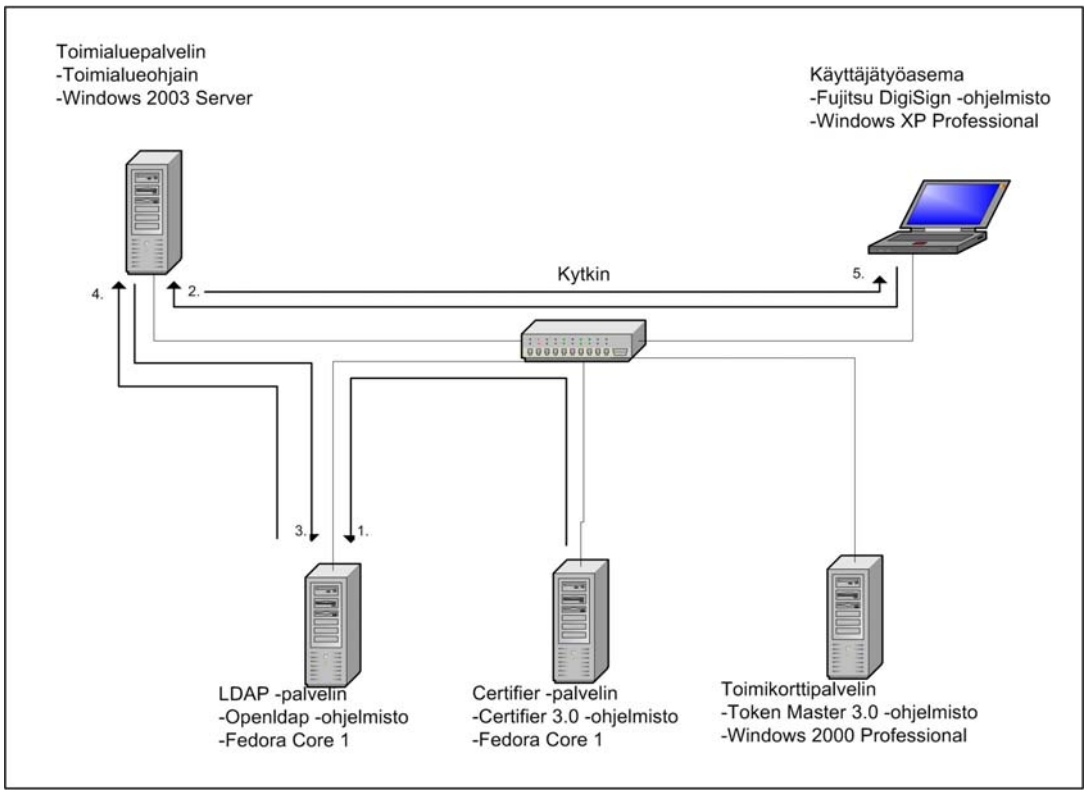
Työhön valittiin Instasec Oy:ssä käytössä oleva Fujitsu DigiSign CSP -ohjelmisto, joka on monipuolisin Instasec Oy:ssä käytettävistä CSP-ohjelmistoista. Myös useat muut CSP-ohjelmistot käyvät tarkoitukseen, esimerkiksi Setec-yrityksen SetWeb-ohjelmisto.

Seuraavaksi työasema liitettiin toimialueeseen. Normaalitilanteessa työasema on yleensä jo valmiiksi liitettynä toimialueeseen.

Työasemat tarvitsevat myös uuden Certifier-ohjelmistolla luodun CA-varmenteen tietokoneen varmennevarastoon, ja hakevat sen automaattisesti ryhmäoikeuksien päivityksen yhteydessä kahdeksan tunnin välein. Päivitystä voi nopeuttaa ajamalla työaseman komentorivillä seuraavan komennon:

```
gpupdate /force.
```

Seuraavassa kuvassa esitellään tiedon kulku palvelimien välillä toimikorttikirjautumistilanteessa. Ensimmäisessä vaiheessa Certifier-palvelin julkaisee sulkulistan LDAP-palvelimelle. Toisessa vaiheessa käyttäjä on asettanut toimikortin toimikortinlukijaan käyttäjätyöasemalla, jolloin käyttöjärjestelmä kysyy toimialuepalvelimelta onko kyseinen käyttäjävarmenne luotettu ja voimassa. Kolmannessa vaiheessa toimialuepalvelin kysyy LDAP-palvelimelta onko kyseinen käyttäjävarmenne luotettu vai sulkulistalla, johon LDAP-palvelin neljännessä vaiheessa vastaa. Jos kyseinen käyttäjävarmenne on voimassa ja luotettu toimialuepalvelimella, viidennessä vaiheessa käyttäjätyöasema saa myönteisen vastauksen.



Kuva 10. Tiedon kulku toimikorttikirjautumisen aikana.

4 TYÖN TULOSTEN ESITTELY JA ANALYSOINTI

Työpaikkani Instasec Oy:n kannalta tärkeimpänä työn tuloksena saatiin käyttöön normaalikirjautumista turvallisempi kirjautuminen sekä siihen tarvittava ympäristö. Ympäristön asennuksesta, konfiguroinnista ja käytöstä koottu dokumentti toimii myös käyttöohjeena, jonka avulla muutkin työntekijät voivat asentaa ja konfiguroida järjestelmää. Järjestelmä on nyt yrityksellä myynnissä, ja sitä voidaan esitellä asiakkaille neuvottelutiloissa tai asiakkaan luona. Instasec Oy:ssä ei tehty tuotekehitystyötä järjestelmään liittyen.

Vahvennettuun käyttäjän tunnistamiseen otettiin mukaan julkisen avaimen menetelmä (PKI) ja toimikortti tiedonsuojausvälineeksi. PKI kehitettiin tarkoituksenaan tietoturvan lisääminen, ja mielestäni varmenteiden ja toimikortin yhteistoiminta lisää tietoturvaa todella merkittävästi. Vahvennetussa käyttäjän tunnistamisessa on siis kaksi elementtiä, jotka tarvitaan, mekaaninen kortti, jota ei voi kopioida sekä

sen käytön mahdollistava pin-koodi. Kummallakaan yksinään ei voi kirjautua. Tämä vähentää asiattomien henkilöiden mahdollisuutta murtautua järjestelmään.

Huonona puolena vahvennetussa käyttäjän tunnistamisessa voidaan pitää lisääntyvien komponenttien vikaantumisriskiä ja komponenttien välillä olevien tietoliikennekomponenttien vikaantumismahdollisuutta. Jos esimerkiksi LDAP-palvelin jostain syystä vikaantuu, vahvennettu kirjautuminen ei onnistu. Myöskin jos yhteys LDAP -palvelimeen katkeaa, vahvennettu kirjautuminen ei onnistu. Tätä riskiä voidaan pienentää niin, että varmentaja voi halutessaan hajauttaa järjestelmää useampaan paikkaan, jolloin yhden yhteyden tai yhden komponentin väliaikainen vikaantuminen ei estä kirjautumista toimialueeseen vahvennetusti.

Lisäksi huonoina puolina voidaan pitää uuteen tekniikkaan siirtymisen kuluja tai mahdollista muutokseen kohdistuvaa vastarintaa työntekijöiden keskuudessa.

Työn jatkokehitysideoina mieleen ovat tulleet e-Token-tietoturvamoduulit. Ne ovat toimikortin kaltaisia tiedonsuojausvälineitä ja valtaavat markkinoita pienen kokonsa, lukijariippumattomuuden ja vastaavan hyvän tietoturvan vuoksi. e-Token on vain noin 5cm pitkä, 1,5cm leveä ja 5mm paksu eikä siis tarvitse minkäänlaista lukijaa, vaan se kytketään suoraan tietokoneeseen. [7]

Myös markkinoille vähitellen tulevat sormenjälkitoimikortinlukijat olisivat hyvä lisäselvityksen kohde, toimikortilla kun on tilaa sormenjälkitiedoillekin. Jo nykyään käytössä oleva toimikortti kävisi tähän tarkoitukseen, vain kortinlukija ja sen mukana tulevat ajurit ja ohjelmisto vaihdettaisiin. Sormenjälki korvaisi silloin pin-koodin. [8]

LÄHTEET

1 Certifier-ohjelmiston ja Token Master -ohjelmiston manuaalit, SSH, 28.6.2004

2 Mikä on varmenne
http://www.hut.fi/atk/ca/ [viitattu 27.1.2005]

3 PKCS#10
http://www.rsasecurity.com/rsalabs/node.asp?id=2132 [viitattu 27.1.2005]

4 HSM
http://www.ncipher.com/hsms/ [viitattu 28.1.2005]

5 Toimikortti
http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/faq/PKI.htm#toimikortti
[viitattu 29.1.2005]

6 Certificate Services
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/Resources/Documentation/windowsserv/2003/all/techref/en-us/w2k3tr_crtsv_what.asp [viitattu 29.1.2005]

7 eToken
http://www.aladdin.com/etoken/default.asp [viitattu 29.1.2005]

8 Sormenjälkitoimikortinlukijat
http://www.precisebiometrics.com/products.asp?GROUPID=20020627_135857_50337051 [viitattu 29.1.2005]

9 PKI
http://www.yliopistojentt.fi/VAHTI-CD/Sivusto/faq/PKI.htm#PKI
[viitattu 13.2.2005]

10 Varmenne
http://www.csc.fi/suomi/funet/middleware/projektit/hstya/muut/lisuri.pdf
[viitattu 21.3.2005]