Sähköiset liput: Tietoturvaa julkisen avaimen teknologiasta

Teemu Tanila

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Pro gradu -tutkielma
Lokakuu 2002

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Teemu Tanila: Sähköiset liput: Tietoturvaa julkisen avaimen teknologiasta
Pro gradu -tutkielma, 48 sivua
Lokakuu 2002

Tässä tutkielmassa esitellään sähköisen kaupankäynnin osa-alue sähköiset liput. Lippujen hallinnalle esitetään tietoturvaratkaisu soveltaen julkisen avaimen teknologiaa.

Aluksi käydään läpi julkisen avaimen teknologian periaatteet ja sähköiset liput. Tässä yhteydessä tutustutaan mm. julkisen avaimen teknologian käyttöön SET-protokollassa ja esitetään vaatimukset tietoturvaratkaisulle. Sen jälkeen esitellään malli tietoturvaratkaisuksi. Tavoitteena oli luoda korkean tason suunnitelma selvittäen julkisen avaimen teknologian mahdollisuuksia.

Lopuksi arvioidaan esitetyn mallin vahvuuksia ja heikkouksia. Mallia vertaillaan vaatimuksiin ja kahteen eri tutkimukseen aiheesta. Vertailussa todetaan mallin sisältävän joitain rajoituksia, mutta täyttävän esitetyt vaatimukset ja tuovan lisäarvoa verrattuna aikaisempiin ratkaisuihin.

Avainsanat ja -sanonnat: sähköinen lippu, tietoturva.

Sisällys

1. Johdanto

Sähköinen kaupankäynti on osa nykypäivää. Eräs keskeisimmistä kysymyksistä sähköisen kaupankäynnin yhteydessä on menetelmien luotettavuus, eli yleistäen, tietoturva.

Käytettävät menetelmät kehittyvät jatkuvasti ja yhä enemmän perinteisiä tapoja käydä kauppaa pyritään siirtämään sähköiseen muotoon. Eräs tällainen kaupankäynnin osa-alue ovat sähköiset liput.

Sähköinen lippu on ajankohtainen ja verraten uusi tulokas sähköisen kaupankäynnin alueella. Viime aikoina on ollut nähtävissä ensimmäisiä käytännön sovelluksia, kuten erilaisia matkapuhelimen kautta käytettäviä tekstiviestilippuja. Ongelmaksi koetaan yhä kuitenkin palvelun tietoturva [HS], [Leitch, Warren, 2000].

Aluetta on tutkittu toistaiseksi varsin niukasti, ehkä juuri käytännön sovellusten vähäisyyden vuoksi. Esimerkiksi Fujimura ja Matsuyama [Fujimura, Matsuyama, 1999] ovat esittäneet menetelmän sähköisten lippujen hallintaan. Heidän ratkaisunsa vaatii keskitetyn tietokannan lipputietojen ylläpitoon, jolloin lippujen käytön edellytyksenä on etäyhteys tietokantaan. Maña ja muut [Maña, Martínez, Matamoros, Troya, 2001] ovat esittäneet GSM-lippu projektissaan menetelmän, jossa tietoturva perustuu matkapuhelimessa olevaan älykorttiin ja sen luotettuun ohjelmistoon. Molemmat edellä mainituista ratkaisuista ovat mielenkiintoisia tutkielmia alueelta. Mallien yhteisenä rajoituksena voitaisiin mainita käyttäjän rajoitetut mahdollisuudet hallinnoida omia lippujaan, kuten esimerkiksi ottaa niistä varmuuskopioita. Lipun varmuuskopiolla tarkoitetaan tässä tutkimuksessa lipun identtistä kopiota, jota voidaan tarvittaessa käyttää alkuperäisen lipun sijasta. Lisäksi GSM-lippu projektissa lippuun sidottava henkilön identifioiva informaatio jää tarkemmin määrittelemättä.

Tässä tutkimuksessa pyritään pureutumaan alussa mainittuihin kahteen asiaan, sähköisiin lippuihin ja niiden tietoturvaan. Tarkoituksena on esittää korkean tason viitekehys sähköisten lippujen tietoturvaratkaisuksi käyttäen julkisen avaimen teknologiaa. Tutkimuksessa keskitytään sähköisten lippujen osalta MeT- (Mobile electronic Transactions) yhteenliittymän esittämään lippukonseptiin, jonka kautta saadaan vaatimukset tutkimuksessa esitettävälle sähköisten lippujen tietoturvaratkaisulle. Tavoitteena on kehittää ratkaisusta

geneerinen, jolloin edellytykset ratkaisun laajemmalle käyttöönotolle olisivat olemassa.

Tutkimus noudattelee Järvisen ja Järvisen [Järvinen ja Järvinen, 1996] esittämän konstruktiivisen eli soveltavan tutkimuksen mallia. Tarkoituksena on soveltaa olemassa olevaa teknologiaa uudella tavalla ja luoda suunnitelma sähköisten lippujen tietoturvaratkaisuksi.

Tutkimus sisältää johdannon lisäksi seitsemän muuta lukua. Toisessa luvussa käsitellään lyhyesti sähköistä kaupankäyntiä ja siihen liittyviä tietoturvakysymyksiä. Kolmannessa luvussa esitellään kattavasti julkisen avaimen teknologian perusteita. Neljännessä luvussa käydään esimerkinomaisesti läpi eräs sähköisen kaupankäynnin protokolla, SET (Secure Electronic Transaction), ja esitellään siinä käytetty tietoturvaratkaisu. Viidennessä luvussa esitellään tämän tutkimuksen kohteena oleva sähköinen lippu. Luvussa määritellään myös vaatimukset luvussa kuusi esiteltävälle tietoturvaratkaisulle. Luvussa seitsemän arvioidaan edellisessä luvussa esitettyä mallia. Viimeinen luku on varattu keskustelulle. Yleisesti voidaan luonnehtia neljän ensimmäisen luvun olevan lukijan johdatusta tutkimuksen taustoihin ja aihepiiriin. Tutkimuksen varsinainen sisältö muodostuu neljästä viimeisestä luvusta.

2. Tietoturva ja sähköinen kaupankäynti

Tässä luvussa käsitellään lyhyesti sähköistä kaupankäyntiä ja siihen liittyviä tietoturvakysymyksiä. Aluksi määritellään sähköinen kaupankäynti, sen jälkeen tarkastellaan aluetta tietoturvan näkökulmasta. Lopuksi molemmat asiat suhteutetaan tähän tutkimukseen.

Kaupankäyntiin liittyy aina tiettyjä elementtejä, kuten vaihdannan osapuolet, tuotteet, maksutapahtuma ja tuotteiden jakelu. Luottamus on toiminnassa keskeinen tekijä. Kaupankäynnin osapuolten on ymmärrettävä ja hyväksyttävä tietyt ehdot, joiden varassa toimintaa harjoitetaan [Steinauer, Wakid, Rasberry, 1997].

Perinteisessä kaupankäynnissä nämä ehdot ovat usein intuitiivisesti selviä. Ostotapahtuma on tilanne, jossa sekä myyjä että asiakas ovat fyysisesti läsnä, jolloin osapuolet voivat tunnistaa toisensa. Asiakas maksaa hankinnan rahalla ja saa vastineeksi konkreettisen tuotteen, joka on välittömästi identifioitavissa kaupankäynnin kohteeksi. Lisäksi myyjä allekirjoittaa asiakkaalle kuitin ostoksestaan.

Sähköinen maksaminen ja sähköiset tuotteet muuttavat tilannetta. Osapuolet eivät välttämättä koskaan kohtaa fyysisesti, ostotapahtuma voi olla alusta loppuun virtuaalinen.

Kerttula [Kerttula, 1999] on määritellyt sähköisen kaupankäynnin tietoverkkojen kautta tapahtuvaksi tavaroiden ja palvelujen ostamiseksi siten, että kauppatapahtumat voidaan jälkikäteen selvittää. Kerttulan määritelmää voidaan toki tarvittaessa laajentaa toteamalla myös esimerkiksi sähköisen markkinoinnin kuuluvan sähköiseen kaupankäyntiin. Sähköisen kauppatapahtuman Kerttula määrittelee miksi tahansa paperittomaksi tietoverkossa tapahtuvaksi datan siirroksi, mikä aiheuttaa vastaavien vastineiden (rahojen) siirtymisen ostajalta myyjälle. Sähköinen kaupankäynti sisältää tavaroita ja palveluita ostavat liiketoiminnot, mutta ei sisällä osakekauppaa eikä rahoituslaitosten välisiä pääomien siirtoja.

Sähköisen maksutapahtuman tietoturvalle voidaan johtaa vaatimuksia geneerisistä tietoturvapalveluista (luottamuksellisuus, eheys, autenttisuus, kiistämättömyys) [Kerttula, 1999] seuraavasti: tapahtuman osapuolten on pystyttävä *autentikoimaan* eli tunnistamaan toisensa luotettavasti, kaikki

tietoliikenne on tarvittaessa pystyttävä *salaamaan* riittävän vahvasti, ja siirrettävän tiedon *eheys*, tapahtumien *jäljitettävyys* ja tiedon *kiistämättömyys* on pystyttävä takaamaan.

Sähköisen kaupankäynnin kohteena ei ole välttämättä aina aineellinen hyödyke, vaan kyseessä voi olla yhtä hyvin sähköinen hyödyke. Esimerkkinä mainittakoon ohjelmisto tai muu suoraan arvoa sisältävä sähköinen objekti, kuten sähköinen lippu. Onkin tarpeen huomioida tietoturvan tarpeen ulottuvan myös juuri em. arvoa sisältävien hyödykkeiden suojaamiseen luvattomalta kopioinnilta.

Sähköisen kaupankäynnin yhteydessä voidaankin karkeasti erotella kaksi eri suojausta vaativaa aluetta, arkaluontoisen informaation salaaminen ja suoraan arvoa sisältävän aineiston suojaaminen väärinkäytöksiltä. Jälkimmäisellä alueella on käytössä useita eri suojausmenetelmiä myös varsinaisten salaustekniikoiden lisäksi.

Tygar [Tygar, 1999] listaa juuri mm. immateriaalioikeuksien (intellectual property rights) hallinnan erääksi sähköisen kaupankäynnin avoimiksi kysymyksiksi. Miten oikeuksia voidaan valvoa ja mitä rajoituksia käytetyillä valvontamenetelmillä on.

Edellä mainittua kysymystä käsittelee myös Wallach [Wallach, 2001], joskin aivan erilaisesta näkökulmasta. Hänen mukaansa kopiointisuojaustekniikka on tuomittu epäonnistumaan. Wallach toteaa kaikkien menetelmien olevan murrettavissa. Ratkaisuna olisi kopiointisuojauksen sijasta uudenlaiset liiketoimintamallit. Liiketoimintamalleissa tarjottaisiin kuluttajalle riittävän edullisesti palvelu tai hyödyke, joka tarjoaisi sellaista lisäarvoa, jota ei saa tuotetta laittomasti kopioimalla.

Sähköisen kaupankäynnin toimintojen atomisuus on myös hyvin tärkeää [Tygar, 1996]. Atomisuudella tarkoitetaan toiminnon joko kokonaan suorittamista, tai suorittamatta jättämistä. Esimerkiksi asiakkaan maksaessa kauppiaalle, rahan on siirryttävä joko kauppiaalle, tai sen on pysyttävä asiakkaalla. Tilanne jossa molemmat menettäisivät rahan, tai saisivat rahan, ei ole hyväksyttävä.

Leitch ja Warren [Leitch, Warren, 2000] puolestaan ovat pohtineet tutkimuksessaan sähköisen kaupankäynnin ja etiikan yhteyttä. He mainitsevat

yhdeksi sähköisen kaupankäynnin yleistymisen esteeksi sen, että käyttäjät eivät ole varmoja voidaanko käytettyihin menetelmiin luottaa. Heidän mukaansa juuri autenttisuus ja tiedon eheys ovat ratkaisevassa asemassa sähköisessä kaupankäynnissä.

Tässä tutkimuksessa keskitytään siis sähköisen kaupankäynnin osa-alueeseen, sähköisiin lippuihin. Tietoturvaratkaisu pyritään luomaan nimenomaan lippujen käytölle ja hallinnalle, jolloin osa tässä luvussa mainituista tietoturvan alueista jää aiheen ulkopuolelle. Esimerkiksi lippujen ostamiseen liittyvät tietoturvakysymykset rajataan tutkimuksen ulkopuolelle.

Kolmannessa luvussa käyn läpi julkisen avaimen teknologiaa, joka tarjoaa menetelmiä tässä luvussa mainittujen ongelmien ratkaisemiseksi.

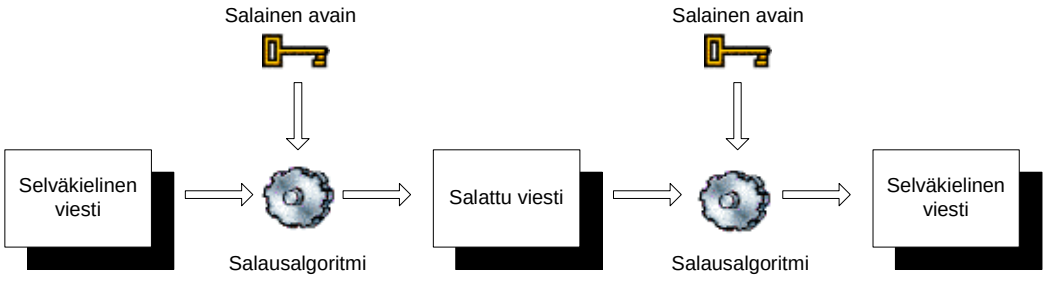
3. Julkisen avaimen teknologia

Tässä luvussa käydään kattavasti läpi perusteet julkisen avaimen järjestelmästä (PKC, Public Key Cryptography ja PKI, Public Key Infrastructure). Julkisen avaimen kryptografia eli epäsymmetrisen avaimen salausteknologia (PKC) ja julkisen avaimen infrastruktuuri (PKI) ovat keskeisiä nykypäivän tietoturvateknologioita. Esittelen seuraavissa kohdissa eri menetelmien toimintaperiaatteita yleisellä tasolla. Aluksi käydään läpi myös ns. salaisen avaimen kryptologiaa eli symmetrisen avaimen salausta, koska sitä käytetään yleensä julkisen avaimen teknologioiden yhteydessä. Tarkoituksena on selvittää eri salausmenetelmien toimintaperiaatteita siinä määrin kuin on tarpeellista tutkimuksen varsinaisen asian ymmärtämisen kannalta. Tarkemmat matemaattiset esitykset lukija voi hakea halutessaan lähdekirjallisuudesta, johon on useita viittauksia.

3.1. Symmetrisen avaimen salaus

Voidakseen kommunikoida turvallisesti, kommunikoinnin osapuolten on salattava välillään kulkeva informaatio. Alla on kuvattu kommunikoinnin salaamiseen tarvittavat vaiheet esimerkkihenkilöiden avulla. Liisa lähettää salatun viestin Pekalle [Schneier, 1996].

1. Liisa ja Pekka sopivat käytettävästä salausjärjestelmästä.
2. Liisa ja Pekka sopivat käytettävästä salausavaimesta.
3. Liisa salaa selväkielisen viestinsä käyttäen salausalgoritmia ja salausavainta. Tuloksena on salattu viesti.
4. Liisa lähettää salatun viestin Pekalle.
5. Pekka purkaa salatun viestin käyttämällä samaa algoritmia ja salausavainta. Lopputuloksena on selväkielinen viesti.



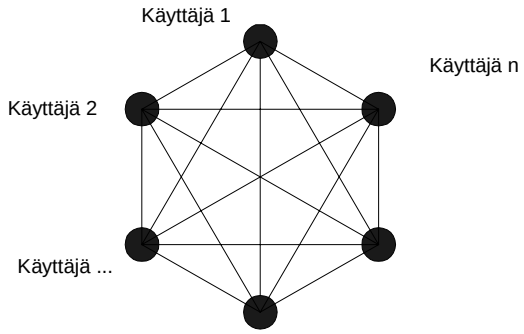
Kuva 3.1: Symmetrinen salaus

Symmetrisen avaimen salauksesta on keskeistä ymmärtää se, että viesti salataan ja salaus puretaan samalla avaimella (kuva 3.1). Hyvän salausjärjestelmän varmuus perustuu käytetyn avaimen salaisuuteen eikä käytetyn algoritmin salaisuuteen [Schneier, 1996]. Tästä syystä avainten hallinta on kriittisessä asemassa.

Liisan ja Pekan on siten löydettävä jokin turvallinen keino sopia käytettävästä avaimesta, jotta avain ei joutuisi mahdollisen salakuuntelijan käsiin. Avaimen on luonnollisesti pysyttävä salaisena niin kauan kuin itse viestin on pysyttävä salaisena.

Salakuuntelija voi siis lukea kaikki kyseisellä avaimella salatut viestit saatuaan avaimen haltuunsa. Saatuaan avaimen haltuunsa, salakuuntelija voi lisäksi teeskennellä olevansa joku kommunikoinnin osapuolista ja lähettää salattuja viestejä toisen nimissä.

Yksi symmetrisen salauksen ongelmista on avainten hallinta. Jos oletetaan, että jokainen verkossa kommunikoiva pari käyttää eri avainta, käytettyjen avainten määrä kasvaa nopeasti käyttäjien määrän kasvaessa. Jos verkossa on *n* käyttäjää, tarvitaan *n(n-1)/2* avainta [Schneier, 1996]. Esimerkiksi 10 käyttäjän verkostossa tarvitaan 45 eri avainta, mutta 100 käyttäjän verkostossa tarvittavien avainten määrä on jo 4950, kun siis oletetaan, että verkoston kaikki jäsenet kommunikoivat toistensa kanssa (kuva 3.2).



Kuva 3.2: Käyttäjäverkoston rakenne symmetrisen avaimen järjestelmässä, [Kerttula, 1999]

Ehkä parhaiten tunnettuja moderneja symmetrisen salauksen algoritmeja ovat mm. DES (Data Encryption Standard) ja IDEA (International Data Encryption Standard). Esimerkiksi Menezes ja muut [Menezes, Oorschot, Vanstone, 1999] selvittävät tarkasti algoritmien toimintaperiaatteita.

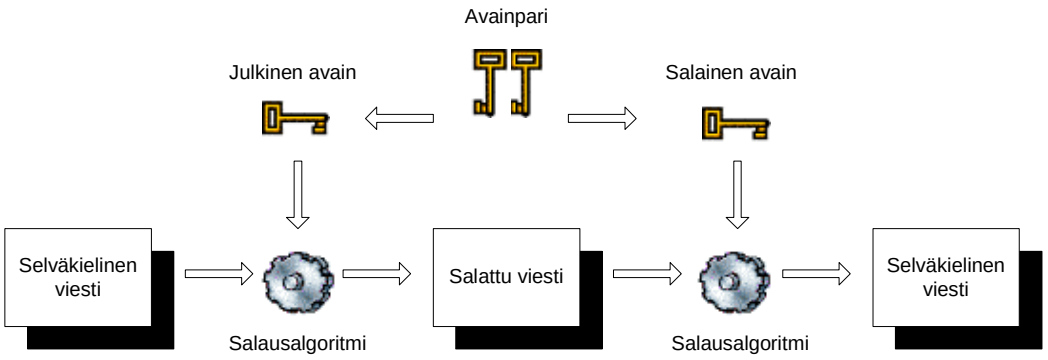
Seuraavassa alakohdassa tarkastellaan epäsymmetrisen avaimen eli julkisen avaimen salausta, joka tarjoaa ratkaisun mm. avainten hallintaan.

3.2. Epäsymmetrisen avaimen salaus

Julkisen avaimen salausta pidetään tärkeimpänä modernina tietoturvateknologiana. Teknologiaa käytetään salaamiseen, autentikointiin ja avainten hallintaan.

Julkisen avaimen salaus perustuu avainparin käyttöön. Jokaisella käyttäjällä on kaksi avainta, jotka muodostavat yhdessä ns. avainparin. Toista avaimista kutsutaan julkiseksi avaimeksi ja toista salaiseksi avaimeksi. Avainten nimeämiskäytäntö muodostuu avainten ominaisuuksien mukaan. Käyttäjän on pidettävä salainen avain nimensä mukaisesti aina salaisena, julkisen avaimen voi sen sijaan paljastaa kenelle tahansa ja itse asiassa se on jopa tarkoituksena. Avaimet toimivat toistensa vastinpareina, salaisella avaimella salattu viesti voidaan saada auki vain vastaavalla julkisella avaimella ja päinvastoin (kuva 3.3).

Käyttäjä voi esimerkiksi siirtää julkisen avaimensa yleiselle tiedostopalvelimelle, josta kuka tahansa voi käydä avaimen hakemassa. Teknologian toimintaperiaatteesta johtuen, kuka tahansa julkisen avaimen haltija voi salata kommunikaation itsensä ja vastaavan salaisen avaimen haltijan kanssa ja olla varma siitä että ainoastaan vastaavan salaisen avaimen haltija voi purkaa salauksen.



Kuva 3.3: Epäsymmetrinen salaus

Kerttula [Kerttula, 1999] on verrannut tilannetta lukittuun postilaatikkoon. Kuka tahansa voi pudottaa kirjeen postilaatikkoon (salaus julkisella avaimella),

mutta ainoastaan postilaatikon omistaja voi avata postilaatikon ja lukea kirjeen (purkaminen salaisella avaimella).

Kuten tämän alakohdan alussa jo mainittiin, julkisen avaimen teknologiaa käytetään salaukseen (ja purkamiseen), autentikointiin eli digitaalisiin allekirjoituksiin sekä avainten jakeluun. Salauksen periaate on selitetty edellisissä kappaleissa, seuraavaksi käydään läpi digitaalinen allekirjoitus sekä tämän tutkimuksen näkökulmasta vähemmän tärkeä avainten hallinta.

Digitaalinen allekirjoitus mahdollistaa luotettavan oikeaksi todistamisen eli *autentikoinnin*, se takaa viestin *eheyden* ja tarjoaa tuen *kiistämättömyydelle*. Lähettäjä allekirjoittaa (salaa) viestin omalla salaisella avaimellaan. Allekirjoitus kohdistetaan koko viestiin tai ns. tiivisteeseen (digest), joka on *hash-funktiolla* alkuperäisestä viestistä saatu pienempi objekti. Luonnollisesti jokainen, jolla on hallussaan allekirjoituksessa käytettyä salaista avainta vastaava julkinen avain, pystyy purkamaan allekirjoituksen. Jos viesti pystytään onnistuneesti julkisella avaimella purkamaan, voidaan olla varmoja, että julkista avainta vastaavan salaisen avaimen haltija on viestin allekirjoittanut (*autentikointi*). Toimintaperiaatteesta johtuen allekirjoittaja ei voi myöskään myöhemmin väittää, ettei olisi allekirjoittanut viestiä (*kiistämättömyys*).

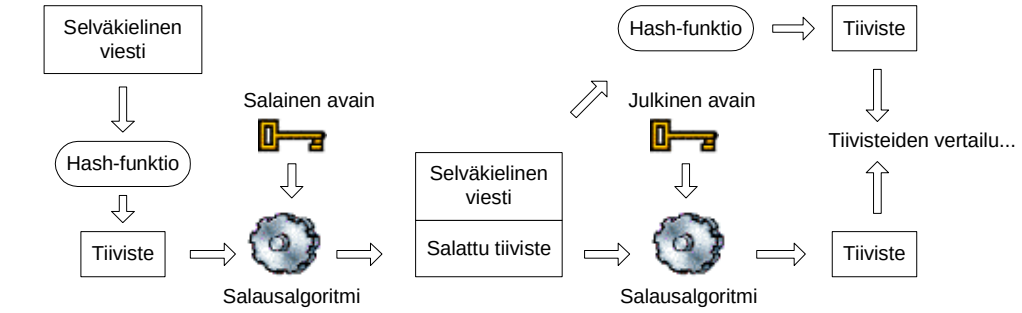
Tiiviste saadaan alkuperäisestä viestistä yksisuuntaisen hash-funktion avulla. Hash-funktio tuottaa alkuperäisestä mielivaltaisen mittaisesta viestistä aina vakiomittaisen tiivisteen (pituus riippuu käytetystä funktiosta). Tiivisteen idea perustuu siihen, että vähänkin toisistaan poikkeavista viesteistä ei voi saada aikaan samanlaista tiivistettä, eikä tiivisteestä voida enää generoida alkuperäistä viestiä.

Tiivistettä voidaan käyttää digitaaliseen allekirjoitukseen symmetriseen salaukseen käytettävien salaisten avainten kanssa, tai vaihtoehtoisesti sitä voidaan käyttää digitaaliseen allekirjoitukseen tässä yhteydessä tarkasteltavan julkisen avaimen järjestelmän kanssa.

Oletetaan, että Liisa haluaa allekirjoittaa Pekalle lähetettävän viestinsä. Liisa muodostaa viestistä tiivisteen, ja salaa sen omalla salaisella avaimellaan. Tämän jälkeen Pekalle lähetetään sekä alkuperäinen viesti että viestistä generoitu salattu tiiviste. Pekka vastaanottaa molemmat ja muodostaa saamastaan viestistä itselleen tiivisteen. Tämän jälkeen Pekka avaa Liisan lähettämän tiivisteen käyttämällä Liisan julkista avainta ja vertaa omaa ja Liisan lähettämää

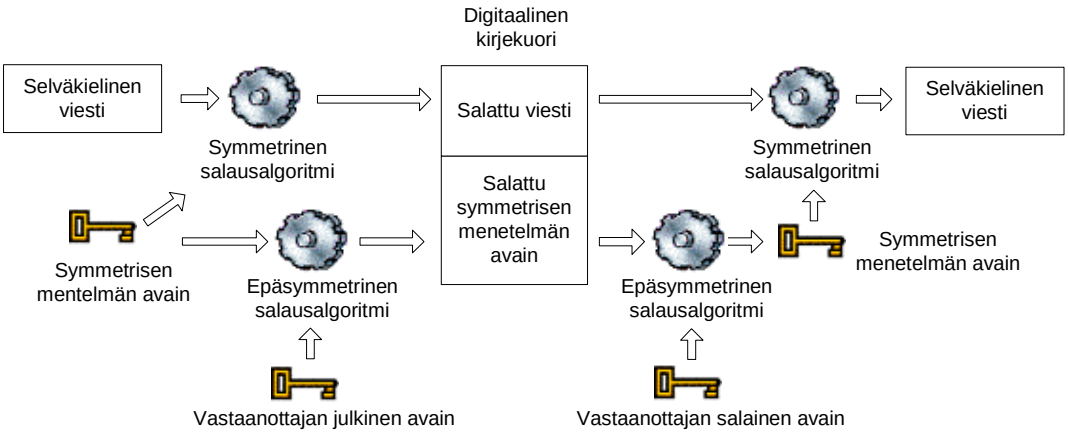
tiivistettä toisiinsa (kuva 3.4). Jos tiivisteet ovat yhtenevät, Pekka voi olla varma siitä, että Liisa lähetti viestin ja ettei kukaan ole muuttanut viestiä (*eheys*).

Tiivistettä käytetään julkisen avaimen järjestelmässä siksi, että varsinainen salaaminen julkisen avaimen järjestelmällä on hidasta. On paljon nopeampaa salata pieni osa viestistä eli tiiviste. Toimintaperiaate ja varmuus säilyvät silti.



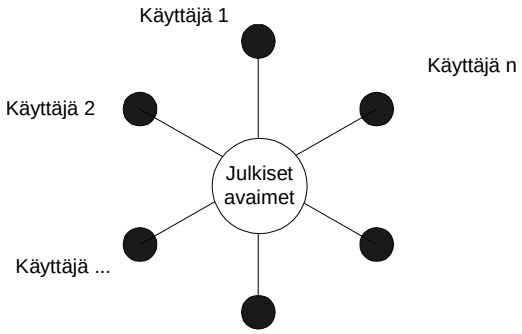
Kuva 3.4: Digitaalinen allekirjoitus

Juuri julkisen avaimen teknologian hitaudesta johtuen käytännön sovelluksissa käytetäänkin symmetristä ja epäsymmetristä salausta yhdessä. Symmetristä salausta ja sen ns. istuntokohtaista salaista avainta käytetään varsinaisen viestin salaamiseen, koska symmetrinen salaus on tyypillisesti nopeampaa kuin epäsymmetrinen salaus. Istuntokohtainen salainen avain salataan vuorostaan vastaanottajan julkisella avaimella. Vastaanottajalle lähetetään siis symmetrisellä menetelmällä salattu varsinainen viesti ja epäsymmetrisellä menetelmällä salattu istuntokohtainen avain. Tätä kokonaisuutta kutsutaan *digitaaliseksi kirjekuoreksi* (kuva 3.5). Näin saadaan aikaan tehokas tapa kommunikoida turvallisesti.



Kuva 3.5: Digitaalinen kirjekuori

Julkisen avaimen menetelmä helpottaa jo itsessään avainten hallintaa. Avaimia tarvitaan huomattavasti vähemmän kuin symmetrisen salauksen menetelmässä, eikä avainten jakelu edellytä salaisia kanavia. Edellisessä alakohdassa mainittiin symmetrisen salauksen vaativan *n(n-1)/2* avainta *n* käyttäjän verkossa, eli 100 käyttäjän verkossa 4950 avainta. Julkisen avaimen menetelmällä tarvitaan vain *2n* avainta, eli jokaista käyttäjää kohden avainpari. 100 käyttäjän verkossa siis vain 200 avainta (kuva 3.6).



Kuva 3.6: Käyttäjäverkoston rakenne epäsymmetrisen avaimen järjestelmässä, [Kerttula, 1999]

Lisäksi mainittakoon kuriositeettina, että esimerkiksi julkisen avaimen kryptografiaan perustuvaa *Diffie–Hellman* algoritmia voidaan käyttää yhteisen salaisen avaimen luontiin ilman salaista jakelukanavaa [Menezes, Oorschot, Vanstone, 1999].

Kaikki julkisen avaimen algoritmit eivät kuitenkaan tue sekä salausta, digitaalista allekirjoitusta ja avainten jakelua. Nykypäivänä julkisen avaimen algoritmeista pidetään tärkeimpänä RSA-algoritmia. Se tukee kaikkia edellä mainittuja ominaisuuksia.

Julkisten avainten algoritmien varmuus perustuu erittäin vaikeaan matemaattiseen ongelmaan, joka RSA:n tapauksessa on luvun tekijöihin jakaminen [Schneier, 1996].

Sekä symmetrisen että epäsymmetrisen salauksen algoritmeja voidaan murtaa usealla eri menetelmällä. Niin sanottua raa'an voiman (brute force) menetelmää voidaan käyttää molempien salaustyyppien yhteydessä. Tekniikka perustuu yksinkertaisesti siihen, että yritetään arvata käytetty salausavain. Käytännössä eri avainvaihtoehtoja käydään läpi niin kauan kunnes viesti saadaan auki eli oikea avain löytyy. Raa´an voiman murron estämisessä ratkaisevassa asemassa on käytetyn salausavaimen pituus. Esimerkiksi 128 bitin avaimella avainvaihtoehtoja on 2^{128}, joka on noin 10^{38} eri vaihtoehtoa. RSA laboratories [RSA] on suositellut avainpituuksia eri menetelmille riippuen käyttötarkoituksesta. Taulukkoon 3.1 on koottu suositukset (toukokuu, 2000) symmetrisen lohkosalaajan ja RSA-menetelmän osalta.

Sovellusalue	**Symmetrinen lohkosalaaja**	**RSA(modulus)**
Henkilökohtaisen tason käyttö	56 / 64 bittiä	768 bittiä
Kaupallisen tason käyttö	128 bittiä	1024 bittiä
Sotilaskäyttö	160 bittiä	2048 bittiä

Taulukko 3.1: Symmetrisen ja epäsymmetrisen menetelmän suositeltuja avainpituuksia

Keskeinen ongelma julkisen avaimen salausteknologiassa on kuitenkin julkisen avaimen luotettavuus. Mistä voimme tietää, että julkinen avain kuuluu juuri tietylle henkilölle, eikä salakuuntelija ole esimerkiksi vaihtanut omaa julkista avaintaan tilalle? Julkisen avaimen infrastruktuuri ratkaisee tämän ongelman. Seuraavassa alakohdassa esitellään mm. keskeisesti julkisen avaimen infrastruktuuriin liittyvä käsite *luotettu kolmas osapuoli*.

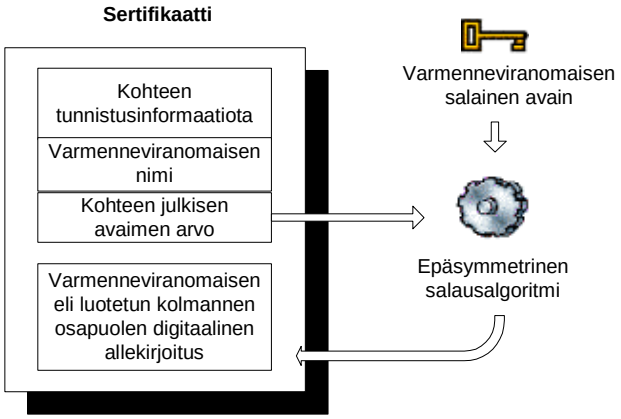
3.3. Julkisen avaimen infrastruktuuri

Julkisen avaimen infrastruktuurilla (PKI, Public Key Infrastructure) tarkoitetaan julkisen avaimen salaukseen, digitaaliseen allekirjoitukseen ja avainten hallintaan tarvittavaa järjestelmää kokonaisuutena, kun taas itse salausta, digitaalista allekirjoitusta ja avainten hallintaa kutsutaan julkisen avaimen infrastruktuurin sovelluksiksi.

Yhtenä PKI:n tärkeimpänä ominaisuutena pidetään järjestelmän transparenttisuutta eli läpinäkyvyyttä käyttäjän näkökulmasta. Toisin sanoen järjestelmän käyttö tulisi olla mahdollisimman helppoa ja huomaamatonta. Läpinäkyvyyden lisäksi PKI-järjestelmän tulee toteuttaa seuraavat toiminnot avainten hallintapalveluja varten [Kerttula, 1999]:

- julkisen avaimen sertifikaatit
- sertifikaattien säilytyspaikka
- sertifikaattien kumoaminen
- avainten varmuuskopiointi ja palauttaminen
- tuki digitaalisten allekirjoitusten kiistämättömyydelle
- automaattinen avainparien ja sertifikaattien päivitys
- avainhistorian ylläpito
- tuki ristiinvarmennukselle
- työaseman ohjelmisto, joka toimii PKI-toimintojen kanssa turvallisella, yhtenäisellä ja luotettavalla tavalla.

Edellä mainittu lista luetteloi toimivan PKI-järjestelmän kannalta välttämättömiä toimintoja. PKI ratkaisee edellisessä alakohdassa mainitun julkisen avaimen luottamusongelman sertifikaatin, eli *varmenteen* muodossa. Varmennetta voidaan pitää esimerkiksi passin vastineena. Varmenne on objekti, joka pitää sisällään henkilön identifioimiseen tarvittavia tietoja, esimerkiksi omistajan nimen. Lisäksi varmenne sisältää omistajan julkisen avaimen (kuva 3.8). Varmenteen allekirjoittaa omalla salaisella avaimellaan ns. *luotettu kolmas osapuoli*, joka käydään läpi seuraavaksi.



Kuva 3.8: Yksinkertainen sertifikaatti eli varmenne, mukaillen [Kerttula, 1999]

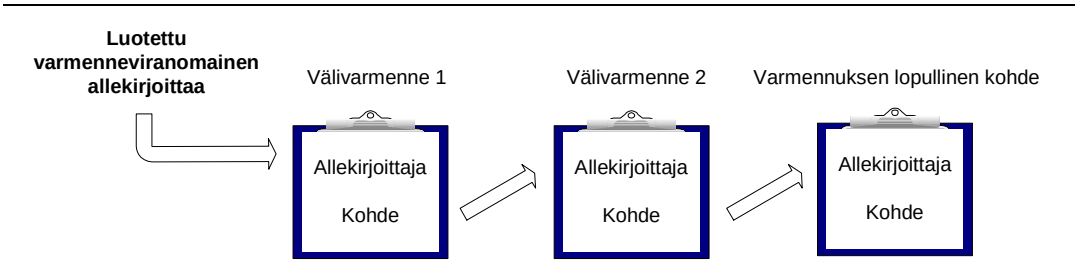
Luotetun kolmannen osapuolen (TTP, Trusted Third Party) palveluja tarjoavia instansseja on ollut olemassa jo pitkään. Esimerkiksi postit ja pankit ovat sellaisia. Kyse on yksinkertaisesti siitä, että jotain tahoa pidetään riittävän luotettavana hoitamaan toisten asioita. Pankin tapauksessa asiakkaat voivat luottaa implisiittisesti toisiinsa, vaikka eivät olisi koskaan luoneet luottamuksellista suhdetta keskenään. Pankki toimii osapuolena, johon kaikki asiakkaat luottavat, joten myös asiakkaiden välille muodostuu luottamussuhde. Se mahdollistaa tässä tapauksessa esimerkiksi varainsiirtojen tekemisen.

PKI:n tapauksessa luotettuna kolmantena osapuolena toimii varmenneviranomainen (CA, Certification Authority). Varmenneviranomaisen keskeinen tehtävä on varmentaa käyttäjien autenttisuus. Toimintaa voidaan verrata henkilölle passin myöntävän viranomaisen toimintaan. Varmenneviranomainen varmentaa samalla tavalla käyttäjän identiteetin (varmenne voidaan myöntää esimerkiksi myös organisaatiolle tai jopa laitteelle) ja myöntää hakijalle passin sijasta elektronisen todisteen autenttisuudestaan, eli varmenteen.

Käyttäjät voivat nyt varmistua varmenteen oikeellisuudesta todentamalla allekirjoituksen varmenneviranomaisen julkisella avaimella eli *juurivarmenteella.* Näin kaikkien varmenneviranomaiseen luottavien käyttäjien välille voi muodostua keskinäinen luottamus.

Varmenneviranomaisen toimintaan liittyy lisäksi kaksi tärkeää käsitettä, varmenneviranomaisen alue (CA-domain) ja ristiinsertifiointi (cross-serfication). Varmenneviranomaisen alueella tarkoitetaan sitä toimialuetta, jolla

varmenneviranomainen on valtuutettu myöntämään varmenteita. Vertauksena passin myöntävä viranomainen, joka voi myöntää passeja vain tietyn maan kansalaisille. Ei olisi myöskään tarkoituksenmukaista, jos yksi varmenneviranomainen hoitaisi kaikkien varmenteiden myöntämisen. Liiketoiminta-alue on avoin kilpailulle ja niinpä on olemassa useita varmenneviranomaisia. Ongelmaksi muodostuu luottamus eri varmenneviranomaisten välillä. Voiko käyttäjä luottaa varmenteeseen, jonka on myöntänyt eri varmenneviranomainen, kuin johon itse luottaa? Ratkaisuna on ristiinvarmennus. Ristiinvarmennuksella tarkoitetaan tilannetta, jossa varmenneviranomainen allekirjoittaa toisen varmenneviranomaisen juurivarmenteen. Näin saadaan aikaan luottamusketju, joka voi olla periaatteessa mielivaltaisen pitkä. Käyttäjällä tarvitsee olla hallussaan mahdollisesti vain yksi juurivarmenne, jonka avulla voidaan osoittaa koko varmenneketju autenttiseksi (kuva 3.9).



Kuva 3.9: Varmennusketju

Ristiinvarmennukseen liittyy myös aina kysymys eri varmenneviranomaisten tietoturvapolitiikasta, onko eri varmenneviranomaisten käytännöt ja niiden nauttima luottamus samalla tasolla. Koko PKI-järjestelmän toiminta perustuu juuri luotetun kolmannen osapuolen luotettavuuteen.

Seuraavassa kohdassa käydään läpi SET-spesifikaatiota, joka käyttää tietoturvaratkaisussaan juuri julkisen avaimen järjestelmää.

4. Julkisen avaimen teknologia SET-protokollassa

Esittelen ensimmäisessä kohdassa järjestelmän yleisellä tasolla, toisessa kohdassa tarkastellaan SET:n tarjoamia ominaisuuksia ja kolmannessa kohdassa käydään läpi SET:n tietoturvaratkaisu.

4.1. Yleistä

SET-protokolla on Visa:n ja MasterCard:n kehittämä avoin standardi. Sen perusajatuksena on mahdollistaa turvallinen maksukorttien käyttö avoimessa verkossa, kuten internetissä. Alla on esitelty SET-protokollan seitsemän alkuperäistä liiketoimintavaatimusta [SET1] ja neljä osapuolta, jotka ovat toimijoina SET-tapahtumassa.

SET-liiketoimintavaatimukset:

1. maksuinformaation ja tilausinformaation luottamuksellisuuden tarjoaminen transaktiossa
2. kaiken siirrettävän informaation eheyden takaaminen
3. autentikaation tarjoaminen maksukortin käyttäjän tunnistamiseksi
4. autentikaation tarjoaminen siten, että voidaan varmistaa myyjän valmius vastaanottaa tietyntyyppisellä maksukortilla tehtäviä transaktioita
5. parhaiden mahdollisten tietoturvakäytäntöjen ja järjestelmän suunnittelutekniikoiden käytön varmistaminen kaikkien transaktion osapuolien suojaamiseksi
6. protokollan luominen, joka ei ole riippuvainen tietoturvaratkaisuista eikä toisaalta estä niiden käyttöä
7. yhteensopivuuden toteuttaminen ja edistäminen ohjelmistotoimittajien ja verkkotoimittajien välillä.

SET-tapahtuman osapuolet:

1. asiakas (kortinhaltija)
2. kauppias
3. asiakkaan pankki
4. kauppiaan pankki.

Yleisellä tasolla SET-tapahtuma on yksinkertainen. Asiakas hankkii pankiltaan maksukortin (esimerkiksi tavallinen luottokortti), jolla voidaan tehdä tilauksia kauppiaalta. Kauppias tarkistaa maksukortin oikeellisuuden pankkien kautta ennen tilauksen hyväksymistä. Todellisuudessa kyseessä on monimutkainen prosessi, joka esitellään tarkemmin kohdassa 4.3 tietoturvaratkaisun esittelyn yhteydessä.

4.2. Ominaisuuksia

SET-protokolla mahdollistaa kaikki samat toimenpiteet, jotka ovat olemassa perinteisessä luottokorttijärjestelmässä [Kerttula, 1999]:

- kortinhaltijan rekisteröinti
- kauppiaan rekisteröinti
- ostopyynnöt
- maksujen vahvistukset
- rahansiirrot (maksujen ottaminen, rahanpalautukset)
- luotot
- luottojen irtisanominen
- pankkikorttitapahtumat.

Autentikointi, luottamuksellisuus ja *sanoman eheys* ovat SET:n keskeiset tietoturvaominaisuudet.

4.3. Tietoturvaratkaisu

SET:n käyttämä tietoturvaratkaisu perustuu julkisen avaimen infrastruktuuriin. Kohdassa 4.1 mainittujen osapuolten lisäksi järjestelmä vaatii toimiakseen viidennen osapuolen, varmenneviranomaisen. Varmenneviranomainen myöntää sertifikaatit asiakkaan ja kauppiaan pankeille. Asiakas ja kauppias rekisteröityvät molemmat SET-järjestelmään omien pankkiensa kautta. SET-ohjelma generoi asiakkaalle julkisen / salaisen avaimen parin rekisteröitymisen yhteydessä. Pankki allekirjoittaa asiakkaan julkisen avaimen ja toimittaa sen sertifikaattina asiakkaalle. Samoin kauppiaan pankki antaa kauppiaalle sertifikaatin rekisteröitymisen yhteydessä.

SET käyttää hash-funktiona 160-bitin pituisen tiivisteen luovaa SHA-algoritmia. Symmetrisenä salausalgoritmina on oletuksena DES, vaikka SET:ssä onkin mahdollista käyttää myös muita symmetrisiä algoritmeja. Kaikissa julkisen avaimen operaatioissa käytetään RSA:n julkisen avaimen algoritmia, siinä käytetty avainten pituus on 1024-bittiä.

[Kerttula, 1999] on esittänyt tyypillisen SET-myyntitapahtuman yhdeksänä eri vaiheena seuraavasti.

1. *Asiakas aloittaa ostamisen*. Asiakas valitsee ostoksensa kauppiaan Web-sivuilta ja täyttää kauppiaan tilauskaavakkeen, joka sisältää tiedot ostoksesta ja toimituksesta. Varsinainen SET-protokolla käynnistyy kun asiakas haluaa lopuksi maksaa ostoksensa ja painaa lomakkeella olevaa ”maksa”-, tms. painiketta. Kauppiaan palvelin lähettää asiakkaalle sanoman, joka lataa asiakkaan koneelle SET-ohjelmiston.

2. *Asiakkaan ohjelma lähettää tilauksen ja maksutiedot.* Asiakkaan SET-ohjelmisto luo kaksi sanomaa. Sanoman, joka sisältää tuotteen tilausinformaation (mm. toimitustiedot) ja sanoman, joka sisältää maksuinformaation (asiakkaan pankkitiedot). Tilausinformaatio salataan symmetrisellä istuntoavaimella ja siitä muodostetaan digitaalinen kirjekuori käyttämällä kauppiaan julkista avainta. Maksutiedot puolestaan salataan käyttämällä kauppiaan pankin julkista avainta. Näin kauppiaalla ei ole missään vaiheessa mahdollisuutta päästä suoraan käsiksi asiakkaan pankkitietoihin, eikä pankilla mahdollisuutta päästä suoraan käsiksi tilaustietoihin. Lopuksi asiakkaan SET-ohjelma laskee tilaus- ja maksuinformaation yhdistelmästä tiivisteen, joka allekirjoitetaan asiakkaan salaisella avaimella. Näin saadaan aikaan ns. kaksoisallekirjoitus, joka mahdollistaa sen, että kauppias ja kauppiaan pankki voivat olla varmoja molempien sanomien eheydestä, mutta samaan aikaan kumpikin voi lukea vain itselleen tarkoitetun informaation.

3. *Kauppias siirtää maksutiedot pankkiin.* Kauppias muodostaa tilausvaltuuspyynnön, josta generoidun tiivisteen kauppias allekirjoittaa salaisella avaimellaan. Pyyntö salataan istuntoavaimella ja pakataan digitaaliseen kirjekuoreen käyttämällä pankin julkista avainta. Lopuksi kauppiaan palvelimen SET-ohjelmisto siirtää pyynnön (asiakkaan maksutiedot) edelleen pankin SET-palvelimelle.

4. *Pankki tarkistaa kortin voimassaolon.* Pankki todentaa kauppiaan identiteetin ja purkaa valtuuspyynnön. Sen jälkeen pankki purkaa asiakkaan maksuinformaation ja todentaa asiakkaan identiteetin. Lopuksi kauppiaan pankki tarkistaa pyynnön asiakkaan pankin kanssa

luomalla oman valtuuspyynnön, jonka se allekirjoittaa ja lähettää asiakkaan maksukortin myöntäjälle (asiakkaan pankille).

5. *Kortin myöntäjä vahvistaa ja allekirjoittaa tilauslipukkeen.* Asiakkaan pankki todentaa kauppiaan pankin identiteetin ja tutkii asiakkaan luottotiedot. Jos tiedot ovat kunnossa, asiakkaan pankki hyväksyy valtuuspyynnön allekirjoittamalla ja lähettämällä sen takaisin kauppiaan pankille.

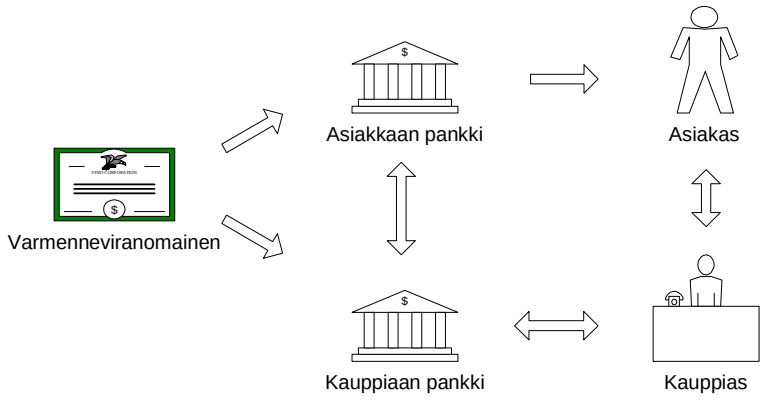
6. *Kauppiaan pankki vahvistaa tapahtuman.* Kauppiaan pankki vahvistaa tilausvaltuuspyynnön allekirjoittamalla ja lähettämällä sen takaisin kauppiaalle.

7. *Kauppiaan Web-palvelin päättää tapahtuman.* Kauppias vahvistaa tilauksen asiakkaalle ja siirtää tilauksen järjestelmäänsä käsiteltäväksi.

8. *Kauppias sulkee tapahtuman.* Lopuksi kauppias lähettää omalle pankilleen lopetusviestin, jolla vahvistetaan ostos. Tämän jälkeen asiakkaan maksukorttitiliä laskutetaan ja kauppiaan tiliä hyvitetään.

9. *Kortin myöntäjä lähettää luottokorttilaskun asiakkaalle.* SET-maksu näkyy asiakkaan tiliotteessa normaalisti muiden maksujen tapaan.

Kuvassa 4.1 havainnollistetaan edellä kuvatun SET-myyntitapahtuman informaatiovirtojen kulkua.



Kuva 4.1: SET-tapahtuman osapuolet

Jokaisessa SET-protokollan vaiheessa suoritetaan autentikointi. Näin voidaan estää tunkeilijan sekaantuminen maksutapahtumaan. Julkisen avaimen teknologialla toteutetaan ja suojataan SET:ssä mm. seuraavia asioita:

- salataan maksuinformaatiota. Maksuinformaatio ei kulje internetissä missään vaiheessa salaamattomana, eikä informaatiota talleteta esimerkiksi kauppiaan palvelimelle
- kauppiaat ja pankit voivat tunnistaa asiakkaan. Näin estetään varastettujen korttien käyttö
- asiakkaat ja pankit voivat tunnistaa kauppiaan. Tällä estetään tunkeutujien esiintyminen kauppiaina
- asiakkaat ja kauppiaat voivat tunnistaa pankit, jolla estetään tunkeutujan esiintyminen pankkina (korttiyhtiönä)
- tapahtumien eheyden takaaminen, jolla estetään suojaamattomassa verkossa kuten internetissä mahdollinen tietojen muuttaminen.

SET on eräs sähköisen kaupankäynnin sovelluksista, jossa tietoturvakysymys on ratkaistu PKI:n avulla. Julkisen avaimen menetelmää käytetään SET-prosessissa salaamaan informaatiota, prosessin osapuolten tunnistamiseen ja informaation eheyden varmistamiseen.

Sähköisten lippujen kohdalla tilanne on tietyiltä osin erilainen. Sähköinen lippu on maksuväline, jolla on itsessään arvoa. Lipun sisältämää informaatiota ei ole tarkoituksenmukaista salata, eikä lipun haltijaa tarvitse välttämättä autentikoida, koska on mahdollista että lippu ei ole henkilökohtainen. Tärkeää on kuitenkin lipun eheyden suojaaminen. Tällä varmistetaan, että esimerkiksi lipun voimassaoloaikaa ei voida muuttaa luvattomasti.

Tämän tutkimuksen tarkoituksena on selvittää julkisen avaimen teknologian mahdollisuuksia sähköisten lippujen tietoturvaratkaisuna. Koska sähköinen lippu on verrattavissa mihin tahansa arvoa sisältävään sähköiseen entiteettiin, on lippujen kopiointisuojaukseen kiinnitettävä erityistä huomiota.

Seuraavassa luvussa esitellään sähköiset liput ja määritellään vaatimuksia tietoturvan ja erityisesti kopiointisuojauksen kannalta.

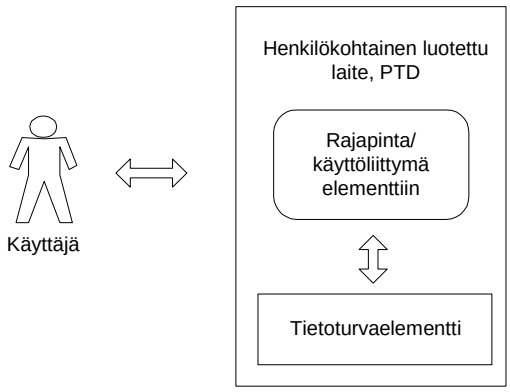
5. Sähköiset liput

Tässä luvussa esitellään MeT-yhteenliittymä ja sen käyttämä käsite sähköinen lippu. Ensimmäisessä kohdassa käydään läpi MeT:n rakennetta yleisellä tasolla. Toisessa kohdassa esitellään MeT:n sähköinen lippu käsite. Lippujen ominaisuuksia käsitellään kolmannessa kohdassa erityisesti tietoturvan näkökulmasta. Neljännessä kohdassa esitellään lippujen jakelua ja hallintaa. Viimeisessä kohdassa kootaan luvun asiat yhteen ja tarkennetaan vaatimukset tietoturvaratkaisulle, jotka seuraavassa luvussa määriteltävällä viitekehyksellä pyritään täyttämään. Ainoastaan tutkimuksen varsinaisen asian ymmärtämisen kannalta tärkeät käsitteet on erikseen selitetty. Muussa tapauksessa lukijalle tarjotaan viite sopivaan lähteeseen.

5.1. MeT

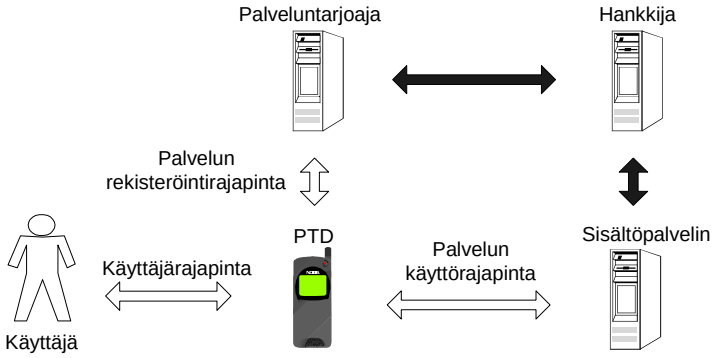
MeT on aloite, jonka ovat käynnistäneet Ericsson, Motorola ja Nokia huhtikuussa 2000. Tavoitteena on luoda yhteinen viitekehys sähköiselle kaupankäynnille käyttäen mobiilia päätelaitetta. Yhteenliittymä julkaisee internetissä spesifikaatioita, joissa määritellään MeT:n eri osa-alueet. Tällä hetkellä spesifikaatioista on julkaistu versiot 1.1 (7.10.2002).

Yhteenliittymä uskoo matkapuhelimen kehittyvän lähitulevaisuudessa henkilökohtaiseksi luotetuksi päätelaitteeksi (PTD, Personal Trusted Device) [MeTPTD], jonka avulla voidaan turvallisesti suorittaa sähköisiä transaktioita. PTD on henkilökohtainen laite, jonka ajatellaan kulkevan käyttäjän mukana suurimman osan ajasta matkapuhelimen tapaan. PTD sisältää tietoturvaelementin, joka suojaa salausavaimia ja jonne esimerkiksi juurivarmenteet voidaan tallentaa. Elementti tarjoaa operaatiot avainten ja varmenteiden käyttöön. Tietoturvaelementti voi olla irrallinen älykortti, jolloin se on toteutettu Wireless Identity Module [WIM] spesifikaation mukaan, tai se voi olla kiinteästi laitteessa joko laite- tai ohjelmistototeutuksena. Elementtiin voidaan kohdistaa operaatioita vasta sen jälkeen, kun käyttäjä on syöttänyt henkilökohtaisen tunnuslukunsa PTD:lle. Tietoturvaelementin tarkoituksena on siis estää luvaton pääsy tietoturvan kannalta kriittiseen informaatioon (kuva 5.1).



Kuva 5.1: PTD:n rakenne

MeT määrittelee geneerisen esityksen [MeTCore], jossa kuvataan sähköisen kaupankäynnin osapuolet ja jota voidaan käyttää lähtökohtana kaikille MeT:n tarjoamille toimintamalleille (kuva 5.2).



Kuva 5.2: MeT:n toiminnan viitekehys, mukaillen [MeTCore]

Malliin sisältyvät luonnollisesti PTD ja sen sisältämä tietoturvaelementti, jotka on kuvattu tämän kohdan alussa.

Sisältöpalvelimen kautta sisällöntuottaja tarjoaa tuotteitaan käyttäjälle. Sisältö voi olla mitä tahansa, esimerkiksi musiikkia, videokuvaa, kirjallisuutta jne.

Hankkija tarjoaa liiketoimintamalleja ja toimii kontaktina sisällöntuottajien ja palveluntarjoajien välillä. Hankkijaa ei välttämättä tarvita kaikissa MeT:n tarjoamissa toimintamalleissa, sisällöntuottaja voi olla suoraan yhteydessä palveluntarjoajiin ja joskus sisällöntuottajana ja palveluntarjoajana voi toimia sama taho.

*Palveluntarjoaja*n kautta käyttäjä voi rekisteröityä tietyn palvelun asiakkaaksi, palvelut voivat olla esimerkiksi sisältöpalveluita, tilipalveluita tai henkilökohtaisen informaation hallintapalveluita.

Entiteettien välille on määritelty luonnollisesti myös rajapinnat. Palveluntarjoajan ja hankkijan sekä sisältöpalvelimen ja hankkijan välisissä rajapinnoissa MeT hyödyntää kaupallisia ratkaisuja(tummat nuolet, kuva 5.2). Muut rajapinnat MeT määrittelee itse.

Palvelun käyttörajapinta määrittelee yhteyden sisältöpalvelimeen. Rajapinnan kautta käyttäjä voi ladata palvelimelta materiaalia turvallisen yhteyden yli.

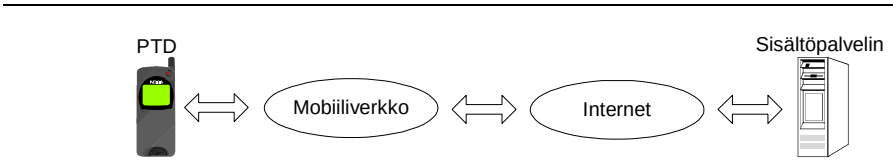
Palvelun rekisteröintirajapinta määrittelee yhteyden PTD:n ja palveluntarjoajan välille. Tämän rajapinnan kautta käyttäjä lataa itselleen palveluiden käyttöön tarvittavat varmenteet.

Käyttäjärajapinta määrittelee yhteyden käyttäjän ja PTD:n välille. Rajapinnan kautta käyttäjälle esitetään informaatiota PTD:n välityksellä, käyttäjältä voidaan pyytää syöte PTD:lle ja hyväksyttää transaktioita.

Tietoturvaelementin rajapinta määrittelee yhteyden PTD:n ja tietoturvaelementin välille (kuva 5.1). Sekä PTD:n siirtokerros että sovelluskerros käyttävät elementin tarjoamia operaatioita.

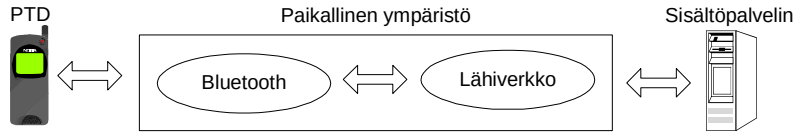
MeT määrittelee kolme erilaista ympäristöä joissa transaktiot tapahtuvat.

Etäympäristössä PTD on yhteydessä sisältöpalvelimeen julkisen mobiiliverkon, esimerkiksi GSM-verkon kautta (kuva 5.3).



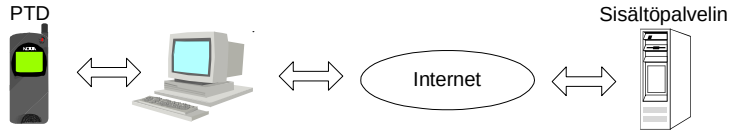
Kuva 5.3: Etäympäristö

Paikallisessa ympäristössä PTD on yhteydessä sisältöpalvelimeen lyhyen kantaman radioverkon, kuten esimerkiksi Bluetooth:n [BT] kautta (kuva 5.4). Tyypillinen käyttökohde on tuotteen maksaminen kaupassa PTD:llä.



Kuva 5.4: Paikallinen ympäristö

Henkilökohtaisessa ympäristössä PTD:tä käytetään ainoastaan käyttäjän autentikointiin ja tapahtuman hyväksymiseen. Varsinainen transaktio tapahtuu esimerkiksi PC:n kautta, johon PTD on liitettynä (kuva 5.5).



Kuva 5.5: Henkilökohtainen ympäristö

MeT:n tarkoituksena on hyödyntää toiminnoissaan olemassa olevia tietoturvateknologioita, kuten WTLS- (Wireless Transport Layer Security) tekniikkaa turvattujen yhteyksien luomiseen [WTLS], WIM- (Wireless Identity Module) teknologiaa salausavainten säilytykseen ja niihin liittyvien operaatioiden suoritukseen [WIM] ja WPKI- (Wireless Public Key Infrastructure) teknologiaa tarjoamaan langattomaan ympäristöön soveltuvan julkisen avaimen infrastruktuurin [WPKI]. Tekniikoita käytetään sähköisen kauppatapahtuman eri muodoissa ja vaiheissa.

5.2. Sähköiset liput

Sähköisten lippujen tarkka määrittely on MeT:llä vielä kesken. Tällä hetkellä käytettävissä on ns. keskusteludokumentti (Discussion Document) [MeTTF], johon on luonnosteltu mm. vaatimuksia sähköisille lipuille ja joitakin lippujen ominaisuuksia. Yleisesti sähköisellä lipulla tarkoitetaan digitaalista objektia, jossa on määritelty oikeus lunastaa tiettyjä tavaroita tai palveluita.

MeT:n on tarkoitus kehittää sähköisistä lipuista konsepti, joka pystyy tarjoamaan vastineen kaikille nykyään käytössä oleville paperilipuille. Tämän tyyppisiä lippuja ovat mm. erilaiset tapahtumaliput, kuten elokuva- ja konserttiliput, lentoliput, julkisen liikenteen liput, lottokupongit, ohjelmistolisenssit ja vähittäistavarakupongit.

Jokaisella lipputyypillä on omat erityisominaisuutensa, jotka joudutaan ottamaan huomioon. Esimerkiksi tapahtumalippu on kertakäyttöinen, mutta se voidaan yleensä siirtää jollekin toiselle henkilölle. Julkisen liikenteen liput taas asettavat hyvin korkeat suorituskykyvaatimukset sen sähköiselle versiolle. Lisäksi julkisen liikenteen lipuilla on tyypillisesti erilaisia jatkuvuusominaisuuksia, ne voivat olla kertakäyttöisiä tai ne voivat sisältää useamman käyttökerran. Lippu voi olla myös voimassa tietyn mittaisen ajanjakson, jonka aikana lippua voidaan käyttää ilman rajoituksia.

Lippujen lopullinen formaatti on keskusteludokumentin [MeTTF] mukaan vielä auki. Ehdotettuja formaatteja ovat mm. XML:ään perustuva formaatti [XMLT], joka on määritelty World Wide Web Consortium:n (W3C) kotisivuilla. Toinen mainittu vaihtoehto olisi käyttää vCard-teknologiaa [VCARD]. Formaatista riippumatta liput tulevat todennäköisesti sisältämään ainakin seuraavanlaisia kenttiä:

1. yleiset kentät. Esimerkiksi otsikko, käyttäjän tunnistenumero, lipun myöntäjän tunnistenumero, myöntäjän puhelinnumero ja sähköpostiosoite jne.

2. toimialaspesifiset kentät. Esimerkiksi tapahtuman nimi, tapahtuman alkamisaika, tapahtuman loppumisaika jne.

3. toimijaspesifiset kentät. Jotkut toimijat saattavat haluta sisällyttää lippuun esimerkiksi omaan tuotemerkkiinsä liittyvää tietoa.

MeT esittää myös sähköisiä lippuja vastaavan sähköisen kuitin käyttöä. Kuitti annettaisiin käyttäjälle vastineeksi sähköisestä lipusta ja se toimisi todisteena lipun hankinnasta. Kuittia voitaisiin käyttää esimerkiksi silloin, kun lippu halutaan vaihtaa uuteen tai palauttaa.

Lippujen ja kuittien säilytystä varten PTD:llä on tarkoitukseen soveltuva tietokanta. Tietokannassa voi olla myös linkki erillisellä palvelimella säilytettävään lippuun varsinaisen lipun sijasta.

5.3. Lippujen ominaisuuksista ja vaatimuksista

MeT:n keskusteludokumentti [MeTTF] määrittelee lipuille seuraavia ominaisuuksia ja vaatimuksia:

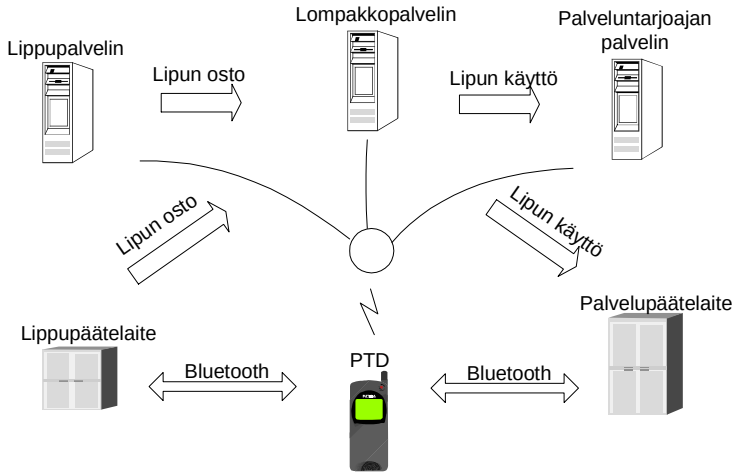
- lippujen tietoturvaratkaisun täytyy estää lippuinformaation luvaton muuttaminen. Ratkaisun on oltava varmuudeltaan vähintään sellainen, että eheyden rikkomisen kustannukset ovat suuremmat kuin saavutettava hyöty. Tämä tarjoaa mahdollisuuden käyttää edullisten lippujen yhteydessä varmuudeltaan heikompaa ratkaisua, joka saattaa olla esimerkiksi toiminnaltaan nopeampi. Ratkaisun on oltava lisäksi sellainen, että sitä voidaan käyttää tarpeen mukaan joko kokonaan, osittain, tai ei ollenkaan
- tietoturvaratkaisun on toimittava myös ilman verkkoyhteyttä, ns. paikallisessa ympäristössä
- lippujen on oltava jäljitettävissä tietyissä tapauksissa. Käyttäjän identifioivaa informaatiota on siis tarvittaessa pystyttävä sitomaan lippuun
- lipun siirtäminen on oltava mahdollista toiselle henkilölle siten, että alkuperäinen lippu menetetään
- lipun siirtäminen on oltava mahdollista omaan varalaitteeseen siten, että alkuperäinen lippu säilyy, tai se menetetään (varmuuskopiointi / varalaitteen käyttö)
- lipun kopiointi toiselle henkilölle on oltava mahdollista. Tämä tulee kysymykseen esimerkiksi kuponkien tapauksessa
- lipun kopioinnin ja siirtämisen estäminen on oltava mahdollista
- lippu voidaan määrittää joko kertakäyttöiseksi, sillä voi olla ennalta määrätty määrä käyttökertoja, se voi olla voimassa tietyn ajanjakson jolloin lippua voi käyttää rajoituksetta tai lippu voi olla voimassa jatkuvasti
- lippuinformaation täytyy olla lipun myöntäjän muokattavissa. Käyttäjä voi esimerkiksi haluta vaihtaa lipun voimassaoloaikaa.

5.4. Lippujen jakelu ja hallinta

Lippujen käytölle esitetään kahta eri mallia. Palvelinmallia ja asiakasmallia. Molemmat mallit sisältävät *lippupalvelimen*, *palveluntarjoajan palvelimen*, *lippupäätelaitteen*, *palvelupäätelaitteen* ja PTD:n. Palvelinmalli sisältää lisäksi ns. *lompakkopalvelimen* (wallet-server). Mallien tarkoituksena on antaa geneerinen kuva mahdollisista toiminnan toteutustavoista.

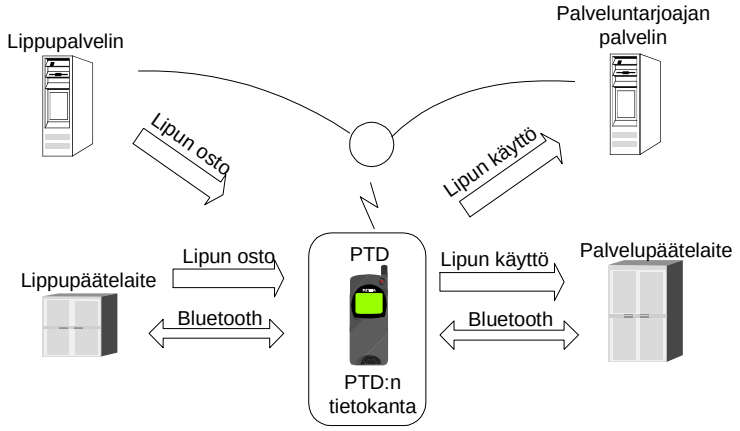
Palvelinmallissa käyttäjä voi hankkia lippuja lippupalvelimelta tai lippupäätelaitteelta. Liput lähetetään aina suoraan maksamisen jälkeen lompakkopalvelimelle, jossa asiakkaan lippuja säilytetään. Asiakkaan lunastaessa palvelua, lippu lähetetään lompakkopalvelimelta joko

palveluntarjoajan palvelimelle tai palvelupäätelaitteelle riippuen luonnollisesti siitä kumman kautta asiakas palvelun lunastaa (kuva 5.6).



Kuva 5.6: Palvelinmalli [MeTTF]

Asiakasmallista lompakkopalvelin puuttuu. Toimintaperiaate on yhtenevä palvelinmallin kanssa muilta osin. Lippujen säilytys tapahtuu lompakkopalvelimen sijasta aina PTD:n paikallisessa tietokannassa (kuva 5.7).



Kuva 5.7: Asiakasmalli, mukaillen [MeTTF]

Lippuja voisi MeT:n suunnitelmien mukaan myös varmuuskopioida esimerkiksi PC:lle tai etäpalvelimelle.

5.5. Vaatimukset tietoturvalle

Tietoturvaratkaisun tulisi siis mahdollistaa vähintään seuraavien kahdeksan ominaisuuden tai vaatimuksen toteutuminen:

1. lippuinformaation eheys on pystyttävä takaamaan
2. järjestelmän on toimittava myös paikallisessa ympäristössä
3. käyttäjän identifioivaa informaatiota on pystyttävä sitomaan lippuun
4. lipun siirtäminen on oltava mahdollista
5. lipun siirtämisen estäminen on oltava mahdollista
6. lipun kopiointi on oltava mahdollista
7. lipun kopioinnin estäminen on oltava mahdollista
8. järjestelmä ei saa estää lippujen käyttörajoitusten toimintaa.

6. Malli sähköisten lippujen tietoturvaratkaisuksi

Tämän luvun ensimmäisessä kohdassa esitellään lukijalle taustatiedoksi aiheeseen liittyvä digitaalisten käyttöoikeuksien hallinta (DRM, Digital Rights management) ja erilaisia kopiointisuojausmenetelmiä. Toisessa kohdassa pyritään määrittelemään julkisen avaimen teknologiaan perustuva järjestelmä, joka täyttäisi sille edellisen luvun lopussa esitetyt vaatimukset.

6.1. DRM:stä ja kopiointisuojaustekniikoista

Digitaalisten käyttöoikeuksien hallinnan menetelmät tarjoavat sisällöntuottajille mahdollisuuden suojata tuottamansa elektronisen sisällön väärinkäytöksiltä [DRM_Adobe]. Käyttöoikeuksien hallinnan perustana on ns. käyttöoikeusmalli, joka määrittelee oikeudet jotka käyttäjällä voi sisältöön olla.

Rosenblatt ja muut [Rosenblatt, Trippe, Mooney, 2002] selvittävät käyttöoikeusmallia perinteisen kirjan kautta. Asiakkaan ostaessa kirjan, hän saa kaupassa fyysisen kirjan lisäksi:

- oikeuden lukea ostamaansa kopiota kirjasta niin usein kuin haluaa
- oikeuden myydä tai antaa kirja jollekin muulle, jonka jälkeen sitä ei voi enää itse lukea.

Kirjaan liittyy myös sellaisia oikeuksia joita ei kaupassa asiakkaalle siirry:

- kirjan teknologian rajoittamia oikeuksia, kirjaa ei esimerkiksi voi katsella sähköiseltä laitteelta
- tekijänoikeuksien rajaamat oikeudet, kuten oikeus kopioida kirjaa myyntitarkoituksessa tai kirjan plagiointi.

Edellä mainitut oikeudet asiakas saa itselleen kirjan hinnalla. Raha siirtyy kustantajalle ja sieltä edelleen osittain kirjailijalle. Tässä kohtaa todettakoon, että myös erilaiset lait ovat yksi tapa toteuttaa käyttöoikeuksien hallintaa, sillä ne määrittelevät luvallisen toiminnan rajat.

Käyttöoikeusmalli kuvaa siis oikeudet jotka käyttäjä saa sisältöön, sekä oikeuksien ominaisuudet, kuten käyttöoikeuden hinta, käyttökertojen määrä jne.

Käyttöoikeuksien hallintaa varten DRM-järjestelmä sisältää myös tarvittavat teknologiset komponentit sisällön varsinaiseen suojaamiseen ja oikeuksien hallintaan. Kopiointisuojaus on siis yksi osa digitaalisten käyttöoikeuksien hallintaa.

Digitaalisen materiaalin kopiointisuojaukseen on olemassa useita erilaisia tekniikoita. Menetelmien murtovarmuus, sovellusalueet ja käytettävyys vaihtelevat suuresti.

Lisenssiavaimet ovat yleisesti käytössä mm. Microsoft:n tuotteissa. Ideana on syöttää ohjelmalle asennuksen aikana uniikki numero- tai lukusarja, jonka käyttäjä saa ostaessaan tuotteen. Avaimen syötön jälkeen asennus voidaan vielä loppuun. Menetelmän murtovarmuus on lähes olematon, sillä tuotteen ja avaimen voi yleensä kopioida sellaisenaan. Toimintaperiaate onkin lähinnä psykologinen. Laittoman kopion käyttö voidaan toki myöhemmin todeta, jos kopion omistajalla ei ole esittää kuittia hankinnastaan ja vastaavasti jollain muulla saman kopion omistajalla on.

Lisenssitiedostot sitovat yleensä käyttäjäkohtaista informaatiota lisenssiin. Lisenssitiedoston informaatio on usein digitaalisesti allekirjoitettu. Sovellus tarkistaa aina käynnistyessään lisenssitiedoston allekirjoituksen. Tämänkään menetelmän murtovarmuus ei ole erityisen hyvä. Sen sijaan liittämällä lisenssitiedostoon laitekohtaista informaatiota, saadaan menetelmästä huomattavasti luotettavampi. Tällä menetelmällä voidaan ohjelmistotuote sitoa tiettyyn laitteeseen. Huonona puolena on se, että käyttäjä ei voi välttämättä muuttaa laitekonfiguraatiotaan.

Vesileimateknologian periaatteet ovat siirtyneet sujuvasti digitaaliaikaan. Perinteisesti vesileimaa on käytetty esimerkiksi painetussa rahassa autenttisuuden osoittajana. Vesileiman tarkoituksena on Rosenblatt:n ja muiden [Rosenblatt, Trippe, Mooney, 2002] mukaan sisällyttää ylimääräistä informaatiota kohteeseen johon se on upotettu siten, että:

- vesileima ei haittaa kohteen käyttöä
- vesileima on erottamattomasti osa kohdettaan.

Vesileimatekniikkaa kutsutaan myös informaation piilottamiseksi, informaation upottamiseksi ja steganografiaksi.

Yleinen digitaalisen vesileimatekniikan sovellusalue on esimerkiksi sisällöntuottajaa identifioivan informaation upottaminen kuvatiedostoihin [Digimarc]. Vesileima upotetaan kuvaan siten, että se on mahdollista havaita tietokoneella, mutta ei ihmissilmällä. Vesileimatekniikkaa tukevalla ohjelmistolla kuvaa käsiteltäessä, käyttäjää voidaan tiedottaa kuvan tekijänoikeuksista.

Mobile Internet Technical Architecture teos [MITA] esittää mobiilille käyttöoikeuksien hallinnalle kahta erilaista lähestymistapaa. Käytäntöjen ja rajoitusten avulla tapahtuva sisällön suojaaminen ja salausmenetelmien avulla tapahtuva sisällön suojaaminen.

Käytäntöjen ja rajoitusten avulla tapahtuva käyttöoikeuksien hallinta perustuu sisällön siirtämiseen ja renderöintiin käytettävien välineiden luotettavuuteen. Varsinainen sisältö on tässä ympäristössä suojaamaton.

Salauslähestymistapaa käytettäessä varsinainen sisältö on aina salattu. Sisällön jakelu ja renderöinti voi tapahtua avoimia kanavia ja laitteita käyttäen. Tähän menetelmään liittyy aina ns. sisällönsuojausavain, jota käyttäen sisältö on salattu. Sisällönsuojausavaimen hallinta on tässä mallissa kriittisessä asemassa.

Seuraavassa kohdassa määriteltävässä mallissa käytetään soveltaen molempia lähestymistapoja.

6.2. Julkisen avaimen järjestelmään perustuva tietoturvaratkaisu

Julkisen avaimen järjestelmän tekninen perusoperaatio on salaus. Operaation sovelluksia ovat varsinainen informaation salaaminen ja digitaalinen allekirjoitus. Niitä soveltaen, seuraavissa alakohdissa esitellään viitekehys sähköisten lippujen tietoturvaratkaisuksi. Ensimmäisessä alakohdassa esitellään toiminnan osapuolet ja suojauksen osapuolille asettamat vaatimukset. Toisessa alakohdassa käydään läpi suojauksen periaate ja tarkastellaan suojauksen käyttöä erityyppisissä tilanteissa.

6.2.1. Toiminnan osapuolet ja vaatimukset osapuolille

Suojauksen kohteena on siis sähköinen lippu, eli elektroninen objekti. Lipun aktiivinen elämänkaari alkaa sen generoinnista ja päättyy sen käyttämiseen. Suojauksen on katettava elämänkaaren kaikki vaiheet. Seuraavat osapuolet liittyvät tapahtumaan suojauksen näkökulmasta:

- varmenneviranomainen

- lippu
- palvelun (lipun) myyjä
- palvelun tarjoaja eli lipun vastaanottaja
- PTD
- käyttäjä.

Lipun myyjänä ja lipun vastaanottajana voi toimia toki myös sama taho. Tässä esityksessä on kuitenkin mielekästä tehdä erottelu mainittujen tahojen välillä selkeyden vuoksi.

Varmenneviranomainen on ns. luotettu kolmas osapuoli, joka myöntää varmenteet käyttäjälle, PTD:lle ja palvelun myyjälle. Varmenneviranomaisen toiminnan on täytettävä luonnollisesti samat edellytykset kuin varmenneviranomaisen yleensäkin. Kuten aikaisemminkin on jo todettu, koko julkisen avaimen järjestelmän luotettavuus perustuu julkisen avaimen luotettavuuteen, jonka takaaminen on varmenneviranomaisen perustehtävä.

Lipulla tarkoitetaan elektronista objektia, joka voi periaatteessa sisältää mitä tahansa informaatiota. Tässä kohtaa riittää todeta, että lippu sisältää lipun käytön kannalta oleellista informaatiota, kuten esimerkiksi lipun uniikin tunnistenumeron, lipun voimassaoloajan jne.

Palvelun myyjän tehtävänä on myydä sähköisiä lippuja. Palvelun myyjällä on oltava käytössään teknologia, jonka avulla lippuja voidaan generoida ja liput voidaan varustaa myyjän digitaalisella allekirjoituksella.

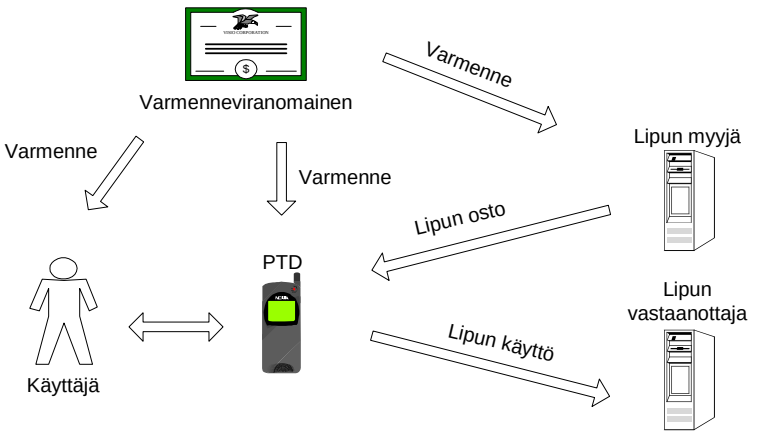
Palvelun tarjoajalla tarkoitetaan tässä yhteydessä sitä tahoa, joka vastaanottaa käyttäjän lipun ja tarjoaa käyttäjälle sitä vastaan lipun osoittamia hyödykkeitä. Palvelun tarjoajalla on oltava käytössään teknologia, jolla se voi tulkita lippuinformaation ja varmistaa tarvittaessa lipussa olevan digitaalisen allekirjoituksen.

PTD:n avulla käyttäjä hallinnoi lippujaan. Seuraavassa alakohdassa esiteltävän mallin toiminnan kannalta on välttämätöntä esittää kaksi PTD:n rakenteeseen kohdistuvaa vaatimusta. Ensinnäkin PTD:lle myönnettävän julkisen avaimen järjestelmän avainparin salainen avain on sidottava kiinteästi laitteeseen. Salaiseen avaimeen voi kohdistaa vain tiettyjä ennalta määrättyjä operaatioita, jotka voidaan suorittaa vain puhelimeen kiinteästi ja suojatusti asennetun ohjelmiston avulla. Näin voidaan yksilöidä jokainen PTD. Erään lipputyypin

suojauksen onnistumisen edellytyksenä on myös samalla periaatteella toimiva pieni tietokanta PTD:ssä. Sitä voidaan käyttää tietojen tallentamiseen vain ennalta määrättyjen operaatioiden kautta suojatun ohjelmiston avulla.

Myös käyttäjälle myönnetään varmenne. Oleellista on avainparin hallinta. Yksi käytännöllinen tapa avainparin säilytykseen on jo aikaisemminkin mainittu älykortti, eli WIM-tietoturvaelementti [WIM].

Kuvassa 6.1 on havainnollistettu yhteenvedonomaisesti edellä mainitut osapuolet ja osapuolten väliset perustoiminnot.



Kuva 6.1: Kopiointisuojauksen osapuolet

6.2.2. Kopiointisuojauksen toimintaperiaate ja sen sovelluksia

Tässä alakohdassa esiteltävän kopiointisuojauksen toimintaperiaate sallii kohteen (lipun) kopioinnin vapaasti eri laitteiden ja käyttäjien välillä. Eräissä kopiointisuojaustekniikoissa yritetään estää suojattavan kohteen varsinainen kopiointi. Tässä mallissa suojaus muodostuu lipun sitomisesta henkilöön tai PTD:hen. Eheyden varmistamiseksi lipun myöntäjä allekirjoittaa aina lippuinformaation ja lipun vastaanottaja vahvistaa allekirjoituksen.

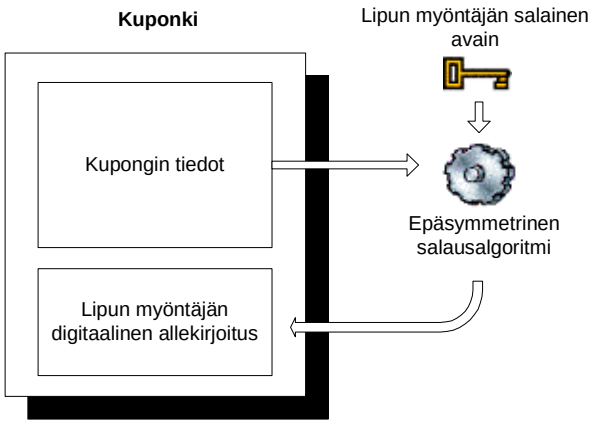
Tarkastellaan suojausta aluksi kolmen eri perustilanteen kautta:

1. lippu on vapaasti kopioitavissa ja siirrettävissä, ainoastaan lipun eheys varmistetaan.

2. lippu sidotaan käyttäjän henkilöllisyyteen. Lipun eheys varmistetaan

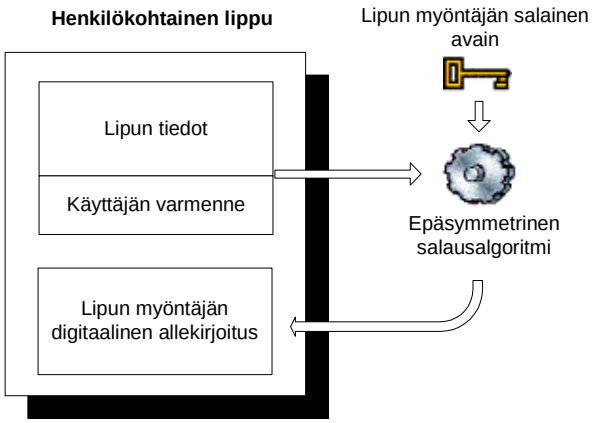
3. lippu sidotaan PTD:hen. Lipun eheys varmistetaan.

Ensimmäisessä tapauksessa lipun tyyppi voi olla esimerkiksi sellainen kuponki, jota voidaan kopioida ilman rajoituksia muille käyttäjille. Lippuinformaatiosta muodostetaan tiiviste, jonka lipun myöntäjä allekirjoittaa. Lippua vastaanotettaessa allekirjoitus ja lipun eheys vahvistetaan. Kuvassa 6.2 on havainnollistettu lipun rakennetta.



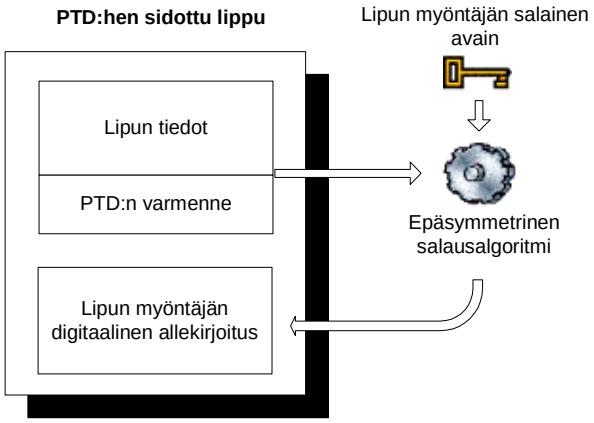
Kuva 6.2: Kuponki

Toisessa tapauksessa lipun tyyppinä on henkilökohtainen lippu, esimerkiksi lentolippu. Lippua voi käyttää ainoastaan yksi, ennalta määrätty henkilö. Lipun rakennetta havainnollistetaan kuvassa 6.3. Lippuun sisällytetään varsinaisen lippuinformaation lisäksi käyttäjän varmenne eli sertifikaatti. Varmenteeseen on mahdollista liittää myös käyttäjän kuva. Lipun myöntäjä muodostaa tiivisteen varsinaisesta lippuinformaatiosta ja käyttäjän varmenteesta, ja lopuksi allekirjoittaa tiivisteen. Lippua vastaanotettaessa allekirjoitus ja lipun eheys vahvistetaan. Vastaanottajalla on nyt käytössään lipussa identifioidun käyttäjän julkinen avain. Käyttäjän henkilöllisyys varmistetaan lähettämällä käyttäjälle (käyttäjän PTD:lle) allekirjoitettavaksi esimerkiksi satunnaisluku. Allekirjoitus palautetaan ja lipun vastaanottaja todentaa sen. Nyt Lipun vastaanottaja voi olla varma siitä, että lippua käyttävä henkilö on sama kuin lippuun on merkitty, koska käyttäjällä on hallussaan julkista avainta vastaava salainen avain. Mahdollisesti varmenteeseen liitettyä kuvaa voidaan myös käyttää tunnistukseen perinteisen passin tavoin.



Kuva 6.3: Henkilöllisyyteen sidottu lippu

Kolmannessa tapauksessa on kyseessä tapahtumalippu, esimerkiksi elokuvalippu. Lippua voi käyttää kuka tahansa, mutta sitä voidaan käyttää vain kerran. Tämä mahdollistuu lisäämällä lippuun informaatiota tapahtumasta ja sitomalla lippu tiettyyn PTD:hen. Lipun rakenne kuvassa 6.4. Lippuun sisällytetään PTD:n varmenne ja tietoa tapahtumasta, esimerkiksi tapahtuman alkamis- ja loppumisaika, tai tapahtumalle annettu tunnus. Lippua vastaanotettaessa toimitaan samoin kuin edellisessä kappaleessa mainitun henkilökohtaisen lipun yhteydessäkin. Nyt varmistuksen kohteena on henkilön sijaan PTD.



Kuva 6.4: PTD:hen sidottu lippu

Molemmissa tapauksissa, henkilökohtaisen lipun ja tapahtumalipun yhteydessä nousee esiin kysymys siitä, miten estetään samaa lippua käytettävän myöhemmin uudelleen. Ratkaisuna on jo edellisessä kappaleessa

mainitun tapahtuman yksilöivän informaation sisällyttäminen lippuun. Informaatio voi sisältää tiedon esimerkiksi juuri tapahtuman aloitus- ja lopetusajasta tms. Tieto voi olla mitä tahansa, kunhan se yksilöi tapahtuman. Lipun vastaanottaja tarkistaa aina ovatko lipun tiedot yhtenevät tapahtuman kanssa. Sama pätee luonnollisesti myös esimerkiksi lentolippuihin.

Asia ei ole kuitenkaan näin yksinkertainen. Jos esimerkiksi henkilökohtaisessa lipussa on määritelty tietty voimassaoloaika, eikä lipulla lunastettavaa hyödykettä ole voitu yksilöidä, täytyy estää käyttäjää käyttämästä lippua uudelleen myöhemmin. Tämä voidaan toteuttaa siten, että jokaiselle lipulle annetaan myöntämisen yhteydessä uniikki tunnus. Riittää jos tunnus on uniikki omassa käyttöympäristössään. Lipun vastaanottaja voi tallentaa käytettyjen lippujen tunnukset tarvittavan mittaiseksi ajanjaksoksi ja suorittaa vertailun jo käytettyjen lippujen kanssa ennen lipun hyväksymistä.

Luonteeltaan geneeristen lippujen, kuten joukkoliikenteen lippujen kanssa nousee myös esiin ongelmia. Tällaisilla lipuilla on tyypillisesti käyttörajoituksia, lippu voi olla kertakäyttöinen tai se voi sisältää useamman, ennalta määrätyn määrän käyttökertoja. Käyttötapahtumaa on vaikea yksilöidä lippuun, eikä lipun vastaanottajan ylläpitämä tietokanta jo käytetyistä lipuista ole käytännöllinen, koska esimerkiksi bussiliikenteessä tietokannan olisi oltava jollain tavalla keskitetty ja bussien ja tietokannan välinen yhteydenpito edellyttäisi etäyhteyttä.

On kuitenkin selvää, että jollain tavalla tässäkin tapauksessa jo käytetyistä lipuista, tai lippujen käyttökerroista, on pidettävä kirjaa. Huomioonottaen lisäksi tässä esitetyn kopiointisuojauksen yleisperiaatteen, jossa lippuja voi kopioida vapaasti eri laitteiden ja käyttäjien välillä, jäljelle jää mahdollisuus ylläpitää tietoja PTD:ssä.

Bussilippu, jota voidaan käyttää tietyn ajanjakson aikana rajattomasti, ei vaadi mitään erityistoimia. Vastaanottaja tarkistaa voimassaoloajan ja hylkää tai hyväksyy lipun. Sen sijaan bussilippu, joka on kertakäyttöinen, tai joka sisältää useamman käyttökerran, vaatii tietokannan PTD:hen. Tietokantaan tallennetaan lipun uniikki tunnus ja käyttökerrat. Tietokannan on oltava luonnollisesti pysyvä ja lisäksi sellainen, että mahdolliset kirjoitusoperaatiot ovat uuden tunnuksen lisääminen ja käyttökertamäärän kasvattaminen. Ohjelmiston on oltava kiinteä osa PTD:tä ja jota ei voi myöhemmin modifioida ilman erikoisvälineitä. Lipun vastaanottaja voi tehdä nyt kyselyn PTD:n

tietokantaan ja vertailla käyttökertoja lipussa ilmoitettuihin käyttökertoihin. Bussiliput on luonnollisesti sidottava myös PTD:hen.

7. Mallin arviointia

Tässä luvussa suoritetaan edellä esitellyn suojausmallin arviointia. Ensimmäisessä kohdassa mallin ominaisuuksia verrataan viidennen luvun lopussa esitettyihin vaatimuksiin. Samalla arvioidaan kunkin osa-alueen toteutuksen vahvuuksia ja heikkouksia. Toisessa kohdassa tarkastellaan mallin muita ominaisuuksia sekä niiden vahvuuksia ja heikkouksia. Kolmannessa kohdassa mallia vertaillaan kahteen olemassa olevaan sähköisten lippujen tietoturvaratkaisuun.

7.1. Mallille esitettyjen vaatimusten täyttyminen

Seuraavassa käydään läpi viidennessä luvussa esitetyt vaatimukset ja tarkastellaan miten edellisessä luvussa esitetyt ratkaisut vastaavat niihin.

Lippuinformaation eheys on pystyttävä takaamaan. Tämä on toteutettu mallissa digitaalisella allekirjoituksella. Lipun myöntäjä allekirjoittaa jokaisen myöntämänsä lipun. Lipun vastaanottajan tehtävä on tarkistaa allekirjoituksen autenttisuus ja päättää tarkistuksen tuloksen perusteella jatkotoimista, joko lipun hyväksymisestä tai sen hylkäämisestä. Digitaalisen allekirjoituksen ansiosta lipun väärentäminen on nykyteknologialla erittäin vaikeaa.

Järjestelmän on toimittava myös paikallisessa ympäristössä. Esitetyn mallin on mahdollista toimia pelkästään paikallisessa ympäristössä. Esimerkiksi lyhyen kantaman radioverkkotekniikan kautta on mahdollista suorittaa kaikki mainitut toiminnot. Etäyhteyden käyttö on kuitenkin mielekästä esimerkiksi lippujen hankinnassa.

Käyttäjän identifioivaa informaatiota on pystyttävä sitomaan lippuun. Kuten edellisessä luvussa käytiin läpi, käyttäjän henkilöllisyys on mahdollista sitoa lippuun liittämällä käyttäjän varmenne osaksi lippuinformaatiota. Lipun haltijan henkilöllisyys varmistetaan lipun käyttötilanteessa tarkistamalla, että lipun haltijalla on varmenteesta löytyvää julkista avainta vastaava salainen avain hallussaan. Tekniikan epävarmuus muodostuu inhimillisistä tekijöistä, eikä niinkään itse käytettävän teknologian heikkoudesta. Käyttäjä voi antaa älykortilla olevan salaisen avaimensa toiselle. Tilannetta voidaan verrata perinteisessä ympäristössä siihen, että käyttäjä antaisi passinsa toiselle.

Lipun siirtäminen on oltava mahdollista. Lippujen siirtäminen mihin tahansa yhteensopivaan laitteeseen on mallissa mahdollista. Tämän ominaisuuden

ansiosta lippuja voidaan siirtää esimerkiksi PC:lle varmuuskopioiksi. Lipun siirtäminen käyttökelpoisena suoraan toiselle henkilölle ei ole kuitenkaan mahdollista. Joissain tapauksissa lipun voisi siirtää toiselle henkilölle lipun myyneen palveluntarjoajan kautta. Alkuperäisen lipun uniikki tunnistenumero tallennettaisiin silloin vertailua varten tietokantaan, josta lipun vastaanottaja voisi käydä tarkistamassa onko lippu voimassa. Tämä ratkaisu vaatii kuitenkin jo aikaisemminkin mainitun keskitetyn tietokantaratkaisun, joten se ei sovellu esimerkiksi joukkoliikenteen lipuille.

Lipun siirtämisen estäminen on oltava mahdollista. Lipun siirtämisellä tarkoitetaan vaatimuksissa sitä tilannetta, jossa käyttäjä voisi siirtää lipun suoraan toiselle henkilölle. Tämä voidaan tarvittaessa estää sitomalla käyttäjän henkilöllisyys lippuun tai sitomalla lippu PTD:hen, jolloin lipusta voi olla olemassa vain yksi käyttökelpoinen kopio.

Lipun kopiointi on oltava mahdollista. Lippuja voidaan kopioida vapaasti yhteensopiviin laitteisiin. Tämä ominaisuus tukee esimerkiksi kuponkeja, joiden kopiointi on sallittua. Luonnollisesti myös varmuuskopioita voidaan luoda vapaasti.

Lipun kopioinnin estäminen on oltava mahdollista. Lipun kopioinnin estämisellä tarkoitetaan vaatimuksissa tilannetta, jossa käyttäjä luo lipusta luvattomia kopioita käytettäväksi uudelleen. Esitetyssä ratkaisussa kopioita voi olla olemassa, mutta niiden käyttö on estetty. Käyttäjän henkilöllisyys voidaan sitoa lippuun ja yksilöidyt tapahtumaliput voidaan sitoa PTD:hen. Geneeriset liput, kuten joukkoliikenteen liput sidotaan myös PTD:hen. Käyttäjän omien kopioiden uudelleenkäyttö estetään PTD:n tietokannalla, joka sisältää lippujen uniikit tunnukset ja niiden käyttökerrat.

Järjestelmä ei saa estää lippujen käyttörajoitusten toimintaa. Mallissa on esitelty lippujen käyttörajoitusten hallintaa esimerkiksi julkisen liikenteen lippujen yhteydessä.

Voidaan siis todeta, että malli täyttää esitetyt vaatimukset poisluettuna mahdollisuus siirtää geneerinen lippu toiselle. Seuraavassa kohdassa tarkastellaan mallin muita ominaisuuksia.

7.2. Muut ominaisuudet

Mallin mukaan on mahdollista kopioida lippuja teknisesti yhteensopiviin laitteisiin rajattomasti. Tämä mahdollistaa erittäin joustavan ja helpon varmuuskopioinnin. Kopioita voidaan luoda samaan laitteeseen johon alkuperäinen lippu on tallennettu, tai kokonaan eri laitteeseen. Malli ei siis ota kantaa siihen miten varmuuskopiointi suoritetaan. Käyttäjä voi hallinnoida lippujaan itse, esimerkiksi halutessaan käyttäjä voi vapaasti tuhota lipun.

Mallin toimintaperiaatteen ansiosta myöskään erillisiä kuitteja ei tarvita. Koska malliin ei sisälly tilannetta, jossa lippu siirtyisi lipun vastaanottajan haltuun sen käyttötilanteessa, voi lippu toimia myös kuittina. Lippu on aina lipun myyjän allekirjoittama, jolloin myyjä ei voi kiistää myyneensä lippua.

PTD:hen on luonnollisesti voitava luottaa, jos käytetään laitteessa olevaa tietokantaa lippujen käyttökertojen tallennukseen. Ainakin teoriassa olisi mahdollista valmistaa ns. väärennetty laite, jossa käyttäjälle tarjottaisiin mahdollisuus manipuloida tietokantaa omaksi edukseen. Tätä asiaa ei ole erikseen mallissa käsitelty, mutta väärinkäytökset olisi mahdollista estää hyödyntämällä jälleen julkisen avaimen teknologiaa. Jokainen laite olisi allekirjoitettava tehtaalla luotetun laitevalmistajan toimesta. Laitteen allekirjoitus voitaisiin lipun käyttötilanteessa varmistaa ja näin vakuuttua laitteen luotettavuudesta.

Eräs mallin etuja on potentiaalisuus huomattavaan läpinäkyvyyteen käyttäjän näkökulmasta. Mallin pohjalta toteutettava ratkaisu ei vaadi käyttäjältä välttämättä ymmärrystä pohjalla olevasta teknologiasta. Myös käyttäjältä vaadittava interaktio maksutapahtumassa on mahdollista minimoida hyvin vähäiseksi tietoturvan näkökulmasta. Vaadittavat toimenpiteet voidaan rajoittaa esimerkiksi henkilökohtaisen tunnusluvun syöttämiseen ja tapahtumien hyväksyntään.

Malli ei vaadi myöskään lippujen myyjiltä ja niiden vastaanottajilta erikoislaitteistoja. Tarvittavat julkisen avaimen operaatiot voidaan suorittaa esimerkiksi PC-alustalla tarkoitukseen soveltuvien ohjelmistojen avulla. Sen sijaan PTD:n täytyy olla erikoisvalmisteinen, kustannukset tästä siirtynevät valmistajien kautta kuluttajille.

7.3. Vertailua muihin ratkaisuihin

Tässä kohdassa käydään läpi lyhyehkösti ensimmäisessä luvussa mainitut kaksi mallia sähköisten lippujen käytölle. Molempien mallien tietoturvaratkaisua verrataan tässä tutkimuksessa esitettyyn ratkaisuun.

Fujimura ja Matsuyama [Fujimura, Matsuyama, 1999] ovat esittäneet erään ratkaisun sähköisten lippujen hallintaan. Heidän mallissaan ostettuja lippuja säilytetään ns. lipputilillä (ticket-account), joka on verkossa olevalla palvelimella. Käyttäjän julkinen avain sidotaan tiliin. Tiliä voi hallinnoida joko käyttäjä itse, tai hallinnointi voidaan delegoida kolmannelle osapuolelle. Tässäkin mallissa liput ovat digitaalisesti allekirjoitettu lipun myyjän toimesta, joten lippujen väärentäminen ei ole käytännössä mahdollista.

Fujimuran ja Matsuyaman mukaan tällä toteutustavalla on useita etuja verrattuna ratkaisuun, jossa lippuja säilytetään ja hallinnoidaan laitteen älykortilla ja sen ohjelmistolla. Jos lipputilin osoite on tiedossa, palveluntarjoajat voivat esimerkiksi lähettää käyttäjän lipputilille kuponkeja tai muuta markkinointi aineistoa ilman, että tarvitaan suoraa yhteyttä käyttäjän päätelaitteeseen. Käyttäjä puolestaan voi käyttää lippuja vaikka ne eivät olisikaan tallennettuna päätelaitteeseen tarjoamalla lipputilin osoitteen.

Lippujen kopioinnin estämiseksi malliin kuuluu lisäksi ns. lippumanageri (ticket-token manager), jonka tehtävänä on pitää kirjaa lipun omistajasta. Lippumanageri on luotetun kolmannen osapuolen ylläpitämä palvelu, joka takaa, että lipulla on olemassa vain yksi laillinen omistaja. Käyttäjän ostaessa lipun, lipun myyjä rekisteröi käyttäjän lipun omistajaksi lippumanagerin tietokantaan. Vastaavasti lipun vastaanottaja tarkistaa aina lippua käytettäessä lippumanagerilta, että käyttäjä on lipun laillinen omistaja.

Mallin puutteiksi voitaneen katsoa tarve etäyhteyteen. Paikallinen käyttö ei ole mahdollista, jos halutaan verifioida lipun omistaja lippumanagerin kautta. Etäyhteysvaatimuksen johdosta malli ei sovellu geneeristen lippujen, kuten bussilippujen käyttöön. Lippujen varmuuskopiointia ei ole mallin yhteydessä käsitelty lainkaan. On kuitenkin selvää, että mahdollinen lippujen varmuuskopiointi jää lipputilipalvelun tarjoajan vastuulle.

Mañan ja muiden [Maña, Martínez, Matamoros, Troya, 2001] esittämä GSM-lippu menetelmä ottaa päinvastaisen lähestymistavan lippujen säilytykseen.

Heidän mallissaan lippuja säilytetään matkapuhelimen älykortilla. Myös tässä mallissa lippuinformaatio allekirjoitetaan digitaalisesti lipun myyjän toimesta.

Malliin liittyvät käsitteet avoin lippu ja suljettu lippu. Käyttäjä ostaa aina avoimen lipun, joka tallennetaan älykortille. Avoin lippu sisältää varsinaisen lipun tiedot ja lisäksi tiedot lipun rajoituksista. Rajoituksena voi olla esimerkiksi avoimesta lipusta luotavissa olevien suljettujen lippujen määrä.

Käyttäjä joutuu aina sulkemaan lipun ennen sen käyttöä. Lippu osoitetaan tässä vaiheessa sille henkilölle, joka lipun tulee käyttämään. Tämä tapahtuu sijoittamalla lippuun käyttäjän identifioivaa informaatiota. Sama (suljettu) lippu voidaan sulkea vain kerran ja sulkemisen täytyy tapahtua sillä älykortilla, jossa avoin lippu sijaitsee. Lipun sulkemisen yhteydessä älykortilla olevan avoimen lipun mahdollisia rajoitetietoja, kuten luotavissa olevien suljettujen lippujen määrää päivitetään.

Kaikki lipuille suoritettavat operaatiot suoritetaan älykortilla. Ratkaisun tietoturva perustuukin älykortin luotettavuuteen. Avoimesta lipusta ei pysty luomaan ennalta määrättyä määrää enempää suljettuja lippuja.

Ratkaisu vaikuttaa turvalliselta, mutta esityksessä ei ole käsitelty lainkaan tilannetta, jossa suljetun lipun haltija tekee suljetusta lipusta itselleen uusia kopioita. Tällä ei ole tietenkään merkitystä silloin jos lippu voidaan yksilöidä johonkin tiettyyn tapahtumaan, vaikkapa elokuvanäytökseen. Esimerkiksi bussilippujen kohdalla tilanne on kuitenkin toinen. Käyttäjän olisi mahdollista tehdä luvattomia kopioita itselleen suljetusta bussilipusta ja käyttää siten samaa lippua uudelleen. Tämä voitaisiin estää keskitetyllä tietokantaratkaisulla, jossa pidettäisiin kirjaa jo käytetyistä lipuista, mutta etäyhteyden käyttö esimerkiksi bussiliikenteessä ei ole käytännöllistä. Varmuuskopioiden ottaminen on jäänyt myös tässä esityksessä kokonaan käsittelemättä.

Molempien edellä mainittujen mallien tietoturvaratkaisu perustuu ainakin osittain luotettuun ohjelmistoon. Ensiksi mainitun mallin yhteydessä lippumanagerin luotettavuuteen ja jälkimmäisen mallin tapauksessa älykortilla olevan ohjelmiston luotettavuuteen. Ohjelmisto on aina riski, ja varsinkin verkkoyhteyden päässä palvelimella sijaitseva lippumanageri on altis hyökkäyksille.

Tässä tutkimuksessa esitetyn mallin tietoturvan varmuus perustuu sen sijaan julkisen avaimen menetelmän luotettavuuteen, poisluettuna esimerkiksi bussilippujen yhteydessä käytettävä PTD:n tietokanta. PTD:n tietokanta on taasen verrattavissa luotettavuudeltaan älykortilla sijaitsevaan ohjelmistoon.

Seuraavan ja samalla viimeisen luvun alussa kootaan tutkimuksen asiat yhteen. Kerrataan tuloksia ja suhteutetaan ne muiden saavuttamiin tuloksiin. Samassa yhteydessä arvioidaan myös saavutettuja tuloksia suhteessa asetettuihin tavoitteisiin. Tämän jälkeen arvioidaan tutkimuksen puutteita ja rajoituksia. Lopuksi annetaan tutkimuksen pohjalta joitain mahdollisia jatkotutkimusaiheita.

8. Keskustelu

Tutkimuksessa on esitelty MeT-yhteenliittymän käyttämä sähköinen lippu käsite sekä suunnitelma lippujen tietoturvaratkaisuksi käyttäen julkisen avaimen teknologiaa.

Edellisessä luvussa todettiin, että suunnitelma täyttää yhtä poikkeusta lukuunottamatta tietoturvaratkaisulle asetetut vaatimukset. Suunnitelmaa verrattiin myös kahteen muuhun sähköisten lippujen tietoturvaratkaisuun. Tässä tutkimuksessa esitetty ratkaisu eroaa periaatteeltaan molemmista vertailuratkaisuista siten, että käyttäjällä on täysin vapaat kädet hallinnoida omia lippujaan. Tämä on saavutettu siirtämällä vastuu lippujen oikeellisuuden tarkastamisesta lippujen vastaanottajalle. Eli lipuista voi olla olemassa kopioita, mutta lipun vastaanottajan on mahdollista erotella joukosta hyväksyttävissä olevat liput ja hylätä muut. Yleisesti mallin vahvuuksia ovat:

- malli toimii paikallisessa- *ja* etäympäristössä
- mahdollisuus käyttää lippuja myös kuittina
- mahdollisuus ottaa lipuista vapaasti varmuuskopioita
- malli soveltuu myös geneeristen lippujen turvaamiseen PTD:hen rakennettavan toiminnallisuuden avulla
- tietoturvan vahvuus on sama kuin yleisesti julkisen avaimen teknologian vahvuus, poisluettuna päätelaitteen toiminnallisuus.

Mallin heikkouksia ovat:

- PTD on altis laiteväärennökselle (voidaan estää allekirjoittamalla laitteet)
- lippujen siirtäminen toiselle käyttäjälle ei onnistu geneeristen lippujen tapauksessa. Se tarkoittaa myös sitä, että käyttäjä ei voi palauttaa lippua ja saada rahojaan takaisin.

Yleisesti tämän tutkimuksen rajoite lienee asioiden käsittely hyvin korkealla tasolla. Se on ollut toisaalta tavoitekin, mutta lähestymistapa jättää runsaasti avoimia kysymyksiä mallin todelliselle käytettävyydelle, mm. tekniikoiden suorituskyvylle. Lähdemateriaalin käyttö on nimenomaan sähköisten lippujen kohdalla ollut ehkä hieman niukkaa, tosin tutkimuksiakaan aiheesta ei ole tehty useita. Julkisen avaimen teknologiaa ennestään tuntemattomalle lukijalle mallin esittely ja arviointi saattaisi vaatia terävöittämistä kokonaiskuvan muodostamisen helpottamiseksi.

Työ tarjoaa useita jatkotutkimusaiheita. Edellä mainittu tekniikoiden suorituskyvyn selvittäminen on tärkeää mallin käytännön sovellettavuuden selvittämiseksi. Miten julkisen avaimen teknologia sopeutuu korkeisiin suorituskykyvaatimuksiin, joita esimerkiksi julkisen liikenteen liput asettavat? Tätä kautta esiin tulevat myös soveltuvien tekniikoiden valinta ja niiden tietoturvan tason selvittäminen. Mallin soveltuvuuteen yleisesti sähköisille lipuille ei tässä työssä oteta kantaa. Sen selvittäminen on myös kiinnostavaa, koska hyvän ratkaisun on oltava geneerinen mikäli sen halutaan yleistyvän. Asiaa kannattaa tutkia myös käyttäjän näkökulmasta ja määrittää lipuille tarkat käyttötapaukset. Tätä kautta voidaan selvittää millä tasolla ratkaisusta saadaan käyttäjälle läpinäkyvä eli mahdollisimman helppokäyttöinen.

Viiteluettelo

[BT] Specification of the Bluetooth system – volume 1 (core) & 2 (profiles), Version 1.1. http://www.bluetooth.com/. Tarkistettu 7.8.2002.

[Digimarc] Digimarc Watermarking Guide, Digimarc Corporation, 1999. http://www.digimarc.com/support/cswater.pdf. Tarkistettu 21.8.2002.

[DRM_Adobe] Jay O'Rear, DRM: Seuraava suuri oikeusliike. http://www.adobe.fi/epaper/features/drm/main.html. Tarkistettu 21.8.2002.

[Fujimura, Matsuyama, 1999] Ko Fujimura, Kazuo matsuyama, Distributed Digital-Ticket Management for Rights Trading System. Proceedings of the first ACM conference on Electronic commerce. ACM Press, 1999. 110-118.

[HS] Helsingin sanomat: Pääsylipun saa pian tekstiviestinä. Kännykkä- ja sähköpostiliput jo koekäytössä. 27.8.2002. http://www.helsinginsanomat.fi/arkisto/juttu.asp?id=20020827ER1. Tarkistettu 30.8.2002.

[Järvinen ja Järvinen, 1996] Pertti Järvinen ja Annikki Järvinen, Tutkimustyön metodeista. Opinpaja Oy, Tampere, 1996, 102-118.

[Kerttula, 1999] Esa Kerttula, Tietoverkkojen tietoturva. Oy Edita Ab, Helsinki, 1999, 35-36, 93, 159, 314, 316-318, 357-358.

[Leitch, Warren, 2000] Shona Leich, Matthew Warren, Ethics and electronic commerce. Selected papers from the second Australian Institute conference on Computer ethics – Volume 1. Australian Computer Society, Inc, 2000. 56-59.

[Maña, Martínez, Matamoros, Troya, 2001] Antonio Maña, Jesús Martínez, Sonia Matamoros, José M. Troya, GSM-Ticket: Generic Secure Mobile Ticketing Service. http://citeseer.nj.nec.com/502869.html. Tarkistettu 16.9.2002.

[Menezes, Oorschot, Vanstone, 1999] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography. CRC Press, Inc, 1997, 250-258, 263-265, 515-520.

[MeTCore] MeT Core Specification, Version 1.1, http://www.mobiletransaction.org. Tarkistettu 26.7.2002.

[MeTPTD] MeT PTD Definition, Version 1.1, http://www.mobiletransaction.org. Tarkistettu 26.7.2002.

[MeTTF] MeT Ticketing Framework, Version 1.0, http://www.mobiletransaction.org. Tarkistettu 26.7.2002.

[MITA] Nokia, Mobile Internet Technical Architecture. IT Press, Edita, 2001, 209-210.

[Rosenblatt, Trippe, Mooney, 2002] William Rosenblatt, William Trippe, Stephen Mooney, Digital Rights Management: Business and technology. M&T Books, USA, 2002, 60, 98.

[RSA] RSA laboratories, Frequently Asked Questions About Today's Cryptography, Version 4.1, ftp://ftp.rsasecurity.com. Tarkistettu 15.7.2002.

[Schneier, 1996] Bruce Schneier, Applied cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc, USA, 1996, 28-29, 461.

[SET1] The SET Standard Book 1 Business Description, http://www.setco.org. Tarkistettu 11.2.2002.

[Steinauer, Wakid, Rasberry, 1997] Dennis D. Steinauer, Shukri A. Wakid, Stanley Rasberry, Trust and traceability in electronic commerce, StandardView**,** September 1997, Volume 5, Issue 3. ACM Press. 118-124.

[Tygar, 1996] J. D. Tygar, Atomicity in electronic commerce. Proceedings of the fifteenth annual ACM symposium on Principles of distributed computing. ACM Press, 1996. 8-26.

[Tygar, 1999] J. D. Tygar, Open problems in electronic commerce. Proceedings of the eightteenth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. ACM Press, 1999. 101.

[VCARD] Internet Mail Consortium, vCard: Your Electronic Business Card. http://www.imc.org/pdi/. Tarkistettu 8.8.2002.

[Wallach, 2001] Dan S. Wallach, Copy protection technology is doomed. Computer, volume 34, issue 10, Oct. 2001. 48-49.

[WIM] Wireless Identity Module specification, WAP Forum, Version 12.7.2001 http://www.wapforum.org. Tarkistettu 5.8.2002.

[WPKI] Wireless Public Key Infrastructure Definition, WAP Forum, Version 24.4.2001 http://www.wapforum.org. Tarkistettu 5.8.2002.

[WTLS] Wireless Transport Layer Security Specification, WAP Forum, Version 6.4.2001 http://www.wapforum.org. Tarkistettu 5.8.2002.

[XMLT] Ko Fujimura, Yoshiaki Nakajima, Jun Sekine, XML Ticket: Generalized Digital Ticket Definition Language. http://www.w3.org/DSig/signed-XML99/pp/NTT_xml_ticket.html. Tarkistettu 8.8.2002.