LAUREA

Henkilön sähköinen identiteetti

Pöysti, Tero

2009 Kerava

Laurea-ammattikorkeakoulu
Laurea Kerava

Henkilön sähköinen identiteetti

Tero Pöysti
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2009

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Kerava
Tietojenkäsittelyn koulutusohjelma
Digitaalinen media

Tero Pöysti

Henkilön sähköinen identiteetti

Vuosi 2009 Sivumäärä 50

Tämän opinnäytetyön aihe on henkilön sähköinen identiteetti. Aihetta käsitellään Finaviassa käynnissä olevan, useita eri aliprojekteja käsittävän henkilöstön sähköisen identiteetin hallintaan liittyvän projektikokonaisuuden näkökulmasta. Tämän laajan hankekokonaisuuden sisältämistä projekteista tässä opinnäytetyössä keskitytään kuvaamaan Finavian myöntämien henkilökorttien uusimiseksi käynnistetyn Monitoiminnallinen sähköinen henkilökortti (Moto) -projektin tavoitteita, toteutusta ja lopputulosta. Opinnäytetyössä syvennytään projektin kuvaamisen lisäksi myös älykorttien tekniikkaan, käyttökohteisiin sekä älykortin käyttöön liittyvään problematiikkaan.

Älykorttitekniikan lisäksi olennainen osa opinnäytetyötä on tutustuminen julkisen avaimen tekniikkaan (PKI). Opinnäytetyössä perehdytään myös julkisen avaimen tekniikkaan perustuvan älykorttijärjestelmän käyttöönottoon kuuluviin varmenteiden tietosisältöä ja käyttöä sekä varmenteiden myöntämiseen ja käsittelyyn liittyviä toimintatapoja kuvaaviin dokumentteihin, jotka ovat tärkeä osa julkisen avaimen järjestelmän käyttöönottoa. Finavialla käyttöön otetun sähköisen henkilökortin elinkaareen ja hallinnointiin liittyvät käytännön prosessit ja niihin liittyvää problematiikka käydään opinnäytetyössä läpi seikkaperäisesti.

Älykortteihin liittyvien asioiden lisäksi opinnäytetyössä tutustutaan laajemmin henkilön sähköiseen identiteettiin liittyviin kysymyksiin. Henkilön sähköisen identiteetin hallinnan haasteet yritysten tietojärjestelmissä ovat nousseet viime vuosina voimakkaasti esiin. Henkilön sähköisen identiteetin hallintaan liittyy suuria haasteita, joiden kuvaamiseen ja niiden haasteisiin liittyvien ratkaisujen löytymiseen perehdytään osana opinnäytetyötä.

Opinnäytetyön perustana olevan projektin tarkoituksena on toteuttaa Finavian myöntämien henkilökorttien uusintaprojekti. Uusien henkilökorttien myötä tulee Finavian ylläpitämillä lentoasemilla työskenteleville henkilöille käyttöön PKI järjestelmään perustuva sähköisen asioinnin mahdollistava henkilökortti. Henkilökortin PKI toiminnallisuus mahdollistaa kirjautumisen tietoverkkoon, sähköisen allekirjoituksen sekä sähköpostiviestien salaamisen. Kortin RFID ominaisuutta käytetään kulunvalvontaan. Kortin käyttöönoton lisäksi Finavialla käynnissä oleva hankekokonaisuus sisältää useita aliprojekteja, joiden tavoitteena on parantaa henkilön sähköisen identiteetin hallintaa yrityksen tietojärjestelmissä. Opinnäytetyön tuloksena syntyy kuvaus Monitoiminnallinen sähköinen henkilökortti -projektin tavoitteista, toteutuksesta ja lopputuloksesta, yhdistettynä älykorttien, julkisen avaimen järjestelmän ja henkilön sähköisen identiteetin muodostamaan aihekokonaisuuteen.

Asiasanat: identiteetti, PKI, varmenne, älykortti

Laurea University of Applied Sciences
Laurea Kerava
Degree Programme in Information Technology
Digital Media

Abstract

Tero Pöysti

Person's digital identity

Year 2009 Pages 50

The aim of this bachelor's thesis is person's digital identity. The case will be approached in this thesis via Finavia´s project whose main goal is to manage employees' digital identity. This larger project combination contains many smaller projects. From those projects this thesis is focused on Finavia's multifunctional digital identity card project. The project's main goal is to implement new multifunctional digital id cards to all employees who work at Finavia's airports. The thesis will also focus on smart card technology, usage targets and problems that can exist when you use smart cards.

Alongside smart card technology, the other main part of this thesis is to introduce Public Key Infrastructure (PKI) technology. The thesis will focus on PKI based smart card implementation procedures that include a lot of documentation. Also Finavia's multifunctional digital identity card life cycle controlling processes and problems that this life cycle managing process could have will be discussed in this thesis.

Alongside the smart card based cases this thesis will also take a wider view to person's digital identity. Person's digital identity managing process is something that many companies have to focus during past few years. Digital identity management has many challenges that this thesis will describe and it will also try to introduce some solutions to how to better manage digital identities.

The thesis' goal is to implement Finavia's identification card renewing project. With this implemented new multifunctional digital identity card, people who work at Finavia's airports will have this new identification card that is based on PKI technology. Id card PKI functionality will allow logging on to network, making digital signatures and email ciphering. Id card RFID functionality will be used the in access control system. The Id card project is a part of a bigger project whose main goal is to make users digital identity managing process in Finavia's network better. The thesis' goal is to describe a/the multifunctional digital identity card project, its objectives, implementation and results combined with the concepts of smart card, public key infrastructure and person's digital identity based complexity.

Key words: certificate, identity, PKI, smart card

Sisällys

1 OPINNÄYTETYÖN LÄHTÖKOHTA

1.1 Opinnäytetyön tausta ja tavoitteet

Opinnäytetyön tavoitteena on kuvata Finavian 25 lentoasemalla käyttöön otetun, lentoasemilla työskentelevän henkilöstön henkilökorttina toimivan sähköisen henkilökortin käyttöönottoa valmistellutta ja toteuttanutta Monitoiminnallinen sähköinen henkilökortti (Moto) -projektia. Henkilökorttiprojektin kuvaamisen lisäksi opinnäytetyössä tutustutaan julkisen avaimen järjestelmään (PKI, Public Key Infrastructure) sekä älykorttien yleisiin toimintaperiaatteisiin ja älykorttien käyttökohteisiin. Opinnäyteyössä luodaan myös laajempi näkemys siihen, mitä henkilön sähköinen identiteetti tarkoittaa sekä käydään läpi Finavialla käynnistettyä projektikokonaisuutta, jonka tavoitteena on parantaa henkilöstön sähköisen identiteetin hallintaa. Opinnäytetyössä käsiteltävä projekti on kotimaan mittakaavassa laaja älykorttien käyttöönottoprojekti. Projektin tavoitteena on uusia Finavian myöntämät henkilökortit, joita on käytössä yli 20000 henkilöllä Finavian isännöimillä lentoasemilla ympäri Suomen. Opinnäytetyössä kuvataan tämän projektin tavoitteita, toteutusta ja lopputulosta.

1.2 Opinnäytetyön rajaukset

Opinnäytetyössä henkilön sähköistä identiteettiä käsitellään henkilöstön sähköisen identiteetin- ja turvallisuudenhallintaan liittyvän prosessikokonaisuuden näkökulmasta. Tämän laajan hankekokonaisuuden sisältämistä projekteista opinnäytetyössä keskitytään kuvaamaan Finavian henkilökorttien uusimiseksi käynnistetyn Monitoiminnallinen sähköinen henkilökortti (Moto) -projektin tavoitteita, toteutusta ja lopputulosta. Henkilökorttiprojektia lähestytään sen teknisten ja toiminnallisten määrittelyjen kautta. Samalla pyritään luomaan kuva siitä mitä haasteita älykortin käyttöönotto organisaatiolle tuo eteen. Lisäksi opinnäytetyössä syvennytään julkisen avaimen järjestelmään (PKI) sekä sähköisten älykorttien tekniikkaan, käyttökohteisiin sekä älykortin käyttöön liittyvään problematiikkaan. Jotta opinnäytetyön kohteeksi valittuihin aiheisiin pystyttäisiin keskittymään riittävän syvällisesti, ei muita Finavian hankekokonaisuuden projekteja käsitellä opinnäytetyössä kuin pintapuolisesti.

1.3 Finavia pähkinänkuoressa

Opinnäytetyössä käsiteltävän aihepiirin pohjustukseksi esitellään seuraavissa kappaleissa lyhyesti Ilmailulaitos - Finaviaa. Pohjustuksen tarkoituksena on muodostaa käsitys siitä kuinka kriittisessä toimintaympäristössä Finavialla toimitaan ja kuinka tärkeää koko Finavian olemassaololle on turvallisuusasioiden ottaminen huomioon sen kaikessa toiminnassa. Asia käy ilmi jo tarkastellessa Finavian arvoja, joita ovat turvallisuus, asiakashyöty, tehokkuus- ja muuntautumiskyky sekä yhteistyö.

Ilmailulaitos - Finavia on valtion liikelaitos, joka ylläpitää 25 lentoaseman lentoasemaverkkoa ympäri Suomen. Finavia tarjoaa turvallisia ja kansainvälisesti kilpailukykyisiä lentoasema- ja lennonvarmistuspalveluja lentomatkustajille, lentoyhtiöille, sotilasilmailulle, elinkeinoelämälle ja koko suomalaiselle yhteiskunnalle. Finavia vastaa lentoasemiensa kunnossapidosta ja huolehtii matkustajien opastamisesta sekä terminaalirakennusten siisteydestä, viihtyisyydestä ja helppokulkuisuudesta. Lisäksi Finavia hoitaa lentoasemilla matkustajien, käsimatkatavaran sekä ruumaan menevän matkatavaran turvatarkastukset. Turvatarkastuksia tekee joko Finavian oma, tehtävään koulutettu henkilökunta tai ulkopuolinen turvapalveluyritys. (Finavia 2008.)

Finavian koko maan kattavat lennonvarmistuspalvelut takaavat turvallisen ja viiveettömän lentoliikenteen Suomessa. Lentoasemilla lähestymislennonjohto johtaa lähtevää konetta ja järjestää laskeutuvat koneet ilmatilassa turvamääräysten mukaisesti. Lähilennonjohto johtaa lentoliikennettä lentoasemien lähialueilla sekä maaliikennettä kenttäalueella. Aluelennonjohto puolestaan johtaa lentoreiteillä tapahtuvaa ilmaliikennettä. (Finavia 2008.)

Finavia vastaa lentoasemien pysäköintipalveluista ja luo edellytykset ulkopuolisten yrittäjien joukkoliikenne- ja autonvuokrauspalveluille. Kahvilat, ravintolat ja lentoasemien kaupat kuuluvat Finavian järjestämiin palveluihin, vaikka niiden käytännön toteutuksesta vastaavat pääsääntöisesti ulkopuoliset yrittäjät. Finavian palveluksessa työskentelee noin 1800 työntekijää, sekä Finavia konserniin kuuluvissa tytäryhtiöissä, joita ovat esimerkiksi Airpro Oy sekä Lentoasemakiinteistöt Oy noin 700 työntekijää. Kaiken kaikkiaan Finavian lentoasemilla toimivien yritysten ja niiden yhteistyökumppaneiden henkilöstön käytössä on yli 20000 Finavian myöntämää henkilökorttia. (Finavia 2008.)

2 JOHDANTO

Perinteinen käyttäjätunnukseen ja salasanaan perustuva tunnistautuminen tietojärjestelmiin ei enää pysty vastaamaan nykypäivän tietojärjestelmille ja niiden tietoturvalle sekä käytettävyydelle asetettuihin vaatimuksiin. Salasana voi olla niin helppo että se on voidaan arvata, tai jos se on riittävän vaikea tulee se helposti kirjoitettua ylös paperilapulle (Linden 2002, 5).

Tietoverkon resursseja käyttävän henkilön identiteetin kiistaton tunnistaminen on ensisijaisen tärkeää. Tämä korostuu varsinkin kriittisissä yritysympäristöissä, jolloin koko yrityksen toiminta on usein riippuvainen sen tietojärjestelmien toiminnasta. Tietojärjestelmien käyttäjien identiteetin aukottoman tunnistamisen lisäksi pitäisi käyttäjien sähköisen identiteetin tunnistamisen päämääränä ehdottomasti olla myös käyttäjäystävällisyys. Tunnistautumisen tietojärjestelmiin pitäisi olla niiden käyttäjille mahdollisimman läpinäkyvää ja helppoa. Tunnistau-

tumisen tietojärjestelmiin pitäisi kuitenkin samalla kyetä täyttämään järjestelmien tietoturvallisuudelle asettavat vaatimukset. Käyttäjätunnukseen ja salasanaan perustuvalla tunnistautumisella tietojärjestelmiin ei pystytä enää vastaamaan edellä mainittuihin haasteisiin.

Yrityksen sisältä käyttäjän tunnistamiseen kohdistuvien vaatimusten lisäksi yrityksille asetetaan nykyisin usein myös ulkopuolelta tulevia vaatimuksia käyttäjien vahvaan tunnistamiseen. Näitä vaatimuksia kohdistuu yrityksiin myös useiden standardien suunnalta (esim. ISO27001, PCI DSS). Edellä mainittujen tekijöiden lisäksi suureksi ongelmaksi on nykyisin noussut samojen käyttäjätunnusten sekä salasanojen käyttäminen useissa eri verkkopalveluissa. Yrityksen sisäisissä järjestelmissä tätä ei välttämättä koeta ongelmaksi, mutta jos työntekijät käyttävät samaa käyttäjätunnusta ja salasanaa, jolla he tunnistautuvat yrityksen sisäiseen tietoverkkoon myös internetin julkisissa palveluissa, on tilanne yrityksen tietoturvan kannalta varsin ongelmallinen. Vaikka työpaikan verkkotunnuksen ja salasanan käyttäminen organisaation ulkopuolisiin palveluihin käyttäjäksi rekisteröidyttäessä on varmasti useimpien organisaatioiden tietoturvaohjeissa kielletty, ei niiden käyttämistä ulkopuolisissa palveluissa voida käytännössä valvoa tai estää.

Yksi suuri henkilön sähköiseen identiteettiin liittyvä ongelma yrityksissä on tietojärjestelmien käyttäjätietojen ajantasaisuus ja työntekijöiden käyttöoikeuksien tarkoituksenmukaisuus. Miten voidaan varmistua siitä, että tieto työntekijän työsuhteessa tapahtuvista muutoksista saadaan välitettyä heti muutoksen tapahduttua hänen sähköiseen identiteettiinsä? Varsinkin kun käyttäjän sähköinen identiteetti on yrityksissä usein pirstoutunut useisiin erillisiin käyttäjätietovarastoihin, joihin taas useimmiten puuttuu koko yrityksen kattava yhtenäinen näkymä. Haasteita on myös siinä, miten varmistaa että työntekijällä on kulloinkin pääsy vain niihin tietoihin ja järjestelmiin, joita hänen työtehtävänsä hoitaminen edellyttää. Jatkuvasti kasvava tarve yritysten operatiivisten järjestelmien avaamiseen kumppanien tai viranomaisten käyttöön asettaa oman haasteensa henkilön sähköisen identiteetin elinkaaren hallinnalle.

Edellä mainittujen ongelmien ratkaisemiseen yksi olemassa oleva ratkaisu on sähköisen, julkisen avaimen järjestelmään pohjautuvan älykortin käyttäminen tietojärjestelmiin tunnistautumiseen. Sähköinen henkilökortti yhdessä Single Sign-On (kertakirjautuminen) -järjestelmän käytön sekä keskitetyn tietojärjestelmien identiteetin- ja pääsynhallintaratkaisun kanssa antaa tietoverkon käyttäjille mahdollisuuden tunnistautua yrityksen tietojärjestelmiin käyttämällä tunnistautumiseen henkilön sähköisen identiteetin sisältämää sähköistä älykorttia.

Käyttämällä edellä mainittuja teknisiä ratkaisuja, voidaan älykortille tunnistautumiseen vaaditun PIN-luvun avulla käyttää älykortin sisältämää henkilön sähköistä identiteettiä tunnistautumiseen jopa kymmeniin tietojärjestelmiin. Samalla voidaan poistaa suuri osa edellisissä kappaleissa kuvatuista käyttäjätunnuksiin ja salasanoihin liittyvistä ongelmista.

Älykortin käyttämisen hyvä puoli on se että kortti tai sen PIN-koodit eivät yksinään mahdollista haltijaansa tunnistautumista tietojärjestelmään. Vaikka toinen niistä häviäisi tai joutuisi ulkopuolisen tietoon, ei siitä synny vakavaa ongelmaa. Vasta kun ulkopuolinen taho on saanut niistä molemmat haltuunsa, voi niiden avulla varastaa kortin haltijan sähköisen identiteetin. Jos kortille tunnistautumiseen vaaditaan PIN-luvun sijasta esimerkiksi biometristä tunnistautumista, on älykortin haltijan sähköisen identiteetin suoja sekä kortin käytettävyys vieläkin parempi. Huonona puolena tässä järjestelmässä voidaan pitää kaiken tunnistautumiseen liittyvä toiminnallisuuden keskittämistä älykortin sisältämään identiteettiin, jolloin kortti voi väärinkäyttötilanteissa antaa haltijalleen pääsyn kaikkiin tietojärjestelmiin joihin sen avulla on mahdollisuus tunnistautua.

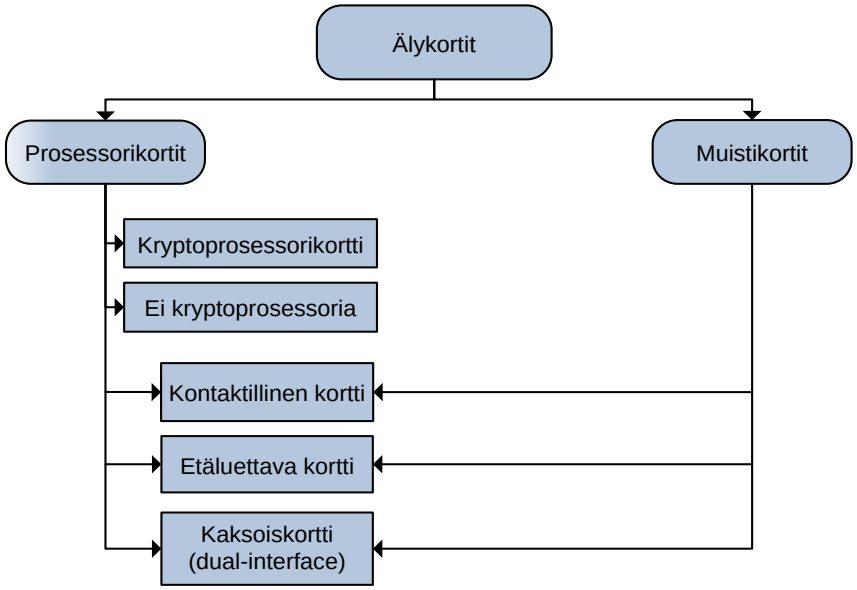
3 ÄLYKORTTI

Älykortti, jota kutsutaan myös nimillä toimikortti, sirukortti tai suoritinkortti (smart card, chip card, integrated circuit card) on useimmiten luottokortin mallinen ja kokoinen muovikortti, johon on upotettu pieni mikropiiri eli siru. Sirun tehtävänä on huolehtia tiedon tallentamisesta ja erilaisten operaatioiden suorittamisesta. Älykortti voi myös olla vain muistia sisältävällä mikropiirillä varustettu muistikortti, kuten esimerkiksi puhelinkortti jolle voi ladata puheaikaa. Älykortti voi olla fyysiseltä kooltaan luottokortin kokoinen ID-1 älykortti tai pienempi ID-000 sirukortti, joka on laajasti käytössä esimerkiksi matkapuhelimien SIM (subscriber identity module) korttina.

3.1 Älykorttien luokittelu

Älykortit voidaan jakaa ominaisuuksiensa mukaisesti karkeasti kahteen eri pääluokkaan: prosessorikortteihin ja muistikortteihin. Älykortteja voidaan jaotella myös niiden käyttämän tiedonsiirtotien mukaisesti kontaktillisiin ja etäluettaviin älykortteihin, sekä nämä molemmat tiedonsiirtotiet yhdistävään kaksoiskorttiin, joka toimii sekä kontaktillisen että etäluettavan rajapinnan kautta. Apuprosessorilla varustetut prosessorikortit muodostavat vielä oman korttiluokkansa. Apuprosessoreista yleisin on kryptoprosessori, jonka tehtävänä on hoitaa epäsymmetristen salausalgoritmien sisältämien funktioiden laskentaa. (Rinne 2002, 14.)

Edellä mainittujen tekijöiden lisäksi yhtenä älykorttien luokitteluperusteena on käytetty niiden käyttöjärjestelmiä, joiden perusteella älykortit voidaan jakaa älykorttivalmistajien omiin valmistajakohtaisiin natiivikäyttöjärjestelmiin ja avoimiin käyttöjärjestelmiin. Kuvassa 1 esitellään muisti- ja prosessikorttiin liittyvä älykorttien luokittelu ja joukko erilaisia älykorttityyppejä.



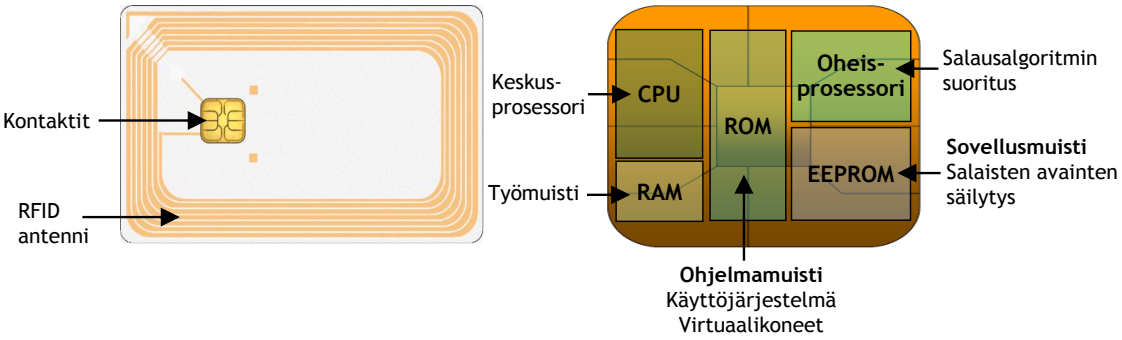
Kuva 1. Älykorttien luokittelu (Rinne 2002, 14).

3.2 Älykorttien tekniikka

Älykorttien muovirunko on valmistettu kestävästä muovista, yleensä joko PVC- tai polykarbonaatista. Älykortin muovirunkoon sijoitetun älykorttipiirin kaksi tärkeintä komponenttia ovat keskusprosessori (CPU) ja muistialueet. Kortilla on lisäksi yksinkertainen I/O-väylä, jonka kautta kortti kommunikoi päätteen kanssa. Älykortin I/O-väylä on käytännössä pelkkä osoite, johon prosessori osaa ohjata kortin ulkoisen tietoliikenteen. Piirille on monesti lisätty useita lisäkomponentteja, joiden tarkoituksena on parantaa jonkin tietyn osa-alueen suorituskykyä (esimerkiksi salausalgoritmien suorittamiseen tarkoitettu kryptoprosessori tai satunnaislukujen autentikointiin ja salausavaimien generointiin tarkoitettu RNG-prosessori). (Rinne 2002, 27.)

Kontaktittoman RFID (Radio frequency identification) älykortin, sekä kontaktillisen että kontaktittoman siirtotien sisältävän kaksoiskortin korttirungon sisään on laminoitu RF-antenni (kuva 2), joka on liitetty älykortilla sijaitsevaan mikrosiruun. Mikrosiru on kiinnitetty korttiaihioon valmistusvaiheessa sirua varten työstettyyn aukkoon.

Älykorttien käyttöä rajoitti aiemmin eniten niiden sisältämän haihtumattoman EEPROM muistin pieni määrä. Muistin määrän kasvamisen on jokainen meistä voinut havaita esimerkiksi matkapuhelinten SIM-korttien tallennuskapasiteetin kasvuna. Nykyisin älykorttien muistikapasiteetti on kasvanut jo niin suureksi, että kortille voidaan sijoittaa useita sovelluksia sekä vaikkapa biometrisessa tunnistamisessa käytettäviä tietoja, kuten kasvokuva tai sormenjälki. Nykyisin yleisimmin käytössä olevat älykortit sisältävät EEPROM muistia 32–72 kilotavua.



Kuva 2. Älykortin rakenne.

3.3 Älykorttien käyttöjärjestelmät

Älykortin laitteiston ja sovellusten ohjaamiseen tarvitaan käyttöjärjestelmä. Älykortin ja sen sirun fyysinen koko ja rajallinen muistikapasiteetti määräävät hyvin vahvasti sen, että älykorttien käyttöjärjestelmän on oltava toteutukseltaan varsin yksinkertainen. Yksinkertaisuudesta on myös hyötyä, koska käyttöjärjestelmän yksinkertainen rakenne tekee älykortista vähemmän alttiin tietoturvauhille.

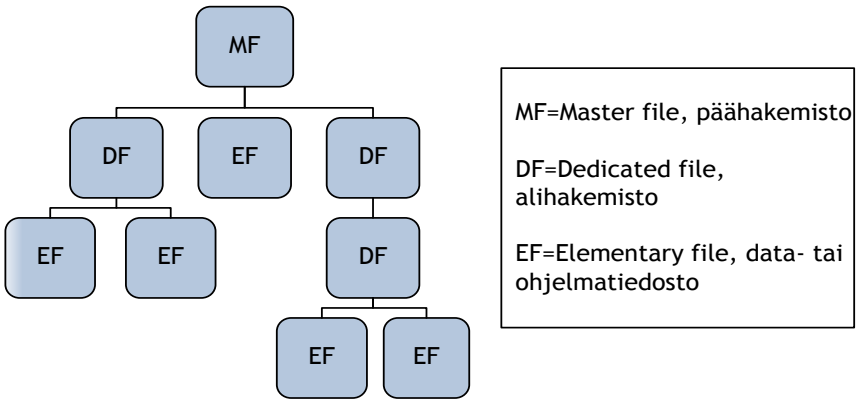
Älykorttien käyttöjärjestelmät on suunniteltu lähinnä I/O-portin näkökulmasta. Älykorttien käyttöjärjestelmien tärkeimmät tehtävät ovat komentojen ja tiedostojen hallinta, datan siirto kortin ja kortin ulkopuolisen sovelluksen välillä sekä kryptografisten funktioiden toteutus. Poikkeustilanteiden käsittely ja tietoturvallisuus vaativat käyttöjärjestelmältä paljon. Käyttöjärjestelmän koodin on oltava virheetöntä. Jos kortin käyttöjärjestelmästä löytyy ongelmia, niiden korjaaminen ei onnistu helposti päivittämällä käyttöjärjestelmää, kuten esim. PC-koneiden käyttöjärjestelmien kohdalla jatkuvasti tehdään. Älykortin sovellusten suojaus on toteutettu siten, etteivät sovelluksen pääse vahingossa tai ettei niiden kautta ole mahdollista päästä tarkoituksella vaikuttamaan haitallisesti toisten sovellusten toimintaan. (Rinne 2002, 41.)

Älykorttien käyttöjärjestelmät ovat aiemmin yleisesti olleet korttien valmistajakohtaisia natiivikäyttöjärjestelmiä, kuten esimerkiksi SetCOS, CardOS, MPCOS. Tästä on seurannut se, että niille tehdyt sovellukset ovat toimineet ainoastaan kyseisen käyttöjärjestelmän kanssa. Älykorttisovellusten yhteensopivuusongelman poistamiseksi on tapahtunut edistystä niin kutsuttujen avointen käyttöjärjestelmien myötä. (Rinne 2002, 42.) Avointen käyttöjärjestelmien tavoite on mahdollistaa käyttöjärjestelmästä riippumaton sovelluskehitys älykorteille. Avoimista käyttöjärjestelmistä esimerkkeinä ovat Basic Card, Java Card,Linux, Multos sekä Windows for Smart Cards.

3.4 Älykorttien standardit

3.4.1 ISO 7816

Kontaktillisten älykorttien tiedostojärjestelmät on kehitetty pääosin ISO 7816 –standardiperheeseen perustuen. ISO 7816 -standardiperheen eri osat määrittelevät esimerkiksi kortin fyysisiä- ja sähköisiä ominaisuuksia, älykortin ja kortinlukijan välistä sovellusprotokollaa sekä älykortilta ulospäin näkyvää kortin sisäistä rakennetta. Lisäksi ISO 7816 -standardiperheessä määritellään älykortin biometristen menetelmien käyttöä kortinhaltijan henkilöllisyyden todentamisessa, standardeja tietorakenteita sekä älykorttisovellusten nimeämistä yksiselitteisellä tavalla. Kaikkiaan ISO 7816 –standardiperhe sisältää tällä hetkellä osat 1-15.



Kuva 3. ISO 7816-4 –standardin mukainen älykortin tiedostohierarkia.

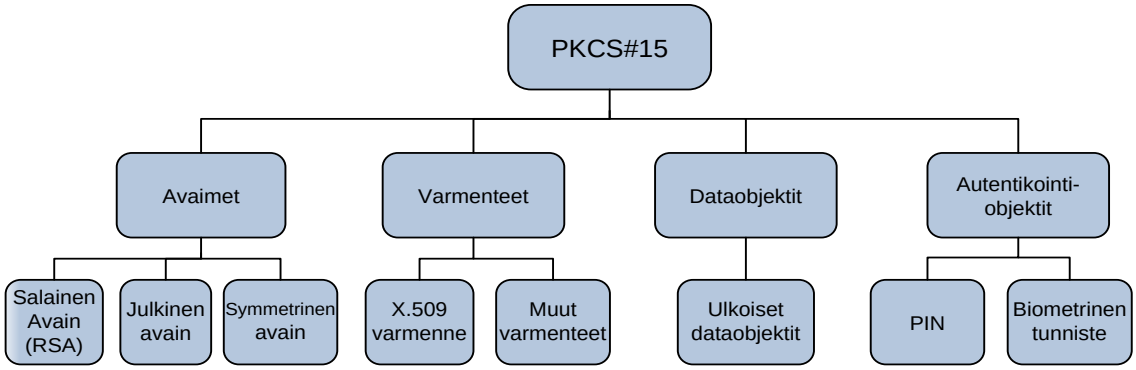
3.4.2 PKCS#15

Toinen älykorttien yhteydessä usein esiin tuleva standardiperhe on amerikkalaisen RSA:n kehittämä PKCS -standardiperhe (Public Key Cryptography Standard), joka määrittelee RSA-algoritmin lisäksi muun muassa digitaalisen allekirjoituksen ja erilaisten varmennesanomien formaatteja. PKCS standardiperhe sai alkunsa vuonna 1998 kun RSA esitteli sen perusteet julkaisemassaan dokumentissa Cryptographic Token Information Format Standard (Rankl & Effing 2006, 833).

PKCS-dokumentit on numeroitu yhdestä viiteentoista ja niistä viimeinen, eli PKCS#15, virallisselta nimeltään Information for Cryptographic Tokens määrittelee nimensä mukaisesti kryptografisiin operaatioihin käytettyjen avaimien ja niihin liittyvien varmenteiden talletusformaatin. PKCS#15 sisältää neljä objektiluokkaa: avaimet, varmenteet, datatiedostot ja tunnistusobjektit. Lisäksi PKCS#15 sisältää suositukset objektien käyttötapauksille ja käyttöoikeuksille. PKCS#15 on mahdollistanut yhdenmukaisen ja valmistajasta riippumattoman tavan käsi-

tellä älykortille talletettuja avaimia ja varmenteita, sekä esittelee älykorttien yhteydessä laajasti käytetyn tiedostorakennemallin (kuva 4).

PKCS#15-määrittelyä on käytetty laajasti sähköiseen tunnistamiseen ja sähköiseen allekirjoitukseen tarkoitetuilla älykorteilla. Suomalaisille erityisen läheiseksi PKCS#15-standardiperheen tekee sen käyttäminen HST-hankkeessa (henkilön sähköinen tunnistaminen). HST-hankkeessa käytetty FINEID-määrittely on suomalainen versio PKCS#15 standardista. (Rinne 2002, 38.)



Kuva 4. PKCS#15 mukainen älykortin objektihierarkia.

3.5 Älykortin edut, käyttökohteet ja turvallisuus

Älykorttien käyttö tarjoaa useita etuja verrattaessa sitä perinteiseen käyttäjätunnukseen ja salasanaan perustuvaan tietojärjestelmiin tunnistautumiseen. Älykortin käyttäminen pystyy tarjoamaan korkeaa tietoturvaa vaativille järjestelmille etuja, joita ei muuten voida saavuttaa. Edut perustuvat älykortin käytön kohdalla erityisesti kolmeen älykortin ominaisuuteen jotka ovat:

- Älykortin hyvä fyysinen tietoturva.
- Älykortin pieni koko.
- Älykortin sisäinen laskentakapasiteetti ja muisti.

Nämä ominaisuudet mahdollistavat osaltaan älykorttien tietoturvallisen, joustavan ja monipuolisen käytön erilaisiin käyttötarkoituksiin. Älykortteja onkin näiden ominaisuuksiensa vuoksi käytetty erilaisina kannettavina tietoturvavälineinä. Älykortin kiistattomiin etuihin kuuluu mahdollisuus tallettaa salausavaimet siten, että avaimet ovat kätevässä koossa omistajansa mukana. Lisäksi avainten talletusalustana älykortti on sellainen, etteivät ulkopuoliset pääse käyttämään avaimia luvatta hyväkseen. (Rinne 2002, 59.)

Salausavaimia käytetään lähes kaikilla älykortin sovellusalueilla. Tietoturvallisuuden kannalta tunnetuin sovellus on datan salakirjoittaminen. Älykorttia voidaan käyttää vaikkapa tiedostojen, sähköpostiviestien tai tietoliikenteen salaamiseen. Toinen tunnettu tietoturvallisuuden sovellusalue älykorteilla on digitaalinen allekirjoitus, jota käyttämällä voidaan varmistua sähköisesti allekirjoitetun datan eheydestä ja sen alkuperästä. Älykortin sovellusalueista tärkeitä tietoturvan kannalta ovat myös erilaiset maksusovellukset, joiden luotettava turvaaminen on erittäin tärkeää. Edellä mainittujen kohteiden lisäksi älykortteja käytetään hyväksi myös lukumääräisesti suurimpana käyttökohteena olevassa matkapuhelinten SIM-korteissa, maksu-tv:n sovelluksissa ja erilaisissa yritysten kanta-asiakas kortteihin perustuvissa sovelluksissa.

3.6 Älykortti osana tietoturvallisuutta

Älykortilla voidaan toteuttaa useita tietoturvallisuuden peruspalveluja. Seuraavaksi on listattu tietoturvallisuuden peruspalveluja, joiden asettamiin haasteisiin voidaan vastata käyttämällä älykorttia osana tietoturvaratkaisuja.

Luottamuksellisuus

- Käytetään älykortin tarjoamia salausmenetelmiä tiedon luottamuksellisuuden turvaamiseen

Eheys

- Älykortin avulla voidaan tehdä sähköinen allekirjoitus, jonka avulla voidaan varmistua esim. sähköpostiviestin eheydestä. Toisin sanoen voidaan olla varmoja siitä, ettei viestin sisältämä data ole muuttunut sen lähettäjän allekirjoitettua viestin sähköisellä allekirjoituksella.

Kiistämättömyys

- Älykortin mahdollistaman sähköisen allekirjoituksen käyttö kiistämättömyysperiaatteen mukaisesti erilaisissa sähköistä allekirjoitusta hyväksi käyttävissä järjestelmissä, kuten esim. sähköiset lomakejärjestelmät ja sähköposti.

Saatavuus

- Älykortin helppo kuljetettavuus ja käyttö esim. yritysten henkilökorttina erilaisiin käyttötarkoituksiin. Älykortti on helppo ja usein jopa pakko pitää aina mukana.

Autentikointi

- Älykortti mahdollistaa haltijansa vahvan tunnistautumisen tietojärjestelmiin.

Autorisointi

- Älykorttia käytetään autorisointiin useimmiten autentikointivaiheessa vahvan tunnistautumisen kautta.

Älykortin käyttäjä on kortin turvallisuuden kannalta kaikkein keskeisimmässä asemassa. Käyttäjän on huolehdittava kortin fyysisestä turvallisuudesta sekä pidettävä kortin PIN-luvut salassa. Kun älykortti on luovutettu turvallisesti kortin oikealle omistajalle, siirtyy vastuu kortin käytöstä kortinhaltijalle. (Rinne 2002, 67.)

Kortin väärinkäyttömahdollisuudet riippuvat siihen liitettyjen sovelluksista. Tavanomaisia väärinkäytön mahdollistavia sovelluksia ovat mm. kulunvalvonta, tunnistautuminen tietoverkkoon, salaustekniikat ja tietojen sähköinen allekirjoittaminen sekä erilaiset maksusovellukset. Kortin haltija on vastuussa kortin väärinkäytöstä ja voi joutua vahingonkorvausvastuuseen kortilla tehdyistä väärinkäytöksistä.

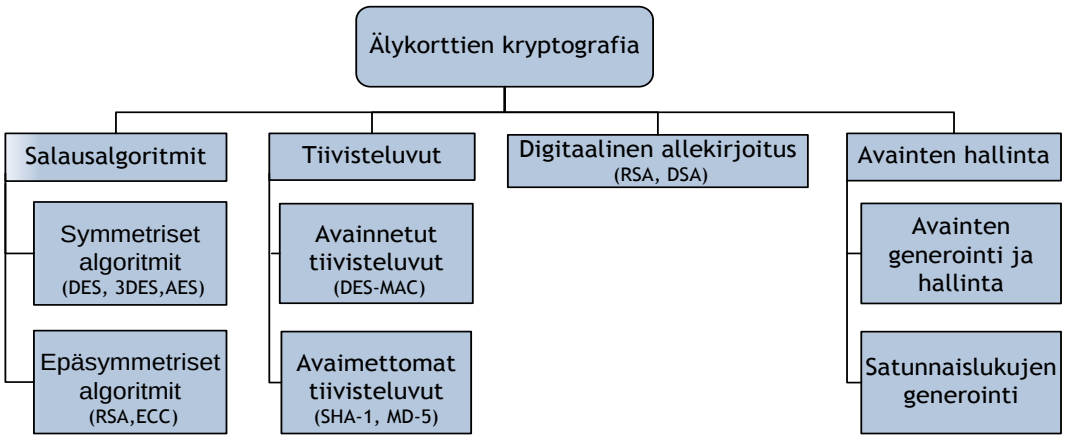
Käytännössä esimerkiksi PIN-koodin tai biometrisen tunnisteen käyttäminen kortille sijoitettujen varmenteiden kanssa tarkoittaa, että voidakseen suorittaa varmenteen käyttöä vaativan operaation on kortin haltijan todennettava identiteettinsä kortille PIN-koodin tai biometrisen tunnistautumisen avulla. Vasta onnistuneen tunnistautumisen avulla kortin käyttäjä pääsee käyttämään varmenteen sisältävää objektia kortin tiedostojärjestelmässä.

4 ÄLYKORTTIEN KRYPTOGRAFIA

Älykorttien toinen päätehtävä kannettavan datan säilytyspaikan ohella on kryptografisten funktioiden eli salakirjoitusmenetelmien mahdollistaminen erilaisissa sovelluksissa. Älykortilla käytetyistä sovelluksista keskeisimpiä ovat digitaaliset allekirjoitukset, datan salaaminen, sähköinen tunnistautuminen sekä maksukorttisovellukset (Rinne 2002, 74.) Tietoliikenteen salaaminen älykortin ja sitä käyttävän sovelluksen välillä onkin olennainen osa älykorttien kryptografiaa ja kokonaistoiminnallisuutta.

Älykorttien näkökulmasta kryptografia voidaan jakaa karkeasti kolmeen osa-alueeseen, jotka esitellään tarkemmin kuvassa 5:

- Salausalgoritmit.
- Tiivistefunktiot ja digitaalinen allekirjoitus.
- Satunnaislukujen ja avainten generointi sekä hallinta.



Kuva 5. Älykorttien kryptografian osa-alueet.

4.1 Symmetrinen salaus

Symmetrisen kryptografian perusominaisuus on se, että datan salaaminen tapahtuu samalla avaimella kuin salauksen purkaminen. Tästä johtuen avaimen tulee olla vain salaajan ja avaajan hallussa, eli salainen. Menetelmän koko turvallisuus perustuu avaimen pitämiseen salassa. (Rinne 2002, 76.)

Symmetrisen salauksen käyttämisessä oleva vaatimus käytettävien salausavaimien salassapidosta tekee siitä käytännössä hyvin epäkäytännöllisen salaustavan. Jotta avain voidaan siirtää turvallisesti henkilöltä toiselle, on se toimitettava henkilökohtaisesti kaikille niille henkilöille, joiden kanssa halutaan käydä salattua viestinvaihtoa. Lisäksi yhdenkin avaimen joutuminen vääriin käsiin johtaa siihen että uusi avain on taas toimitettava kaikille osapuolille. Toinen vaihtoehto on toki käyttää omaa avainta jokaisen henkilön kohdalla, mutta tämäkin vaihtoehto osoittautuu hyvin nopeasti epäkäytännölliseksi, koska avainten määrän kasvaessa avainhallinta muuttuu pian mahdottomaksi.

Etuina symmetrisillä salausalgoritmeilla ovat nopeus ja niiden kyky pystyä salaamaan suuria datamääriä kerralla. Suorituskyky ja nopeus ovat tärkeitä osatekijöitä etenkin tietoliikenteessä, jossa juuri symmetriset salausalgoritmit ovat parhaimmillaan. (Rinne 2002, 76.)

Symmetrinen salausmenetelmä: salaukseen ja avaukseen käytetään samaa salausavainta

Kuva 6. Symmetrisen salausmenetelmän periaate.

4.2 Epäsymmetrinen salaus

Epäsymmetristen salausalgoritmien kehitys sai alkusykäyksensä symmetrisiin salausmenetelmiin liittyvistä avaintenhallintaongelmasta. Epäsymmetrisiä salausalgoritmeja kutsutaan myös julkisen avaimen salausmenetelmäksi. Epäsymmetrisessä salauksessa salaukseen ja salauksen purkamiseen käytetään kahta eri avainta. Toinen avaimista on salainen ja se on pysyttävä vain omistajansa hallussa. Toinen avaimista on julkinen ja sen voi nimensä mukaisesti asettaa julkisesti saataville. Kun lähettäjä haluaa salata vastaanottajalle lähetettävän viestin, hän käyttää salaukseen vastaanottajan julkista avainta. Kun vastaanottaja vastaanottaa lähetetyn viestin, hän käyttää viestin salauksen avaamiseen omaa salaista avaintaan. (Rinne 2002, 80.)

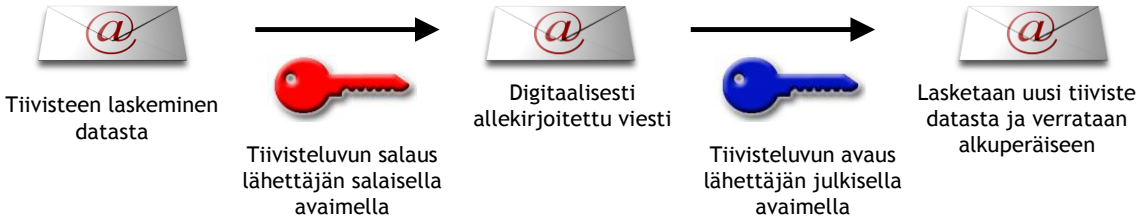
Epäsymmetrinen salausmenetelmä: salaukseen ja avaukseen käytetään eri salausavainta

Kuva 7. Epäsymmetrisen salausmenetelmän periaate.

4.3 Digitaalinen allekirjoitus

Digitaalinen allekirjoitus on yksi epäsymmetristen salausmenetelmien merkittävimpiä käyttökohteita. Digitaaliseen allekirjoitukseen käytetään yleisesti joko RSA- tai DSA-salausalgoritmia tai avainnettuja tiivistealgoritmeja. Älykortilla digitaalinen allekirjoitus toteutetaan usein RSA:lla. (Rinne 2002, 89.)

Digitaalista allekirjoitusta luotaessa allekirjoituksen luonti aloitetaan laskemalla tiivisteluku (SHA-1 tai MD-5) allekirjoitettavasta datasta. Tämän jälkeen digitaalisen allekirjoituksen tekijä salaa tiivisteluvun omalla salaisella avaimellaan. Näin muodostuu digitaalisesti allekirjoitettu viesti. Kun sähköisesti allekirjoitettu data on toimitettu vastaanottajalle , tapahtuu seuraavaa. Vastaanottaja avaa lähettäjän julkisella avaimella tiivisteluvun, laskee itse uuden tiivisteluvun ja vertaa näitä tiivistettä toisiinsa. Jos tiivisteet ovat samanlaiset, digitaalisesti allekirjoitettua dataa ei ole muutettu digitaalisen allekirjoituksen tekemisen jälkeen ja viesti on eheä ja muuttumaton. Jos digitaalinen allekirjoitus on kunnossa, voidaan myös olla varmoja siitä että datan sähköisesti allekirjoittanut taho on allekirjoitukseen käytettyyn julkiseen avaimeen liittyvän salaisen avaimen haltija.



Kuva 8. Digitaalisen allekirjoituksen periaate.

Sähköisen allekirjoituksen juridinen asema on kotimaassa määritelty vuonna 2003 voimaanastuneella lailla sähköisistä allekirjoituksista. Lain tarkoituksena on edistää sähköisten allekirjoitusten käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa sekä sähköisen kaupankäynnin ja sähköisen asioinnin tietosuojaa ja tietoturvaa. Laki sähköisestä allekirjoituksesta mahdollistaa organisaatioiden sisäisen ja ulkoisen sähköisen allekirjoituksen käytön. (Laki sähköisistä allekirjoituksista 2003.)

5 JULKISEN AVAIMEN JÄRJESTELMÄ

Julkisen avaimen järjestelmä (PKI, Public Key Infrastructure) on varmenteiden myöntämisen, jakelun, hallinnoinnin ja ylläpidon muodostama kokonaisuus. Sen tarkoitus on tehdä varmenteiden käytöstä kattavaa, helppoa ja turvallista. (Järvinen 2003, 165.)

Toimiva PKI -järjestelmä ja varsinkin sen suunnittelu ja käyttöönotto ei ole pelkästään tekniikkaa, vaan se sisältää myös merkittävän määrän dokumentaatiota. Dokumentaatioon sisältyy varmenteiden käsittelyä, myöntämistä ja hallinnointia käsitteleviä asiakirjoja, joissa kuvatuilla määrittelyillä rakennetaan pohja toimivalle PKI -infrastruktuurille. PKI -järjestelmän tavoitteena on käsitellä varmenteita koko niiden elinkaaren ajan siten, että varmenteisiin voidaan luottaa kaikissa tilanteissa.

5.1 Varmenteet

Epäsymmetriseen salaukseen perustuvissa salausjärjestelmissä julkisella avaimella ei käytännössä tee mitään, ellei tiedä kenelle tämä kyseinen julkinen varmenne kuuluu. Tämä onkin yksi syistä varmenteiden eli digitaalisten sertifikaattien olemassaololle. Varmenteet liittävät julkisen avaimen ja sen haltijan henkilöllisyyden toisiinsa. Varmenne pitääkin nähdä ennen kaikkea tietorakenteena, joka sisältää julkisen avaimen lisäksi avaimen haltijan nimen, avaimen käyttötarkoituksen, pituuden ja voimassaoloajan sekä muuta tietoa avaimen käytöstä. (Rinne 2002, 90.) Varmenteita voidaan myöntää erilaisiin käyttötarkoituksiin ja erilaisille hal-

tijoille. Varmenteen haltijoita voivat olla esimerkiksi henkilöt, tietokoneet, tietokoneen sisäiset palvelut tai verkkolaitteet.

Varmenteita ja niiden tietosisältöä on standardoitu ITU:n (International Telecommunication Union) X.509-standardissa. X.509-standardista on julkaistu kolme eri versiota, joista vanhin versio 1 julkaistiin jo vuonna 1988, versio 2 vuonna 1993 ja nykyisin laajimmin käytössä oleva versio 3 vuonna 1996. X.509-standardi sisältää pakollisia ja valinnaisia kenttiä sekä laajennuksia, jotka voidaan määritellä kriittisiksi tai ei-kriittisiksi.

X.509 varmenne	v1	v2	v3
Versionumero	X	X	X
Sarjanumero	X	X	X
Allekirjoitusalgoritmi	X	X	X
Myöntäjän nimi	X	X	X
Voimassaoloaika	X	X	X
Kohteen nimi	X	X	X
Kohteen julkinen avain	X	X	X
Myöntäjän yksikäsitteinen nimi		X	X
Kohteen yksikäsitteinen nimi		X	X
Laajennukset			X
Myöntäjän digitaalinen allekirjoitus	X	X	X

Koodattu myöntäjän yksityisellä avaimella

Taulukko 1. X.509-varmenteen tietosisältö.

5.2 Varmennemallit

Varmenteita myönnetään useisiin eri käyttötarkoituksiin. Erilaisten teknisten käyttötarkoitusten (esim. sähköinen allekirjoitus, tunnistautuminen, salaus) lisäksi varmenteita voidaan luokitella myös varmenteen haltijan eri roolien perusteella. Seuraavaksi esitellään lyhyesti muutamia erilaisia varmenteen haltijan rooliin liittyviä varmennemalleja.

<u>Laatuvarmenne</u>

Laatuvarmenteen tulee täyttää sähköisistä allekirjoituksista säädetyssä laissa (7 §, 2. mom.) asetetut vaatimukset. Laatuvarmenteen myöntää lain 10 § - 15 § :ssä säädetyt vaatimukset täyttävä varmentaja. (Laki sähköisistä allekirjoituksista, 2003.)

Palvelinvarmenne

Palvelinvarmennetta käytetään tietojärjestelmän komponenttien aitouden varmistamiseen. Se asennetaan yleensä www-palvelinohjelmiston yhteyteen. ja sitä käytetään useimmiten SSL-protokollan käyttämiseksi yhteyden salauksessa. Palvelinvarmenteen avulla käyttäjä voi myös autentikoida palvelimen. (Kallio 2005, 50.)

Työvarmenne

Työvarmenteilla eli roolivarmenteilla tarkoitetaan organisaation eri asemissa toimiville henkilöille myönnettyjä varmenteita. Työvarmenteen avulla osoitetaan henkilön asema yrityksen tai organisaation laillisena ja toimivaltaisena edustajana. Työvarmenteiden avulla voidaan hallita esimerkiksi organisaation nimenkirjoitusoikeuden käyttöä. (Kallio 2005, 50.)

Henkilövarmenne

Henkilövarmenne sitoo julkisen avaimen haltijansa nimeen. Henkilövarmenteen avulla tietoverkkoon tunnistautuva henkilö tunnistetaan yksilöidysti ja liitetään hänet tämän tiedon perusteella esimerkiksi käyttöoikeudet sisältävään käyttöoikeusryhmään, jonka mukaan määräytyvät henkilölle valtuutetut resurssit. Henkilövarmennetta voidaan käyttää tunnistautumisen ja todentamisen lisäksi myös sähköisiin allekirjoituksiin. (Kallio 2005, 50.)

Rooli- tai attribuuttivarmenne

Henkilövarmenteen käytön vaihtoehtoina voisivat olla rooli- ja attribuuttivarmenteet. Perinteisessä henkilövarmenteessa pääsynvalvonta suorittaa kaksivaiheisen päättelyketjun: julkinen avain → käyttäjän nimi → käyttövaltuudet. (Kallio 2005, 51.)

Roolivarmenteessa julkista avainta ei sidota tiettyyn henkilöön (nimeen) vaan kyseisen avaimen haltijalle kuuluviin valtuuksiin: julkinen avain → käyttövaltuudet. (Kallio 2005, 51).

Käyttämällä rooli- tai attribuuttivarmenteita on mahdollista välttää eräitä nimiavaruuteen liittyviä ongelmia, joita aiheutuu esimerkiksi varmenteiden käyttäjien saman nimisyydestä. Roolivarmennetta hyödynnettäessä voidaan rakentaa erilaisia varmenneketjuja ja valtuuksien delegointi olisi helppoa. Käytännössä roolivarmenne voidaan toteuttaa esimerkiksi X.509v3-varmenteen laajennuskenttien avulla. (Kallio 2005, 51.)

Välimuodon henkilövarmenteen ja roolivarmenteen välille tarjoaa attribuuttivarmenne. Attribuuttivarmenne kytkee henkilön nimen hänelle kuuluviin oikeuksiin. Tällöin pääsynvalvonta suorittaisi kaksivaiheisen päättelyketjun: julkinen avain → käyttäjän nimi → valtuudet. (Kallio 2005, 51.)

Tällöin pääsynvalvonnan ensimmäinen osa tapahtuisi henkilövarmenteen avulla ja jälkimmäinen attribuuttivarmenteen avulla. Perinteisen henkilövarmenteenkin tietosisältöön voisi sisällyttää myös rooli- ja valtuustietoja, mutta erillisen attribuuttivarmenteen käytössä on etuja, kuten attribuuttivarmenteen lyhyempi voimassaoloaika henkilövarmenteeseen verrattuna. Jos attribuuttivarmenne varmentaa esimerkiksi henkilön asemaa yrityksessä, voi tämä asema muuttua vuosien saatossa. Jos varmenne on henkilön aseman muutoksen jälkeen voimassa, se joudutaan asettamaan sulkulistalle. (Kallio 2005, 51.)

5.3 Varmennepalvelut

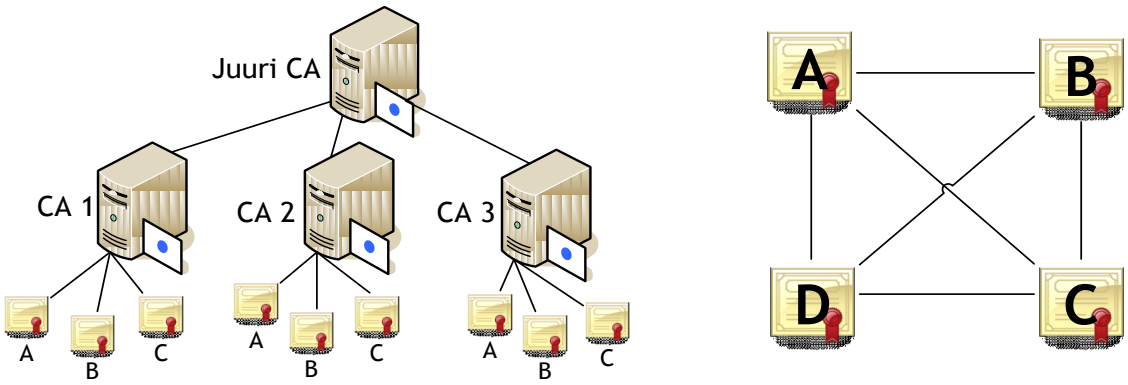
Varmennepalvelut ovat julkisen avaimen järjestelmän selkäranka. Varmennepalvelujen toteutus pitää sisällään sekä teknisiä että toiminnallisia määrittelyjä. Varmennepalvelut voidaan teknisesti toteuttaa monella eri toimintaperiaatteella, joista toteutustapa valitaan tarpeen mukaisesti. Varmennepalvelujen käyttöönotto ei ole helppo prosessi. Varmennepalvelujen käyttöönottoprojekteissa tavanomaista on se että vain pieni osa projektia on valitun teknisen toteutuksen käytännön toteutusta. Toteutuksen tekninen määrittely, varmenteiden käyttöön liittyvät politiikat, lausumat ja niihin liittyvän dokumentoinnin pitäisi olla merkittävässä osassa varmennepalveluiden käyttöönotossa.

5.4 Luottamusmallit

Varmenteisiin perustuvan todentamisen pohjalle on syntynyt erilaisia luottamusmalleja, joiden perusteella määritellään se kenen myöntämiin varmenteisiin luotetaan. Nykyisin PKI -järjestelmässä laajasti käytössä on hierarkkinen luottamusmalli. Tällöin kaikki järjestelmän jäsenet luottavat omaan varmentajaansa. Varmentajat voivat edelleen solmia keskenään luottamussuhteita, jolloin esim. kahden eri varmentajan jäsenet voivat luottaa toisiinsa (kuva 9). (Rinne 2002, 93).

Toinen luottamusmalli on luottamuksen verkko (web of trust), joka syntyi kun PGP-salausmenetelmän käyttäjät loivat luottamussuhteita toisiin käyttäjiin, käyttämättä keskitettyä varmentajaa. Luottamuksen verkko ei sovellu luottamusmalliksi verkkoihin, joiden käyttäjämäärät ovat suuret, koska käyttäjän on itse allekirjoitettava käytännössä jokainen avain (kuva 9). (Rinne 2002, 95.)

Hierarkisesta luottamusmallista ja luottamusverkosta on kehitetty myös erilaisia yhdistelmiä. Alla olevassa kuvassa on vasemmalla kuvattu hierarkisen luottamusmallin ja oikealla luottamusverkon periaatteet.



Kuva 9. Hierarkisen luottamusmallin ja luottamusverkon periaatteet.

Internetissä suuntaus on kohti laajamittaista ammattimaista varmentamistoimintaa ja sen myötä kohti puumaista varmennearkkitehtuuria. Tällöin varmentajana toimii esimerkiksi kaupallinen yritys, joka hankkii varmentamistoimintaan tarvittavan erityisosaamisen sekä laitteiston ja myy varmennepalveluja asiakkailleen. On olemassa suuri määrä kaupallisia varmentajia kuten Verisign, Entrust ja Thawte. Tunnettuja kaupallisia kotimaisia varmentajia ovat Väestörekisterikeskus, Elisa ja Sonera. Monet yritykset varmentavat itse sisäiseen käyttöön tarkoitettuja varmenteitaan. (Linden 2003, 49.)

Puumaisessa varmennearkkitehtuurissa luottamuksen lähtökohta eli juuri (root) on varmennehierarkiassa varmentajan julkinen avain. Usein varmentaja allekirjoittaa julkisen avaimensa omalla yksityisellä avaimellaan, jolloin syntyy itseallekirjoitettu (self-signed) juurivarmenne. Tämä ei kuitenkaan ole välttämätöntä. Itseallekirjoitetun varmenteen tunnistaa siitä, että varmenteeseen sisältyvä tieto varmentajan nimestä sekä varmenteen haltijan nimi ovat samat. Kaikki muut varmennehierarkiasta löytyvät varmenteet on allekirjoitettu joko varmentajan juureen liittyvällä yksityisellä avaimella tai alivarmentajan varmenteeseen liittyvällä yksityisellä avaimella.

Varmenteisiin luottavan osapuolen tehtävä on varmennetta käyttäessään todentaa koko varmenteista muodostuva ketju juuresta alkaen. Ketjun jokaisen lenkin on oltava aito, voimassaoleva varmenne. (Linden 2003, 50.)

5.5 Varmenteiden sulkupalvelut

Varmenteiden sulkupalvelu on olennainen osa toimivaa PKI -järjestelmää. Mahdollisuus varmenteen sulkemiseen onkin välttämätön osa PKI -järjestelmää. Sulkemalla varmenne, eli laittamalla se varmentajan julkaisemalle varmenteiden sulkulistalle, voidaan varmistua, että vääriin käsiin päätyneen varmenteen käyttö on mahdollista estää ennen varmenteen voimassaoloajan päättymistä. (Komar 2004, 189.) Varmentajan julkaisema varmenteiden sulkulista

(certificate revocation list, CRL) on varmentajan digitaalisesti allekirjoittama ja julkaisema luettelo varmenteista, jotka on mitätöity ennen niiden voimassaoloajan päättymistä.

Jotta sulkulistapalvelusta olisi hyötyä PKI -järjestelmälle, on tieto sulkulistalle asetetetuista varmenteista saatava varmenteisiin luottavan tahon tietoon. Varmenteiden sulkulistoja voidaan julkaista vain yrityksen sisäiseen käyttöön sekä julkisesti esimerkiksi internetissä. Jos varmennepalvelu on tarkoitettu vain yrityksen sisäiseen käyttöön, voi riittää että sulkulista julkaistaan vain yrityksen sisäverkossa. Luotettavassa PKI -ympäristössä on kuitenkin tärkeää, että varmenteisiin luottava osapuoli voi aina halutessaan tarkistaa varmenteen oikeellisuuden julkisessa tietoverkossa sijaitsevalta sulkulistan jakelupisteeltä. Sulkulistan saatavuuden turvaamiseksi olisi se hyvä julkaista usealla eri alustalla. Tavallisimpia sulkulistan julkaisualustoja ovat LDAP- (Lightweight Directory Access Protocol), www- ja ftp-palvelimet sekä tiedostopalvelinten tiedostojaot. Varmenteessa oleva erillinen tietokenttä kertoo varmenteeseen kohdistuvan sulkulistan sijainnin.

Varmenteiden sulkupalvelut ovat koko PKI -järjestelmän käytön kannalta krittinen komponentti. Voimassaolevan sulkulistan puuttuminen voi estää varmenteisiin ja älykortteihin perustuvan työasemakirjautumisen, vaikka itse varmenteet sekä muu PKI -infrastuktuuri olisivat kunnossa. Tästä johtuen on sulkulistan julkaiseminen suunniteltava siten, että voidaan aina varmistua sulkulistan saatavuudesta. Hyvä käytäntö on julkaista sulkulistaa useammalle eri palvelimelle, siten että sulkulista on julkaistu eri palvelimilla eri protokollilla. Julkaistussa varmenteiden sulkulistassa on tieto kyseisen sulkulistan voimassaoloajasta. Sulkulistan voimassaoloajan perusteella varmenteeseen luottava osapuoli voi varmistua sulkulistan ajantasaisuudesta.

Sulkulistalla olevien varmenteiden käsittelyyn liittyy tiettyjä ongelmia. Esimerkiksi Microsoftin käyttöjärjestelmien sulkulistan käsittelytoiminnallisuus on toteutettu siten että sulkulista ladataan verkkoliikenteen minimoimiseksi työaseman CryptoAPIn välimuistiin. Tällöin työasema tarkistaa varmenteen kelpoisuuden sulkulistan voimassaoloajan ensisijaisesti paikallisen koneen CryptoAPIsta. Tällöin manuaalisesti julkaistu sulkulista, jolle vääriin käsiin joutunut varmenne on laitettu jätetään huomioimatta. Vääriin käsiin joutunutta varmennetta voidaan tällöin käyttää esimerkiksi työasemakirjautumiseen, vaikka se onkin jo lisätty sulkulistalle.

Sulkulistan toiminnallisuuteen liittyvät ongelmat on tunnistettu ja niihin on kehitetty ratkaisuja, jotka mahdollistavat varmenteita käytettäessä niiden reaaliaikaisen oikeellisuuden tarkistamisen. Yksi tämän ongelman ratkaisemisen kehitetty ratkaisu on Microsoftin Windows Vista sekä Windows Server 2008 käyttöjärjestelmiin sisäänrakennettu ja niissä oletusarvoisena käytetty varmenteiden oikeellisuuden varmistamiseen käytettävä Online Certificate State Protocol (OCSP), jonka toiminnallisuus on määritetty Internet Engineering Task Forcen (IETF)

dokumentissa RFC 2560 (Shivaram 2007, 57). Sen avulla voidaan varmenteen käyttökelpoisuus tarkistaa varmennepalvelusta reaaliaikaisesti joka kerta, kun sertifikaattia käytetään. OCSP protokollaa voidaan käyttää yhdessä perinteisen sulkulistapalvelun kanssa. OCSP toiminnallisuus on sisäänrakennettu osassa muita käyttöjärjestelmiä, joista esimerkkinä ovat eräät Linux jakelut. Windows XP käyttöjärjestelmässä OCSP toiminnallisuus voidaan ottaa käyttöön kolmannen osapuolen ohjelmistoratkaisuiden avulla.

5.6 Julkisen avaimen järjestelmän osapuolet

Seuraavaksi esitellään PKI -järjestelmän eri osapuolet, joiden kokonaisuudesta rakentuu PKI -järjestelmän toiminnallisuus. Jokaisella PKI -järjestelmän osapuolella on omat vastuunsa ja velvollisuutensa, ja kun he toiminnallaan täyttävät ne, syntyy tästä kokonaisuudesta luotettava PKI -järjestelmä.

Varmentaja

Varmentajan tehtävänä on allekirjoittaa varmenteet, joilla todistetaan yksityisen avaimen kuuluminen sen haltijalleen. Varmentaja julkaisee myös digitaalisesti allekirjoittamaansa ja julkaisemaa luetteloa ennen varmenteen voimassaolon päättymistä käytöstä poistetuista varmenteista, eli sulkulistaa (CRL, certificate revocation list). Sulkulistalle laitetaan varmenteet joiden yksityinen avain on paljastunut, kadonnut tai joutunut vääriin käsiin. Varmentajan varmenteeseen luottava osapuoli on velvollinen tarkastamaan aina ennen varmenteen käyttöä, ettei varmenne ole sulkulistalla. (Linden 2003, 52.)

Jos varmentajan julkaisemien varmenteiden oikeellisuuden varmentamiseen on mahdollista käyttää OCSP -protokollaa, on varmentajan tehtävänä ylläpitää myös OCSP -toiminnallisuuden tarvitsemaa tietoverkkoresurssia, josta varmenteen voimassaolo voidaan sitä käytettäessä tarkistaa. OCSP -resurssin toteuttaminen on tarpeellista vain, jos varmenteeseen on sisällytetty tieto OCSP -resurssin olemassaolosta.

Rekisteröijä

Rekisteröijän (registration authority, RA) tehtävänä PKI -järjestelmässä on varmistaa että varmenteen tiedot pitävät paikkansa. Hänen tulee myös varmistua että varmenteen luovutushetkellä yksityinen avain on varmenteen haltijan hallussa ja että hänen kauttaan myönnettyjen varmenteiden tiedot pitävät muutenkin paikkansa. (Linden 2003, 53.)

Varmennehakemisto

Varmentajan myöntämät varmenteet sijaitsevat varmennehakemistossa. Varmentajan allekirjoittamien varmenteiden ja niihin liittyvän sulkulistan pitää olla varmenteisiin luottavan osapuolen saatavilla. Varmennehakemisto voi olla joko julkinen (esimerkiksi Väestörekisterikes-

kuksen myöntämän kansalaisvarmenteet) tai sitten vain rajatulle kohderyhmälle julkaistu (esimerkiksi yrityksen sisäinen varmennepalvelu). (Linden 2003, 53.)

Varmennearkisto

Varmennearkisto on paikka johon siirretään varmenteet joiden voimassaoloaika on päättynyt. Myös sulkulista korvautuu varmennehakemistossa uuden sulkulistan julkaisun myötä ja sulkulistalla olevat varmenteet poistuvat sulkulistalta kun niiden voimassaoloaika päättyy. (Linden 2003, 54.)

Varmenteen haltija

Varmenteen haltija on itse asiassa PKI -järjestelmän avainhenkilö. Varmenteen haltija on se henkilö tai muu toimija, jonka nimi on kirjattu varmenteeseen varmenteen kohteeksi ja joka on varmenteeseen liittyvän yksityisen avaimen haltija. Varmenteen haltijan pitää parhaan kykynsä mukaan suojata yksityistä avainta katoamiselta ja paljastumiselta. Jos näin pääsee tapahtumaan, tulee hänen viipymättä ilmoittaa asiasta varmentajalle joka asettaa varmenteen sulkulistalle. (Linden 2003, 55.)

Varmenteeseen luottava osapuoli

Varmenteeseen luottavan PKI -järjestelmän osapuolen tulee hankkia varmentajan juurivarmenne ja rakentaa siitä varmenneketju aina varmenteen haltijan varmenteeseen asti. Varmenteeseen luottavan osapuolen on aina tarkastettava, että varmenteen allekirjoitukset on aina tehty ketjun edelliseen varmenteeseen liittyvällä yksityisellä avaimella. Lisäksi hänen on varmistuttava, että varmenne on voimassa, eikä sitä ole asetettu sulkulistalle. (Linden 2003, 55.)

5.7 Key Escrow -menetelmä

PKI -järjestelmän tekninen toteutus voi mahdollistaa varmenteiden salaisten avainten palauttamisen Key Escrow –menettelyn kautta. Salaisen avaimen palauttaminen on mahdollista silloin, kun varmenteeseen liittyvä käyttäjän salainen avain luodaan jossain muualla kuin älykortilla. Tämä voidaan toteuttaa esimerkiksi siten, että varmentajalta tehtävän varmennepyynnön yhteydessä tallennetaan varmenteeseen liittyvä salainen avain varmennepalvelun tietokantaan, josta se voidaan tarvittaessa palauttaa. Salaisen avaimen palautusmahdollisuus antaa mahdollisuuden esimerkiksi salatun sähköpostiviestin tai tiedoston avaamiseen sen salaukseen käytetyn älykortin rikkouduttua. Ilman salaisen avaimen palauttamista ei salattuun dataan pääse enää käsiksi.

Key Escrow -menettely on herättänyt vastustusta, koska salaisen avaimen palauttamisen mahdollisuus on katsottu yksilönsuojaa loukkaavaksi. Key Escrow -menetelmä ei ole käytössä

esimerkiksi Väestörekisterikeskuksen myöntämissä kansalaisvarmenteissa, mutta sitä käytetään yleisesti yritysten sisäiseen käyttöön tarkoitetuissa varmennepalveluissa.

6 HENKILÖN SÄHKÖINEN IDENTITEETTI FINAVIASSA

Finaviassa on tiedostettu opinnäytetyössä jo aiemmin kuvatut henkilön sähköisen identiteetin hallinnan haasteet, joita on lähdetty ratkaisemaan laajalla Turvallisuussuunnittelu -hankekokonaisuudella. Hankkeen tavoitteena on saada Finavian henkilöstön sähköinen identiteetti työsuhteen eri vaiheissa paremmin hallintaan.

Seuraavissa kappaleissa kuvataan lyhyesti Turvallisuussuunnittelu -hankekokonaisuuteen kuuluvia eri aliprojekteja, jotka ovat läheisessä tekemisessä Monitoiminnallinen sähköinen henkilökortti -projektin kanssa. Hankekokonaisuuteen kuuluvien projektien lyhyen läpikäynnin tavoitteena on luoda kuva siitä, miten laajasta kokonaisuudesta on kysymys, ja tuoda esille nykypäivän tietotekniikkaprojekteihin sekä koko tietotekniseen kokonaisuuteen liittyvä suuntaus järjestelmien integroitumisesta yhä enemmän ja enemmän toistensa kanssa.

6.1 eLomake

eLomake -projektin tavoitteena oli hankkia Finavian käyttöön sähköinen lomakejärjestelmä, joka ohjaa turva- ja henkilöstöhallinnon, sekä tieto- ja viestintätekniikan prosesseja työntekijän työsuhteen elinkaaren eri vaiheissa. eLomake -järjestelmän tavoitteena on tuottaa perustieto Finavian henkilöstön työsuhteen elinkaaresta. eLomake -järjestelmästä nämä henkilön sähköiseen identiteettiin liittyvät tiedot välitetään järjestelmäintegraatioiden avulla useisiin Finavian tietojärjestelmiin.

eLomake -järjestelmä hyödyntää sähköisen henkilökortin ominaisuuksista sen tarjoamaa mahdollisuutta vahvaan tunnistautumiseen tietojärjestelmään, sekä sähköisten lomakkeiden allekirjoittamiseen käytettävää sähköistä allekirjoitusta. eLomake -järjestelmä on tällä hetkellä käytössä Finavia konsernissa, mutta sen käyttö on tarkoitus laajentaa myös Finavian henkilökortteja henkilöstölleen tarvitseviin ulkopuolisiin yrityksiin.

6.2 Monitoiminnallinen sähköinen henkilökortti

Monitoiminnallinen sähköinen henkilökortti -projektin tavoitteena oli ottaa käyttöön Finavian lentoasemilla työskentelevien yritysten henkilöstön tunnisteena toimiva monitoiminnallinen sähköinen henkilökortti, jota voidaan hyödyntää sekä kulunvalvontaan että Finavian tietoverkkoon tunnistautumiseen ,sekä myöhemmässä vaiheessa kortille mahdollisesti liitettävien

muiden sovellusten avulla toteuttaa esimerkiksi sähköinen kukkaro toimintoja eri Finavian järjestelmissä. Monitoiminnallisen sähköinen henkilökortin toiminnallisuudelle perustuvat useat Turvallisuussuunnittelu projektikokonaisuuden aliprojektit.

6.3 Varmennepalvelu

Varmennepalvelu (CA, Certification Authority) projektin tavoitteena oli hankkia Finavian käyttöön sähköisen henkilökortille sijoitettavien varmenteiden myöntämiseen tarvittava varmennepalvelu. Projektissa kilpailutettiin varmennepalveluiden tarjoajia ja valittiin niiden joukosta Finavian varmennepalvelun tekninen toimittaja.

6.4 Kulunvalvontajärjestelmän uusiminen

Kulunvalvontajärjestelmäprojektin tavoitteena oli hankkia Finavian kaikilla 25 lentoasemalla käyttöönotettava kulunvalvontajärjestelmä. Kulunvalvontajärjestelmän kulunvalvontatunnisteena käytetään monitoiminnallisen sähköisen henkilökortin RFID-toiminnallisuutta.

6.5 Korttikirjautumisen selvitysprojekti

Korttikirjautumisen selvitysprojektin (Korki) tavoitteena oli kartoittaa sähköisellä monitoiminnallisella henkilökortilla tapahtuvan tietoverkkoon kirjautumisen vaikutuksia käyttäjille ja Finavialla käytettäville tietojärjestelmille.

Projektin tavoitteena oli selvittää esimerkiksi yhteiskäyttöisten verkkotunnusten tarpeellisuus sekä tietojärjestelmien toiminnallisuus kirjauduttaessa tietokoneelle henkilökortilla. Korttikirjautumisen selvitysprojektin tuloksia voitiin käyttää lähdetietona käyttövaltuuksien ja pääsynhallinnan esiselvitysprojektissa.

6.6 Käyttövaltuuksien ja pääsynhallinta

Vuoden 2008 tammikuussa aloitetun käyttövaltuuksien ja pääsyhallinta (IAM, Identity and Access management) esiselvitysprojektin tavoitteena oli selvittää Finavian tietojärjestelmien käyttövaltuuksien- ja pääsynhallinnan nykytila sekä määritellä tavoitetila. IAM -projekti tulee jatkumaan vuonna 2009 IAM -järjestelmän hankintaan ja käyttöönottoon tähtäävän projektin muodossa.

7 SÄHKÖISEN HENKILÖKORTIN KÄYTTÖÖNOTTO FINAVIASSA

Opinnäytetyössä tutustutaan Finaviassa käyttöönotetun monitoiminnallisen sähköisen henkilökortin (Moto) suunnittelu- ja käyttöönottoprojektiin. Projektin tavoitteena oli hankkia Finavian käyttöön kulunvalvontaan ja tietoverkkokirjautumiseen käytettävä sähköinen henkilökortti ja henkilökorttien tuottamiseen tarvittavat tietojärjestelmät.

Sähköisen henkilökortin käyttöönottoa varten perustettuun Moto -projektiin nimettiin projektiryhmä, jonka vastuulla oli määritellä ja toteuttaa projekti yhdessä projektin aikana valittujen järjestelmätoimittajien kanssa. Moto -projektiryhmään kuuluivat projektipäälliköksi nimetty Finavian ulkopuolinen konsultti, henkilöitä Finavian eri yksiköistä sekä järjestelmätoimittajan edustajat, yhteensä noin kymmenen henkilöä. Projektin ohjausryhmä koostui Finavian yksikköjen esimiehistä ja asiantuntijoista sekä järjestelmätoimittajien edustajista ja projektipäälliköstä.

7.1 Projektin tavoitteet

Moto -projektille määritettiin alussa tavoitteet, jotka projektin avulla pyrittiin saavuttamaan. Asetettujen tavoitteiden pohjalta hahmotettiin edelleen hankittavan kokonaisuuden ominaisuuksia ja sille asetettavia vaatimuksia. Niitä taas käytettiin myöhemmin perustana henkilökorttiprojektin käytännön toteutukselle. Seuraavassa on listattu projektin tavoitteita ja asioita, joihin monitoiminnallisen sähköisen henkilökortin avulla tavoiteltiin parannusta.

- Tietoturvallisuuden parantuminen. Tietojärjestelmiin ja työasemaan tunnistautuminen ainoastaan henkilökortilla.
- Luovutaan tietojärjestelmiin tunnistautumiseen tarvittavien käyttäjätunnusten ja salasanojen käytöstä soveltuvilta osin. Käyttäjän tarvitsee henkilökorttia käyttäessään muistaa vain yksi PIN-koodi useiden sovelluskohtaisten käyttäjätunnusten ja salasanojen sijaan.
- Tietoverkon ja sovellusten käyttöoikeudet on sidottu henkilökorttiin.
- Käyttäjätunnuksen ja salasanan tiedottamisesta uudelle käyttäjälle aiheutuvat ongelmat poistuvat.
- Mahdollistetaan sähköisen allekirjoituksen käyttö eLomake -järjestelmässä, sekä sähköpostin sähköinen allekirjoitus ja salaus.
- Henkilökortti toimii kulunvalvontatunnisteena.
- Henkilökortti mahdollistaa biometriikan käytön erityissuojattavissa kohteissa.
- Palvelussuhteen päättyessä, henkilökortin luovutus esimiehelle poistaa käyttöoikeudet kulunvalvonta- ja tietojärjestelmistä.
- Asiakasyritysten on mahdollista hyödyntää kortin ominaisuuksia omiin tarpeisiinsa niiltä osin, joita ei ole rajattu Finavian käyttöön.

7.2 Projektin riskit

Henkilökorttiprojektin alkuvaiheessa projektiryhmä teki ohjausryhmän hyväksymänä projektiin kohdistuvista riskeistä riskikartoituksen. Samassa yhteydessä määriteltiin kaikille tunnistetuille riskeille ehkäisevät toimenpiteet, sekä kullekin riskille vastuuhenkilöt, joiden tehtävänä oli seurata riskien toteutumista ja tarvittaessa puuttua laukeaviin riskeihin ennen kuin ne aiheuttavat ongelmia projektin toteutukselle. Lisäksi sovittiin koko projektin ajan jatkuvasta riskien arvioinnista ja projektipäällikön vastuulle kuuluneen riskitaulukon ylläpidosta.

Projektiin arvioitiin riskikartoituksen perusteella kohdistuvan seuraavia riskejä:

- Finavian henkilöstö ei ehdi osallistua projektiin riittävästi tai ole käytettävissä.
- RA-pisteiden käyttöön tulevia tietokoneita ei saada aikataulussa.
- Järjestelmäintegraatiot eivät toimi.
- Toimittajan resurssit eivät riitä hankkeen läpivientiin.
- Uuden henkilökorttijärjestelmäohjelmisto -version käyttöönotto viivästyy.

7.3 Sähköisen henkilökortin määrittelyt

Osana henkilökorttiprojektia tehtiin projektipäällikön, projektiryhmän ja järjestelmätoimittajan yhteistyönä henkilökortista ja sen personoimiseen käytetystä personointiympäristöstä toiminnallinen ja tekninen määrittely. Dokumenttien tarkoituksena oli kuvata ja määritellä sähköisen henkilökortin ja personointiympäristön toiminnallisuutta ja teknistä toteutusta.

7.3.1 Henkilökortin toiminnallinen määrittely

Moto -projektin toiminnallisen määrittelyn tarkoituksena on kuvata personointipisteiden ja personointiohjelmiston toiminnallisuus ja toiminnot personoinnin eri vaiheissa. Dokumentissa kuvataan personointiohjelmistolle asetetut toiminnalliset vaatimukset, jonka perusteella järjestelmätoimittaja toteuttaa Finavialle määrittelyn mukaisen järjestelmän. (Keski-Valkama 2007b, 5.)

Toiminnallisessa määrittelyssä luotiin pohja sille, millainen käyttöönotettavan teknisen ratkaisun toiminnallisuuden tulisi olla. Lisäksi dokumentissa kuvattiin seuraavia asioita: Henkilökorttien personointiin käytettävien tietojärjestelmien arkkitehtuuri, laite- ja ohjelmistoasennukset, personointiohjelmiston toiminnallisuus, personointipisteiden arkkitehtuuri (kevyt- ja täydellinen personointipiste), personointiohjelmiston käyttöliittymään liittyvät määrittelyt, järjestelmäintegraatiot, varmennepalvelun toiminnallisuus soveltuvilta osin, biometrian käyttö henkilökortilla, henkilökortin vastaanottositoumus, personointipisteen virkailijan toiminta, valtuudet ja oikeudet, VPN-kortin hallinnointi, sulkulistapalvelu, henkilö-

kortin toiminnallisuudet (ID, RFID, PKI), henkilökorttiaihioiden logistiikka, personointiprosessit (kevyt- ja täydellinen personointipiste, lukkiutuneen PIN-koodin avaus) ja niihin liittyvät käyttötapaukset.

7.3.2 Henkilökortin tekninen määrittely

Moto -projektin tekninen määrittelydokumentti sisältää Finavian turvallisuushallinnan kulunvalvontaprojektin monitoiminnallisen henkilökortin ja sen tekemiseen käytettävän personointijärjestelmän teknisen määrittelyn. Dokumentin tarkoitus on kuvata toiminnallisen määrittelyn mukaisten toimintojen teknistä toteutusta Finavian personointipisteillä, sekä personointiin liittyvien järjestelmien integrointitietojen hakutoiminnoissa ja päivityksissä. Teknisen määrittelyn pohjalta tehdään varsinainen henkilökorttien personointijärjestelmän tekninen toteutus. (Keski-Valkama 2007a, 4.)

Teknisen määrittelyn tavoitteena oli siis kuvata se, miten henkilökortti ja sen personointiympäristö on teknisesti toteutettu. Teknisessä määrittelydokumentissa kuvattiin seuraavia asioita: Personointipisteen järjestelmäarkkitehtuuri, personointijärjestelmän tietoliikenne, henkilökortin tekniset ominaisuudet (visuaaliset, sähköiset, RFID, biometria), henkilökortin käyttämät standardit ja määritykset, personointijärjestelmä (PC, korttitulostin, kamera ja kuvauslaitteisto, muut laitteet), personointiohjelmisto, PKI -toiminnallisuus, RFID -toiminnallisuus, avainhallinta, personointipisteiden tekninen toiminnallisuus ja prosessit, järjestelmäintegraatiot ja niihin liittyvät rajapinnat (henkilörekisteri, Active Directory ja varmennepalvelu). (Keski-Valkama 2007a, 4.)

Dokumenttia täydennettiin projektin edetessä sekä projektiryhmän että järjestelmätoimittajan toimesta. Valmis dokumentti sisälsi täydellisen teknisen kuvauksen henkilökortin ja sen luomiseen käytettävän personointiympäristön teknisestä toteutuksesta.

8 SÄHKÖISEN HENKILÖKORTIN KÄYTTÖÖNOTON VALMISTELU

Ennen kuin varsinainen henkilökorttien personointi RA-pisteissä pääsi käyntiin, oli projektiryhmän toimesta tehty mittava määrä etukäteisvalmisteluja, joiden tavoitteena oli varmistaa henkilökorttien personointipisteiden ja henkilökorttien sujuva käyttöönotto. Osa projektin aikaisista tehtävistä oli puhtaasti teknisiä, mutta teknisen toteutuksen lisäksi oli myös erittäin tärkeää että kaikista projektin osa-alueista ja projektikokonaisuudesta oli tehty tarkat määrittelyt ja ne oli dokumentoitu. Kokonaisuuden kannalta yksi oleellisen tärkeä tekijä oli kaikkien RA-pisteissä toimivien henkilöiden koulutuksen suunnittelu. Seuraavissa luvuissa kuvataan

henkilökorttien personointijärjestelmän sekä PKI -infrastruktuurin käyttöönotossa tarvittavia osa-alueita.

8.1 Varmennepalvelu

Henkilökorteille vietävien varmenteiden tarvitseman varmennepalvelun hankkimiseksi kilpailutettiin osana henkilökorttiprojektia teknisen varmennepalvelun toimittajat. Varmennepalvelun toteutusta valmistelleen projektin vaihtoehtoina teknisen varmennepalvelun toteuttamiseen olivat oman sisäisen Windows Server 2003 -sertifikaattipalvelimen käyttäminen, ulkoisen kaupallisen varmennepalvelun käyttäminen sekä korttien tekemisen ulkoistaminen.

Näistä vaihtoehdoista todettiin Windows Server 2003 -sertifikaattipalvelun olevan pois laskuista, koska sen ominaisuudet olivat rajoitetut, ja tarvittavaa ammattitaitoa varmennepalvelun ylläpitoon varmennepalvelulle määritetylle prioriteetille ei löytynyt Finavian it-yksiköstä.

Myös esimerkiksi Väestörekisterikeskuksen, ja joidenkin kaupallisten toimijoiden tarjoama varmennepalvelukonsepti, joka piti sisällään varmennepalvelun lisäksi henkilökorttien tekemisen osittaisen ulkoistamisen, todettiin Finavian käyttöön soveltumattomaksi. Henkilökorttien tekoprosessi haluttiin säilyttää kokonaisuudessaan Finavian hallussa.

Henkilökorttien tuottamisen kokonaan Finavian omassa organisaatiossa etuja olivat: mahdollisuus tuottaa henkilökortteja nopeasti sekä korttien luontiprosessiin liittyvä logistiikka. Muita henkilökorttien personoinnin pitämistä omissa käsissä tukevia seikkoja olivat halu käyttää henkilökorteissa mahdollisimman avoimia teknisiä ratkaisuja, henkilökortin käyttäminen kulunvalvontajärjestelmän tunnisteena sekä muiden kortille tulevaisuudessa mahdollisesti liitettävien sähköisen asioinnin ratkaisujen toiminnallisuuden varmistaminen.

Edellä mainittujen seikkojen perusteella päädyttiin hankkimaan varmenteet ja varmennepalvelu Insta DefSec Oy:ltä. Instan valintaan vaikuttavina tekijöinä olivat vankka kokemus varmennepalvelujen toimittamisesta ja heidän tarjoamansa palvelun soveltuvuus Finavian käyttöön. He pystyivät toimittamaan oikean ratkaisun Finavian tarpeisiin. Ratkaisussa yhdistyivät korkea käytettävyys ja toimittajan aiemmissa varmenneprojekteissa todennettu yhteensopivuus Finavian RA-pisteissä käytettävään personointiohjelmistoon.

8.2 Varmennepalvelun käyttöönottoon liittyvät dokumentit

Varmenteiden ja PKI -infrastruktuurin käyttöönottoon organisaatiossa liittyvät olennaisesti erilaiset varmenteiden käyttöön ja niiden hallinnointiin liittyvät dokumentit. Dokumenttien tuottaminen liitettiin varmennepalvelujen teknisen toimittajan valinnan tehneen projekti-

ryhmän tehtäviin. Finavialla näiden dokumenttien tekemiseen käytettiin ulkopuolista konsulttia, joka laati yhteistyössä Finavian tieto- ja viestintätekniikan edustajien kanssa PKI -järjestelmän käyttöönotossa tarvittavat dokumentit, joissa kuvataan PKI -infrastruktuurin eri osa-alueiden toteutusta Finavialla. Laadittuja dokumentteja olivat varmennepolitiikka, varmennekäytäntölausuma sekä henkilökortille vietävien varmenteiden varmenneprofiilit. Näiden dokumenttien sisältöä ja tarkoitusta kuvataan seuraavissa luvuissa.

8.2.1 Varmenneprofiili

Varmenneprofiilin (Certificate Profile) tarkoituksena on kuvata varmentajan myöntämien varmenteiden tietosisällöt. Varmenneprofiilissa käsiteltäviä asioita on kuvattu sekä X.509-standardissa että IETF:n julkaisemassa RFC 3280 ” Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” dokumentissa.

Laadittujen varmenneprofiilien perusteella Finavian varmennepalvelu Finavia General CA myöntää kolmea erilaista varmennetyyppiä, joiden varmenteen tietosisällöt on määritelty varmenneprofiili dokumentissa. Finavia General CA:n myöntämiä varmenteita ovat tunnistautumis-, salaus- ja allekirjoitusvarmenne. (Vatka 2007c, 5.)

8.2.2 Varmennepolitiikka

Varmennepolitiikalla (Certificate Policy, CP) tarkoitetaan varmentajan laatimaa yleistä kuvausta menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan. Politiikka sisältää myös varmenteisiin luottavien osapuolien vastuiden määrittelyn ja yleiset käyttöehdot. Muita keskeisiä varmennepolitiikan osa-alueita ovat varmenteen hakijan tunnistamiseen, teknisiin turvajärjestelyihin sekä järjestelmän fyysisiin, toiminnallisiin ja henkilöstöturvallisuuteen liittyvät kysymykset. (Väestörekisterikeskus, Varmennepolitiikat.)

Varmennepolitiikka on julkinen dokumentti joka on oltava kaikkien PKI -järjestelmän osapuolten saatavilla. Varmentajan myöntämiin varmenteisiin luottavat tahot perustavat luottamuksensa varmenteisiin varmennepolitiikassa kuvattuihin varmenteiden käsittelyyn liittyviin käytänteisiin.

Varmennepolitiikassa kuvataan ne menettelytavat ja toimintaperiaatteet, joita varmentaja varmenteita myöntäessään noudattaa. Varmennepolitiikassa kuvataan Finavian asettamat vähimmäisvaatimukset menettelytavoille ja periaatteille varmenteita myönnettäessä. Finavian varmennepolitiikka perustuu ETSI:n (European Telecommunications Stardards Institute) määrittelemään, sähköisen allekirjoituksen direktiivin (1999/93/EY) standardoinnin yhteydessä tehtyyn muita kuin laatuvarmenteita koskevaan varmennepolitiikkamääritykseen. Kyseinen

määritys on jaettu kolmeen tasoon, joista Finavia noudattaa vahvinta, varmennekortit sisältävää mallia (NCP+). Kaikki Finavian varmentajan alaisuudessa toimivat tai sille varmennepalvelua tuottavat tahot ovat velvollisia noudattamaan tätä politiikkaa ja luomaan varmennekäytäntölausumansa tai niitä vastaavat muut dokumentit sitä noudattaen. (Vatka 2007b, 6.)

8.2.3 Varmennekäytäntölausuma

Varmennekäytäntölausuma (Certificate Practice Statement) asiakirjat kuvaavat varmennetyypeittäin ne toimintatavat ja käytännöt joita noudatetaan varmennepolitiikassa mainittujen tavoitteiden toteutumiseksi. Varmennekäytäntölausuma on periaatteessa varmentajan tekninen opas, jossa on dokumentoitu kaikki varmenteiden hallintaan liittyvät kriteerit, periaatteet ja toimintatavat, sekä kokonaisprosessin ulkopuolisen tarkistuksen menettelyt. Varmennekäytäntölausuma ei ole julkinen asiakirja.

Varmennekäytäntölausuma on kuvaus käytännöistä ja toimintatavoista, joita Finavia on toimeenpannut täyttääkseen varmennepolitiikan mukaiset velvollisuutensa toimiessaan varmentajana ja rekisteröijänä. Itse varmenteiden tekninen tuottaminen on ulkoistettu kolmannelle osapuolelle, Insta DefSec Oy:lle. Finavian varmennekäytäntölausumassa on kaksi keskeistä kokonaisuutta: rekisteröintipisteessä tapahtuvat toimenpiteet ja varmenneympäristössä tapahtuvat toimenpiteet. Varmennekäytäntölausumassa kuvataan rekisteröintipisteeseen liittyvät käytännöt. Varmenneympäristön käytännöt on Finavialla kuvattu varmennepalvelun palvelukuvauksessa. (Vatka 2007a, 4.)

8.3 Älykorttikirjautuminen Windows 2003 toimialueella

Ennen teknisen varmennepalvelun käyttöönottoa oli tehtävä useita teknisiä valmisteluja. Osana näitä valmisteluja oli Finavian käyttämän Windows Server 2003 toimialueen valmisteleminen älykortilla tapahtuvaan tietojärjestelmään tunnistautumiseen. Seuraavissa luvuissa kuvataan, miten Finavialla otettiin käyttöön älykortilla tapahtuva kirjautuminen Active Directoryyn käytettäessä kolmannen osapuolen julkaisemia varmenteita.

Koska Finavialla käyttöönotettu varmenteiden käyttöön perustuva ratkaisu ei perustu Microsoftin omaan sertifikaattipalveluun on sähköisellä henkilökortilla tietoverkkoon kirjautumisen mahdollistamiseksi tehtävä Active Directoryyn erinäisiä muutoksia ennen kuin älykorttikirjautuminen onnistuu.

Microsoftin julkaiseman Knowledge Base artikkelin 281245 mukaisesti käytettäessä työasemakirjautumiseen älykorttia jonka varmenteet ovat kolmannen osapuolen varmennepalvelun (CA) julkaisemia, on Active Directoryn työasemakirjautumisen mahdollistamiseksi tehtävä

seuraavat asetukset Active Directoryn tietokantaan sekä sen toimialueen ohjauskoneisiin (Domain Controller). (Microsoft a. Guidelines for enabling smart card logon with third-party certification authorities.)

- Active Directoryssa on oltava älykorttikirjautumiseen käytettävän kolmannen osapuolen varmennepalvelun palvelinvarmenne NTAuth -säilössä.
- Toimialueen ohjauskoneilla on oltava toimialueen ohjauskone varmennemallin (domain controller authentication) mukainen palvelinkohtainen varmenne.
- Lisäksi Microsoft suosittelee lisäämään työasemakirjautumiseen käytettävän kolmannen osapuolen varmennepalvelun juurivarmenteen ryhmäkäytäntöjen luotetuiden päämyöntäjien (Trusted root CA store) säilöön.

Koska Finavialla on käytössä myös yrityksen sisäinen Microsoft Server 2003 toimialueen Enterprise varmennepalvelin, ei toimialueen ohjauskoneille ollut tarvetta luoda toimialueen ohjauskone varmennemallin mukaista varmennetta, vaan toimialueen ohjauskoneet hakevat tämän varmenteen automaattisesti Finavian sisäverkon Microsoft varmennepalvelimen varmennepalvelusta.

Muut Microsoftin dokumentin mukaiset toimenpiteet oli sen sijaan tehtävä myös Finavian Active Directoryyn. Finavia General CA:n juurivarmenne julkaistiin Finavian Active Directoryn NTAuth store säilöön komennolla certutil –dspublish -f julkaistavanvarmenteennimi.crt NTAuthCA. Tämän jälkeen tarkistettiin että NTAuthstoreen julkaistu CA varmenne löytyi Active Directorysta polusta CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration, DC=domain,DC=name. (Microsoft b. How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store.)

8.4 Active Directory scheman laajennus

Henkilökorttiprojektin määrittelyvaiheessa kävi selville että RA-pisteiden käyttäjäystävällisen toiminnallisuuden takaamiseksi on osa henkilökorttia personoitaessa tarvittavasta tiedosta vietävä keskitettyyn tietovarastoon. Tietojen tarkoituksenmukaisesta tallennuspaikasta tehdyn analyysin jälkeen tiedot päädyttiin tallentamaan Finavian Active Directoryyn. Tietojen tallentaminen Active Directoryyn päädyttiin tekemään laajentamalla Active Directoryn schemaa uudella luokalla ja sen sisältämiltä attribuuteilla. Koska scheman laajentamisen suunnittelussa ja toteutuksessa oli kysymys erityisosaamista vaativasta tehtävästä, päätettiin työn suorittamiseen hankkia ulkopuolista asiantuntija apua.

Tavoitteena henkilökorttiin liittyvien tietojen tallentamisessa Active Directoryyn oli se, että tiedot on kyettävä suojaamaan siten, että pääsy tietoihin on vain henkilöillä joiden on työteh-

täviensä vuoksi päästävä niitä käsittelemään. Näitä henkilöitä Finavialla ovat RA-pisteissä työskentelevät virkailijat sekä tieto- ja viestintätekniikan palveluyksikön Active Directory -järjestelmän ylläpitäjät.

Active Directoryn scheman laajennuksessa lisättiin Active Directory käyttäjäobjektin sisältämiin tietoihin seuraavat lisäkentät:

- Tunnistautumisvarmenteen sarjanumero
- Allekirjoitusvarmenteen sarjanumero
- Toimikortin sirun sarjanumero
- Toimikortin PUK koodi
- Henkilön henkilökorttijärjestelmän henkilönumero.

Henkilökorttiprojektissa tarvittavien tietojen sekä mahdollisten muiden tulevaisuudessa ilmenevien Active Directoryn scheman laajennustarpeiden vuoksi päätettiin lisätä Active Directoryn schemaan oma luokka Finavian nykyisiä ja tulevia tarpeita varten. Koska Active Directoryyn vietävät tiedot ovat luottamuksellisia, piti tiedot pystyä suojaamaan luvattomalta käytöltä. Ratkaisuna tähän päädyttiin tekemään lisättävistä attribuuteista sellaisia, joiden käyttöoikeudet pystytään rajaamaan vain niille henkilöille, joiden on työtehtäviensä perusteella oikeutus päästä lukemaan ja kirjoittamaan näitä tietoja.

Active Directory on hyvä paikka melko staattisen tiedon tallentamiseen (Kouti & Seitsonen 2004, 861). Active Directoryn käyttöoikeusmallin mukainen, Active Directoryyn tallennettujen tietojen oletusarvoinen näkyminen kaikille Active Directoryyn tunnistautuneille käyttäjille oli ristiriidassa tietojen tallentamiselle asetetun luottamuksellisuus tavoitteen kanssa. Tästä johtuen päädyttiin Active Directoryyn talletettavat arkaluontoiset henkilökorttitiedot suojaamaan seuraavassa kappaleessa kuvatulla tavalla.

Active Directoryyn tallennettua informaatiota voidaan suojata käyttäen Active Directoryn käyttöoikeuksia. Windows Server 2003 Service Pack 1:ssä esiteltiin uutena ominaisuutena Active Directory confidential -attribuutti. (Microsoft c. How to mark an attribute as confidential in Windows Server 2003 Service Pack 1). Microsoft käyttää itse confidential -attribuuttia esimerkiksi Windows Vistan Bitlocker -levynsalauksen palautusmerkkijonojen tallentamiseen sekä siirtyvien varmenteiden tallentamiseen ja Windows Server 2003 R2:n Active Directory Unix -integraatiossa Unix salasanojen tallentamiseen (Seitsonen 2007, 5).

8.5 Älykortin käyttö työasemassa

Microsoftin käyttöjärjestelmät mahdollistavat älykortilla tapahtuvan käyttöjärjestelmään kirjautumisen Windows 2000:ssa ja sitä uudemmissa käyttöjärjestelmissä (De Clerq, Smart Cards). Koska Windows XP sisältää natiivisti vain muutaman suuren kansainvälisen älykorttivalmistajan älykorttien ajuriohjelmistot, jotka mahdollistavat älykorttien käytön ilman kolmannen osapuolen laitteistoajurien asentamista työsemaan, oli sähköisen henkilökortin PKI -ominaisuuksien käytön työasemissa mahdollistamiseksi hankittava jokaiseen työasemaan jolla älykorttikirjautumista haluttiin käyttää älykortin käytön mahdollistava CSP -ohjelma (Cryptographic Service Provider). CSP -ohjelmaksi Finavialla valittiin Aventra Oy:n Avesign.

CSP -ohjelman lisäksi piti kaikkiin Finavian työasemiin hankkia älykortinlukijat. Älykorttilukijoiden testaamisen ja vertailun jälkeen päädyttiin hankkimaan Omnikey merkkiset älykortinlukijat, jotka olivat työasemissa USB- ja kannettavissa PC Card -liitännällä varustettuja. Tärkeimpinä kortinlukijoiden valintakriteereinä olivat hyvä käytettävyys ja tuki, sekä tieto siitä, että valitut älykortinlukijat ovat maailmalla laajasti käytössä.

9 SÄHKÖISEN HENKILÖKORTIN TEKNIIKKA

Seuraavissa luvuissa kuvataan monitoiminnallisen sähköisen henkilökortin teknistä toteutusta, teknisen toteutuksen perustana olevia määrittelyjä sekä perusteita sille, miksi on valittu käyttöön otettu tekniikka.

Monitoiminnallisen sähköisen henkilökortin valintaperusteena käytettiin valitun ratkaisun toimivuutta käytännössä. Koska henkilökorttia käytetään Finavialla sekä visuaalisena tunnistusvälineenä, sähköisessä asioinnissa sekä kulunvalvonnassa oli tärkeää, että valittu ratkaisu täyttäisi kaikkien edellä mainittujen käyttökohteiden asettamat vaatimukset.

Finavialla Monitoiminnallinen sähköinen henkilökortti -projektin tuloksena käyttöönotettu henkilökortti on fyysisiltä ominaisuuksiltaan ISO7811 standardikokoinen (CR80) laminoitu PVC-muovikortti, jonka korttirunko on esipainettu offset-menetelmällä (Aventra 2007, 6). Henkilökortti on ns. Dual-Interface -kortti, jolloin kortilla on sekä kontaktillinen siru, johon on kytketty kortin sisällä oleva antenni kontaktitonta kommunikointia varten. Kortin sisältämän muistin kokonaiskapasiteetti on 72 kt, joka mahdollistaa sen, että kortille on mahdollista tulevaisuudessa viedä muita älykorttisovelluksia.

9.1 Java Card

Java Card on alun perin SUNin kehittämä alykorttialusta, jota ylläpitää nykyisin avoin kehitysfoorumi Java Card Forum. Java Card ei ole puhdas käyttöjärjestelmä, vaan Java muodostaa virtuaalikoneen käyttöjärjestelmän ja sovellusten välille. Java on avoimista korttijärjestelmästä suosituin. (Rinne 2002, 44.)

FInavian henkilökortin ohjelmallinen toiminnallisuus perustuu Java -teknologiaan. Sen sisältämä Java -teknologia on tallennettu kiinteästi kortin sirulle jo tehtaalla. Käyttöjärjestelmään sisältyy Java -virtuaalikone, eli ohjelmisto joka kykenee suorittamaan Java -ohjelmointikielestä käännettyä tavukoodia, sekä mahdollistaa kortin sisäisten komponenttien kuten kryptoprosessorin sekä ulkoisten liitäntöjen tarvitsemaa koodia. (Aventra 2007, 8.)

Varsinainen kortin sovellustoiminnallisuus toteutetaan Java -kielisinä sovelluksina eli appletteina. Nämä appletit voidaan viedä sirulle jo sen valmistusprosessissa, tai ne voidaan ladata kortille vasta myöhemmin. (Aventra 2007, 8.)

Java -filosofia tuo useita etuja verrattuna perinteisen ohjelmakehityksen toimikortteihin. Alimman kerroksen turvakriittiset laiteriippuvat ohjelmistot kehitetään vain yhden kerran ja niiden kustannukset voidaan jakaa kaikkien Java -teknologiaa korteillaan käyttävien organisaatioiden kesken. Varsinainen Java -tekniikkaan perustuva sovelluskehitys voidaan helpommin toteuttaa asiakaskohtaisesti, ja näiden ohjelmien turvallisuus on helpompi toteuttaa. (Aventra 2007, 8.)

9.2 RFID

Radio frequency identification (RFID) eli radiotaajuinen etätunnistus on menetelmä tiedon etälukuun ja -tallentamiseen käyttäen RFID-tunnisteita. RFID-tunniste on pieni laite, joka voidaan sisällyttää tuotteeseen valmistusvaiheessa, tai liimata tuotteeseen jälkikäteen tarralla. RFID-tunnisteet sisältävät antennin, jonka avulla ne lähettävät ja vastaanottavat radiotaajuisia kyselyitä RFID-lähetin-vastaanottimelta.

Finavialle RFID-tunnisteita käytetään henkilökortilla tapahtuvaan kulunvalvontajärjestelmän lukijoille tunnistautumiseen. Tällöin kulunvalvontajärjestelmään kuuluva lukija tunnistaa henkilökortin sen sisältämän tiedon perusteella, ja henkilö pääsee liikkumaan lentoasema alueen kulunvalvotuissa tiloissa henkilökortin avulla.

9.3 MIFARE

MIFARE on maailmanlaajuisesti käytössä oleva standardi, joka määrittelee etäluettavan muistikortin toiminnallisuutta. MIFARE -kortin fyysiset ominaisuudet noudattavat älykorttistandardia ISO 14443. MIFARE -kortin ja lukijan välinen tietoliikenne on salattua. MIFARE -tekniikkaan perustuvan älykortin muisti jakautuu alueisiin, jotka voidaan haluttaessa suojata lukemiselta ja kirjoittamiselta. (Aventra 2007, 8.)

9.4 Biometria

Biometrian käyttö on yksi keino jolla voidaan suojata resurssien väärinkäyttöä ja identifioida tietojärjestelmälle siihen tunnistautuva käyttäjä. Älykorttien kohdalla tämä tarkoittaa jonkin käyttäjään liittyvän biometrisen tiedon tallentamista älykortille. Tällöin kortille tallennettua biometristä tietoa verrataan kortin käyttäjästä vertailuhetkellä saatavaan biometriseen tietoon ja päätellään, ovatko ne peräisin samasta henkilöstä. (Aventra 2007, 9.)

Biometrinen tunnistaminen on viime vuosina tullut varteenotettavaksi vaihtoehdoksi käyttäjän tunnistamiselle erilaisissa ympäristöissä. Biometriikkaa käytetään yleisesti käyttäjätunnusten ja salasanojen korvaamiseen. Älykorttien alueella menetelmä on saavuttanut jalansijaa PIN-luvun korvaajana. (Rinne 2002, 38.)

Biometrisiä tunnistamismenetelmiä on useita. Biometriseen tunnistamiseen voidaan käyttää esimerkiksi seuraavia tunnisteita: sormenjälki, käden geometria, kasvonpiirteet sekä silmänpohja ja iiris. Älykorttien yhteydessä sormenjälki on edellä mainituista menetelmistä käyttökelpoisin. (Rinne 2002, 38.)

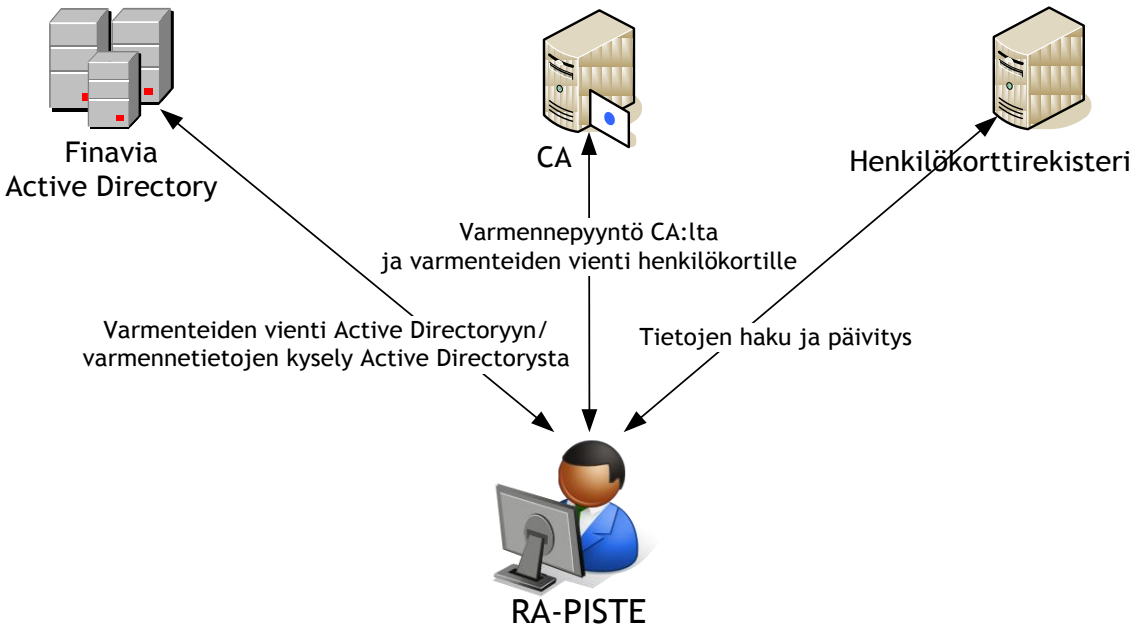
Finavian henkilökortissa on mahdollista käyttää biometrisiä tunnisteita. Alkuvaiheessa kortille on viety käyttäjän valokuva, joka mahdollistaa esimerkiksi kasvontunnistukseen perustuvan biometrisen tunnistautumisen tietojärjestelmille. Sitä voidaan käyttää hyväksi vaikkapa turvakriittisillä alueilla liikuttaessa tukemaan RFID -pohjaista kulunvalvontajärjestelmälle tunnistautumista.

10 RA-PISTE

Registration Authority eli RA-piste on Finavialla paikka jossa sähköiset henkilökortit personoidaan käyttäjille RA-pisteissä toimivien lupatoimiston virkailijoiden toimesta. Finavian lentoasemilla toimivissa RA-pisteissä personoidaan kaikki Finavian myöntämät sähköiset henkilökortit. RA-pisteitä on lentoasemilla ympäri Suomen siten, että suurimmilla Finavian lentoasemilla

ja lennonvarmistuskeskuksissa joita on yhdeksän kappaletta on ”täydellinen personointipiste” joka sisältää kannettavan tietokoneen, kameran ja salamavalot, korttitulostimen johon on integroitu sekä kortin visuaalisten tunnisteiden tulostus että RFID- sekä älykorttikooderi, älykorttilukijoita sekä jokaiselle RA-pisteen virkailijalle henkilökohtaisen VPN -älykortin suojatun yhteyden muodostamiseen varmennepalveluun.

Suuremmilla lentoasemilla sijaitsevissa täydellisissä personointipisteissä personoidaan paikallisen lentoaseman henkilökorttien lisäksi myös täydellisen personointipisteen alaisuudessa toimivien pienempien lentoasemien henkilökortit. Näiden kohdalla kortin personointiprosessi toimii siten, että henkilöt kuvataan ”kevyissä personointipisteissä”, jonka jälkeen henkilökortti tulostetaan täydellisissä personointipisteissä. Tulostamisen jälkeen henkilökortti lähetetään postitse kevyeeseen personointipisteeseen, joita on kaikkiaan 13 kappaletta, jossa henkilökortti luovutetaan haltijalleen. Jos henkilökortilla on varmenneominaisuus, vaihtaa käyttäjä kevyessä rekisteröintipisteessä hänelle korttia luovutettaessa kortin PIN-koodit.



Kuva 10. RA-pisteen henkilökortin luontitapahtuman prosessikuvaus.

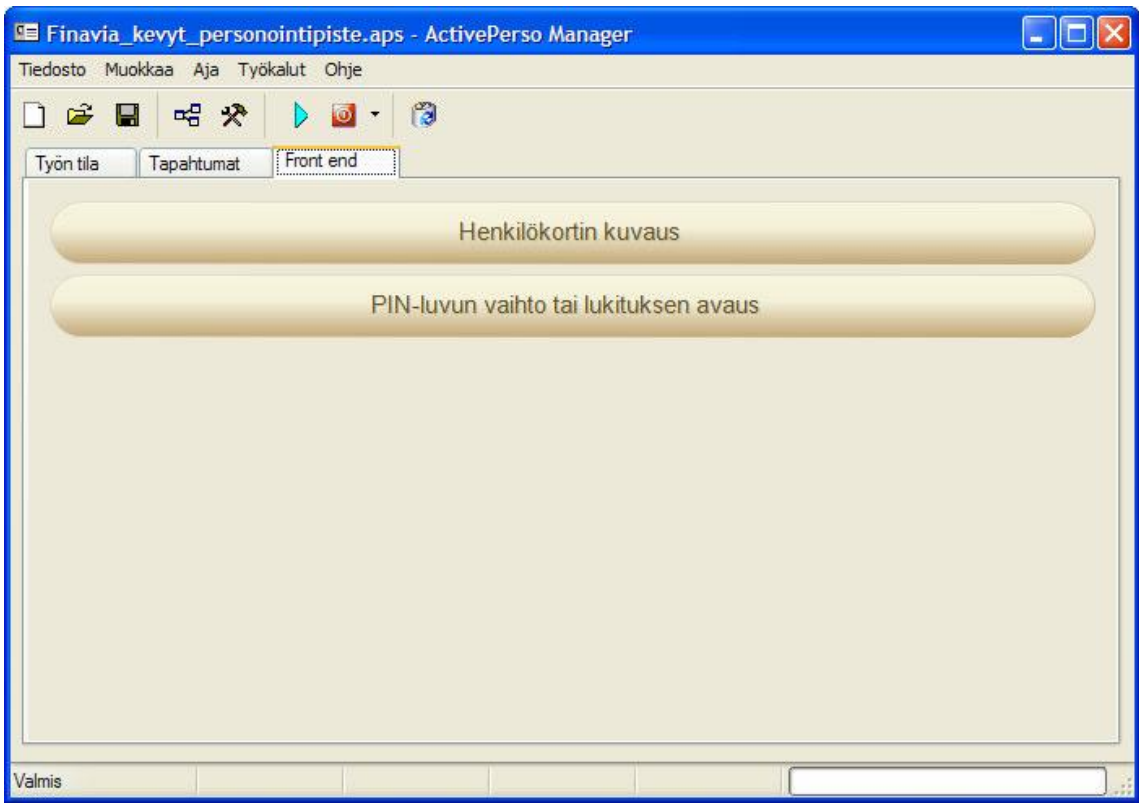
10.1 Henkilökortin personointijärjestelmä

Henkilökorttiprojektin alusta asti oli nähtävissä, että projektin onnistumisen kannalta oli ensiarvoisen tärkeää saada RA-pisteissä henkilökorttien personointiin käytettävä ohjelmisto mahdollisimman helppokäyttöiseksi. Sama helppokäyttöisyysvaatimus koski myös personointipisteissä henkilökorttien personointiin käytettävää laitteistoa. Vaatimus henkilökorttien personoinnin helppoudesta korostui, koska RA-pisteissä henkilökortteja tekevinä RA-pisteen virkailijoina toimivat henkilöt ovat pääsääntöisesti tietoteknillisiltä taidoiltaan "peruskäyttäjiä",

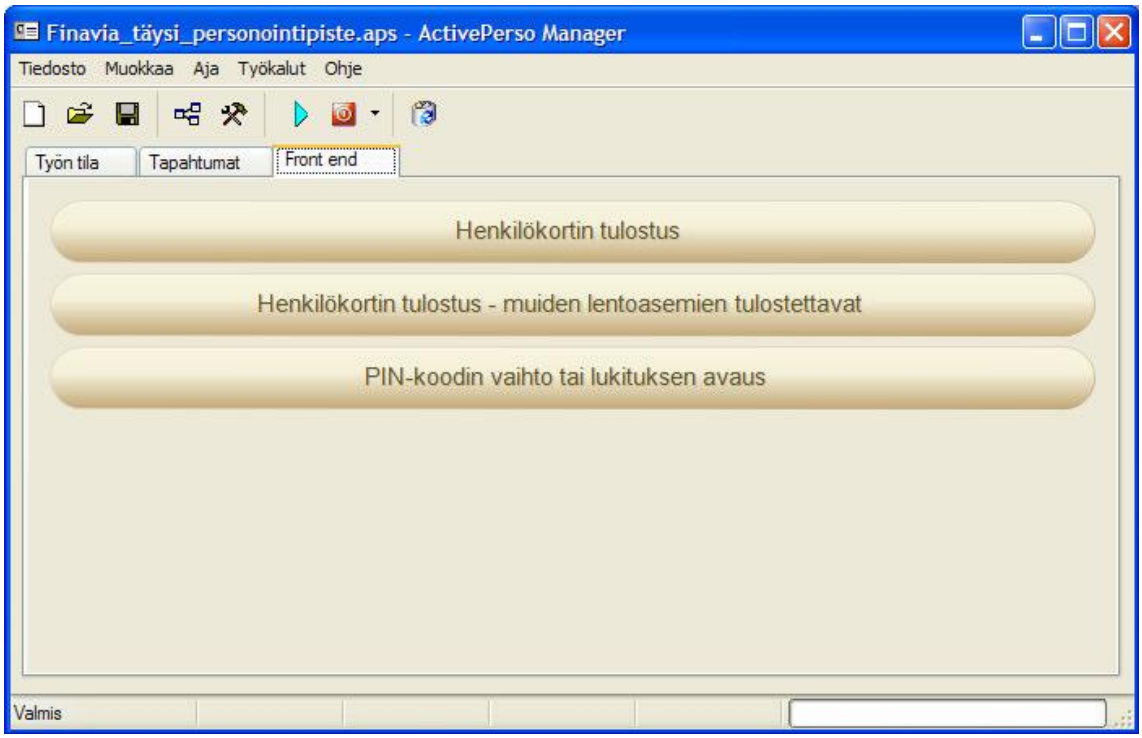
joille on pystyttävä tarjoamaan työkalut jotka mahdollistavat mahdollisimman yksinkertaisen kortin luontiprosessin. Useissa muissa organisaatiossa joissa on otettu käyttöön PKI -teknologiaa käyttävät sähköiset henkilökortit, tuottaa kortit yrityksen IT-osasto, jossa on usein erityisosaamista PKI -teknologian käytöstä, sekä laajaa osaamista tietotekniikasta.

Aventra Oy, joka valittiin toimittajaksi Monitoiminnallinen sähköisen henkilökortti -projektiin, toimitti personointipisteiden käyttöön ActicePerso Manager (APM) ohjelmiston. APM on osoittautunut erittäin hyväksi työkaluksi henkilökorttien personoinnissa. Korttia personoitaessa tapahtuu ohjelmiston erittäin yksinkertaisen käyttöliittymän takana paljon asioita, joiden monimutkaisuus on kyetty piilottamaan RA-pisteen virkailijalle avautuvasta käyttöliittyvästä (kuvat 11 ja 12).

APM-ohjelmistoa RA-pisteessä käytettäessä sujuu uuden henkilökortin personointi yhtä nappia painamalla. Samalla taustalla tapahtuu monimutkainen toimintosarja, joka täydellisessä personointipisteessä varmenteellista henkilökorttia tulostettaessa pitää sisällään lähes 70 erilaista toimintoa personointiprosessiin liittyvien taustajärjestelmien kanssa.



Kuva 11. Kevyt personointipiste APM-ohjelmiston käyttöliittymä.



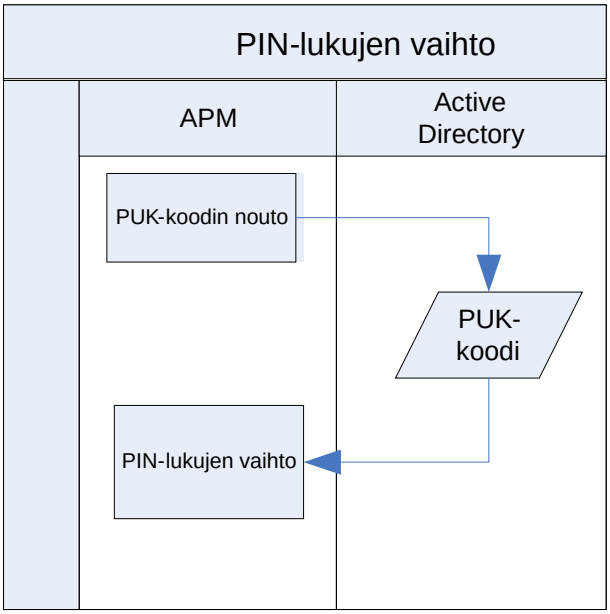
Kuva 12. Täydellinen personointipiste APM-ohjelmiston käyttöliittymä.

10.2 Henkilökortin personointiprosessi

Henkilökortin personointiprosessin tekniseen- ja toiminnalliseen määrittelyyn käytettiin projektin aikana huomattava määrä työtunteja. Kuten jo aiemmin mainittiin, on RA-pisteissä työskentelevien henkilöiden tietotekninen osaaminen usein "peruskäyttäjä" tasolla. Tämä asettaa huomattavia käytettävyysvaatimuksia kortin personointiprosessille. Henkilökortin personointiprosessin pitäisi olla RA-pisteen virkailijalle mahdollisimman yksinkertaista.

Henkilökortin personointiprosessia projektiryhmän toimesta suunniteltaessa, määriteltiin käyttötapaukset henkilökortin eri personointiprosesseille. Täydellisessä personointipisteessä käyttötapauksia olivat: henkilökortin personointi, muiden lentoasemien henkilökorttien personointi ja PIN-luvun vaihto tai kortin lukituksen avaus. Kevyessä personointipisteessä käyttötapauksia olivat: henkilön kuvaus ja PIN-luvun vaihto tai kortin lukituksen avaus. Myöhemmin projektin aikana sekä täydellisen- että kevyen personointipisteen korttien personoinnin käyttötapauksiin lisättiin myös henkilökortin poistoprosessi.

Projektiryhmä kävi läpi kaikki käyttötapaukset ja loi niistä määrittelyn, jossa kuvattiin kunkin käyttötapauksen mukainen kortin personointiprosessi. Käyttötapauksen mukaisessa kortin personointiprosessissa oli useita eri vaihtoehtoja sen mukaan, onko kyseessä Finavian oma työntekijä vai ulkopuolisen yrityksen työntekijä, sekä tapahtuuko personointiprosessi täydellisessä tai kevyessä personointipisteessä.



Kuva 13. Lukittuneen PIN-luvun vaihto prosessikaavio.

11 HENKILÖKORTTIEN ELINKAAREN HALLINTA

Henkilökorttien ja niiden sisältäminen varmenteiden elinkaaren hallinta oli yksi haastavimpia osa-alueita PKI -pohjaisissa henkilökorttiprojekteissa. Henkilökorttien elinkaaren hallintaan jouduttiin Finaviallakin kiinnittämään erityistä huomiota. Jotta voitiin varmistua siitä, että henkilökorttien elinkaaren hallinta pysyy hallittuna prosessina luotiin henkilökorttien elinkaaren hallintaan prosessit, joita noudattamalla voidaan varmistua henkilökortin olevan koko elinkaarensa ajan turvallinen ja luotettava väline käytettiinpä sitä kulunvalvonnan tunnisteena tai tietoverkkoon tunnistautumiseen. Suuri osa henkilökortin elinkaaren hallinnan määrittelyyn käytetystä ajasta kului elinkaarenhallintaa käsittelevän dokumentaation sekä määritysten parissa, ja kun tämä työ oli tehty, päästiin sitten käytännön tekniseen ja toiminnalliseen toteutukseen.

11.1 Uusien sekä uusittavien henkilökorttien myöntäminen

Uudet ja uusittavat henkilökortit ovat henkilökorttien elinkaaren hallinnan lähtökohta. Kortit tehdään ja luovutetaan käyttäjille lentoasemilla sijaitsevissa RA-pisteissä. Saadakseen henkilökortin on korttia hakevan henkilön todistettava henkilöllisyytensä viranomaisen myöntämällä kuvallisella henkilöllisyystodistuksella. Henkilökorttia personoitaessa siirtyvät kortin tiedot automaattisesti taustajärjestelmiin ja käyttäjä voi heti henkilökortin saatuaan käyttää sitä kulunvalvonnan tunnisteena ja tietoverkkoon tunnistautumiseen.

11.2 Kadonneet ja rikkinäiset henkilökortit

Kadonneet ja rikki menneet henkilökortit ovat haaste sähköisen henkilökortin käyttöönotossa. Kadonneiden henkilökorttien kohdalla Finavialle on olemassa koko valtakunnan laajuisesti yksi 24/7 toimiva palvelunumero, johon ilmoitetaan kadonneista henkilökorteista. Kun palvelupiste on saanut tiedon henkilökortin katoamisesta, suljetaan kortilla olevat kulkuoikeudet välittömästi, sekä laitetaan kortilla mahdollisesti olevat varmenteet sulkulistalle. Sulkulistalle laitetut varmenteet estävät PKI -toiminnallisuuteen perustuvat toiminnot, kuten kortin käyttämisen työasemakirjautumiseen, sähköisen allekirjoitukseen ja salaukseen.

Kortin katoaminen tai rikkoutuminen RA-pisteiden aukioloajan ulkopuolella on merkittävä haaste sähköisen henkilökortin käytölle. Kortin kadotessa tai rikkoutuessa ei rikkoutuneen kortin haltija pysty liikkumaan kulunvalvotuista ovista eikä kirjautumaan kortilla tietoverkkoon. Kaikkia kortin katoamiseen tai rikkoutumiseen RA-pisteiden aukioloajan ulkopuolella liittyviä haasteita ei projektin aikana vielä saatu ratkaistua. Projektiryhmä kuitenkin loi projektin aikana ehdotuksen siitä, kuinka toimitaan siinä tilanteessa että kortti katoaa tai menee rikki RA-pisteen aukioloajan ulkopuolella. Tämän ongelman ratkaisemiseksi hahmoteltuja mahdollisia toimintamalleja käsitellään opinnäytetyössä lyhyesti seuraavassa korttien sulkupalveluja käsittelevässä luvussa.

11.3 Korttien sulkupalvelu

Korttien sulkupalvelu on PKI -infrastuktuurin yksi tärkeimpiä toimintoja. Koska Finavialle on käytössä ulkoistettu varmennepalvelu, jossa sulkulistan julkaisu tapahtuu ulkoistetun palveluntarjoajan järjestelmässä, päädyttiin ratkaisuun jossa sulkulista julkaistaan sekä palveluntarjoajan vikasietoisessa julkisessa LDAP-hakemistossa että Finavian sisäisessä Active Directoryssä.(Insta DefSec 2007, 10.)

Julkisessa tietoverkossa sijaitseva sulkulistan julkaisupiste on ehdoton vaatimus rakennettaessa luotettavaa PKI -järjestelmää. Tällöin sulkulista on PKI -filosofian mukaisesti saatavilla myös silloin, kun korttia käytetään muualla kuin Finavian verkossa. Tällöin kaikilla tahoilla, jotka luottavat Finavia General CA:n myöntämiin varmenteisiin, on mahdollista tarkistaa varmenteiden oikeellisuus.

Sulkulistan ensisijaiseksi julkaisupaikaksi on kuitenkin varmenneprofiileissa määritetty Finavian Active Directory, jonne sulkulista julkaistaan varmennepalvelun toimittajan toimittaman ohjelman avulla. Ohjelma hakee ajastetusti sulkulistan varmennepalvelun toimittajan julkisesta hakemistosta, jonka jälkeen sulkulista julkaistaan Finavian Active Directoryyn, josta se on saatavilla Finavian tietoverkon käyttäjille mahdollisimman helposti ja nopeasti. Active

Directory on myös PKI -järjestelmän teknisen toiminnallisuuden kannalta optimaalinen sulkulistan julkaisupaikka, koska varmenteita sisältäviä henkilökortteja käytetään pääasiassa Finavian sisäverkossa. Koska Active Directoryn ohjauspalvelimia on Finaviassa käytössä useita, on Finavian sisäinen sulkulistan julkaisupiste samalla myös vikasietoinen.

Mahdollisissa varmennepalvelun toimittajaan kohdistuvissa sulkulistan julkaisemiseen liittyvissä ongelmatilanteissa on ongelmatilanteiden varalle sovittu etukäteen menettelytavat varmennepalvelun toimittajan kanssa. Ne mahdollistavat sulkulistan toimittamisen manuaalisesti Finavian tietohallintoon, joka ongelmatilanteissa hoitaa manuaalisesti sulkulistan julkaisun sisäverkon Active Directoryssa sijaitsevaan sulkulistan jakelupisteeseen. Vikasietoisuuden parantamiseen on pyritty myös määrittelemällä sulkulistan voimassaoloaika siten, että sen julkaisuun liittyvät ongelmat eivät välittömästi vaikuta esimerkiksi työasemakirjautumiseen. Samalla on kuitenkin pyritty varmistumaan siitä, että Finavian -PKI -järjestelmän tietoturvalle määritetyt vaatimukset saavutetaan kaikissa tilanteissa.

Henkilökortin PKI -toiminnallisuus varmenteineen on yleisesti ottaen huomattavasti vähemmän haavoittuvainen kuin henkilökortin kulunvalvontaominaisuus. Kortilla sijaitsevien varmenteiden käyttäminen on mahdotonta ilman PIN-koodia. Vaikka joku löytäisikin kadotetun kortin, ei sen käyttäminen onnistu ilman että kortin löytäjä saa tietoonsa myös löytämänsä kortin PIN-koodit. Syötettyään PIN-koodin väärin muutaman kerran kortti lukittuu, ja sen voi avata vain käymällä RA-pisteessä. Tällöin henkilökortin lukituksen avaamiseksi vaaditaan kortin haltijan henkilöllisyyden todentaminen virallisesta viranomaisen myöntämästä henkilöllisyystodistuksesta. Kulunvalvonnassa taas voidaan korttia mahdollisesti käyttää sellaisenaan kulunvalvontatunnisteena, jos sillä olevia kulkuoikeuksia ei ole suljettu.

Henkilökortin käytön laajentuessa on tarkoitus perustaan Helsinki-Vantaan lentoasemalle 24/7 toimiva RA-piste, josta henkilökortin haltija voi kortin vioittuessa tai kadotessa varsinaisen RA-pisteen aukioloajan ulkopuolella saada uuden kortin tai avata lukkiutuneen PIN-koodinsa. Myös muiden lentoasemien yhteyteen on suunniteltu tarpeen mukaan vastaavaa toiminnallisuutta, tai tekniikan kehittyessä on hahmoteltu jopa mahdollisuutta kortin etäpersonoinnnin käyttöön ottamiselle.

12 MUUT HENKILÖKORTIN KÄYTTÖKOHTEET

Työasemakirjautumisen, sähköisen allekirjoituksen ja salaustoiminnallisuuden sekä kulunvalvonnan tunnisteena toimimisen lisäksi monitoiminnallista sähköistä henkilökorttia on mahdollista käyttää myös muihin sähköisen asioinnin mahdollistamiin toimintoihin. Koska Finavialla käytettävissä henkilökorteissa on suuri muistikapasiteetti (72kt), mahdollistaa se kortin käy-

tön tulevaisuudessa uusiin käyttötarkoituksiin. Uusien henkilökortin käyttökohteiden toteutus voidaan toteuttaa joko kortille vietävien uusien älykorttisovellusten, tai kortin nykyistä toiminnallisuutta hyväksi käyttävien tietojärjestelmien avulla. Seuraavissa kappaleissa kuvataan muutamia henkilökortin mahdollisia ja jo toteutuneita käyttökohteita.

Langaton tietoverkko

Finavialla on tarkoitus ottaa käyttöön henkilökortti Finavian henkilökunnan käytössä olevan langattoman WLAN-verkon kautta tietoverkkoon tapahtuvaan tunnistautumiseen. Henkilökortin käytöllä mahdollistetaan vahva ja tietoturvallinen tunnistautuminen tietoverkkoon ja turvallinen langattoman verkon käyttö.

Paikoitusjärjestelmä

Helsinki-Vantaan lentoaseman alueella sijaitsevien henkilökunnan paikoitusalueiden nykyinen paikoitusjärjestelmä on tarkoitus uusia ja tällöin on suunniteltu otettavaksi käyttöön henkilökorttiin pohjautuva paikoitusalueiden käytönvalvonta. Nykyisin paikoitusjärjestelmässä ovat käytössä erilliset parkkikortit, joiden vaihtaminen henkilökortin käyttöön tuo merkittävät taloudelliset säästöt.

Mobiililaitteet

Finavian henkilökorttia käytetään Finnairin henkilökorttien personointijärjestelmään kuuluvien mobiilipäätteiden käyttäjien vahvaan tunnistautumiseen Finavian tietojärjestelmään. Yhteyden kautta viedään tietoja Finnairin henkilöistä Finavian henkilökorttirekisteriin. Tulevaisuudessa on tarkoitus käyttää Finavian henkilökorttia myös lentoasemilla toimivien turvatarkastusyritysten turvatarkastajien mobiilipäätteissä. Näillä Finavian ylläpitämillä mobiilipäätteillä voidaan henkilökortin avulla suorittaa vahvaan käyttäjän todentamiseen perustuva tunnistautuminen Finavian tietojärjestelmiin.

Extranet

Finavian extranet -projektissa on tunnistettu tarpeita käyttää vahvaa tunnistautumista pääsynhallintaan osaan extranetissä julkaistavaa materiaalia. Tällöin extranetiin tunnistautumiseen on mahdollista käyttää Finavian myöntämää henkilökorttia.

13 PROJEKTIN ONNISTUMINEN

Monitoiminnallinen sähköinen henkilökortti -projekti päättyi 7.3.2008. Projektipäällikön yhdessä projektiryhmän kanssa tuottamassa projektin loppuraportissa, jonka projektin ohjausryhmä hyväksyi, käsiteltiin projektin onnistumista. Projektin ohjausryhmä totesi loppuraportin hyväksyessään projektin onnistuneen hyvin. Seuraavassa taulukossa on käyty läpi projektin loppuraporttiin kirjattu näkemys projektin onnistumisesta.

Tavoite	Toteutus
Käytössä on vai yksi kortti	Henkilökortti toimii ID- ja kulunvalvontajärjestelmän tunnisteena sekä työasemakirjautumisessa.
Henkilökortti toimii kulunvalvontajärjestelmän lukijoissa	Kulunvalvontajärjestelmän lukijat noudattavat samaa Mifare-teknologiaa kuin henkilökortin RFID-ominaisuus.
Henkilökortti mahdollistaa PKI:n mukaisen toiminnallisuuden	Henkilökortille talletetaan käyttäjän varmenteet, jotka mahdollistavat työasemakirjautumisen, sähköisen allekirjoituksen ja salauksen.
Henkilökortti mahdollistaa biometrian käytön	Henkilökortin personoinnissa sirulle talletetaan henkilökortin haltijan valokuva.
Ulkopuoliset yritykset ja Finavian muut yksiköt voivat hyödyntää henkilökortin teknologiaa omissa järjestelmissään.	Muut yritykset ovat ottaneet käyttöön kortin kulunvalvontatunnisteena. Finavia ottaa käyttöön henkilökortin Helsinki-Vantaan pysäköintitalojen kulunvalvonnassa.
Lentoasemat tuottavat itse henkilökorttinsa	Jokaiselle lentoasemalle on asennettu oma henkilökorttien personointijärjestelmä.
Henkilökorttijärjestelmän koulutus RA-pisteiden virkailijoille	Kaikkien Finavian RA-pisteiden virkailijat koulutettiin ensin yhteiskoulutuksella ennen asennusvaiheen alkua ja sen jälkeen RA-pisteiden asennuksen yhteydessä
RA-pisteiden käyttöönotto	RA-pistekohtaisen asennuksen ja koulutuksen jälkeen järjestelmä siirrettiin välittömästi tuotantoon.
Finavian henkilökorttien vaihto	Henkilökorttien vaihto käynnistettiin heti RA-pistekohtaisen asennus/koulutuksen jälkeen

Taulukko 1. Henkilökorttiprojektin arviointi.

14 YHTEENVETO

Opinnäytetyön tekeminen ja siihen liittynyt henkilökorttiprojekti antoivat vahvan näkemyksen PKI -pohjaisen älykorttiprojektin toteutuksesta. Opinnäytetyön yhdistäminen työelämäprojektiin osoittautui todella onnistuneeksi ratkaisuksi. Opinnäytetyön ja työelämäprojektin yhdistäminen antoi mahdollisuuden tutustua projektin aihepiiriin kuuluviin tekniikoihin huomattavasti syvällisemmin kuin niihin muuten olisi tullut tutustuttua. Tästä syntyi selkeää lisäarvoa projektityöskentelyyn. Opinnäytetyöhön oleellisesti kuuluvan teoreettisen pohjatiedon oppiminen tapahtui luontevasti yhdessä projektityöskentelyn kanssa.

Kuten aiemmissa luvuissa on jo kuvattu, onnistui itse henkilökorttiprojekti hyvin. Projekti pysyi aikataulussaan, alkuperäisessä kustannusarviossaan ja projektin alkuvaiheessa tehdyt tekniset ja toiminnalliset määrittelyt otettiin käyttöön henkilökortissa ja sen luontiin käytetyssä personointiympäristössä suunnitellussa muodossa. Nyt kun henkilökorttiprojektin päättymisestä on jo kulunut useita kuukausia, on projektin tuotos vaikuttanut edelleen onnistuneelta, eikä merkittäviä ongelmia kortin käytön, tai RA-pisteiden toiminnan suhteen ole esiintynyt.

Turvallisuussuunnittelu projektikokonaisuus on edelleen käynnissä. Tässä yhteydessä tullaan monitoiminnallisen sähköisen henkilökortin teknisiä ja toiminnallisia määrityksiä täydentämään henkilökorttiprojektin päättymisen jälkeen havaittujen seikkojen osalta. Mahdollisista henkilökorttiin tulevista muutoksista mainittakoon muutamat tarkennukset varmenteiden tietosisältöön ja varmenneprofiileihin. Myös korttien PIN-koodien lukittumiseen sekä rikkoontuneiden ja kadonneiden korttien uusimiseen RA-pisteiden aukioloajan ulkopuolella tulee löytää pysyvä ratkaisu. Nämä ongelmat on tiedostettu jo henkilökorttiprojektin aikana, ja niihin on jo osittain löydetty ratkaisut jotka pitää pyrkiä ottamaan käyttöön.

Projektikokonaisuuden onnistumista arvioitaessa on huomioitava se, että monitoiminnallisen henkilökortin on Turvallisuussuunnittelu projektikokonaisuudessa suunniteltu toimivan useiden siihen liittyvien projektien työkaluna ja pohjaratkaisuna, jonka perustalle rakennetaan useiden järjestelmien toiminnallisuus. Siksi olikin tärkeää, että sekä Monitoiminnallinen sähköinen henkilökorttiprojekti onnistui hyvin. Itselleni opinnäytetyön tekijänä ja projektiryhmän jäsenenä taas oli tärkeää että käytännön projektityöskentely ja opinnäytetyö onnistuivat tukemaan toisiaan ja niiden lopputulos oli onnistunut.

Lähteet

De Clercq, J. Smart Cards. [www-dokumentti]. <http://www.microsoft.com/technet/security/guidance/identitymanagement/scard.mspx>. (Luettu 25.3.2008).

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo.

Komar, B. 2004. Microsoft Windows Server 2003 PKI and Certificate Security. Washington: Microsoft Press.

Kouti, S. & Seitsonen, M. 2004. Inside Active Directory Second Edition: A System Administrator's Guide. Boston: Addison Wesley.

Laki sähköisistä allekirjoituksista. 2003. [www-dokumentti]. <http://www.finlex.fi/fi/laki/alkup/2003/20030014>. (Luettu 15.11.2007).

Linden, M. 2002. Henkilön sähköinen tunnistaminen yliopistoissa ja ammattikorkeakouluissa. [pdf-dokumentti]. <http://www.csc.fi/downloadPublication?uid=502087fe3bdf17c0809a9a84ffe28dca>. (Luettu 3.1.2008).

Microsoft Corporation a. Guidelines for enabling smart card logon with third-party certification authorities. [www-dokumentti]. <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q281245>. (Luettu 8.12.2007).

Microsoft Corporation b. How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store. [www-dokumentti]. <http://support.microsoft.com/kb/295663>. (Luettu 15.11.2007).

Microsoft Corporation c. How to mark an attribute as confidential in Windows Server 2003 Service Pack 1. [www-dokumentti]. <http://support.microsoft.com/kb/922836>. (Luettu 15.11.2007).

Rankl, W. & Effing, W. 2006. Smart card handbook, Third Edition. John Wiley & Sons.

Rinne, T. 2002. Älykortit – tekniikka, sovellusalueet ja käyttöönotto. Jyväskylä: Gummerus Kirjapaino Oy.

Shivaram, H. 2007. Windows Vista Smart Card Infrastructure. MIcrosoft. <http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en>

Väestörekisterikeskus, Varmennepolitiikat.[www-dokumentti]. <http://www.fineid.fi/vrk/fineid/home.nsf/pages/6093070598676C11C2256FFF003A24C9>. (Luettu 5.5.2008).

Julkaisemattomat lähteet

Aventra Oy. 2007. Finavia: Turvallisuushallinnan kulunvalvontaprojektin tekninen määrittely: monitoiminnallinen henkilökortti. Aventra Oy. Espoo.

Finavia. 2008. Finavian esittely. Vantaa.

Insta DefSec Oy. 2007. Finavia: Tekninen varmennepalvelu – Tekninen määrittely. Insta DefSec Oy. Tampere.

Kallio, J. 2005. Älykorttien käyttö tunnistukseen yrityksen sisällä ja exranet-palveluissa. Diplomityö. Teknillinen korkeakoulu. Espoo.

Keski-Valkama, J. 2007a. Turvallisuushallinnan kulunvalvontaprojektin tekninen määrittely: monitoiminnallinen henkilökortti. Redicon Oy. Helsinki.

Keski-Valkama, J. 2007b. Turvallisuushallinnan kulunvalvontaprojektin toiminnallinen määrittely: monitoiminnallinen henkilökortti. Redicom Oy. Helsinki.

Linden, M. 2002. Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa. Tampereen teknillinen yliopisto. [pdf-dokumentti]. <http://www.csc.fi/downloadPublication?uid=cd50d1d89e0c6ce01684590816922643>. (Luettu 3.1.2008).

Seitsonen, M. 2007. Finavia - Active Directoryn scheman laajennus. FC Sovelto Oy. Helsinki.

Vatka, V. 2007a. Finavia: Varmennekäytäntölausuma. Redicom Oy. Helsinki.

Vatka, V. 2007b. Finavia: Varmennepolitiikka. Redicom Oy. Helsinki.

Vatka, V. 2007c. Finavia: Varmenneprofiili. Redicom Oy. Helsinki.