Janne Kauppinen

Avaimet sähköiseen kaupankäyntiin

toimikortit osana julkisen avaimen infrastruktuuria

Tietojärjestelmätieteen
pro gradu -tutkielma
12.03.2002

Jyväskylän yliopisto
Tietojenkäsittelytieteiden laitos
Jyväskylä

ABSTRACT

Kauppinen, Janne Markus

Keys to the electronic commerce, smartcards as a part of public key infrastructure /Janne Kauppinen

Jyväskylä: University of Jyväskylä, 2001.

111 p.

MSc Thesis

In this research the applicability of smart cards is evaluated in PKI (public key infrastructure) based electronic commerce. Also in this research the information security requirements in the electronic commerce process are introduced and explained how these requirements appear in the trade process and in its part-processes. The problems in current PKI and how these problems could be solved with the use of smart cards are evaluated in the context of this trade process.

This subject is one of the most essential in the problems of electronic commerce because the deficiency in information security and people's distrust in electronic business are considered as biggest barriers against the growth of electronic commerce. The handling of this subject is based on the basics of electronic commerce and its information security requirements. The perspective to deal with electronic commerce is the trade process wherein different areas of information security are studied.

The main findings of this research are the definition for information security requirements and explanation for information security's meaning in different parts of the trade process. This research shows that information security is the main barrier in electronic commerce and that fulfilling the requirements for information security means new design for the trade process.

KEYWORDS: PKI, Smart Card, CA, PGP, information security, trade process

TIIVISTELMÄ

Kauppinen, Janne Markus

Avaimet sähköiseen kaupankäyntiin, toimikortit osana julkisen avaimen infrastruktuuria /Janne Kauppinen

Jyväskylä: Jyväskylän yliopisto, 2001.

111 s.

Tutkielma

Tutkielmassa arvioidaan toimikorttien soveltuvuutta julkisen avaimen arkkitehtuuriin (Public Key Infrastructure, PKI) perustuvaan elektroniseen kaupankäyntiin. Tutkielmassa esitellään elektronisen liiketoiminnan yleiset ja erityiset tietoturvavaatimukset ja määritellään miten nämä vaatimukset ilmenevät kaupankäyntiprosessin eri vaiheissa ja osaprosesseissa. Tässä kaupankäyntiprosessin kontekstissa arvioidaan nykyisiin PKI-järjestelmiin liittyviä ongelmia ja sitä, miten toimikorttien avulla ongelmia voidaan helpottaa.

Aihe on elektronisen liiketoiminnan problematiikan keskeisimpiä, sillä elektroniseen liiketoimintaan siirtymisen eräänä suurimpina esteenä pidetään epäluottamusta tietoturvaan ja yksityisyyden suojaan. Aiheen käsittely perustuu sähköisen kaupankäynnin lähtökohtiin ja tietoturvavaatimuksiin. Sähköisen kaupankäynnin käsittelyn näkökulmana on kaupankäyntiprosessi, jossa tietoturvaa eri osa-alueineen tarkastellaan.

Tutkielman keskeisimpinä tuloksena on sähköisen kaupankäyntiprosessin eri vaiheiden tietoturvavaatimusten kuvaaminen ja toimikorttien mahdollisuudet näissä vaiheissa. Tutkielma osoittaa myös, että tietoturva on merkittävin este sähköisen kaupan yleistymiselle ja että tietoturvavaatimusten täyttäminen vaatii kaupankäyntiprosessien uudelleensuunnittelua.

AVAINSANAT: PKI, toimikortti, varmentaja, PGP, tietoturva, tietosuoja, kaupankäyntiprosessi

SISÄLLYSLUETTELO

1 JOHDANTO

Tässä luvussa esitellään tutkielman lähtökohtia, tavoitteita, käytettyjä menetelmiä ja niiden soveltuvuutta valittuun aihealueeseen sekä luodaan katsaus tutkielman sisältöön.

Tietoturva, tietosuoja ja henkilön luotettava sähköinen tunnistaminen ovat menestyksen perusedellytyksiä elektronisessa liiketoiminnassa ja sen kehittymisessä. Nämä voidaan saavuttaa usealla tavalla, mutta ehdottoman turvallisia ja helppokäyttöisiä menetelmiä ei vielä ole otettu käyttöön kuin muutamia. PKI-järjestelmät ja toimikortit yhdessä kuitenkin tarjoavat yhden ratkaisun näihin ongelmiin, joilla on tällä hetkellä suurimmat mahdollisuudet yleistyä jokapäiväisessä liiketoiminnassa. Tietosuojalla tarkoitetaan tietoverkoissa toimivien henkilöiden yksityisyyden ja henkilötietojen suojaamista. Tietoturvalla puolestaan tarkoitetaan yksinkertaistetusti sitä, että viestin lähettäjä voi suojata viestinsä teknisesti.

Tässä tutkielmassa elektronisen liiketoiminnan ja sähköisen kaupankäynnin käsitteitä käytetään synonyymeinä ja niillä viitataan erityisesti tietoverkoissa tapahtuvaan kaupankäyntiin. Elektronisen liiketoiminnan tarkastelussa näkökulmana on pääasiassa kuluttajille suuntautuva kauppa (B2C). Tutkielman keskeisimmät käsitteet ovat tietoturva, tietosuoja ja henkilön sähköinen tunnistaminen. Näiden käsitteiden taustalla oleva kryptografia, jonka varaan PKI-järjestelmät rakentuvat, on käsitelty liitteessä siksi, että sen avulla voidaan paremmin ymmärtää tutkielmassa käsiteltyjä asioita. Kryptografia on oma tutkimusalansa, joka tutkii pääasiassa salakirjoitusta ja useimmat nykyisistä tietoturvaratkaisuista perustuvat siihen. Käytetyin kryptografian sovellusalue on PKI (Public Key Infrastructure), joka tarkoittaa julkisen avaimen infrastruktuuria. PKI:n voidaan lyhyesti sanoa olevan systeemi, joka mahdollistaa julkisen avaimen sitomisen avaimen käyttäjään ja avainten jakelun.

Varsinaisena tutkimusongelmana on selvittää miten tällä hetkellä käytössä olevilla PKI-järjestelmillä ja toimikorteilla voidaan vaikuttaa kaupankäyntiprosessiin ja miten niillä voidaan täyttää elektronisen liiketoiminnan asettamia vaatimuksia tietoturvalle ja

tietosuojalle. Tutkielmassa selvitetään myös PKI:hin liittyviä ongelmia ja mahdollisia syitä niihin sekä selvitetään miten toimikorteilla voidaan näitä ongelmia vähentää. Oman lisänsä tietoturva – ja tietosuojaongelmien joukkoon tuo elektronisen kaupan kansainvälisyys sekä elektronista kauppaa koskeva, monilta osin keskeneräinen lainsäädäntö. Näihin ongelmiin ei tässä tutkielmassa kuitenkaan puututa.

Tämä tutkielma on luonteeltaan analysoiva selvitys, jonka pohjalta määritellään elektronisen liiketoiminnan tietoturvavaatimukset ja perustellaan ratkaisuja osaan selvityksessä ilmenneistä tietoturvan ongelmista. Tutkielmassa on analysoitu enimmäkseen kirjoitettua materiaalia, mutta tutkielma perustuu osittain myös omiin käytännön kokemuksiin erilaisten toimikorttien, ja sertifikaattien käytöstä eräässä hierarkkisessa varmentajajärjestelmässä. Kaupankäyntiprosessin tuntemus perustuu lähes pelkästään kirjallisuuteen, mikä on vaikeuttanut PKI:n ja toimikorttien mahdollisuuksien arvioimista prosessien muuttamiseksi ja tehostamiseksi. Myös PKI:n ja toimikorttien käytännön sovellusten vähäisyys elektronisessa liiketoiminnassa on rajoittanut niiden toimivuuden omakohtaista tutkimista ja arvioimista. Näin ollen suurin osa tutkielmassa esitetyistä väittämistä ja päätelmistä perustuu alan teorioihin, artikkeleihin ja kirjallisuuteen. Suuri osa aiheeseen liittyvästä materiaalista on PKI-järjestelmiä ja toimikortteja kehittävien ja toimittavien tahojen tekemää ja siksi usein kritiikitöntä. Tutkielmassa käytetystä materiaalista vain pieni osa oli alle vuoden ikäistä, mikä myös heikentää nopeasti kehittyvän aihealueen nykytilan tarkastelua. PKI:n ja toimikorttien laajemmalla empiirisellä tutkimisella olisikin voinut saavuttaa selkeämpiä ja perustellumpia tuloksia tutkielman aiheen tämänhetkisestä tilasta.

Tutkielman tarkoituksena on määritellä elektronisen liiketoiminnan vaatimukset tietoturvalle ja tietosuojalle ja se, miten nämä ilmenevät elektronisessa kaupankäyntiprosessissa. Tarkoituksena on myös analysoida nykyisiä julkisen avaimen infrastruktuurin järjestelmiä ja toimikortteja ja miten niillä voidaan vastata elektronisen liiketoiminnan vaatimuksiin ja vaikuttaa kaupankäyntiprosessiin. Tutkielmassa selvitetään myös PKI:hin liittyviä ongelmia ja toimikorttien tarjoamia ratkaisuja niihin. Käsittely kohdistuu siis pääasiassa PKI-järjestelmiin ja toimikortteihin sekä niiden toimintaan kaupankäyntiprosessissa.

Työn motiivina toimii elektronisen kaupankäynnin tarve toisaalta ehdottoman luotettavaan henkilön sähköiseen tunnistamiseen ja toisaalta tarve anonyymiin ja pseudonyymiin asiointiin sekä tietoliikenteen turvaamiseen. Näihin tarpeisiin PKI-järjestelmät voivat tarjota ratkaisuja. Nykyiset PKI-järjestelmät tosin sisältävät lukuisia ongelmia ja heikkouksia. Hyödyntämällä toimikortteja voidaan kuitenkin ratkaista osa näistä ongelmista ja saavuttaa riittävä turvallisuustaso sähköiselle asioinnille. Tällaisia ratkaisuja on jo sovellettu käytäntöön, mutta useiden käytännön ongelmiensa takia ne eivät ole vielä suurempaa suosiota saavuttaneet, eivätkä siksi laajemmin yleistyneet. Tutkielman tavoitteena on siis määritellä elektronisen liiketoiminnan vaatimukset tietoturvalle, tietosuojalle ja tunnistamiselle sekä selvittää mitä nämä merkitsevät kaupankäyntiprosessissa.

Tutkielmassa aiheen käsittely lähtee liikkeelle toisessa luvussa elektronisen liiketoiminnan ja siinä toimivan kaupankäyntiprosessin tarkastelulla. Luvussa käydään läpi kaupankäyntiprosessi sekä sen osaprosessit ja se, miten ne voivat muuttua elektronisessa liiketoiminnassa. Kolmannessa luvussa määritellään vaatimukset elektronisen liiketoiminnan tietoturvalle ja selvitetään tietoturvan osa-alueet sekä keskeiset käsitteet. Lisäksi selvitetään miten PKI-järjestelmät ja toimikortit täyttävät määriteltyjä tietoturvan vaatimuksia. Luvun lopussa käsitellään henkilön sähköistä tunnistusta ja siihen liittyvää problematiikkaa. Neljännessä luvussa käsitellään PKI-järjestelmiä ja niihin liittyviä keskeisiä käsitteitä, joita ovat sertifikaatit, luottamus ja sen syntyminen sähköisessä maailmassa sekä luotettu kolmas osapuoli. Luvussa käsitellään kahta erilaista PKI-mallia ja selvitetään niihin liittyviä ongelmia. Viidennessä luvussa käsitellään puolestaan toimikortteja, niiden käyttöä PKI:ssä ja elektronisessa liiketoiminnassa sekä sitä, miten niillä voidaan täydentää PKI:tä ja ratkaista siinä esiintyviä ongelmia ja siten paremmin täyttää elektronisen liiketoiminnan tietoturvavaatimuksia. Kuudennessa luvussa tarkastellaan tietoturvaa ja tunnistusta kaupankäyntiprosessissa sekä prosesseihin liittyviä tietoturvan osa-alueita. Luvussa seitsemän ovat tutkielman loppupäätelmät ja yhteenveto.

2 KAUPANKÄYNTIPROSESSIN KUVAUS ELEKTRONISESSA LIIKETOIMINNASSA

Tässä luvussa käsitellään elektronista liiketoimintaa yleensä ja etenkin elektronista kaupankäyntiprosessia sekä sen osaprosesseja.

Elektroninen liiketoiminta muuttaa joitakin kaupankäynnin perinteisiä malleja. On kuitenkin tärkeää huomata, että monet perinteiset kaupankäynnin osat siirtyvät sellaisenaan elektroniseen maailmaan. Perinteiset kaupankäynnin käytännöt ovat muodostuneet vuosituhansien saatossa ja siksi ihmiset ovat oppineet ymmärtämään niitä ja luottamaan niihin. Elektronisen liiketoiminnan menestymisen edellytys on, että se onnistutaan sovittamaan näihin perinteisiin ja luotettuihin malleihin. (Steinauer ym. 1997, 118)

Steinauerin väite pitää siltä osin paikkansa, että varsinainen kaupankäyntiprosessi ei elektronisen kaupankäynnin myötä muutu, mutta sen osaprosessit muuttuvat ja aiheuttavat sen, että ihmiset joutuvat omaksumaan uusia kaupankäynnin käytäntöjä ja menetelmiä. Tähän eräänä syynä ovat tietoturvan ja sähköisen tunnistamisen vaatimukset, joita ei voida täyttää ottamatta käyttöön uusia, elektroniseen liiketoimintaan soveltuvia menetelmiä.

Internetin käyttö ja elektronisen liiketoiminnan yleistyminen asettaa suuria paineita tietoturvalle, jonka voidaankin väittää olevan tämän hetken suurin pullonkaula elektronisen liiketoiminnan kasvulle. Tukea väitteelle antaa Tietoyhteiskunta 2000+ -projektin selvitys Pk-yritysten sähköisen liiketoiminnan tarpeista, jossa todettiin, että jopa 44 % prosenttia haastatteluihin vastanneista piti tietoturvaa esteenä elektronisen liiketoiminnan hyödyntämiselle (Helsingin kauppakamari, 2001). Tämän vuoksi tietoturvan voidaan sanoa olevan myös tärkeimpiä ja kiireellisimpiä asioita tietotekniikassa ja elektronisessa liiketoiminnassa tällä hetkellä. Tietoturvasta puhuttaessa on myös muistettava tietosuojan käsite, joka lisää sähköiseen kauppaan

omat ongelmansa ja vaatimuksensa. Seuraavassa on Laineen (2001, 136) määritelmä verkkokaupan turvallisuudelle:

> "Sähköisen verkkokaupan turvallisuus tarkoittaa lähtökohtaisesti sitä, että kukaan ulkopuolinen ei voi tunkeutua luvatta muiden järjestelmiin ja estää järjestelmien käyttöä taikka muuttaa, vahingoittaa tai kopioida asiakkaiden kulutus- tai tilitietoja taikka yrityksen liikesalaisuuksia."

Eräs tietoturvan oleellinen osa on henkilöiden luotettava sähköinen tunnistaminen Internetissä. Jotta elektroninen kauppa yleistyisi, on sen voitettava ihmisten luottamus siihen, kenen kanssa verkossa asioidaan. Sama pätee myös toisinpäin, sillä Internetissä palvelujaan tarjoavat kauppiaat haluavat myös varmistua siitä, että asiakas on todellinen ostoaikeissa oleva henkilö eikä huijari.

Henkilön sähköiseen tunnistamiseen on olemassa useita menetelmiä, kuten salasanat, biometriset menetelmät, julkisen avaimen menetelmät ja kryptografiset laitteet (esim. toimikortti). Tässä tutkielmassa käsitellään kuitenkin lähinnä vain kahta viimeksi mainittua. Salasanat ovat epäkäytännöllisiä, sillä ihmiset unohtavat helposti salasanansa varsinkin kun muistettavien salasanojen määrä jatkuvasti kasvaa. Lisäksi monet käyttävät helposti arvattavia salasanoja tai kirjoittavat ne ylös paikkaan, josta sivulliset voivat ne helposti löytää. Biometrisille menetelmille on puolestaan vielä vähän käytännön sovelluksia ja niiden yleistymistä kaupalliseen käyttöön voidaankin odottaa vasta lähitulevaisuudessa. Elektronisen liiketoiminnan tietoturvaan ja sähköiseen tunnistamiseen palataan luvuissa 3 ja 6.

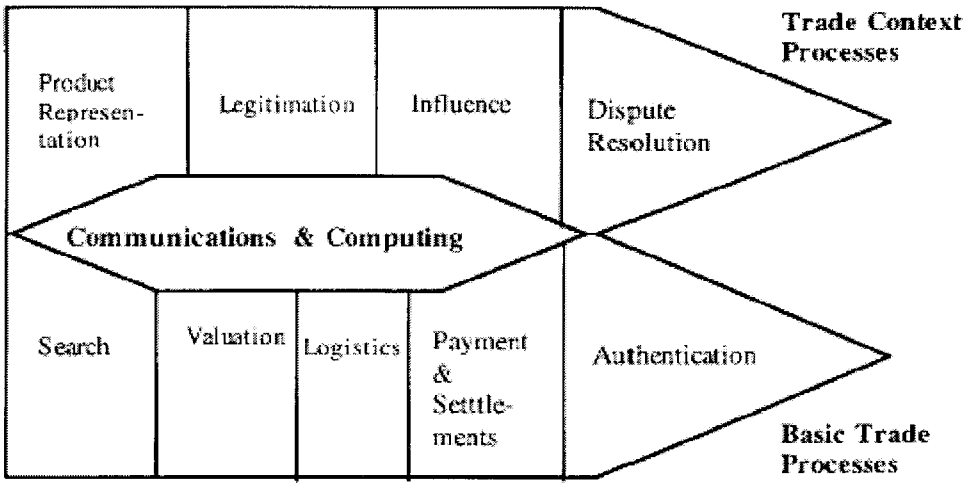
2.1 Kaupankäyntiprosessi

Elektronisen liiketoiminnan tietoturvan ja sähköisen tunnistamisen vaatimusten selvittämiseksi tarkastellaan kaupankäyntiprosessia ja sen muuttumista siirryttäessä perinteisestä liiketoiminnasta sähköiseen. Myöhemmissä luvuissa selvitetään PKI:n ja toimikorttien toiminta ja niiden sovellettavuus kaupankäyntiprosessiin.

Kambil ja Van Heck (1998, 4) ovat määritelleet kaupankäyntiprosessin seuraavan kuvan mukaisen viitekehyksen avulla. Heidän mukaansa tämä viitekehys on hyödyllinen

uusien markkinajärjestelmien suunnittelijoille sekä niille, jotka tutkivat markkinoita arvioidakseen ja selittääkseen informaatioteknologisten aloitteiden onnistumisia ja epäonnistumisia uusilla markkinoilla (Kambil ja Van Heck 1998, 18). Tässä tutkielmassa viitekehystä hyödynnetään analysoitaessa PKI:n ja toimikorttien vaikutuksia kaupankäyntiprosessiin lähinnä tunnistamisen ja tietoturvan näkökulmasta ja sitä kautta koko elektroniseen liiketoimintaan. Kaaviota tarkasteltaessa on syytä huomata, että jokaisessa laatikossa vaikuttaa aina kaksi osapuolta: myyjä ja ostaja. Tässä tutkielmassa kaaviota käsitellään molempien osapuolten kannalta, mutta pääpaino on kaupankäynnin heikomman osapuolen eli ostajan aseman tarkastelussa.

KUVA 1. Kaupankäyntiprosessi (Kambil ja Van Heck 1998, 4)



Yleisesti ottaen voidaan todeta, että siirryttäessä perinteisestä kaupankäynnistä sähköiseen, edellisen kuvan prosesseja on mahdollista muuttaa tarkemmiksi, käytännöllisemmiksi ja kustannustehokkaammiksi. Kuten myöhemmin todetaan, tämä tarkoittaa käytännössä lähinnä prosessien välisten yhteyksien muuttumista. Sähköisessä maailmassa on kuitenkin mietittävä uudelleen miten käyttäjien luottamus uudistuneisiin prosesseihin voidaan säilyttää. Luottamusta ei enää välttämättä voidakaan synnyttää perinteisestä kaupankäynnistä totutuilla menetelmillä. Tärkeimpänä luottamuksen synnyttäjänä voidaan nähdä tietoturva, jonka saavuttamiseksi vaadittavia menetelmiä tässä tutkielmassa käsitellään. Seuraavassa taulukossa on purettu auki kaaviota ja selvitetty mistä osaprosesseista kaupankäyntiprosessi muodostuu. Prosesseista on myös lyhyet kuvaukset.

TAULUKKO 1. Kaupankäyntiprosessin osaprosessit ja niiden kuvaukset Kambilia ja Van Heckiä (1998, 5 – 6) mukaillen.

Prosessi	**Kuvaus**
Kommunikointi (Communications and Computing)	Kommunikointi liittyy kaikkiin prosesseihin. Kehittyneet kommunikointimahdollisuudet prosessien sisällä ja niiden välillä muuttavat kaikkien osapuolten transaktiokustannuksia.
Peruskaupankäyntiprosessit (Basic Trade Processes)	Prosessit, jotka liittyvät tavaroiden ja palveluiden transaktioihin.
Etsintä (Search)	Prosessi, jossa ostajat ja myyjät keräävät ja arvioivat tietoa tunnistaakseen mahdollisuuksia. Tällaisia mahdollisuuksia ovat myyjän halu myydä tuote ja ostajan halu ostaa tuote.
Arvotus (hinnanmuodostus) (Valuation)	Prosessi, joka muodostaa myynti- ja ostohinnat. Erilaiset hinnanmuodostusprosessit, kuten erilaiset huutokauppatavat, jakavat kustannukset eri tavalla myyjien, ostajien sekä "välikäsien" välillä.
Logistiikka (Logistics)	Prosessi, jossa tavara toimitetaan myyjältä ostajalle.
Maksaminen (Payment and Settlements)	Prosessi, joka määrittelee ehdot ja menetelmät maksamiselle. Kolmannet osapuolet tarjoavat tähän useimmiten infrastruktuurin.
Tunnistus (Authentication)	Tämä prosessi sisältää toimintoja, joilla varmistetaan tuotteen laatu ja ominaisuudet sekä eri osapuolten autenttisuus ja valvotaan sopimusten pitävyyttä. Tunnistus voi tapahtua kolmansien osapuolten kautta, jotka voivat taata myös esimerkiksi tapahtumien kiistämättömyyden.
Kaupankäynnin kontekstiprosessit (Trade Context Processes)	Prosessit, jotka muodostavat transaktiokustannukset kaupankäynnin eri osapuolille.
Tuotteen esittely (Product Representation)	Tämä prosessi määrää miten tuotteen ominaisuudet esitellään ostajalle tai muille osapuolille. Standardimenetelmät tuotteen esittelylle vähentävät tämän prosessin aiheuttamia kustannuksia. Hyvin esitelty tuote myös vähentää ostajan epävarmuutta.
Laillistaminen (vahvistaminen) (Legitimation)	Tämä prosessi vahvistaa kaupan tai sopimuksen. Se määrittelee millaiset tarjoukset ja sopimukset ovat hyväksyttäviä ja miten osapuolet sitoutetaan niihin.
Vaikuttaminen (Influence)	Tämä prosessi sisältää keinoja tukien tai palkkioiden ja sanktioiden määräämiseen riskien vähentämiseksi. Nämä voivat olla esimerkiksi palkkioita sopimuksen noudattamisesta ajallaan tai sanktioita tuotteen väärin esittelemisestä.
Kiistojen ratkaisu (Dispute Resolution)	Kaupankäynti tapahtuu laajassa laillisessa ja institutionaalisessa kontekstissa, joka tarjoaa keinoja kiistojen ratkaisuun. Osapuolet voivat sopia kiistatilanteiden ratkaisuista keskenään tai kolmansien osapuolten, kuten oikeuslaitoksen, välityksellä.

Kaupankäyntiprosessista voidaan siis erottaa kymmenen eri prosessia, joilla voidaan analysoida markkinoiden rakennetta ja kustannusten syntyä. Nämä prosessit voidaan jakaa peruskaupankäyntiprosesseihin, kaupankäynnin kontekstiprosesseihin ja kommunikointiprosessiin. Näistä ensin mainitut ovat erillisiä prosesseja, joita tarvitaan kaikissa tavaroihin ja palveluihin liittyvissä transaktioissa. Jälkimmäiset prosessit muodostavat ja lisäävät tai pienentävät kustannuksia perusprosesseissa. Kommunikointi on puolestaan osa jokaista prosessia ja käsittää lähinnä ostajan ja myyjän vuorovaikutuksen ja sen eri menetelmät. Nämä kymmenen prosessia muodostavat

transaktioiden kustannukset kaupankäyntiprosessin eri osapuolille. Kustannukset ja prosessien monimutkaisuus kasvaa sitä mukaa kun tuotteet monimutkaistuvat ja markkinat muuttuvat epävarmoiksi (Kambil ja Van Heck 1998, 3).

Elektronisen liiketoiminnan tietoturvavaatimusten täyttämiseksi voidaan tarkastella kaupankäyntiprosessin osaprosesseja ja etsiä prosesseja, joihin PKI:llä ja toimikorteilla voitaisiin tehdä parannuksia. Kambilin ja Van Heckin määrittelemistä prosesseista tämän tutkielman kannalta kiinnostavimpia ovat lähinnä maksaminen, tunnistus, arvotus, tuotteen esittely, laillistaminen, kiistojen ratkaisu ja kaikkia prosesseja yhdistävä kommunikointi. Näitä prosesseja voidaan siis uudistaa ja näin mahdollistaa sähköisen kaupan asettamien tietoturvavaatimusten täyttäminen. Näihin asioihin palataan tarkemmin myöhemmissä luvuissa.

2.1.1 Maksaminen

Nykyiset maksujärjestelmät perustuvat suurelta osin paperipohjaisiin prosesseihin. Joitain yksittäisiä maksutapahtuman osia on automatisoitu ja muutettu sähköiseen muotoon, mutta koko prosessia ei ole suunniteltu uudelleen. Maksuprosessin uudelleen suunnittelulla nykyistä teknologiaa hyödyntäen voitaisiin kuitenkin saavuttaa merkittäviä etuja nykyisiin prosesseihin nähden. (Leinonen 2000, 7)

Leinosen (2000, 7) mukaan useat käyttäjätottumusten ja teknologioiden muutokset näyttävät vaativan maksuprosessien uudelleen suunnittelua. Yksi tällainen esimerkki, joka on tämän tutkielman kannalta merkittävä, on modernia kryptografiaa hyödyntävä tietoturvainfrastruktuuri ja turvallisten mikrosirujen (esim. toimikortti) käyttö, jotka vaativat Leinosen mukaan maksuprosessin uudistamista ja joilla voidaan myös tehostaa prosessia. Prosessin tehostuminen perustuu näiden teknologioiden tarjoamiin autentikoinnin, tiedon eheyden ja turvallisen tiedonsiirron ratkaisuihin.

Leinosen (2000,7) mukaan prosessien muutokset tulisi kohdistaa maksuprosessin kahteen vaiheeseen, jotka ovat maksutiedon kulku maksavalta asiakkaalta vastaanottavalle asiakkaalle ja pankkien välinen tiedonsiirto. Tavoitteena prosessien

uudistamisessa tulisi Leinosen mukaan olla täysin elektronisen, koko järjestelmän läpi ulottuvan prosessin luominen. Tämä tarkoittaa ihannetapauksessa sitä, että maksutiedon siirto tapahtuu automaattisesti ja reaaliajassa kaikkien osapuolien välillä. Tällaisia järjestelmiä on jo toteutettu esimerkiksi suurten suomalaisten pankkien Internet-maksujärjestelmissä.

2.1.2 Tunnistus

Kambil ja Van Heck (1998, 5) ovat määritelleen tunnistus-prosessin tarkoittavan kaupankäynnin osapuolten tunnistamisen lisäksi myös tuotteen ominaisuuksien ja laadun varmistamista sekä sopimusten pitävyyden valvomista. Heidän mukaansa tunnistukseen voi liittyä kolmansia osapuolia, jotka vähentävät epävarmuutta ostajien ja myyjien välillä tarjoamalla esimerkiksi henkilöiden luottotietojen tarkastukseen ja notaarisointiin liittyviä palveluja.

Sähköisessä kaupankäynnissä tunnistusprosessi poikkeaa huomattavasti perinteisen kaupankäynnin vastaavasta. Perinteisesti ostaja ja myyjä kohtaavat fyysisesti ja voivat siten helposti varmistua toistensa identiteetistä. Myös tuotteiden laadun arviointi on helppoa, kun ostaja näkee tuotteen luonnossa ja voi monesti myös kokeilla sitä, eli ostaja voi hyödyntää aistejaan tuotteen arvioinnissa. Sähköisessä ostoprosessissa eivät edellä mainitut seikat ole mahdollisia, mikä hankaloittaa merkittävästi sen toteutusta. Tunnistuksen parantamisella voidaan siis selkeästi vaikuttaa sähköisen ostoprosessin sujuvuuteen ja myös kustannuksiin. Julkisen avaimen kryptografiaan perustuvat PKI-järjestelmät ovat avainasemassa tämän prosessin parantamisessa.

2.1.3 Kommunikointi

Kommunikointi liittyy kaikkiin kaupankäyntiprosessin osaprosesseihin ja siksi sen muuttamisella on suuret mahdollisuudet tehostaa ja sujuvoittaa koko kaupankäyntiprosessia. Kommunikointi käsittää esimerkiksi jokaisessa prosessissa yhtenä osana olevan osapuolten identifioinnin ja sivuaa siten tunnistusta. Siksi tähän

prosessiin pätee osittain samat, tietoturvan mahdollistamat parantamismahdollisuudet kuin tunnistusprosessiinkin. Tässä tutkielmassa pääpaino on kommunikoinnissa, joka yhdistää peruskaupankäyntiprosessin ja kaupankäynnin kontekstiprosessin osia. Luvussa kuusi kaupankäyntiprosessia tarkastellaankin juuri kommunikoinnin kannalta.

Yleisesti ottaen voidaan todeta, että kaupankäynnin sähköistäminen jo sinänsäkin parantaa kommunikointia, kun kauppaa voidaan käydä ajasta ja paikasta riippumatta lähes reaaliajassa. Tämä on merkittävä muutos varsinkin, kun puhutaan elektronisessa muodossa olevista tuotteista, jolloin muun muassa tuotteiden etsintä tehostuu kehittyneiden hakukoneiden vuoksi. Logistiikkakustannuksetkin ovat lähes olemattomat, sillä tuote voidaan siirtää asiakkaalle sähköisessä muodossa suoraan tietoverkon ylitse. Logistiikkaprosessin muuttuessa sähköiseksi myös sen tietoturvavaatimukset tulevat konkreettisiksi, kun varsinainen tuotekin voidaan siirtää suojaamattoman siirtotien ylitse. Tässä korostuu siis tiedon luottamuksellisuus ja eheys, jotta voidaan varmistaa, että asiakkaan tilaama tuote on juuri se, minkä hän on tilannut. Kommunikointia ja sen turvallisuutta edistämällä saavutetaan myös paremmat mahdollisuudet etätyöskentelyyn, kun yrityksen luottamuksellisia tietoja voidaan käsitellä Internetin ylitse mistä tahansa. Tässä tutkielmassa esiteltävillä tietoturvan parantamisen menetelmillä voidaan kommunikointiin lisätä elektronisen liiketoiminnan siltä vaatimaa turvallisuutta ja lisätä myös kuluttajien luottamusta siihen, että turvallinen kommunikointi Internetissä yleensä on todellakin mahdollista.

2.1.4 Laillistaminen

Sähköisessä kaupankäynnissä kaupan vahvistava laillistamisprosessi poikkeaa oleellisesti perinteisistä menetelmistä. Perinteisimmillään kauppa vahvistuu, kun ostaja suorittaa maksun kauppiaalle ja saa itselleen tuotteen. Sähköisessä kaupassa laillistaminen on siinä mielessä hankala prosessi, että ostotapahtuman yhteydessä kauppias ei välttämättä voi varmistua maksun saamisesta, eikä ostaja tavaran toimittamisesta. Laillistamisprosessi, kuten muutkin mainitut prosessit vaativat siis uudistamista.

Käytössä olevia laillistamismenetelmiä elektronisessa kaupassa ovat esimerkiksi sähköposti tai puhelinsoitto. Näistä ensimmäisessä ostaja saa erillisen vahvistuksen kaupasta sähköpostitse ja jälkimmäisessä voidaan ostajalta puhelimitse kysyä esimerkiksi luottokortin numero maksun hoitamiseksi ja kaupan vahvistamiseksi. Tähänkin prosessiin myöhemmin esiteltävät PKI ja toimikortit voivat kuitenkin tarjota parempia ratkaisuja.

2.1.5 Tuotteen esittely

Elektronisessa liiketoiminnassa myös tuotteen esittelyn prosessia voidaan tehostaa keräämällä tietoja asiakkaista, mikä on helposti toteutettavissa esimerkiksi vaatimalla asiakkaita rekisteröitymään verkkokauppaan ja tallentamalla tietoa asiakkaan toimista verkkokaupassa. Myös esimerkiksi Internet-osoite, josta asiakas on yhteydessä ja sivu, jolta hän on verkkokauppaan tullut, on helposti selvitettävissä. Tällöin asiakkaista voidaan kerätä kattaviakin demografisia ja henkilökohtaisiin mieltymyksiin liittyviä tietoja. Näin voidaan kohdentaa tiedotusta ja markkinointia, profiloida asiakkaita sekä personoida palveluita käyttäjäkohtaisesti. Tällainen tietojen keräys voi kuitenkin loukata henkilöiden yksityisyyttä.

Tämän tutkielman kannalta tuotteen esittely ei kuitenkaan ole merkittävä osa kaupankäyntiprosessia, sillä siihen ei juuri liity tietoturvaan liittyviä kysymyksiä siirryttäessä perinteisestä kaupankäynnistä sähköiseen. Sähköisen tunnistamisen osalta voidaan tuotteen esittelyllä nähdä oleva merkitystä esimerkiksi tapauksessa, jossa eri asiakkaille myönnetään erilaisia tarjouksia. Näin myös PKI:lla ja toimikorteillakin voidaan vaikuttaa tähän prosessiin. Tuotteen esittelyyn palataan lyhyesti vielä myöhemmin.

2.1.6 Etsintä

Elektronisessa liiketoiminnassa etsintä muuttuu merkittävästi, kun asiakas on käytännössä vain muutaman napin painalluksen päässä valtavasta määrästä yrityksiä ja

tuotteita ja palveluita. Myös yritysten puolelta etsintäprosessi muuttuu, kun Internetin avulla on mahdollista laajentaa asiakaskunta globaaliksi. Tämä tuo mukanaan uusia mahdollisuuksia ja riskejä molemmille osapuolille. Myöskään etsintä ei ole tässä tutkielmassa kiinnostava prosessi samoista syistä kuin tuotteen esittely, eikä siihen myöhemmin enää palata.

2.1.7 Arvotus

Sähköinen kaupankäynti luo uusia mahdollisuuksia myös arvotusprosessissa tapahtuvaan tuotteiden ja palveluiden hinnanmuodostukseen. Tästä on hyvänä esimerkkinä Kambilin ja Van Heckin (1998) esittelemät sähköiset huutokauppamenetelmät. Myös kauppiaiden ja varsinkin asiakkaiden suorittama hintavertailu helpottuu ja nopeutuu samoista syistä kuin tuotteiden ja palveluiden etsintä edellä mainitussa prosessissa.

Arvotusprosessiin kuitenkin palataan myöhemmin, sillä sähköisen kaupan hinnanmuodostuksessa vastaan tulee henkilöiden sähköiseen tunnistukseen ja tietoturvaan liittyviä kysymyksiä. Näihin, kuten muihinkin perinteisestä kaupankäyntiprosessista sähköiseen siirtymistä seuraavista kysymyksistä voivat myöhemmin käsiteltävät PKI-järjestelmät ja myös toimikortit tarjota ratkaisuja.

3 TIETOTURVA ELEKTRONISESSA LIIKETOIMINNASSA

Tässä luvussa käydään läpi ja määritellään elektronisen liiketoiminnan vaatiman tietoturvan osa-alueet, jotka ovat olennaisia PKI-järjestelmien ja toimikorttien mahdollistaman tietoturvan ymmärtämisen kannalta. Luvussa käsitellään ensin tietoturvaa ja sen osa-alueita, joiden yhteydessä todetaan miten PKI-järjestelmät ja toimikortit voivat niitä parantaa. Sen jälkeen tarkastellaan tietosuojan käsitettä. Luvun lopussa käsitellään henkilön sähköistä tunnistamisesta ja sähköistä identiteettiä.

Laine (2001, 131) näkee sähköisen kaupankäynnin ongelmana kuluttajien luottamuksen ja viestinnän luottamuksellisuuden, koska avoimessa tietoverkossa luottamuksellisuuden säilyttäminen on vaikeaa. Tämän vuoksi suuretkin yritykset ovat hidastelleet verkkokauppaan lähtemistä, sillä asiakastietojen paljastuessa on luottamus menetetty ja yrityksen ulkoinen kuva kärsii. Tutkimusten ja haastattelujen mukaan näiden ongelmien ratkaisusta riippuukin koko sähköisen kaupankäynnin tulevaisuus (Laine 2001, 131).

Kuten elektronisen liiketoiminnan käsittelyn yhteydessä todettiin, tietoturva on tällä hetkellä monien mielestä suurin yksittäinen este elektronisen liiketoiminnan yleistymiselle. Yleisen käsityksen mukaan ihmiset eivät luota siihen, että heidän luottamukselliset tietonsa pysyisivät salassa ja muuttumattomina siirrettäessä niitä tietoverkoissa. Suuri osa tästä tietoturvan kokemisesta puutteelliseksi johtuu epäluottamuksesta Internetissä tapahtuvaan maksamiseen, johon on olemassa vain rajoitettu määrä turvallisiksi koettuja keinoja. Laine (2001, 278) toteaakin: "Turvallista, yleisesti käytössä olevaa suoraa maksutapaa Internet-kauppaan ei vielä ole". Toistaiseksi suomalaisten tuomioistuinten tai viranomaisten käsittelyyn on tullut kuitenkin hyvin harvoin sähköiseen kauppaan tai maksamiseen liittyviä tapauksia. Sähköisen kaupan yleistyessä myös näiden ongelmien odotetaan yleistyvän (Laine 2001, 278, 279). Siksi maksujärjestelmien tutkimiselle ja kehittämiselle onkin annettu suuri paino. Maksaminen on kuitenkin vain yksi osa käsiteltäessä elektronisen liiketoiminnan tietoturvallisuutta, eikä tässä tutkielmassa tähän aiheeseen siksi

perehdytä syvällisemmin. Sähköisen kaupankäynnin maksamista ovat käsitelleet laajemmin muun muassa Ojala (1998), Leinonen (2000) ja Laine (2001, 247 – 329).

PKI:n ja myös toimikorttien taustalla oleva ja niiden toiminnan ymmärtämisen kannalta olennainen kryptografia on käsitelty liitteessä 1. Kryptografia tarjoaa monia keinoja nykyisten tietoturvavaatimusten täyttämiseksi ja henkilön sähköisen identiteetin luomiseksi ja sitä kautta henkilön luotettavaan sähköiseen tunnistamiseen. Käytettäessä kryptografiaa henkilön tunnistamiseen puhutaan useasti yksinkertaisesta tunnistamisesta salaisen avaimen kryptografian tapauksessa, ja vahvasta tunnistamisesta julkisen avaimen kryptografian yhteydessä. Kryptografian sovelluksista on selvitetty tarkemmin julkisen avaimen kryptografia ja suppeammin salaisen avaimen kryptografia. Myös digitaaliset allekirjoitukset ja Hash-funktiot, jotka ovat niin ikään olennaisesti sidoksissa PKI:hin, on käsitelty liitteessä 1.

Kryptografiaan perustuvien tietoturvaratkaisujen lisäksi on olemassa myös muita keinoja elektronisen liiketoiminnan tietoturvan parantamiseksi. Ojala (1998, 44) on listannut tällaisiksi muun muassa tapahtumien valvonnan reaaliaikaisesti tai lokitietojen tutkimisen jälkikäteen (tilastolliset analyysit), tapahtumien verifiointi vanhenemispäivämäärän ja suoritettujen tapahtumien määrän perusteella, erilaisten tapahtumiin liittyvien rajoitusten käyttö, laitteiston molemminpuolinen verifiointi tapahtumien yhteydessä sekä yksilöllisten PIN-koodien liittäminen tapahtumiin. Tässä tutkielmassa keskitytään kuitenkin lähinnä vain kryptografiaan perustuviin ratkaisuihin.

Tiedon salausta pidetään usein tietoturvan merkittävimpänä osana ja se saatetaan käsittää jopa synonyymiksi tietoturvalle. Vaikka salauksella voidaan saavuttaa suurin osa seuraavassa taulukossa määritellyistä tietoturvan osista, on salaus kuitenkin vain yksi osa tietoturvaa. Tavoitteena onkin saavuttaa tasapainoinen kokonaisuus tietoturvan eri osa-alueiden kesken. Seuraavassa taulukossa on määritelty lyhyesti käsitteitä, joista tietoturvan voidaan sanoa koostuvan ja jotka ovat myös tietoturvan keskeisimmät tavoitteet sekä elektronisen liiketoiminnan vaatimukset tietoturvalle. Käsitteet on esitelty tarkemmin seuraavissa luvuissa.

TAULUKKO 2. Tietoturvan tavoitteita ja määritelmiä Gutheryä ja Jurgensenia (1998, 201-204) sekä Ojalaa (1998, 26) mukaillen.

Tavoite	**Määritelmä**
Luottamuksellisuus (Confidentiality)	Tiedon pitäminen salassa niiltä, jotka eivät ole oikeutettuja tietoon.
Autentikointi (Authentication)	Henkilön identiteetin varmistaminen.
Auktorisointi (Valtuuttaminen) (Authorization)	Oikeuksien myöntäminen tiettyyn informaatioon.
Yksityisyys (Privacy)	Esimerkiksi henkilön kyky päättää häneen liittyvän informaation julkaisusta.
Tiedon eheys (Integrity)	Tiedon muuttumattomuuden varmistaminen.
Kiistämättömyys (Nonrepudiation)	Tiedon tai toiminnon jälkeenpäin tapahtuvan kiistämisen estäminen.
Käytettävyys (Usability)	Tietojärjestelmien on oltava käytettävissä, ajan tasalla ja helppokäyttöisiä.
Tapahtuman jäljitettävyys (Audit-trail)	Tapahtumista on voitava jälkeenpäin selvittää siihen liittyvät osapuolet ja kaikki tapahtuman vaiheet.

Branchaudin (1997, 1) mukaan Internetin ongelmat tietoturvan kannalta jakautuvat vain kahteen kategoriaan: yksityisyys ja autentikointi. Näihin ongelmiin liitteessä 1 käsitelty kryptografia voi tarjota ratkaisun, mutta tarkasteltaessa tietoturvaa elektronisen liiketoiminnan kannalta tarvitaan myös muita taulukossa 2 mainittuja käsitteitä, joihin kryptografia yksinään ei voi tarjota toimivaa ratkaisua.

Hendry (1997, 235) puolestaan toteaa, että tietoturva on tasapaino toisaalta tietoturvan vaatimusten ja toisaalta soveltuvuuden, kustannusten sekä luotettavuuden välillä. Hänen mukaansa realistinen vaatimus tietoturvalle on, että tietoturvassa pitäisi pyrkiä siihen, että järjestelmän murtamiseen vaadittavat resurssit ovat arvokkaampia kuin siitä saatava hyöty. Tämä ei tosin päde poliittisiin ja uskonnollisiin fanaatikoihin, joille saavutettavalla rahallisella hyödyllä ei välttämättä ole merkitystä (Hendry 1997, 244).

Whittenin (1999, 1) mukaan käyttäjien tekemät virheet ovat suurin tietoturvan pettämisen syy, mikä johtuu osittain tietoturvan hallinnan käyttöliittymien kömpelyydestä, hämmentävyydestä tai puuttumisesta. Hänen mukaansa tehokas tietoturva vaatii erilaisen käytettävyysstandardin ja että sitä ei voida saavuttaa muiden

ohjelmien käyttöliittymien standardien mukaisella suunnittelulla. Whitten myös todisti väitteensä käytännön testillä, jossa käytettiin tietoturvaohjelmistoa (PGP 5.0) ja, jossa oli yleisen standardin mukaisesti hyvä käyttöliittymä. Testin tuloksena oli, että käyttöliittymässä oli puutteita, jotka saattavat aiheuttaa tietoturvan pettämisen, eikä yli puolet testiryhmästä suoriutunut vaadituista tehtävistä.

Kuten Whitten (1999, 1) toteaakin, eivät vahva kryptografia, oikeat protokollat ja virheetön ohjelmakoodi voi taata tietoturvaa, mikäli käyttäjät ovat huolimattomia, epätietoisia vaatimuksista tai eivät osaa käyttää tai konfiguroida tarvittavia ohjelmia. Tietoturvasta puhuttaessa täytyykin aina muistaa, että ihmiset ovat siinä yhtenä, usein epävarmimpana osapuolena. Tämä tarkoittaa, että inhimillisiä erehdyksiä tapahtuu.

Whitten (1999, 3) toteaa myös, että käyttäjät eivät ole yleensä motivoituneita tietoturva-asioissa. Hänen mukaansa tietoturvan ja etenkin tietoturvan käyttöön vaadittavien käyttöliittymien suunnittelijoiden ei pitäisi olettaa, että käyttäjät haluavat itsenäisesti opiskella tietoturvaominaisuuksien käyttöä. Niinpä jos tietoturva on hankalakäyttöistä ja vaatii ylimääräistä opiskelua, voi sen käyttö jäädä tehottomaksi tai jopa kokonaan käyttämättä. Lisäksi Whitten (1999, 3) toteaa, että kaikkien tietoturvajärjestelmien kanssa tekemisissä olevien käyttäjien pitäisi olla hyvin tietoisia tietoturvasta ja sen tärkeydestä. Lisäksi tällaisten henkilöiden pitäisi saada sen käyttöön riittävä koulutus, sillä yleisesti tiedetään, että varsinkin tietokoneverkoissa turvallisuus on vain yhtä vahva kuin sen heikoin lenkki. Niinpä taulukossa 2 mainittujen tietoturvan tavoitteiden täyttyminenkään ei takaa aukotonta tietoturvaa Internetissä.

3.1 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan sitä, että informaatiota pidetään vain niiden tahojen tiedossa, joilla siihen on oikeus. Käsitettä salaisuus käytetään usein myös synonyyminä luottamuksellisuudelle ja yksityisyydelle. Tiedon luottamuksellisuus voidaan saavuttaa useilla tavoilla, kuten esimerkiksi fyysisellä suojaamisella tai kryptografisilla menetelmillä. Laine (2001, 132) on määritellyt luottamuksellisuuden tarkoittavan verkkokaupan yhteydessä sitä, että palvelut ja tavarat toimitetaan perille ja erityisesti

sitä, että asiakkaiden tiedot ovat vain niiden käytettävissä, joille ne on tarkoitettu. Luottamuksellisuus kattaa siis eri osapuolten informointi- ja salassapitovelvollisuudet.

Suurin osa Internetissä siirretystä datasta on vailla tietosuojaa, eikä sitä siksi voida pitää luottamuksellisena. Internetissä liikkuva suojaamaton tieto on periaatteessa kenen tahansa luettavissa, kopioitavissa ja muutettavissa. Internetissä välitettyjä sähköpostiviestejä onkin verrattu postikortteihin luottamuksellisuutensa puolesta. Tämä johtuu osin siitä, että nykymuotoisen Internetin alkuperäisenä ideana ei ollut siirtää luottamuksellisia tietoja vaan se perustui lähinnä ilmaiseen tiedon levitykseen. Nykyisistä Internetin käyttömuodoista etenkin sähköinen kauppa asettaa kuitenkin selkeitä vaatimuksia Internetissä liikkuvan tiedon luottamuksellisuudelle.

PKI:ssä luottamuksellisuus saavutetaan julkisen avaimen sertifikaateilla. Käyttäjä voi salaisen avaimen avulla, joko digitaalisesti allekirjoittaa tai salata dokumentteja, jolloin niiden luottamuksellisuus voidaan varmistaa salaista avainta vastaavan sertifikaatin avulla. Ja kuten myöhemmin todetaan, ehdottoman luottamuksellisuuden saavuttamiseksi tarvitaan myös TTP:tä. Tämän vuoksi voidaan todeta, että TTP:tä käyttävissä varmentajajärjestelmissä voidaan saavuttaa parempi luottamuksellisuus kuin PGP:hen perustuvissa järjestelmissä, joissa luottamus perustuu periaatteessa henkilöiden väliseen luottamukseen.

Toimikorttien käytöllä luottamuksellisuutta pyritään parantamaan kahdella tavalla. Toisaalta taataan kortilla olevien tietojen, kuten esimerkiksi henkilön sairaustietojen tai tilitietojen luottamuksellisuus ja toisaalta sellaisten, tietojärjestelmiin tallennettujen tietojen, joihin voi päästä käsiksi vain toimikortilla (Hendry 1997, 18). Toimikorteilla voidaan siis vahvistaa PKI:n tarjoamaa tiedon luottamuksellisuutta, sillä kuten luvussa 5 todetaan, toimikortit ratkaisevat sellaisia PKI-järjestelmien ongelmia, jotka voivat heikentää myös tiedon luottamuksellisuutta. Tärkein näistä seikoista on salaisen avaimen tallentaminen kortille, josta se ei voi helposti joutua sivullisten käsiin.

3.2 Autentikointi

Autentikoinnilla, josta voidaan käyttää myös termejä tunnistaminen tai todentaminen, tarkoitetaan toisen osapuolen luotettavaa tunnistamista tai sanoman alkuperän luotettavaa selvittämistä. Guthery ja Jurgensen (1998, 201) ovat puolestaan määritelleet autentikoinnin tarkoittavan identiteetin liittämistä transaktioon. Autentikoinnin voidaan sanoa olevan osa henkilön sähköistä tunnistamista, jota on käsitelty tarkemmin myöhemmin. Autentikoinnin tavoitteena on siis, että kahden tietoverkossa kommunikoivan osapuolen on voitava tunnistaa toisensa ja heidän toisilleen lähettämä tieto on voitava autentikoida siten, että tiedon lähettäjä, tiedon sisältö ja lähetyksen aika voidaan varmistaa (Menezes 1997, 4). Autentikointi onkin yksi tärkeimpiä tietoturvan vaatimuksia ja se on edellytys muun muassa tiedon eheyden varmistamiselle ja kiistämättömyydelle (Menezes 1997, 24).

Sähköisessä maailmassa autentikointi on ongelmallista, sillä osapuolten välillä on harvoin mitään fyysistä kontaktia, jolloin esimerkiksi henkilöt voisivat luotettavasti tunnistaa toisensa. Voidaankin sanoa, että mitään ehdottoman luotettavaa menetelmää ei ole olemassa, sillä tietoverkoissa eri osapuolten välinen autentikointi perustuu aina siihen, että osapuolet joutuvat luottamaan johonkin tahoon, jota kutsutaan yleensä luotettavaksi kolmanneksi osapuoleksi. Mutta kuten aiemmin jo todettiin, luottamista luotettuun kolmanteen osapuoleen voidaan yleisesti pitää riittävänä luotettavalle autentikoinnille varsinkin, jos kyseessä on viranomaistaho.

PKI:ssä autentikointi perustuu salaisen avaimen ja sitä vastaavan julkisen avaimen sertifikaatin käyttöön. Varmentajajärjestelmissä autentikoinnin voidaan sanoa olevan varmempaa kuin PGP:ssä, kuten luottamuksellisuudenkin yhteydessä. Tämä perustuu siihen, että varmentajajärjestelmissä luotettu kolmas osapuoli on vastuussa henkilön identiteetin liittämisestä julkiseen avaimeen ja se myös digitaalisesti allekirjoittaa henkilölle myönnetyn sertifikaatin. PGP:ssä tällaista menettelyä ei ole ja luottamus sertifikaatin autenttisuuteen on siis vain henkilökohtaisen luottamuksen varassa.

Toimikortti voidaan nähdä itsenäisenä, aktiivisena (vrt. esim. passi, joka on passiivinen autentikointiväline), mukana kannettavana ja turvallisena välineenä, joka voi sisältää erittäin tarkkaan autentikointiin vaadittavan määrän luottamuksellista henkilökohtaista tietoa. Aktiivisuus tarkoittaa sitä, että toimikortti voi suorittaa luottamuksellisia autentikointiin liittyviä toimintoja itsenäisesti ja riippumatta laitteesta, jossa sitä käytetään.

Toimikorttien avulla voidaan suorittaa kaksivaiheinen autentikointi. Ensimmäisessä vaiheessa henkilö autentikoidaan käyttämällä PIN-koodia tai biometristä tunnistusta, joita verrataan kortille tallennettuihin tietoihin. Tämän jälkeen kortti autentikoituu palvelulle käyttämällä PKI:hin perustuvia varmenteita. Toimikortille voidaan tallentaa myös lisäinformaatiota käyttäjästä luotettavuuden lisäämiseksi. Toimikorttien nykyiset muistirajoitukset estävät kuitenkin suuren tietomäärän tallentamisen ja suuntauksena onkin ollut kortilla olevien tietojen minimointi ja lisätietojen tallentaminen tietokantoihin, joista ne haetaan käyttäjän autentikoinnin jälkeen.

Ojala (1998, 51) toteaa, että toimikorttien käyttö PKI:ssä mahdollistaa molemminpuolisen autentikoinnin elektronisessa liiketoiminnassa ja tuo siihen kaivattua lisävarmuutta. Molemminpuolisella autentikoinnilla tarkoitetaan sitä, että esimerkiksi sähköisessä kauppapaikassa asiakkaan autentikoinnin yhteydessä myös kauppapaikka autentikoituu asiakkaalle. Tämä tosin monimutkaistaa kaupankäynnin järjestelmiä, mutta lisää turvallisuutta merkittävästi, sillä näin voidaan suojautua Suomessakin vasta tapahtunutta palvelun naamioitumista vastaan. Tässä hyökkäyksessä perustettiin huijauskauppapaikka, jonka avulla kerättiin asiakkaitten henkilötietoja sisältäen muun muassa luottokorttinumeroita.

3.3 Auktorisointi

Autentikoinnin lisäksi elektronisessa kaupankäynnissä tarvitaan usein myös menetelmiä järjestelmän sisäisten ”sääntöjen” noudattamisen mahdollistamiseksi sekä käyttäjien luokittelemiseksi siten, että heillä on eritasoisia oikeuksia tietoihin tai palveluihin. Tästä käytetään termiä auktorisointi. Samasta asiasta voidaan käyttää myös termejä

valtuuttaminen tai oikeuttaminen. Auktorisointi siis tarkoittaa lyhyesti ilmaistuna oikeuksien liittämistä transaktioon (Guthery ja Jurgensen 1998, 202).

PKI-järjestelmistä auktorisointia voidaan toteuttaa järkevästi vain varmentajajärjestelmissä. Hierarkkisen rakenteensa takia myös eritasoisten käyttöoikeuksien myöntäminen on mahdollista. Esimerkiksi Windows-ympäristössä voidaan käyttää sertifikaatteihin perustuvaa autentikointia, jolloin auktorisointikin voidaan hoitaa sertifikaattiperusteisesti, käyttäen Windowsin sisäisiä menetelmiä käyttöoikeuksien määrittelyyn. PGP-mallissa auktorisointi ei ole helposti toteutettavissa eikä PGP:tä ole sovellettukaan sellaiseen käyttöön, jossa oikeuksien määrittely on tarpeen.

Toimikortteja käytetään auktorisoinnissa samaan tapaan kuin autentikoinnissakin ja auktorisointi voidaankin nähdä itse asiassa sen järjestelmän ominaisuudeksi, jossa toimikortteja käytetään. Tämä voi tarkoittaa käytännössä esimerkiksi sitä, että sähköiseen kauppapaikkaan voi autentikoitua toimikortilla eritasoisia käyttäjiä. Tavallisten asiakkaiden lisäksi käyttäjällä voi olla esimerkiksi kauppapaikan ylläpito-oikeudet. Auktorisointitieto voi kyllä sijaita toimikortillakin, mutta yleisesti kyseinen tieto sijaitsee järjestelmässä sen helpomman muutettavuuden ja ylläpidon kannalta.

Ranklin ja Effingin (1997, 381) mukaan toimikortteihin perustuvaa auktorisointia voidaan käyttää muun muassa pääsynvalvonnassa. Tällöin rakennuksen oviin voidaan asentaa kortinlukijat ja jakaa käyttäjille toimikortit. Käyttäjät jaetaan ryhmiin joilla on erilaisia kulkuoikeuksia rakennuksessa. Käyttäjän kulkumahdollisuus tietyistä ovista todetaan käyttäjän laittaessa kortin lukijaan ja syöttäessä PIN-koodin, jolla tunnistaudutaan kortille. Nyt kortilla olevia käyttäjän tietoja verrataan joko kortinlukijan muistissa oleviin käyttäjiin tai mikäli kortinlukija on verkossa, tietokannassa oleviin tietoihin ja tehdään päätös kulkuoikeudesta. Tällaisen järjestelmän tulee toimia nopeasti, jotta sen käytettävyys vaatimus täyttyy. Ranklin ja Effingin (1997, 381) mukaan prosessi ei saisi kestää paljon sekuntia kauempaa saadakseen käyttäjien hyväksynnän.

3.4 Yksityisyys

Yksityisyys tarkoittaa sitä, että vain transaktioon liittyvät osalliset saavat tiedon itse transaktion tapahtumisesta tai sen yksityiskohdista (Guthery ja Jurgensen 1998, 203). Toistaiseksi yksityisyyden suojaamiseksi Internetissä on käytetty lähinnä muita kuin teknisiä ratkaisuja. Tällaisia ovat esimerkiksi lainsäädäntö ja erilaiset suositukset toimintatavoiksi, kuten Suomen valtion henkilörekisterilaki ja perustuslaki sekä EU:n tietosuojadirektiivi. Teknisiäkin ratkaisuja on kuitenkin jo olemassa, kuten Liitteessä 1 käsitelty vahva kryptografia, jonka avulla on mahdollisuus tarjota käytännön ratkaisu yksityisyyden ongelmaan (Laine 2001, 137).

Sähköisessä kaupankäynnissä yksityisyyden ongelma aiheutuu suurelta osin henkilöllisyyden tunnistamisen ja yksityisyyden välisestä ristiriitaisuudesta, sillä järjestelmien pitäisi pystyä mahdollisimman luotettavasti tunnistamaan ja todentamaan käyttäjät yksityisyyttä loukkaamatta. Asiakkaille yksityisyyden varjeleminen on tärkeää, mistä esimerkkinä eräiden WWW-kauppapaikkojen raportit jopa 50 prosentin pudotuksista tietoliikenteessä sen jälkeen, kun kyseiset kauppapaikat alkoivat vaatia sivuilleen rekisteröintiä. Yleisesti voidaan todeta, että yksityisyyden suoja vaarantuu henkilöstä tallennettujen tietojen määrän kasvaessa. Tämä on totta varsinkin silloin, kun sähköisen kaupan järjestelmiä toteutetaan perinteisten tietojärjestelmien tapaan tunnistaen käyttäjät ja tallentaen käyttötapahtumatiedot (Ojala 1998, 54, 55).

PKI:ssä yksityisyyden saavuttaminen perustuu pääasiassa tiedon salaukseen, joka voidaan toteuttaa niin varmentajajärjestelmissä kuin PGP:ssäkin. Toimikorttien tuoma lisä yksityisyyden suojeluun perustuu yksinkertaisesti siihen, että henkilö voi pitää mukanaan toimikortilla sijaitsevat kryptografisesti suojatut, tiedon salaukseen käytettävät avaimet.

3.5 Tiedon eheys

Tiedon eheys sisältää informaation ja tietojenkäsittelyn oikeellisuuden, aitouden ja ajantasaisuuden sekä näiden ominaisuuksien ylläpidon (Laine, 2001, 134). Gutheryn ja Jurgensenin (1998, 203) mukaan tiedon eheys tarkoittaa sitä, että transaktioon liittyvä tieto pysyy muuttumattomana sekä transaktion aikana että sen jälkeen. Takaamalla tiedon eheys voidaan siis taata viestin alkuperäinen sisältö. Internetissä siirrettävä suojaamaton tieto on helposti luettavissa ja muutettavissa. Ei siis voida varmistua siitä, että vastaanottajan saama sanoma on juuri sellainen kuin lähettäjä sen tarkoitti olevan. Sähköisessä kaupassa tämä voisi tarkoittaa sitä, että verkossa lähetetyn tilauksen tai laskun sisältöä voisi joku asiansa osaava muuttaa ennen kuin se päätyy oikealle vastaanottajalle. Tällaista mahdollisuutta ei voida kaupankäynnissä sallia ja siksi tiedon eheyden varmistamiseen tarvitaan ehdottoman turvallisia keinoja. Jotta tiedon eheys voidaan taata, täytyy olla keino havaita tiedon luvaton käsittely. Tiedon käsittely tässä yhteydessä tarkoittaa tiedon lisäystä, poistoa tai muuttamista.

Sähköisessä maailmassa tietoverkkojen ulkopuolella tiedon eheys on helposti varmistettavissa tallentamalla tieto esimerkiksi CD-R-levylle, johon kerran tallennettua tietoa ei voida enää muuttaa. Internetiä hyödyntävässä sähköisessä kaupankäynnissä tällä ei kuitenkaan ole juuri merkitystä, sillä nimenomaan verkon yli siirrettävän tiedon eheys täytyy voida varmistaa.

Tiedon eheys sähköisessä maailmassa voidaan varmistaa helpoiten liitteessä 1 käsitellyillä digitaalisilla allekirjoituksilla tai pelkillä tiivistefunktioilla, joilla voidaan varmistaa, että esimerkiksi Internetin ylitse siirrettyä tietoa ei ole muutettu matkalla. Tiedon eheys voidaan taata sekä varmentajapohjaisilla PKI järjestelmillä, että PGP:ssä. Toimikorttien käytöllä ei saavuteta merkittäviä uudistuksia tiedon eheyden saavuttamisen keinoihin, mutta tietoturvan kannalta ajateltuna myös tiedon eheys voidaan varmistaa luotettavammin. Voidaan kuitenkin todeta, että toimikorteilla voidaan myös taata esimerkiksi tiedon eheyden varmistamiseen käytettyjen allekirjoitusavaintenkin eheys. Tämä on mahdollista, sillä toimikortille tallennetujen tietojen muuttaminen on estetty monin fyysisin ja ohjelmallisin keinoin.

3.6 Kiistämättömyys

Gutheryn ja Jurgensenin (1998, 204) mukaan kiistämättömyydellä varmistetaan, että yksikään transaktioon liittyvä osapuoli ei voi jälkeenpäin kiistää osallistumistaan kyseiseen transaktioon. Laineen (2001, 43) mukaan Internetissä ei kuitenkaan ole valmista mekanismia liiketoimen kiistämiseen jälkeenpäin. Tämän vuoksi henkilön sähköiseen tunnistamiseen on pyritty liittämään digitaalinen allekirjoitus, jolla kiistämättömyys voidaan taata. Digitaalisia allekirjoituksia on käsitelty tarkemmin liitteessä 1. Tapahtumien kiistämisestä syntyvien ongelmien ratkaisemiseksi on oltava myös omat keinonsa. Tähän vaaditaan usein luotetun kolmannen osapuolen mukanaoloa (Menezes 1997, 4).

Toimikorttien käyttö kiistämättömyyden saavuttamiseksi kaupankäyntiprosessissa esimerkiksi digitaalisilla allekirjoituksilla voi parantaa sähköisen kaupankäynnin tietoturvaa. Näin voidaan välttää muun muassa PKI:n ongelmien yhteydessä mainitut ongelmat ohjelmistovarmenteiden käytössä. Tapahtuman kiistämättömyys on varmistettavissa vain niin kauan, kuin salainen avain pysyy turvassa. Myös tästä syystä toimikortit ovat parempi väline kiistämättömyyttä vaativien toimenpiteiden suorittamiseen, kuin PKI:ssa käytetyt ohjelmistovarmenteet, jotka voivat helposti joutua vääriin käsiin. Kiistämättömyydestä puhuttaessa on syytä huomata, että se on myös laissa huomioitu. Tästä syystä esimerkiksi tapahtuman kiistämättömyyden mahdollistavasta digitaalisesta allekirjoituksesta on pystyttyvä selvittämään aukottomasti henkilön identiteetti. Tästä taas seuraa, että PGP:tä käyttäen ei voida suorittaa kiistämättömiä tapahtumia sen puutteellisten identifiointiominaisuuksien takia.

3.7 Käytettävyys

Edellä mainittujen tietoturvan osa-alueiden joukkoon on syytä lisätä myös tiedon käytettävyys. Laine (2001, 134) on määritellyt käytettävyyden tarkoittavan olotilaa, jossa data, manuaalisesti ylläpidetty informaatio ja tietojärjestelmät ovat sekä ajan tasalla että muullakin tavoin saatavissa käyttöön. Käytettävyydellä voidaan tarkoittaa

myös helppokäyttöisyyttä ja helposti opittavuutta. Käytettävyyden merkitys korostuu erityisesti sähköisen kaupankäynnin järjestelmissä, koska niiden tulisi palvella mahdollisimman suurta käyttäjäjoukkoa. Kun samalla kuitenkin vaaditaan korkeaa tietoturvan tasoa, syntyy ristiriita käytettävyyden ja tietoturvan välille, sillä tietoturvan tason korotus heikentää lähes poikkeuksetta käytettävyyttä. (Ojala 1998, 26)

Ojala (1998, 34) toteaakin, että tietoturva pitäisi pyrkiä piilottamaan käyttäjältä, sillä sähköisen kaupankäynnin korkeat tietoturvavaatimukset monimutkaistavat järjestelmiä ja siten hankaloittavat käytettävyyttä. Tästä voi hänen mukaansa seurata myös se, että itse järjestelmän monimutkaisuus voi olla tietoturvaratkaisuja suurempi kompleksisuuden aiheuttaja. Kuten myöhemmin käsiteltävissä PKI:n ongelmakohdissa todetaan, voi huono käytettävyys romahduttaa koko järjestelmän tietoturvan. Tämän vuoksi tietojärjestelmien tietoturvan käytettävyys ja sitä tukevien käyttöliittymien suunnittelu on huomioitava kaikissa sähköisen kaupankäynnin prosesseissa. Etenkin autentikointiin, maksamiseen ja tilausten vahvistamiseen (laillistaminen) liittyvissä prosesseissa käytettävyydellä on suuri merkitys prosessien sujuvoittamisen ja tehostamisen kannalta. Käytettävyys ja käyttöliittymien suunnittelu ovat kuitenkin sen verran laajoja alueita, että niihin ei tässä tutkielmassa syvällisemmin puututa.

Elektronisella liiketoiminnalla on siis korkeat vaatimukset tietoturvan suhteen, mutta käytettävyys ei kuitenkaan saa heikentyä. Tämä pätee myös henkilön sähköiseen tunnistamiseen, jossa tällä hetkellä käytössä olevat luotettavat tunnistusmenetelmät ovat ristiriidassa käytettävyyden kanssa. Kertakäyttösalasanat ja avainlukulistat pysyvien käyttäjätunnusten ja salasanojen lisänä hankaloittavat tunnistamisprosessia siinä määrin, että niitä ei ole otettu käyttöön kuin kaikista suurimman tietoturvan vaatimissa sovelluksissa, kuten pankkipalvelujen käytössä. Tällaisen menettelyn käyttö elektronisessa liiketoiminnassa johtaisi kuitenkin siihen, että jokaisella kauppapaikalla olisi omat avainlukulistansa tai että kauppapaikat toimisivat yhteistyössä keskenään tunnistamisen osalta. Nämä vaihtoehdot eivät kuitenkaan ole todennäköisiä niiden yleistymisen kannalta.

PKI:tä hyödyntävässä sähköisessä kaupankäynnissä käytettävyyttä voidaan parantaa käyttämällä toimikortteja. Käytettävyys paranee, kun esimerkiksi salaukseen ja

allekirjoitusten tekoon vaadittava sertifikaatti ja avaimet kulkevat aina käyttäjän mukana, eikä niitä tarvitse asentaa erikseen koneelle, jolta esimerkiksi verkko-ostoksia tehdään. Tämä tietysti vaatii, että käytettävällä koneella ja kauppapaikalla on valmius toimikorttien hyödyntämiseen.

Toimikortit vastaavat hyvin käytettävyyden ongelmaan, sillä korttia käytettäessä vaaditaan muistettavaksi vain yksi PIN-koodi eikä hankalia avainlukulistoja tarvita. Lisäksi ihmiset ovat jo tottuneet käyttämään automaatti –, puhelin- ja maksukortteja, eikä toimikortti tuo käytäntöön juuri muutosta. Käytättäjän kannalta ainoana ongelmana on erillisen kortinlukijan hankkiminen ja sen asentaminen ohjelmistoineen ennen kuin kortin käyttö omalta koneelta on mahdollista. Toimikortti myös piilottaa hyvin salaustekniikan ja periaatteet verrattuna esimerkiksi PGP:hen, joka vaatii PKI:n perusteiden ymmärtämisen käyttöönoton ja tehokkaan hyödyntämisen onnistumiseksi.

Tällä hetkellä toimikorttien käytettävyyttä heikentää niiden heikko laskentateho pöytäkoneisiin verrattuna. Tästä seuraa, että pitkiä salausavaimia käytettäessä kortin käyttö tiedon salauksessa ja digitaalisten allekirjoitusten teossa hidastuu selvästi päätelaitteille asenettujen ohjelmistovarmenteiden käyttöön verrattuna. Lisäksi käyttäjien hyväksymät odotusajat tietojärjestelmiä kohtaan ovat koko ajan laskeneet. Myös se, että toimikorttien käytännön sovelluksissa käytetään huomattavasti enemmän laskentatehoa vaativia julkisen avaimen kryptografiaan perustuvia avaimia hidastaa korttien käyttöä ja heikentää siten käytettävyyttä. Nämä asiat on syytä huomioida myös kaupankäyntiprosessin eri osissa, jos pyritään mahdollisimman nopeaan prosessin läpivientiin. Toimikorttien laskentateho kuitenkin kasvaa koko ajan, eikä tätä voida siksi pitää merkittävänä esteenä niiden käytölle.

3.8 Tapahtuman jäljitettävyys

Niin elektronisessa kuin perinteisessäkin liiketoiminnassa on olemassa vaatimus tapahtumien jäljitettävyydelle (audit-trail). Ongelmatilanteiden sattuessa on voitava selvittää ketkä osapuolet olivat osallisina tapahtumaan ja mitä vaiheita tapahtumassa oli. Sekä Gutheryn ja Jurgensenin (1998, 201–204) että Ojalan (1998, 26) määrittelemistä

tietoturvan osa-alueista tapahtuman jäljitettävyys kuitenkin puuttuu. Tämä on kuitenkin merkittävä osa tietoturvaa ja käyttäjien luottamusta lisäävä tekijä niin perinteisissä kuin elektronisen kaupankäynnin järjestelmissäkin. Tapahtuman jäljitettävyydelle sähköisessä maailmassa ei löydy mitään tarkkoja määritelmiä eikä sovittuja käytäntöjä saati standardeja. Tapahtuman jäljitettävyyden voidaan sanoa olevan eräänlainen kartta, joka kuvaa koko transaktion käyttäjän ostoaloitteesta kaupankäyntiprosessin läpi aina tavaran tai palvelun toimittamiseen asti (Lange 1999).

Langen (1999) mukaan tapahtuman jäljitettävyydellä on kolme tärkeää merkitystä elektronisessa liiketoiminnassa.

1. Mahdollistaa vastaaminen asiakkaiden kysymyksiin ja valituksiin tarjoamalla tiedot kaikista transaktioista,

2. Tarjoaa pohjan kaikkien kuittien tallennuksen varmistamiseen ja ettei mitään toimituksia ole tehty ilman kunnolla tallennettuja tietoja,

3. Ja varmistaa, että myynneistä, toimituksista ja kuiteista on historiallinen kirjanpito, jota voidaan käyttää esimerkiksi suunnitteluun tai budjetoinnin apuna.

Yleensä tapahtumien jäljitys tietojärjestelmissä ja sähköisessä kaupassa suoritetaan erilaisten lokien perusteella. Näistä ei kuitenkaan välttämättä voida aukottomasti tunnistaa tapahtumaan liittyviä osapuolia. Digitaalisilla allekirjoituksilla ja julkisen avaimen sertifikaateilla voidaan kuitenkin parantaa tapahtumien jäljitettävyyttä merkittävästi, sillä näiden menetelmien avulla voidaan tapahtumiin liittää niihin osallistuneiden henkilöiden identiteetit.

Steinauer ym. (1997, 119,129) on kirjannut tapahtumien jäljitettävyyden yhdeksi tärkeimmistä kuluttajien luottamusta lisäävistä tekijöistä. Hänen mukaansa luottamus kaupankäyntitapahtumaan lisääntyy, mikäli kaikki osapuolet tietävät, että tapahtuma voidaan jäljittää alusta loppuun asti. Tämä siksi, että mikäli tapahtumassa ilmenee ongelmia tai osapuolten välille syntyy ristiriitoja, voidaan prosessi selvittää askel

askeleelta ja selvittää missä virhe on tapahtunut ja kuka on mahdollisesti vastuussa siitä. Perinteisessä kaupankäynnissä esimerkiksi kuitit takaavat tapahtuman jäljitettävyyden. (Steinauer ym. 1997, 119)

Tapahtumien jäljitettävyys voi kuitenkin loukata henkilön yksityisyyttä, sillä esimerkiksi verkkokauppa voi kerätä kaikki tietyn henkilön eri aikoina tekemät tapahtumat ja yhdistää ne myöhemmin kyseiseen henkilöön. Tämä on myös ristiriidassa anonyymin asioinnin vaatimuksen kanssa, jota käsitellään tämän luvun lopussa.

3.9 Tietosuoja

Tietosuojalla tarkoitetaan yksinkertaistaen ulkopuolisten velvollisuuksia varmistaa yksityistä henkilöä koskevien tietojen suojaa. Tietosuojan tavoitteena on osaltaan turvata kansalaisten yksityisyys varmistamalla, ettei henkilötietoja käytetä väärin. Tietosuojan varmistaminen ja sen selkeä määrittely ovat keskeisiä vaatimuksia elektronisessa liiketoiminnassa. Tällä hetkellä tiedon keruu ja sen käyttö tietoverkoissa on vielä melko holtitonta vaikka siihen on olemassa lakeja ja määräyksiä. Tähän on eräänä syynä tietosuojan hankala valvottavuus. Tämän vuoksi on alkanut syntyä kysyntää sille, että henkilö voisi myös itse vaikuttaa tietosuojaansa. Lainsäädännön taholta tietosuojaan liittyvät seuraavat lainsäädäntöön kirjatut määräykset

- mitä henkilöitä koskevia tietoja saa kerätä,
- kuka tietoja saa kerätä sekä
- kenelle tietoja saa luovuttaa?

Tietoverkkojen käytöstä jää aina jälkiä, jotka voivat vaarantaa käyttäjien tietosuojan. Sähköisiä jälkiä syntyy muun muassa IP-tason verkkoliikennöinnistä, sähköpostiliikenteestä sekä WWW-palvelujen käytöstä. Verkoissa on myös käyttäjiä koskevia julkisia rekistereitä, kuten Internetin nimipalvelu, sähköpostiosoiteluettelot tai puhelinluettelot. Yrityksillä ja viranomaisilla on hallussaan yksityisiä rekistereitä kuten

WWW-palvelujen ja sähköpostipalvelujen käyttäjärekisterit. Jälkiä ja rekistereitä on myös operaattoreilla, loppupalvelujen tarjoajilla ja käyttäjien työnantajilla yrityksen sisäisissä verkoissa. (Liikenneministeriö 1998)

Tietosuojan ja tietoturvan välillä on kiinteä yhteys. Tietosuojaa koskevat määräykset asettavat vaatimuksia henkilötietoja sisältävien järjestelemien ja henkilötietoja siirtävien verkkojen tietoturvaratkaisuille. Työnantajien, operaattoreiden, loppupalveluntarjoajien ja viranomaisten verkkojen ja tietojärjestelmien on oltava riittävästi suojattuja, etteivät henkilötiedot joudu vääriin käsiin tai muutu. (Liikenneministeriö 1998)

PKI:ssä ja toimikorttien käytössä tietosuoja perustuu pääasiassa tiedon salaukseen ja Laineen (2001, 137) mukaan myös digitaalisen allekirjoitukset voivat tarjota osaratkaisun tietosuojan ongelmiin. Digitaalisia allekirjoituksia on käsitelty liitteessä 1. PKI:llä ja toimikorteilla voidaan myös ratkaista tietosuojaan läheisesti liittyvän sähköisen tunnistamisen ongelmia, joita on käsitelty luvun lopussa.

Useissa nykyisissä verkkokaupoissa kauppias voi kerätä asiakkaiden tietoja itselleen. Näin kauppiaan on mahdollista luoda ostoprofiileja ja suunnitella paremmin toimintaansa. Tämä synnyttää kuitenkin epäluottamusta asiakkaiden keskuudessa, sillä riski tietojen väärinkäytöstä kasvaa, kun useat kauppiaat keräävät ja säilyttävät asiakkaiden tietoja. Väärinkäytökset voivat olla tarkoituksellisia, jos kauppias esimerkiksi myy tietoja eteenpäin. Tietojen myynti on laitonta, mutta sitäkin on tapahtunut. Väärinkäytös voi tapahtua myös kauppiaan kannalta tahattomasti esimerkiksi tietomurron yhteydessä. Maailmalta on uutisoitu useita tapauksia, joissa verkkokauppaan on murtauduttu ja tuhansien käyttäjien tiedot, mukaan lukien luottokorttien numerot, on joutunut vääriin käsiin. Asiakkaiden tietojen kerääminen siis muodostaa merkittävän tietosuojariskin.

On kuitenkin mahdollista, että asiakas luo oman ostoprofiilinsa, jota hän säilyttää itsellään ja luovuttaa ainoastaan ostotapahtuman yhteydessä kauppiaalle. Näin asiakastiedon kontrolli on kuluttajalla itsellään ja väärinkäytösten mahdollisuus pienenee. Toimikortit mahdollistavat teoriassa sen, että tämä ostoprofiili voitaisiin tallentaa toimikortille, jolloin se on kryptografisesti suojattu ja aina kuluttajan mukana.

Tämä lisää sen käytettävyyttä ja turvallisuutta verrattuna tietokoneelle tallennettuun ostoprofiiliin. Tällöin vältytään myös asiakastietojen menetykseltä tietomurroissa, koska tietoja ei ole tallennettuna missään keskitetysti. Näin vältytään myös monimutkaisten kontrollijärjestelmien ja säännöstöjen luomiselta kauppiaiden tiedon keruuta koskien. Nykyisissä toimikorteissa muistin pieni määrä kuitenkin rajoittaa tämän tyyppisten tietojen tallennusta, mutta tallennuskapasiteetin kasvaessa siitä tulee varteenotettava toimikortin käyttömuoto.

3.10 Henkilön sähköinen tunnistaminen

Henkilön sähköisestä tunnistamisesta käytetään myös termejä todentaminen ja identifiointi (identification). Myös autentikoinnista käytetään termiä todentaminen, mutta tässä tutkielmassa on syytä huomata, että autentikointi suppeampana käsitteenä, ja henkilön sähköinen tunnistaminen kuitenkin poikkeavat toisistaan.

Elektronisessa liiketoiminnassa keskeisimpänä vaatimuksena voidaan pitää henkilön sähköistä tunnistamista. Henkilön sähköinen tunnistaminen perustuu yleisesti ottaen kolmeen tekijään, joita ovat: jotain mitä tiedät, olet tai omistat. Kaikkia näitä on käytetty menestyksellisesti henkilöiden tunnistamiseen, mutta elektroniseen maailmaan siirryttäessä voidaan sanoa, että riittävän luotettavuuden saavuttamiseksi vaaditaan vähintään kahden ominaisuuden yhdistämistä. Kahden tai useamman ominaisuuden yhdistäviä tunnistusmenetelmiä on kuitenkin hyvin vähän käytössä tällä hetkellä.

Toimivana esimerkkinä sähköisestä tunnistamisesta voidaan mainita Osuuspankin käyttämä HST-korttia hyödyntävä tunnistautuminen verkkopankkipalveluihin. Tällä hetkellä henkilön tunnistamiseksi monet verkkokaupat vaativat asiakkaalta kuitenkin perinteisten käyttäjätunnuksen ja salasanan lisäksi vaihtelevan määrän henkilökohtaisia rekisteröintitietoja, kuten osoitteen, puhelinnumeron ja sähköpostiosoitteen. Järvelän ja Tinnilän (2000, 89) mukaan näin kerätyt tiedot eivät kuitenkaan ole luotettavia vaan jopa joka kolmas Internet-käyttäjistä on antanut vääriä tietoja itsestään rekisteröintilomakkeisiin. Tästä voidaankin päätellä, että verkkokaupassa on kysyntää

salanimellä tapahtuvalle sekä nimettömänä ja tunnistamattomana eli anonyyminä asioimiselle.

Elektronisen kaupankäynnin ja sähköisten palvelujen tarjontaa on jo pitkään rajoittanut käyttäjien ehdottoman luotettavan sähköisen tunnistamisen puuttuminen sekä olemassa olevien luotettaviksi laskettavien menetelmien hankaluus. Nykyisin laajemmassa käytössä olevia luotettaviksi laskettavia menetelmiä ovat lähes ainoastaan edellä mainitun kaltaiset kertakäyttösalasanoihin perustuvat tunnistusmenetelmät, joita esimerkiksi pankit käyttävät sähköisissä palveluissaan. Tällaiset menetelmät ovat kuitenkin hankalia sekä käyttäjän että palvelun tarjoajan kannalta. Henkilö joutuu pitämään kertakäyttöavainten listaa mukanaan ja lisäksi muistamaan vielä käyttäjätunnuksensa ja henkilökohtaisen salasanansa.

Luotettavan sähköisen tunnistamisen saavuttamiseksi tarvitaan usein jonkun kolmannen, luotetun osapuolen varmentamaa tunnusta, kuten väestörekisterikeskuksen myöntämä HST-kortti tai esimerkiksi puhelinnumero (Laine 2001, 42). Joitain toimikortteihin perustuvia tunnistusratkaisuja on myös jo sovellettu käytäntöön, kuten HST-kortin käyttömahdollisuus kirjauduttaessa verkkopankki-palveluihin. Toimikortteihin perustuva tunnistus on vielä melko vähän sovellettu, mutta tulee olemaan merkittävä menetelmä lähitulevaisuudessa.

Kuten kappaleen alussa mainittiin, henkilön sähköinen tunnistaminen perustuu periaatteessa kolmeen tekijään tai niiden yhdistelmiin, joita ovat: jotain mitä tiedät (esim. tunnussanat), jotain mitä omistat (esim. toimikortti) tai jotain mitä olet (esim. biometriset ominaisuudet) (Rankl ja Effing 1997, 237). Kahden ensimmäisen heikkoutena on, että henkilö joutuu muistamaan jotain tai kantamaan jotain mukanaan, kolmas on puolestaan varsin monimutkainen ja muihin verrattuna kallis menetelmä. Tässä tutkielmassa keskitytään lähinnä käyttäjän omistamiin tunnistusobjekteihin (engl. token) ja vielä tarkemmin toimikortteja hyödyntävään käyttäjän tunnistukseen, sillä se on tällä hetkellä lupaavin tekniikka luotettavaan henkilön sähköiseen tunnistamiseen. Siinä myös yhdistyy kaksi tekijää, sillä toimikorttien yhteydessä käytetään yleensä henkilökohtaista tunnusta (esim. PIN-koodi).

Biometristen menetelmien tulo käytännön sovelluksiin näyttää ilmeiseltä ja niiden odotetaan syrjäyttävän muut tekniikat, mutta lähitulevaisuudessa niiden kaikkia käytännön ongelmia saadaan tuskin selvitettyä ja siksi toimikortit ovatkin seuraava askel ennen biometristen menetelmien tuloa. Toistaiseksi vähäisessä käytössä on myös toimikorttien ja biometrisen tunnistusmenetelmien yhdistelmiä, joissa kortille tunnistaudutaan PIN-koodin sijasta esimerkiksi sormenjäljellä. Tällaiset menetelmät saattavat myös saavuttaa suuren suosion tulevaisuudessa turvallisuutensa ja helppokäyttöisyytensä vuoksi.

Seuraavassa taulukossa on Lainetta (2001, 204) mukaillen määritelmät turvallisen tunnistamisen välineeltä vaadituille ominaisuuksille, sekä esimerkki siitä, miten omakätinen ja digitaalinen allekirjoitus täyttävät nämä vaatimukset. Ei-sähköisessä maailmassahan omakätinen allekirjoitus on yleisin henkilön tunnistamisen menetelmä, joka täyttää tietoturvan vaatimukset riittävissä määrin. Taulukon ominaisuuksista neljä ensimmäistä ovat toiminnallisia ominaisuuksia ja neljä seuraavaa näitä tukevia lisäominaisuuksia.

TAULUKKO 3. Turvallisen tunnistusvälineen ominaisuudet ja määritelmät Lainetta (2001, 204) mukaillen.

Ominaisuus	**Määritelmä**	**Täyttää vaatimuksen**	
		Omakätinen allekirjoitus	**Digitaalinen allekirjoitus**
Tiedon alkuperän tunnistaminen	Allekirjoitus liittyy yksiselitteisesti sen allekirjoittajaan	Kyllä	Kyllä
Kiistämättömyys	Henkilön sitoutuminen siihen transaktioon, johon hän osallistuu	Kyllä	Kyllä
Eheys	Tiedon mahdollinen myöhempi muuttaminen voidaan havaita	Kyllä	Kyllä
Allekirjoittajan identifiointi	Allekirjoittajan henkilöllisyys voidaan varmistaa	Kyllä	Kyllä
Linkki sisältöön	Linkki oikeustoimen sisältöön	Kyllä	Kyllä
Helppo todentaa	Tunnistusvälineen oikeellisuus on helposti todennettavissa.	Kyllä (suljetussa ympäristössä); ei (avoimessa ympäristössä)	Kyllä
Vaikea väärentää	Tunnistusväline on hankala kopioida tai muuttaa.	Ei	Kyllä
Todennettavissa niin kauan kuin oikeustoimella on oikeudellista merkitystä	Tunnisteen on säilyttävä riittävän kauan. Esimerkiksi testamentin allekirjoituksen säilyminen kauan kuemmin kuin allekirjoittanut henkiö on elossa.	Kyllä	Kyllä, mutta siihen liittyy kustannuksia

Kaaviosta voidaan huomata, että omakätinen allekirjoitus täyttää eheysvaatimuksen. Tämä kuitenkin edellyttää, että esimerkiksi monisivuisen sopimuksen myöhemmän muuttamisen havaitsemiseksi jokainen sivu on allekirjoitettava. Omakätinen allekirjoitus ei siis selkeästi täytä kaikkia turvalliselta todentamiselta vaadittavia ominaisuuksia varsinkaan helpon väärennettävyytensä takia, mutta se on kuitenkin muodostunut vallitsevaksi ja käytännössä hyvin toimivaksi todentamisen välineeksi ei-sähköisessä maailmassa. Paperidokumenttien korvautuessa yhä nopeammin sähköisillä dokumenteilla kasvaa, myös vaatimus sähköisille tunnistusmuodoille, sillä sähköisiin dokumentteihin ei voida liittää omakätisiä allekirjoituksia. Omakätinen allekirjoitus voidaankin korvata sähköisellä, mikäli sen ominaisuudet täyttävät vähintään yllä olevassa taulukossa määritellyt, samantasoiset toiminnalliset vaatimukset kuin omakätinen allekirjoitus (Laine 2001, 205). Kaaviosta voidaan todeta, että digitaalinen allekirjoitus täyttää turvalliselta tunnistusvälineeltä vaaditut ominaisuudet paremmin

kuin omakätinen ja pystyy siksi todennäköisesti saavuttamaan myös omakätisten allekirjoitusten aseman yleisesti hyväksyttynä tunnistusmenetelmänä.

Henkilön sähköisen tunnistamisen käytännön ongelmana on kuitenkin Laineen (2001, 43) mukaan yhteensopivuus muiden kotimaisten ja ulkomaisten varmenteiden kanssa. Ongelmana hänen mukaansa on myös se, etteivät ehdotetut PKI-järjestelmät tunnista vaihtoehtona esimerkiksi anonyymiä luotettavaa osapuolta, sillä hänen mukaansa aina ei ole tarkoituksenmukaista tunnistaa toista osapuolta. Tällä hetkellä henkilön sähköinen tunnistus varmentajajärjestelmissä perustuu sertifikaatteihin ja luotettuun kolmanteen osapuoleen, joka ainakin toistaiseksi tarkoittaa henkilön identiteetin ehdotonta tunnistamista. PGP:ssä tunnistus perustuu niin ikään sertifikaatteihin, mutta kuten jo aiemmin mainittiin, on PGP-sertifikaatissa henkilön tunnisteena sähköpostiosoite, jolloin henkilön identiteettiä ei voida sähköisesti varmistaa.

Elektronisen liiketoiminnan vaatimuksissa henkilön sähköiselle tunnistamiselle todettiin, että riittävän turvallisuuden saavuttamiseksi vaaditaan vähintään kahden tunnistamisominaisuuden (tieto, omistus, ominaisuus) yhdistämistä. Kryptografisesti suojattu ja murtovarma toimikortti on erinomainen tunnistusväline, sillä siinä voidaan yhdistää kaksi näistä ominaisuuksista. Nämä ovat jotain mitä tiedät (PIN-koodi) tai jotain mitä olet (sormenjälki) ja jotain mitä omistat (toimikortti). Lisäksi toimikortille voi olla tallennettuna henkilön tunnistamiseen liittyvää lisätietoa, kuten henkilötunnus, asiakastunnus, kryptografiset avainparit tai henkilön biometrisiä tietoja. Biometristen tunnistuksen yhdistämisellä voidaan periaatteessa yhdistää kaikki kolme tunnistusominaisuutta, mutta näin saavutetulle erittäin korkealle tietoturvalle ei käytännön elämässä ole ainakaan toistaiseksi tarvetta. Toimikorteilla tapahtuvaa henkilön sähköistä tunnistamista voidaan siis pitää riittävän turvallisena elektronisen liiketoiminnan vaatimuksille.

Toimikortit on useimmiten toteutettu siten, että kortilla olevien tietojen käyttö vaatii PIN-koodin, jolla käyttäjä autentikoituu kortille. Tämä vaikeuttaa kortin väärinkäyttöä huomattavasti verrattuna magneettiraitakorttiin, jota periaatteessa kuka tahansa voi käyttää pienten summien maksamiseen, mikä ei useinkaan vaadi henkilöllisyyden todistamista. Verkossa tapahtuvassa luottokortilla maksamisessa ei korttia käyttävää

henkilöä voida usein lainkaan luotettavasti identifioida. Toimikortti siis täyttää henkilön sähköisen tunnistamisen vaatimuksen toisin kuin luottokortti tai muu magneettiraitakortti.

3.11 Sähköinen identiteetti

Jotta käyttäjä voidaan tunnistaa sähköisesti, täytyy hänellä olla sähköinen identiteetti. Sähköinen identiteetti voi olla esimerkiksi käyttäjän yksikäsitteinen nimi tietojärjestelmässä tai avainpari julkisen avaimen infrastruktuurissa. Käytännön esimerkkinä Suomessa on väestörekisterikeskuksen myöntämä HST-kortti, joka toimii sekä sähköisenä tunnistuskorttina että tavallisena henkilökorttina. HST-kortissa sähköisenä identiteettinä toimii henkilölle luotu yksikäsitteinen, sähköinen asiointitunnus.

Sähköisessä kaupassa osapuolten identiteetin eli henkilöllisyyden tunnistaminen on oikeustoimen pätevyyden ja sähköisten palveluiden asiointiturvallisuuteen liittyvä perusedellytys. Sähköisessä maksamisessa pieniin transaktioihin liittyvän vähäisen riskin vuoksi osapuolten identiteetin varmistaminen ei kuitenkaan välttämättä ole aina tärkeää. Tällöin riittää, että maksun suorittamisesta saadaan varmuus. Maksun suorittamiseen maksajan ja maksujärjestelmän välisessä suhteessa liittyy kuitenkin aina jonkin tasoinen identiteettikontrolli. Sähköinen maksaminen on tämän takia vain harvoin anonyymiä (Laine 2001, 293). Tähän on yksinkertaisesti syynä se, että sähköisen sopimuksen osapuolten maksukyvyn varmistaminen, muun suorituskyvyn selvittäminen tai pätevän sopimuksen tekeminen on mahdotonta tai ainakin riski, jos osapuolen identiteettiä ei tunneta (Laine 2001, 294). Luotettujen kolmansien osapuolten avulla PKI:ssä anonyymi asiointi on kuitenkin periaatteessa mahdollista toteuttaa.

Elektronisen liiketoiminnan tietoturvavaatimusten täyttämiseksi vaaditaan siis myös luotettuja kolmansia osapuolia. Niitä tarvitaan henkilöiden tunnistamisen lisäksi etenkin avainten hallinnan, avainten vaihdon ja sertifikaattien hallinnan toteuttamiseen, jotka ovat keskeisiä toimintoja PKI:ssä. Luotetun kolmannen osapuolen tärkein tehtävä on

kuitenkin varmistaa kaupankäynnin osapuolille, että juuri he ovat keskenään vuorovaikutuksessa (Ojala 1998, 52).

Sähköisessä tunnistamisessa yleisesti käytettyjen käyttäjätunnuksen ja salasanan yhdistelmä ei ole juridisesti pätevä ratkaisu sähköisen identiteetin todentamiseen eli esimerkiksi tapahtuman kiistämättömyyttä ei voida varmistaa. Myöskään nykyisten vaatimusten mukaista sähköistä identiteettiä ei tällä tavoin saavuteta. Henkilön sähköinen identiteetti on välttämätön tietoturvan kannalta, koska sillä on suora yhteys lähes kaikkiin tietoturvan perustekijöihin. Niiden lisäksi myös moniin muihin verkossa tapahtuviin toimenpiteisiin siis vaaditaan nykyisin sähköisen identiteetin liittäminen. Käytännöllisimmille ja turvallisimmille tunnistusmenetelmille sekä menetelmille sähköisen identiteetin muodostamiseksi on siis olemassa selkeä tarve.

3.12 Tunnistuksen problematiikka

Aiemmissa luvuissa on käynyt jo ilmi, että tunnistus sähköisessä maailmassa on varsin ongelmallista. Ei pelkästään sen vuoksi, että henkilön luotettava tunnistus on hankalasti toteutettavissa vaan myös siksi, että esimerkiksi sähköisessä kaupassa olisi tarve varmistaa henkilön olemassaolo ja "kelvollisuus" paljastamatta kuitenkaan hänen oikeaa identiteettiään. Aiemmin käsiteltyjen tietosuojan ja henkilön sähköisen tunnistamisen käsitteisiin liittyykin läheisesti myös anonymiteetti. On nimittäin olemassa palveluita joiden käyttäjät eivät halua, että heidät tunnistetaan. Ja kuten Ojalakin (1998, 54) toteaa, kuuluu kaupankäynnin luonteeseen perinteisesti tietty anonymiteetti ja jäljittämättömyys. Sähköisessä asioinnissa tästä voi olla esimerkkinä verkossa olevat lääkäripalvelut, joiden käyttäjät voivat pelätä sairauksiaan koskevien henkilökohtaisten tietojensa pääsyä ulkopuolisten käsiin. Tällaiset palvelut voivat kuitenkin vaatia henkilön vahvaa tunnistamista esimerkiksi palvelun rajoitettujen käyttöoikeuksien tai mahdollisten väärinkäytösten vuoksi. Näin arkaluontoiset tiedot voi olla mahdollista yhdistää tiettyyn henkilöön. On siis selvästi tarvetta menetelmälle, jossa käyttäjä voidaan tunnistaa anonyyminä.

Ojala (1998, 54) on todennut, että kokonaan anonyymisti tapahtuva asiointi on mahdollista vain, jos käyttäjää ei tunnisteta ollenkaan tai jos jätetään tunnistaminen luotettavan kolmannen osapuolen tehtäväksi. Halevi ja Krawczyk (1998, 126, 127) ovat kuitenkin artikkelissaan kuvanneet protokollan, jota käyttämällä PKI:ssä voidaan mahdollistaa elektronisen liiketoiminnan vaatimusten mukainen anonymiteetti sähköisessä asioinnissa. Artikkelin teknisyys kuitenkin ylittää tämän tutkielman asioiden käsittelyn tason, eikä sitä ole siksi tarkemmin selvitetty.

PKI-järjestelmissä anonyymi asiointi on siis helposti saavutettavissa ainoastaan luotetun kolmannen osapuolen avulla. Tämä voidaan toteuttaa niin, että käyttäjälle annettaan niin sanottu pseudo-identiteetti, jonka perusteella ainoastaan luotettava kolmas osapuoli pystyy yhdistämään käyttäjän oikean identiteetin ja pseudo-identiteetin (Ojala 1998, 55). Tällöin käyttäjän on mahdollista pseudo-identiteettinsä suojaamana esimerkiksi ostaa tuotteita verkkokaupasta niin, että kauppias ei voi selvittää käyttäjän oikeaa identiteettiä. Kauppias saa kuitenkin vakuuden käyttäjän olemassaolosta ja mahdollisesti myös maksukyvystä TTP:ltä, joka myös vakuuttaa käyttäjälle, että hän todella asioi oikean kauppiaan kanssa. Viranomaisten hallinnoimissa varmentaja-järjestelmissä edellä mainittu on tuskin mahdollista, sillä niissä yleisenä periaatteena on nimenomaan se, että sähköisessä asioinnissa henkilö voidaan aukottomasti tunnistaa. Tämän johdosta onkin todennäköistä, että sähköistä kaupankäyntiä varten kehittyy tulevaisuudessa omat varmentaja-järjestelmät, joissa anonyymi asiointi on mahdollista.

Anonymiteettiin liittyy eräs merkittävä oikeudellinen ongelma. Sähköiset maksutavat eivät nimittäin mm. rahanpesua koskevien säännösten takia voi olla täysin anonyymejä samalla tavalla kuin on maksaminen laillisilla maksuvälineillä (esim. käteinen raha) (Laine 2001, 324). Myös tämän vuoksi luotettujen kolmansien osapuolten käyttö anonyymin asioinnin mahdollistamiseksi on välttämätöntä. Esimerkiksi huijaustapauksissa TTP:ltä voidaan saada viranomaisten vaatimuksesta tiedot henkilön pseudo-identiteetin ja oikean identiteetin yhdistämiseksi ja selvittää näin tapaus. Viranomaisilla täytyy siis olla oikeus päästä käsiksi kaupallisten varmentaja-järjestelmien tietoihin väärinkäytösten estämiseksi, eli viranomaisten on voitava toteuttaa avainten palautus (key escrow).

Anonyymi asiointi on mahdollista saavuttaa myös toimikorteilla samaan tapaan kuin PKI:ssä. Korttia käyttäen henkilö voidaan tunnistaa siten, että todennetaan henkilön identiteetti, mutta ei paljasteta sitä kauppiaalle, jolloin henkilön anonymiteetti säilyy. Henkilö voi asioida myös pseudonyyminä, jolloin kauppias saa tietoonsa henkilön valitseman käyttäjänimen, jonka ei tarvitse liittyä mitenkään henkilön omaan identiteettiin. Muun muassa HST-kortti mahdollistaa sekä anonyymin, että pseudonyymin asioinnin elektronisissa palveluissa. Näin toteutettu anonyymi asiointi tosin vaatii myös TTP:n läsnäolon samoista syistä kuin PKI:ssäkin.

Anonyymi asiointi on saavutettavissa helpoiten toimikorttien off-line käytöllä. Tällöin kortille on ladattu elektronista rahaa, joka siirtyy maksutapahtuman yhteydessä kauppiaalle ilman että henkilön identiteettiä tarvitsee tarkistaa. Tällaisessa menettelyssä luottamus perustuu ainoastaan siihen, että toimikortilla olevia tietoja ei voida muuttaa. Siksi tätä menettelyä käytetäänkin vain pieniä rahasummia vaativien ostosten tekoon. Samalla tavoin voitaisiin menetellä myös Internetin online käytössä, jossa luotettavuutta voitaisiin lisätä esimerkiksi kortin sulkutietojen online tarkistuksilla. On kuitenkin arveltu, että PKI:n ja toimikorttien käyttö pienten maksujen yhteydessä saattaa muodostua liian raskaaksi ja kalliiksi menettelyksi saavutettuun hyötyyn nähden. Kuten aiemmin todettiin, pienten maksujen yhteydessähän henkilöiden tunnistus ei ole välttämättä edes tarpeellista.

Käyttäjän tunnistamiseksi on siis olemassa periaatteessa kolme tasoa. Nämä ovat anonyymi, pseudonyymi ja vahvasti tunnistettu käyttäjä. Käyttäjän tunnistamiseen vaadittava ja toisaalta hyväksyttävä taso riippu monesta tekijästä, kuten elektronisen liiketoiminnan asettamista vaatimuksista tietoturvalle ja toisaalta tunnistusta rajoittavasta lainsäädännöstä. Henkilön tunnistuksen taso onkin aina harkittava tapauskohtaisesti ja mietittävä mitä mahdollisia hyötyjä ja haittoja tietyn tasoisesta tunnistamisesta seuraa. Seuraavassa luvussa henkilön sähköisen tunnistuksen merkitystä on käsitelty kaupankäyntiprosessin kannalta.

4 PKI-JÄRJESTELMÄT

Tässä luvussa käsitellään PKI-järjestelmiä, sekä niihin liittyviä ongelmia. PKI on nimensä mukaisesti infrastruktuuri ja sitä voidaan verrata vaikka tieverkostoon. Sellaisenaan siitä ei ole paljon hyötyä vaan sen tarjoamia sertifikaatteja ja palveluja täytyy myös tehokkaasti hyödyntää sovelluksissa ja tietojärjestelmissä. PKI:n soveltamista kaupankäyntiprosessin osaprosesseihin käsitellään myöhemmissä luvuissa.

Kohlas ja Maurer (2000, 94) ovat määritelleet ytimekkäästi PKI:n tarkoittavan koko laillista, teknistä ja organisatorista viitekehystä, joka muodostuu johtopäätöksien tekemiseen annetusta joukosta sertifikaatteja, luottamussuhteita ja muita todisteiden osia. PKI voidaan myös määritellä tarkoittavan joukkoa laitteita, ohjelmia, ihmisiä, käytäntöjä ja proseduureja, joita tarvitaan luomaan, hallinnoimaan, säilyttämään, jakelemaan ja lakkauttamaan julkisen avaimen kryptografiaan perustuvia julkisen avaimen sertifikaatteja. PKI-järjestelmät perustuvat julkisen avaimen kryptografiaan (LIITE 1), joka tarjoaa perustan useille tietoturvan osa-alueille, kuten kiistämättömyys, tiedon eheys ja autentikointi. Se on myös tärkeä osa Internetissä turvalliseen tiedonsiirtoon käytetyssä SSL (Secure Socket Layer) protokollassa (Jøsang 2000, 1).

Globaaleista PKI-järjestelmistä on tullut perusedellytys nykyvaatimukset täyttävän tietoturvan saavuttamiseksi laajoissa tietoverkoissa ja elektronisessa liiketoiminnassa. Kuten Maurer (1996, 1) toteaa: PKI:n toiminnan perusmekanismit ovat jo hyvin ymmärrettyjä, kun taas laajojen hajautettujen PKI-järjestelmien toteuttaminen ei ole. Vaikka Maurerin toteamuksesta on jo kulunut aikaa, vieläkään ei ole mitään yleisesti käytössä olevaa menetelmää laajan PKI-järjestelmän rakentamiseksi. Tähän on vieläkin eräänä syynä standardoinnin puutteellisuus.

Digitaalisista allekirjoituksista ja informaation suojaamisen tekniikoista on tullut uusi vaihtoehto myös yritysten etsiessä kilpailuetua. Kilpailuetuun pyrkiessä ja tämän päivän tietoturvan vaatimusten täyttämisessä on PKI-järjestelmistä tullut muita suositumpia. PKI-ratkaisut ovat tosin olleet viime vuosiin saakka vielä teorian tasolla johtuen osittain

kesken olevasta standardoinnista ja siitä, että tuotteita ei ole ollut vielä saatavilla. (Kerttula 1999, 355)

PKI-järjestelmien tilasta ja kypsyysasteesta kertoo jotain se, että tällä hetkellä kehittymässä on useita PKI malleja, kuten X.509, PKCS (Public Key Cryptography Standards), PGP (Pretty Good Privacy), SPKI (Simple Public Key Infrastructure) ja SDSI (Simple Distributed Security Infrastructure). SDSI-mallia on kuvannut esimerkiksi (Branchaud, 1997, 67 – 77). Ei ole kuitenkaan olemassa mitään yhtä standardia PKI-järjestelmien rakentamista varten, joka mahdollistaisi eri mallien yhteensopivuuden keskenään. Edes X.509 standardia noudattavat PKI-järjestelmät eivät ole yhteensopivia keskenään (He ym. 1998, 377). He ym. (1998) esittävät artikkelissaan oman ratkaisunsa yhteensopivuusongelmiin. Heidän ratkaisunsa perustuu eräänlaisten turva-agenttien (Security Agent) käyttöön raskaiden hierarkkisten mallien sijasta, jotka osaavat hyödyntää erilaisia sertifikaatteja ja autentikointimenetelmiä. Tämä ratkaisu on kuitenkin vielä keskeneräinen ja jättää vielä monia ongelmia avoimiksi, eikä sitä ole siksi tarkemmin käsitelty.

Jøsangin (2000, 2-3) mukaan PKI-järjestelmät voidaan jakaa kahteen eri tyyppiin, joita ovat Web-PKI ja "hallinnoitu-PKI". Web-PKI toimii nimensä mukaisesti Internetissä ja perustuu siihen, että kaikki tunnettujen varmentajien juuri-sertifikaatit toimitetaan käyttäjille selaimen mukana itse allekirjoitettuina X.509 sertifikaatteina. Hallitussa PKI:ssä ei juuri-sertifikaatteja sen sijaan toimiteta selainten mukana, vaan sertifikaattien hallinta perustuu PKI:tä hallinnoivan organisaation omiin menetelmiin. Yleisin tapa on, että käyttäjät hakevat sertifikaatit organisaation ylläpitämältä sertifikaattipalvelimelta. Tässä PKI-tyypissä organisaatio voi hallita koko luottamusketjua ja voi siksi olla erittäin turvallinen. Tällainen PKI ei tosin voi helposti saavuttaa globaalia kattavuutta toisin kuin Web-PKI.

Tässä tutkielmassa PKI-järjestelmistä lähempään tarkasteluun on valittu rakenteeltaan hierarkkiset varmentajajärjestelmät, kuten hallinnoitu-PKI ja verkkomaisesti rakentunut PGP (Pretty Good Privacy). Varmentajajärjestelmällä tarkoitetaan PKI-rakennetta, jossa ylimpänä varmennehierarkiassa on jokin varmenneviranomainen. PGP on puolestaan ohjelmisto, jonka avulla käyttäjät voivat itse luoda varmennerakenteen. Nämä kaksi on

valittu, koska ne ovat selvästi käytetyimpiä ja tutkituimpia tällä hetkellä käytössä olevista PKI-järjestelmistä. Lisäksi ne ovat lupaavimpia laajemman yleistymisen kannalta ja poikkeavat selvästi toisistaan niin rakenteellisesti kuin luottamusmalliensakin puolesta ja ovat siksi käsittelyn kohteena. Luvussa käsitellään myös luottamusta PKI-järjestelmissä sekä sertifikaatteja. Luvun lopussa käsitellään PKI-järjestelmien turvallisuuskysymyksiä sekä ongelma-alueita.

PKI-järjestelmän tärkeimmän ominaisuuden sanotaan olevan sen transparenttisuus eli läpinäkyvyys mikä merkitsee, että käyttäjän ei tarvitse ymmärtää, miten PKI operoi avaimia ja sertifikaatteja salauksessa ja digitaalisessa allekirjoituksessa (Kerttula 1999, 357). PKI:n voidaan ajatella koostuvan viidestä komponentista, jotka ovat:

- Varmentaja (Certification Authority, CA), joka myöntää ja lakkauttaa sertifikaatteja.

- Rekisteröintiviranomainen (Registration Authority, RA), joka vastaa julkisen avaimen ja sertifikaatin haltijan identiteetin yhdistämisestä.

- Julkisen avaimen sertifikaatin haltija, joka voi allekirjoittaa tai salata digitaalisia dokumentteja.

- Asiakkaat (Client), jotka vahvistavat digitaalisia allekirjoituksia ja sertifikaattipolkuja luotetun varmentajan julkisesta avaimesta.

- Tietovarastot, jotka varastoivat ja asettavat saataville julkisen avaimen sertifikaatteja ja sertifikaattien sulkulistoja.

Nämä tosin pätevät lähinnä X.509-pohjaisiin varmentajajärjestelmiin eikä esimerkiksi PGP:ssä voi eritellä kaikkia edellä mainittuja komponentteja. Branchaudin (1997, 11) mukaan kaikille PKI-järjestelmille voidaan kuitenkin löytää kaksi yhteistä toimintoa, joiden soveltaminen on PKI-järjestelmien määräävin perusominaisuus. Näistä ensimmäinen on sertifiointi, joka tarkoittaa prosessia, jossa julkisen avaimen arvo sidotaan henkilöön, tietoon tai johonkin muuhun kohteeseen. Toinen toiminto on

vahvistus, jossa varmistetaan, että sertifikaatti on edelleen pätevä. Edelleen Branchaudia (1997, 13) mukaillen PKI-järjestelmistä voidaan erottaa kolme pääpiirrettä:

1. Sertifikaatin sisältämä tieto,
2. varmentajan, sertifikaatin käyttäjän ja sertifikaatin kohteen välinen suhde
3. kolmen edellä mainitun osapuolen väliset luottamussuhteet.

PKI-järjestelmän käyttäjän täytyy olla ehdottoman varma, että luottaessaan julkiseen avaimeen toisen osapuolen kanssa kommunikoidessa, tämä toinen osapuoli omistaa varmasti vastaavan salaisen avaimen. Tämä luottamus saavutetaan käyttämällä julkisen avaimen sertifikaatteja, joita käsitellään seuraavassa luvussa.

Mikäli edellä mainittu luottamus täyttyy, voidaan olettaa, että turvallinen kommunikointi onnistuu turvattoman tietoverkon ylitse ilman, että osapuolten tarvitsisi tavata avaimia vaihtaakseen. Mikäli luottamusta ei voida saavuttaa, järjestelmä voidaan murtaa murtamatta itse salausta. (Menezes 1999, 27)

4.1 Sertifikaatit

Tässä kappaleessa käsitellään PKI-järjestelmien sertifikaatteja, niiden toimintaa ja rakennetta sekä sertifikaattien vahvistamiseen ja lakkauttamiseen liittyviä asioita. Tässä tutkielmassa sertifikaateilla tarkoitetaan nimenomaan digitaalisia julkisen avaimen sertifikaatteja. Asiayhteydestä riippuen sertifikaatti-termiä käytettäessä voidaan tarkoittaa henkilöön tai johonkin muuhun kohteeseen sidottuja identiteetti-sertifikaatteja tai tietoon tai valtuuteen sidottuja attribuutti-sertifikaatteja.

Sertifikaattien eniten käytetyin sovellus on suojattujen Internet-yhteyksin luonti SSL-protokollaa hyödyntämällä. SSL mahdollistaa luotettavan yhteyden kahden Internetissä olevan koneen välille. Yleensä SSL:ssä autentikoidaan palvelin, mutta myös asiakkaan (client) autentikointi on mahdollista. Muita suosittuja käyttökohteita ovat sähköpostin

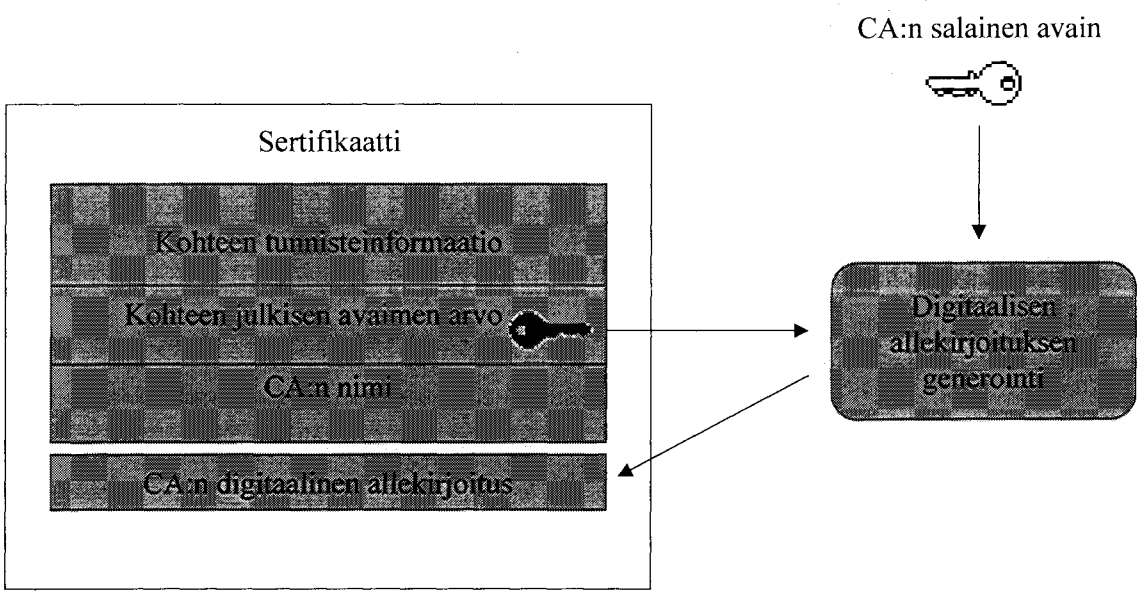
salaus ja digitaalinen allekirjoittaminen sekä ohjelmistokomponenttien digitaalinen allekirjoittaminen. (Jøsang 2000, 3)

Julkisen avaimen järjestelmissä on Maurerin (1996, 4) mukaan seuraavanlainen perusongelma: kohteen tai henkilön X julkinen avain on täysin hyödytön kohteelle Y, mikäli Y ei voi vakuuttua siitä, että julkinen avain on juuri X:n luoma ja vain hänellä on vastaava salainen avain. Julkisen avaimen järjestelmien haasteena on siis tarjota mekanismi sille, kuinka henkilö voi saada toisen henkilön julkisen avaimen ja luottaa siihen, että henkilö ja avain ovat autenttisia ja sidottuja toisiinsa. Tämä voidaan tietysti saavuttaa vaihtamalla avaimia henkilökohtaisesti, mutta käytännöllisempi ratkaisu olisivat digitaaliset julkisen avaimen sertifikaatit, jolloin sertifikaatti vahvistaa julkisen avaimen liittymisen tiettyyn henkilöön.

Sertifikaatit eivät kuitenkaan sinällään paranna minkään järjestelmän turvallisuutta, vaan vaaditaan myöhemmin käsiteltävä luotettava kolmas osapuoli sertifikaatin luomiseksi ja sen luotettavuuden varmistamiseksi. Luottamuksen synnyttämiseksi tällä tavalla vaaditaan myös digitaalisten allekirjoitusten käyttöä. Edelleen vaatimuksena on, että järjestelmää käyttävät henkilöt luottavat siihen, että luotettu kolmas osapuoli on todella luotettava ja oikeutettu myöntämään sertifikaatteja. (Barton ym. 1997, 1,2)

PKI:ssä sertifikaatin voidaan yksinkertaisimmillaan ajatella olevan vain julkisen avaimen arvo, mutta perinteisemmin sertifikaatti kuitenkin käsitetään kokoelmaksi tietoa, jonka sertifikaatin myöntäjä on digitaalisesti allekirjoittanut (Branchaud 1997, 12). Sertifikaatit voidaan jakaa kolmeen luokkaan sisältämiensä tietojen perusteella. Nämä ovat identiteetti-sertifikaatti, attribuutti-sertifikaatti ja tunniste- (credential) sertifikaatti.

KUVA 2. Julkisen avaimen sertifikaatti



Kuten kuvasta kaksi ilmenee, sertifikaatti sisältää yksinkertaisimmillaan kohteen tunnisteinformaation ja julkisen avaimen arvon, jotka on digitaalisesti allekirjoitettu. Varmentaja-järjestelmissä käytettävissä sertifikaateissa on myös sertifikaatin myöntäneen varmentajan tunnistetiedot ja tämän digitaalinen allekirjoitus. Kohteen tunnisteinformaationa on yleensä kohteen nimen lisäksi muitakin attribuutteja kuten osoite, sertifikaatin myöntämis- ja voimassaoloajat, avaimen käyttötarkoitus, sertifikaatin sarjanumero ja sertifikaattien sulkulistan osoite. Uusimmassa sertifikaatti-standardin muodossa (X.509v3) voidaan sertifikaattiin lisätä kenttiä vapaasti.

Sertifikaatteja käytetään pääasiassa allekirjoitetun datan vahvistamiseen. Kyseinen prosessi sisältää X.509 PKI:ssä seuraavat toimenpiteet:

- Allekirjoitetun datan vastaanottaja varmistaa, että lähettäjän väittämä henkilöllisyys vastaa sertifikaatissa olevaa henkilöllisyyttä.

- Vastaanottaja varmistaa, että yksikään sertifikaatti sertifikaattipolussa ei ole lakkautettu. Tämä voidaan tehdä hakemalla sulkulistapalvelusta sen hetkinen sulkulista tai suorittamalla kysely johonkin sertifikaattien tilan online palveluun.

Tässä vaiheesa varmistetaan myös sertifikaatin voimassaolo sertifikaatin kentistä.

- Vastaanottaja varmistaa, että tiedoissa ei väitetä olevan mitään arvoja, mihin allekirjoittajalla ei ole sertifikaatin mukaan lupaa.

- Vastaanottaja varmistaa, että tietoja ei ole muutettu allekirjoituksen jälkeen käyttämällä sertifikaatin julkista avainta.

- Jos kaikki varmistukset menevät läpi, käyttäjä voi hyväksyä, että tieto oli muuttumatonta ja väitetyn henkilön allekirjoittamaa.

Edellä kuvatulla toimenpiteellä voidaan esimerkiksi autentikoida palvelin, jolle on myönnetty digitaalinen sertifikaatti. Tämä on yleinen käytäntöä muodostettaessa suojattuja SSL-yhteyksiä web-palvelimille. Näin suoritetaan kuitenkin vain yksisuuntainen autentikointi ja mikäli halutaan suorittaa kaksisuuntainen autentikointi (mutual authentication) täytyy myös asiakkaalla olla sertifikaatti. Näin molemmat osapuolet voivat autentikoida luotettavasti toisensa käyttäen sertifikaatteja.

4.1.1 Sertifikaattien ja salaisen avaimen säilytys

Sertifikaattien säilytyksestä puhuttaessa on muistettava, että käytännössä tarkoitetaan salaisen avaimen säilytystä, joka voi fyysisesti sijaita eri paikassa kuin sertifikaatti. Sertifikaattien henkilökohtaiseen säilytykseen on periaatteessa kaksi mahdollisuutta: päätelaite ja mukana kuljetettava kryptografisesti suojattu erillinen lisälaite, kuten toimikortti. Julkisen avaimen sertifikaatteja säilytetään myös keskitetyissä tietokannoissa ja hakemistoissa. Päätelaitteella säilytettäviä sertifikaatteja kutsutaan usein ohjelmistovarmenteiksi. Mikäli sertifikaatti ja salainen avain on samassa tiedostossa, käytetään nimitystä ”software token”. Toimikorteista käytetään puolestaan nimitystä varmennelaite (hardware token). Sertifikaateille ja varsinkin salaisille avaimille paras säilytyspaikka on jokin mukana kuljetettava kryptografisesti suojattu ”laite”, kuten toimikortti, joka takaa tehokkaan suojan murtautumisyrityksiä vastaan

(tamper resistant) ja mahdollistaa sertifikaattien joustavan käytön. Ohjelmistovarmenteita käytettäessä varmenne täytyy asentaa erikseen jokaiselle koneelle, jossa sitä halutaan käyttää, eikä se siksi ole kovin käyttäjäystävällinen tapa.

Sertifikaattien säilytyksessä ovat yleistyneet LDAP (Light Weight Directory Acces Protocol) hakemistot, joka onkin yleisyytensä ja standardiasemansa takia paras tapa julkisen avaimen sertifikaattien säilytykseen ja jakeluun. LDAP hakemistot pystyvät myös käsittelemään suuria hakumääriä ja hakujen vasteajat ovat hyvin lyhyet (Kerttula 1999, 368).

4.1.2 Sertifikaattien validointi

Sertifikaatteja hyödyntävässä autentikoinnissa, henkilön sähköisessä tunnistamisessa ja tiedon eheyden varmistamisessa on olennaista varmistaa, että käytetty sertifikaatti on pätevä. Sertifikaatin validoinnilla tarkoitetaan sertifikaatin pätevyyden ja voimassaolon tarkistamista.

Validoinnin tekee sertifikaattia käyttävä sovellus, joka yleensä ensimmäisenä tarkistaa sertifikaattiin merkityn voimassaolopäivän ja toteaa onko sertifikaatti vanhentunut. Tämä tapahtuu samalla tavalla sekä online- että off-line-yhteydessä, jolloin tarkastetaan ainoastaan sertifikaatin voimassaolokenttä. Seuraavaksi voidaan tarkistaa onko sertifikaatti voimassaolevalla sulkulistalla. Tämä tapahtuu hakemalla sulkulista sertifikaatissa olevalta sulkulistan osoitekentän viittaamalta sivulta. Sulkulistan tarkistus vaatii yleensä online-yhteyden sulkulistapalvelua tarjoavaan palvelimeen. Sulkulista voi tosin sijaita off-line käytössä myös paikallisella koneella, mutta tällöin ei saada reaaliaikaista tietoa sertifikaatin tilasta, ja näin ollen se ei sovellu korkeaa turvallisuutta vaativiin sovelluksiin.

Sulkulistoja ylläpitää yleensä varmentaja tai joku kolmas osapuoli, jonka toiminta on kuitenkin varmentajan vastuulla. Sulkulistojen tulee olla julkisesti kaikkien saatavilla ja aina ajan tasalla, jotta sertifikaattien sulkeminen toimisi tarkoituksenmukaisesti. Sulkulista on listamuotoinen tiedosto, joka sisältää yleensä suljettujen sertifikaattien

sarjanumeroita, sulkijan identiteetin tiedot, sulkemisajankohdan ja syyn sulkemiseen. Tämä lista on varmentajan digitaalisesti allekirjoittama, joten myös sen oikeellisuus ja eheys voidaan todeta. Samoja sulkulistoja voi olla useissa eri paikoissa, joten niiden täytyy replikoida keskenään ajantasaisuuden säilymiseksi. Sulkulistojen käyttö on kuitenkin vielä tänä päivänä vähäistä ja siihen liittyy useita ongelmia, kuten esimerkiksi sulkulistojen koon kasvu ajan myötä, kasvavan replikoinnin määrän kasvattama tietoliikenne ja sulkutietojen hakuaikojen hitaus. Nämä ongelmat eivät kuitenkaan ole merkityksellisiä tämän tutkielman kannalta. Niitä on käsitellyt tarkemmin esimerkiksi Cooper (1999).

4.2 Luottamus PKI-järjestelmissä

Tässä kappaleessa käsitellään luottamusta ja sen muodostamista PKI-järjestelmissä sekä luotettuja kolmansia osapuolia. Jøsangin (2000, 2) mukaan digitaaliset sertifikaatit ja PKI-järjestelmät yrittävät matkia ei-sähköisen maailman mekanismeja henkilöiden identiteetin selvittämiseen ja luottamuksen synnyttämiseen tehden siitä mekaanisen ja automaattisen prosessin. Hänen mielestään nykyiset sovellukset tosin perustuvat rajoittuneisiin luottamusmalleihin ja ovat siksi sopimattomia yleisiksi työkaluiksi luottamuksen määrittelyssä ja päätöksenteossa. Seuraavissa kappaleissa kuitenkin selvitetään ja perustellaan miten luottamus voidaan synnyttää sähköisessä maailmassa ja voidaankin todeta, että etenkin seuraavassa luvussa käsiteltävän luotetun kolmannen osapuolen tarjoamia palveluja hyödyntämällä voidaan saavuttaa teknisesti riittävä taso luottamuksen synnyttämiseksi sähköisessä kaupankäynnissä.

Luottamus kahden kohteen välillä perustuu yleensä johtopäätöksiin, joita kohde tekee toisesta kohteesta omaamien tietojensa ja kokemuksiensa perusteella. Luottamusta ei yleensä voi määritellä yksiselitteisesti esimerkiksi nollaksi tai ykköseksi eikä se ole käytännöllistäkään, sillä PKI-järjestelmissä luottamus perustuu usein suosituksiin tai muihin epäsuoriin tietoihin (Maurer 1996, 2). Tästä on esimerkkinä tapaus, jossa henkilö A ei tunne henkilö B:tä, mutta tuntee kuitenkin henkilö C:n, joka vakuuttaa henkilö B:n olevan luotettava. PKI-järjestelmissä onkin tärkeää se, miten luottamus voidaan synnyttää sellaisten kohteiden välille, jotka eivät ennalta omaa mitään tietoa

toisistaan. Maurer (1996, 2) esittää luottamukseen tarvittavien tietojen hankkimiselle PKI-järjestelmissä keinoja, joita ovat esimerkiksi tiedon hankinta virallisista sertifikaattipalveluista, Internetin sertifikaattivarastoista tai automaattinen tietojen vaihto kahden kohteen välillä. Edellä mainitut menetelmät eivät kuitenkaan usein yksin riitä vaan mukaan tarvitaan myös luotettuja kolmansia osapuolia (Trusted Third Party, TTP) ja niiden tarjoamia palveluja, joita käsitellään seuraavassa luvussa.

PKI-järjestelmien toimivuus siis perustuu aina siihen, että käyttäjät luottavat johonkin toiseen henkilöön kuten PGP:n tapauksessa tai varmentajapohjaisissa PKI-järjestelmissä johonkin kohteeseen tai instituutioon (TTP), kuten esimerkiksi pankkiin. Muun muassa Kohlasin ja Maurerin (2000, 93) mukaan luottamus on usein epävarma todiste kohteen (tässä tapauksessa julkisen avaimen) autenttisuudesta ja niinpä tämä lisää inhimillisen epävarmuustekijän kryptografisesti ajateltuna lähes täysin turvallisiin PKI-järjestelmiin.

4.2.1 Luottamusmallit

Kerttulan (1999, 371) mukaan PKI-järjestelmän yksi tärkeimmistä topologisista ominaisuuksista on sertifiointirakenteiden sopimukset eli PKI-järjestelmän luottamusmallit. Luottamusmallit jaetaan yleensä hierarkkisiin ja verkkomaisiin malleihin, joista voidaan käyttää myös nimitystä horisontaalinen malli. Hierarkkisissa malleissa, kuten top-down malli (esim. X.509), varmentajat myöntävät sertifikaatteja toisilleen systemaattisella ja ennalta sovitulla tavalla. Horisontaalisessa mallissa sertifikaatteja myönnetään sen sijaan joustavammin ja vähemmän järjestäytyneellä tavalla, kuten ristiinsertifiointia käyttävässä vapaassa verkkomaisessa mallissa (esim. PGP). Yleiskäyttöisissä PKI-malleissa sovelletaan näiden välimuotoa, joka riippuu sovellusympäristöstä ja tietoturvapolitiikasta. (Kerttula 1999, 371)

Hierarkkisissa varmentajajärjestelmissä luottamus perustuu yleensä siihen, että varmennuspalvelun tarjoaja on tunnettu ja yleisesti luotettu yritys, joten myös sen myöntämiin sertifikaatteihin voidaan luottaa. Tällaisissa tapauksissa varmentajasta käytetään nimitystä luotettu kolmas osapuoli. PGP:n tapauksessa luottamus perustuu pääasiassa siihen, että henkilö luottaa toiseen henkilöön henkilökohtaisella tasolla.

Myös PGP:ssä voi olla luotettuja kolmansia osapuolia, joita kutsutaan esittelijöiksi. Tällainen henkilö on siinä määrin luotettu, että hänen luottamiinsa henkilöihinkin voidaan luottaa tuntematta heitä itse.

PKI-järjestelmissä luottamus julkisiin avaimiin siirtyy sertifikaattien luottamusketjuja pitkin. Hierarkkisissa malleissa, kuten X.509, luottamus keskittyy ketjun ylimpään varmentajaan jota kutsutaan myös juurivarmentajaksi (root CA). Tästä luottamus siirtyy hierarkkisesti alempiin varmentajiin ja edelleen käyttäjille. Tällaisissa järjestelmissä kaikki käyttäjät omaavat juurivarmentajan julkisen avaimen, jolla voidaan varmistaa muiden ketjussa esiintyvien julkisten avainten aitous. Juurivarmentajan julkista avainta ei tarvitse varmentaa, sillä kaikkien järjestelmän osapuolten oletetaan omaavan sen. Varsinkaan laajemmissa järjestelmissä ei voida olettaa kaikkien luottavan samaan juurivarmentajaan. Tällöin voidaan käyttää useampia hierarkkisia rakenteita, joilla on oma juurivarmentaja. Nämä juurivarmentajat ristiinvarmentavat toisensa ja näin luottamus säilyy rinnakkaisissakin rakenteissa (Adams ym. 2000, 98).

PGP on yleisin verkostomaisia luottamusmalleja käyttävä PKI-järjestelmä. Tässä mallissa jokainen käyttäjä muodostaa oman luottamusverkostonsa määrittelemällä kriteerit luottamuksen syntymiselle. Kun käyttäjä saa käsiinsä jonkun toisen käyttäjän julkisen avaimen, hän voi määritellä tälle avaimelle jonkun seuraavista neljästä luottamustasosta.

- Täysin luotettu (completely trusted), jolloin kaikki avaimet, jotka on allekirjoitettu tällä avaimella, voidaan myös lisätä luotettujen avainten ketjuun.

- Osittain luotettu (marginally trusted), jolloin kaikki avaimet, jotka on allekirjoitettu tällä avaimella, täytyy olla allekirjoitettu myös toisella (tai useammalla, jos niin halutaan) osittain luotetulla avaimella.

- Ei luotettu (untrusted), jolloin tällaista avainta ei käytetä määriteltäessä, voidaanko avain lisätä avainketjuun.

- Tuntematon (unknown), jolloin avaimen luotettavuus on tuntematon, mikä tarkoittaa käytännössä samaa kuin edellinen. (Branchaud 1997, 30)

Näiden kriteerien lisäksi voidaan vielä tarkemmin määritellä luottamusta esimerkiksi siten, että avain on luotettu ainoastaan silloin kun sen on allekirjoittanut kaksi täysin luotettua tai vähintään kolme osittain luotettua avainta.

Kohlasin ja Maurerin (2000, 104) mukaan tästä seuraa kuitenkin ongelma. Kun luottamus edellä mainitulla tavalla kohdistuu avaimiin eikä henkilöihin, on mahdollista, että henkilö A voikin saada henkilö B:n luottamaan virheellisesti henkilöön C. Tämä on mahdollista tapauksessa, jossa henkilö C on B:n mielestä vain osittain luotettu ja B on määritellyt, että hän hyväksyy luotetuksi vain avaimia, joilla on kaksi osittain luotettua allekirjoitusta. Nyt henkilö A voi allekirjoittaa kaksi C:n luomaa erilaista avainta ja B hyväksyykin nyt C:n avaimen, mitä hän ei olisi tehnyt pelkästään C:ltä saamallaan sertifikaatilla. Tämän vuoksi korkean turvallisuustason saavuttamisen kannalta on tärkeää, että luottamus määritellään viime kädessä aina perustuen henkilöihin eikä pelkästään jonkun muun suosituksiin.

4.2.2 Luotettava kolmas osapuoli

Luotettavien ja turvallisten palvelujen tarjoamiseen tietoverkoissa tarvitaan monia tietoturvateknologioita, kuten aiemmin mainitut kryptografiaan perustuvat menetelmät. Nämä eivät kuitenkaan yksin riitä, vaan mukaan tarvitaan myös luotettuja kolmansia osapuolia (Trusted Third Party, TTP) ja niiden tarjoamia palveluja, jotka on lähes poikkeuksetta toteutettu julkisen avaimen infrastruktuurin päälle. TTP-palvelut ja PKI:n merkitys on jatkuvasti kasvamassa ja kuten (Kerttula 1999, 327) toteaakin:

> "Luotetun kolmannen osapuolen (TTP) palvelut ja niiden toteuttamiseksi tarvittava julkisen avaimen infrastruktuuri (PKI) tulevat olemaan turvallisen ja luotettavan verkkoympäristön kulmakiviä."

ISO/IEC:n määritelmän mukaan TTP tarkoittaa turvallisuusviranomaista tai tämän valtuuttamaa tahoa, johon käyttäjät luottavat ja joka tarjoaa tietoturvallisuuteen liittyviä

palveluja. TTP:n tarjoamat palvelut liittyvät luottamuksellisuuden, eheyden, todentamisen ja kiistämättömyyden toteuttamiseen. TTP:n avainpalvelut ovat yleensä julkisen avainten rekisteröintiin, varmentamiseen ja jakeluun liittyviä palveluja, mutta voivat olla myös salaisten avainten luontiin ja levitykseen (käytettäessä salaisen avaimen menetelmiä) liittyviä palveluja. (Liikenneministeriö 1998)

TTP-määritelmää käytetään usein myös yksinkertaisesti tarkoittamaan jotakin tahoa, johon muut luottavat. Tämä taho on yleensä yritys tai organisaatio, mutta sen ei välttämättä tarvitse olla viranomainen tai viranomaisen valtuuttama. Esimerkiksi PGP:ssä luotettu kolmas osapuoli voi olla yksityinen henkilö. TTP:n toiminnan luotettavuus voi siten perustua joko viranomaisten valtuutukseen tai johonkin muuhun seikkaan, jonka vuoksi tahon luotettavuuteen uskotaan. Suomessa luotettavan kolmannen osapuolen roolissa toimii esimerkiksi Väestörekisterikeskus, joka myöntää muun muassa HST (Henkilön Sähköinen Tunniste) kansalaisvarmenteita.

Luotettava kolmas osapuoli siis jakaa ja hallinnoi sertifikaatteja. Sertifikaattien jakaminen perustuu luottamushierarkiaan, joka tarkoittaa, että sertifikaatteja voidaan jakaa useilla eri tasoilla siten, että hierarkian ylimmällä tasolla toimiva osapuoli jakaa aina juurivarmenteen. Sertifikaattien jako voi tapahtua myös ilman keskitettyä varmentajaa, kuten avointen luottamusverkkojen (esim. PGP) tapauksessa. (Ojala 1998, 52).

Ojalan (1998, 54) mukaan luotettavien kolmansien osapuolten käyttö sähköisessä kaupankäynnissä kuitenkin monimutkaistaa useita asioita. Koska kaupankäynnin järjestelmään tulee yksi osapuoli lisää, kokonaisuuden kompleksisuus kasvaa. Asiakkaan kannalta onkin tärkeää, kuinka käyttäjäystävällinen tällainen järjestelmä lopulta on. Kompleksisuuden ja osapuolten lukumäärän kasvu kasvu lisäävät myös mahdollisia tietoturvariskejä.

4.3 Varmentaja-malli

Yleisesti ottaen varmentaja-mallit voidaan jakaa kahteen eri tyyppiin: yleinen hierarkia ja top-down hierarkia. Ensimmäisessä tyypissä jokainen varmentaja varmentaa sekä itseään ylempänä (parent), että alempana (child) hierarkiassa olevat varmentajat. Jälkimmäisessä tyypissä varmentaja varmentaa vain itseään alempana olevat varmentajat. Molemmissa tyypeissä voi kuitenkin ilmetä ristiinvarmennusta, joka ei noudata hierarkkisia rakenteita. On myös mahdollista, että käytetään useampaa juurivarmentajaa. Varsinkin globaalien varmentajajärjestelmien tapauksessa vain yhden juurivarmentajan käyttö olisi varsin epäkäytännöllistä. Siksi laajoissa varmentajajärjestelmissä on yleensä mahdollista, että varmentajat voivat ristiinvarmentaa toisia varmentajia. Niinpä jos käyttäjä luottaa varmentaja X:ään, voi hän luottaa automaattisesti myös varmentaja Y:hyn, mikäli varmentaja X on varmentanut varmentaja Y:n. Kahden käyttäjän välissä voi siis periaatteessa olla mikä tahansa määrä varmentajia. (Branchaud 1997, 13 - 17)

Varmentaja-malli on hierarkkinen ja sopii näin ollen hyvin suurille ja hierarkkisesti muodostetuille organisaatioille. Adamsin ym. (2000, 100) mukaan sitä voidaan pitää parhaiten soveltuvana sekä yritysten omaan, että yritysten väliseen käyttöön (B2B). Hänen mukaansa varmentaja-malli sopii myös yritysten ja kuluttajien (B2C) väliseen sähköiseen asiointiin, jossa osapuolet ovat usein toisilleen tuntemattomia, ja jossa siksi tarvitaan luotettuja kolmansia osapuolia. Tällöin kaupankäynnin vaatiman luottamuksen synnyttämiseksi luotettuja kolmansia osapuolia tarvitaan ikään kuin ”erittäin luotettuina” esittelijöinä (vrt. PGP-malli). Tällaista luottamusta eivät PGP-mallin esittelijät voi taata. Branchaud (1997) on kuitenkin todennut, että käytäntö on osoittanut varmentaja-mallin sopimattomaksi etenkin sähköpostikäytössä Internetissä, sillä Internet ei ole kovin hierarkkisesti rakentunut. Turvallisen sähköpostin käyttöön soveltuukin paremmin seuraavaksi esiteltävä PGP-malli.

4.4 PGP-malli

PGP:tä voidaan pitää yleisimpänä PKI:n sovelluksena ja se onkin yleisin turvallisen sähköpostin käyttöön tarkoitettu ohjelmisto. PGP on saavuttanut jo standardin aseman puhuttaessa sähköpostin turvallisuudesta. PGP hyödyntää sekä julkisen avaimen että salaisen avaimen menetelmiä ja sisältää tiedon salauksen ja digitaalisen allekirjoituksen toiminnot. PGP:n ensimmäiset versiot perustuivat vapailta markkinoilta saataviin algoritmeihin ja suurimpana syynä sen yleistymiseen on ollut sen maksuton saatavuus Internetistä. PGP:ssä ei ole keskitettyjä luotettuja kolmansia osapuolia kuten varmentajajärjestelmissä, vaan se perustuu jokaisen käyttäjän luomiin luottamusverkkoihin. Käyttäjä muodostaa oman luottamusverkoston luomalla paikallisen "avainrenkaan", jossa ovat kaikki luotetut julkiset avaimet. Avainten vaihtaminen voi tapahtua joko suoraan henkilöitten välillä tai avainpalvelimia käyttäen. Tällaiseen palvelimeen voi kuka tahansa julkaista julkisen avaimensa tunnistetietoineen (eli julkisen avaimen sertifikaatin) ja hakea muiden käyttäjien julkisia avaimia liitettäväksi henkilökohtaiseen avainrenkaaseen.

Kuten aiemmin mainittiin, luottamus PGP:ssä perustuu esittelijöihin eli henkilöihin, joihin tietty käyttäjä luottaa ja voi siten luottaa myös esittelijän allekirjoittamiin eli luotettavaksi todistamiin avaimiin. Avain voi myös olla usean, ennestään tuntemattoman esittelijän allekirjoittama, mutta siihen voidaan varmuudella luottaa vain silloin, kun yksikin esittelijöistä on ennalta tunnettu ja luotettu. Ihmiset voivat olla kuitenkin huolimattomia ja allekirjoittaa vääriä avaimia, joiden omistajia he eivät tunne eivätkä normaalitilanteessa luottaisi heihin. PGP:ssä tähän voi varautua esimerkiksi siten, että määrittelee jokaiselle avaimelle vaatimukseksi vähintään kahden tunnetun ja luotetun esittelijän allekirjoitukset. (Adams ym. 2000, 101)

Adamsin ym. (2000, 101) mukaan ovela hyökkääjä voi kuitenkin saada kaksi tai useammankin kokemattoman esittelijän allekirjoittamaan "väärän" avaimen. PGP:n luottamusmallin mukaan tämä ei ole kuitenkaan ongelma, sillä kenenkään ei pitäisi luottaa esittelijöihin, jotka ovat helposti huijattavissa tai muuten kokemattomia tai huolimattomia. Jos taas epäluotettavat esittelijät allekirjoittavat valeavaimia, ei

kenenkään pitäisi tulla huijatuksi, sillä jokainen määrittelee itse esittelijöiksi ainoastaan sellaisia henkilöitä, joihin varmasti luottaa. Lisäksi mikäli käyttäjä saa käsiinsä avaimen, jolla ei ole yhtään luotettua esittelijää, PGP vaatii ettei sellaista avainta hyväksytä. PGP:ssä voi myös syntyä esittelijöitä, jotka ovat hyvin laajasti luotettuja ja jopa toimia kokopäivätoimisesti avainten allekirjoittajana. Tällaiset esittelijät vastaavat varmentajia hierarkkisissa PKI-järjestelmissä.

Edelleen Adamsin ym. (2000, 101) mukaan varmentajia vastaavien esittelijöiden synty PGP:ssä ei ole haitallista, mikäli kyseistä esittelijää on todellakin pidetty laajalti luotettuna. Tällaisissa tapauksissa PGP:n luottamusmalli alkaa muistuttaa hierarkkisten X.509 järjestelmien luottamusmallia ja Adams ym. väittääkin, että ei ole tilannetta, missä PGP:tä ei voida hallita ja käyttää X.509 luottamusmallin mukaisesti. PGP mahdollistaa hänen mukaansa vielä paljon enemmän, sillä se antaa käyttäjälle laajemmat mahdollisuudet hallita PKI:tä omien näkemystensä mukaisesti ja on sietokykyinen inhimillisille virheille.

4.5 Key Recovery ja Key Escrow

Avainten palautus (Key Escrow tai Key Recovery) tarkoittaa, että valtuutetulle taholle voidaan joissakin tilanteissa antaa mahdollisuus salatun liikenteen tai aineiston purkuun. Järjestelmässä yksi tai useampi luotettu osapuoli säilöö kopiot salaisista avaimista tai ns. palautusavaimet (recovery keys), joiden avulla voidaan määrittää salauksessa ja salauksen purussa käytetty avain. Avainten palautuksella on kaksi eri merkitystä. Key Recovery:llä tarkoitetaan lähinnä yrityksissä tapahtuvaa varmuuskopioitujen avainten pelastamista, kun taas Key Escrow:lla tarkoitetaan lain toimeenpanemaa menettelyä salattujen viestien purkamiseksi. (Kerttula 1999, 365)

Key Escrow:n ajatuksena on, että viranomaisilla tai jollain muulla kolmannella osapuolella on oikeudet saada salainen avain haltuunsa. Tämä on siinä määrin merkittävä asia, että sen täytyy olla määriteltynä lainsäädännössä. Oikeuden salatun aineiston purkuun voi saada vain laissa määriteltyjen rikosten selvittämisessä ja valtion turvallisuutta uhkaavissa tapauksissa. Työnantajan oikeudet saada työntekijän salainen

avain haltuunsa liittyy lähinnä työtehtävien hoidossa käytettyyn avaimeen ja työnantajan omistamien tietojen salausten purkamiseen. Työnantaja voi tällöin olla yksityinen yritys tai julkinen taho ja/tai viranomainen. (Liikenneministeriö 1998)

Key escrow -järjestelmiä voidaan toteuttaa toiminnallisesti eritasoisina. Useimmissa järjestelmissä salaisen avaimen luovutus merkitsee, että valtuutettu taho pääsee käsiksi kaikkeen käyttäjän salattuun liikenteeseen ja aineistoihin. Teknisesti on kuitenkin mahdollista toteuttaa myös järjestelmiä, jotka mahdollistavat pääsyn vain osaan käyttäjän liikenteestä tai aineistoista. Esimerkiksi USA:ssa vahvaan kryptografiaan perustuvat tuotteet on määritelty sotatarvikkeiksi ja näitä koskee vientikielto. Kieltoa on lievennetty vahvoja salausmenetelmiä käyttävien tuotteiden osalta, mikäli ne tukevat Key Escrowta. (Liikenneministeriö 1998)

Key Recovery -järjestelmällä voidaan toteuttaa avainten varmistus, jolloin avaimen palautus omistajalleen olisi mahdollista esimerkiksi sen tuhoutuessa tai kadotessa (Liikenneministeriö 1998). Avainten palautuksessa on huomioitava, että nimenomaan tiedon salaukseen käytetyn avaimen palautus on oltava mahdollista, sillä muuten kaikki salattu tieto menetetään salausavaimen tuhoutuessa. Digitaalisten allekirjoitusten tekoon käytettävän salaisen avaimen palautuksen ei sen sijaan tarvitse olla mahdollista, sillä allekirjoitetut dokumentit säilyvät luettavassa muodossa avaimen tuhouduttuakin. Tietoturvan kannalta ajateltuna digitaalisiin allekirjoituksiin käytettävää salaista avainta ei saisi palauttaa missään tapauksessa, että esimerkiksi tapahtuman kiistämättömyyden takaavia allekirjoituksia ei olisi mahdollista päästä jälkeenpäin muuttamaan palauttamalla avain luvattomasti.

Kuluttajan kannalta Key Recovery-menetelmästä on hyötyä ainoastaan siinä tapauksessa, että hänen varmuuskopioimaton salainen avaimensa katoaa tai tuhoutuu. Tällöin avain on mahdollista palauttaa kolmannelta osapuolelta. Muissa tapauksissa Key Recovery ja varsinkin Key Escrow voidaan nähdä kuluttajan tietosuojaa ja yksityisyyttä heikentävänä menetelmänä, joka voi myös vähentää yleistä luottamusta kolmansien osapuolten toimintaan. Sekä Key Escrow:sta, että Key Recovery:stä seuraa myös tietoturvauhka, kun salaisia avaimia kerätään keskitettyihin tietokantoihin. Tällaiset tietokannat ovat nimittäin omiaan houkuttelemaan tietomurtajia.

4.6 PKI-järjestelmien ongelmakohtia

PKI:stä on tullut tämän hetken tietotekniikan "muoti-ilmiö" ja kuten jokaisen uuden vähänkin lupaavan tekniikan kohdalla, lukuisat yritykset yrittävät hyödyntää PKI:täkin voittojen maksimoinnissa. Varsinkin nyt, kun tietoturvasta on tullut merkittävä tekijä, yrittäjiä riittää. Tästä on ollut seurauksena, kuten Ellison ja Schneier (2000, 1) toteavat, että suurin osa aiheesta julkaistusta materiaalista on PKI-järjestelmien suunnittelijoiden ja toimittajien itsensä kirjoittamia eikä siis kovin kriittistä. Kirjoituksissa käsitellään vain PKI:n parhaita puolia ja lukuisat käytännön ongelmat jäävät lähinnä sivuhuomautuksiksi, jos niitä yleensä mainitaan.

Ellison ja Schneier (2000, 1) myös kyseenalaistavat koko PKI:n tarpeellisuuden elektronisessa liiketoiminnassa. Heidän mukaansa väite siitä, että PKI:tä tarvittaisiin elektronisen liiketoiminnan kukoistamiseen on virheellinen, sillä elektroninen liiketoiminta kukoistaa jo nyt ilman PKI:täkin. He väittävätkin, että tilanne on päinvastainen: PKI vaatii elektronista liiketoimintaa menestyäkseen. Väite pitää kyllä osittain paikkansa, sillä elektroninen liiketoiminta on nimenomaan se alue, missä PKI:tä todella tarvitaan. Toisaalta käytäntö on kuitenkin osoittanut, että juuri tietoturvaratkaisujen puute on juuri se asia, joka tällä hetkellä hidastaa elektronisen liiketoiminnan kehitystä (Helsingin kauppakamari, 2001).

Edelleen Ellisonin ja Schneierin (2000, 2) mukaan julkisen avaimen infrastruktuurin epäkohtana on, että digitaalisella allekirjoituksella vahvistettua tapahtumaa ei voida jälkeenpäin kiistää. Jos käytetään esimerkiksi työasemalle tallennettuja ohjelmistovarmenteita, on mahdollista, että kuka tahansa työasemaan käsiksi pääsevä voi varmentaa tapahtumia jonkun toisen henkilön nimissä eikä tämä toinen pysty kiistämään osallisuuttaan kyseisiin tapahtumiin. Ellison ja Schneier (2000, 2) vertaavat digitaalisella allekirjoituksella vahvistettua sähköistä tilausta puhelin- tai postitilaukseen. He toteavat, että henkilö voi kiistää tehneensä puhelin- tai postitilauksen, jolloin todistustaakka tapahtumasta siirtyy kauppiaalle, mutta digitaalisella allekirjoituksella vahvistettua tilausta ei voida kiistää. Tämä ei kuitenkaan ole PKI:hin liittyvä ongelma, sillä vaikka henkilö ei voisikaan kiistää tehneensä

digitaalista allekirjoitusta, niin kuten aiemmin todettiin, ainakin Suomessa kaupan voi jälkeenpäin perua. Tähän Ellison ja Schneier (2000, 2) eivät kuitenkaan artikkelissaan ota kantaa.

On tosin syytä huomata, että huolimaton tai tietämätön käyttäjä voi digitaalisella allekirjoituksella epähuomiossa vahvistaa jotain paljon helpommin kuin esimerkiksi omakätisellä allekirjoituksella. Tähän voi osittaisena syynä olla digitaalisten allekirjoitusten uutuus, puutteelliset ja epäinformatiiviset käyttöliittymät ja se, ettei niiden lainvoimaisuutta olla vielä täysin sisäistetty.

Eräs perustavaa laatua oleva ongelma syntyy, jos PKI-järjestelmissä sidotaan oikeuksia tai valtuuksia henkilön nimeen, sillä nimi ei ole ainutkertainen tunniste. Esimerkiksi Adamsin (2000, 99) mukaan varsinkin järjestelmissä, joissa määritellään auktorisointitietoa, näitä tietoja ei pitäisi sitoa henkilön nimeen vaan julkiseen avaimeen, joka on ainutkertainen toisin kuin henkilön nimi. Näin voidaan hänen mukaansa välttää tilanne, jossa samanniminen väärä henkilö saisi valtuuksia hänelle kuulumattomiin tietoihin. Lähes saman ongelman ovat todenneet myös Ellison ja Schneier (2000, 3), joiden mukaan sertifikaateissa käytetty julkisen avaimen yhdistäminen henkilön nimeen ei ole käytännöllisiä, sillä on todennäköistä, että laajassa PKI-järjestelmässä on samannimisiä henkilöitä. Käytännön ratkaisuissa käytetäänkin usein sähköpostiosoitetta, asiakasnumeroa tai muuta vastaavaa tunnistetta, joiden ainutkertaisuus voidaan helposti varmistaa. Yleisesti perinteisissä valtion palveluissa ja myös jossain määrin liiketoiminnan alueella käytettyä sosiaaliturvatunnusta ei voida PKI:ssä lain mukaan käyttää tunnisteena, sillä esimerkiksi julkisen avaimen sertifikaattiin liitettynä se olisi kaikkien nähtävillä.

Vaikka Adams ym. (2000, 101) väittää, että PGP:llä voi tehdä kaiken minkä varmentajaperusteisilla järjestelmilläkin, ei PGP:kään ole soveltuva kaikkiin käyttötarkoituksiin. Esimerkiksi Branchaudin (1997, 32) mukaan PGP-sertifikaatti ei ole laajennettavissa ja sisältää vain sähköpostiosoitteen, julkisen avaimen arvon ja luottamuksen asteen attribuutin. Niinpä PGP-sertifikaatti ei ole kovinkaan hyvä henkilön tunnistamiseen eikä itse asiassa tarjoa lainkaan keinoa vahvaan henkilön tunnistamiseen. Hänen mukaansa PGP soveltuu ainoastaan tavalliseen sähköposti-

käyttöön. Branchaud (1997, 33) myös väitti, että PGP sertifikaatteja ei voida lakkauttaa, mutta nykyisissä PGP sertifikaateissa on jo viittaus sulkulistapalveluun.

PKI-järjestelmät, joissa varmenteet ja avaimet on tallennettu ohjelmallisesti tietokoneille (software token), ovat osoittautuneet hankaliksi käyttää ja hallinnoida. Sen vuoksi mukana kuljetettavia "varmennelaitteita" (hardware token) on alettu hyödyntää PKI:ssä. Tässä ratkaisussa avaimet ja algoritmit on tallennettu esimerkiksi toimikortille, jolloin vältytään muun muassa huolimattomien käyttäjien sekä tietokoneiden ja niiden kovalevyjen rikkoutumisen aiheuttamilta ongelmilta. (Bakker 1999, 7)

Suurimpana ongelmana ohjelmallisissa varmenteissa onkin, että käyttäjä voi vahingossa poistaa salaisen avaimensa tai se voi muuten tuhoutua esimerkiksi laitevian tai melko usein tapahtuvan käyttöjärjestelmän uudelleen asennuksen yhteydessä. Mikäli salaista avainta ei ole erikseen varmuuskopioitu ja säilötty turvalliseen paikkaan, ovat kaikki kyseisellä avaimella salatut tiedot lopullisesti saavuttamattomissa. Tämä ongelma koskee kuitenkin vain tiedon salaukseen käytettävää avainta, sillä digitaalisesti allekirjoitetut dokumentit ovat edelleen luettavissa salaisen avaimen tuhouduttuakin, koska dokumenttia ei ole salattu.

PKI-järjestelmien eräänä ongelmana on, että niiden hallinnan käyttöliittymät on tehty perinteisten sovellusten käyttöliittymästandardien mukaisesti. Tietoturva ja PKI ovat kuitenkin sen verran uusia asioita loppukäyttäjien sovellusten tasolla, että niiden käytettävyyteen olisi kiinnitettävä enemmän huomiota. Uudenlaista suunnittelua vaaditaan myös siksi, että kaikkien tietyn järjestelmän käyttäjien on ymmärrettävä tietoturvan merkitys ja sen hallintaohjelmistojen käyttö niin hyvin, että kriittisiä virheitä ei pääsisi syntymään. Sillä, kuten aiemmin on mainittu, yksikin virhe voi johtaa koko järjestelmän tietoturvan romahtamiseen. Esimerkiksi Whitten (1999) on tutkinut PGP 5.0 ohjelman käytettävyyttä ja todennut, että suurin osa koehenkilöistä ei pystynyt suoriutumaan vaadituista tehtävistä niin, että turvallisen sähköpostin lähetys ja vastaanotto olisi onnistunut. Tämä johtui osaltaan testatun ohjelman käyttöliittymän suunnittelun puutteista ja myös siitä, että ihmiset eivät ymmärtäneet, mitä olivat tekemässä ja mitä seurauksia teoilla oli. PKI:tä ennalta tuntemattomat henkilöt eivät siis

ymmärtäneet riittävästi sen toimintaa ja käyttöä yksinkertaisesta käyttöliittymästä huolimatta.

Ollakseen täysin turvallisia ja muodostaakseen häiriöttömiä luottamusketjuja PKI-järjestelmät vaativat myös muuta kuin tietoverkoissa tapahtuvaa kommunikointia (käytetään usein termiä out-of-band). Tällaista kommunikointia on muun muassa juurivarmenteen jakelu varmentajapohjaisissa järjestelmissä ja salaisen avaimen turvallinen jakelu missä tahansa PKI-järjestelmässä. Koska elektronisessa liiketoiminnassa pyritään tehokkuuteen ja turvallisuuteen voidaan nämä seikat nähdä PKI-järjestelmien ongelmakohtina, sillä enää ei voidakaan toimia täysin elektronisesti vaadittavan turvallisuustason saavuttamiseksi. (Jøsang ym. 2001, 7)

Adamsin ym. (2000, 98) mukaan yrityksen tai yhteisön on harkittava tarkkaan, ennen kuin alkaa rakentaa kallista PKI-järjestelmää, ja mietittävä millainen järjestelmä on sopivin aiottuun tarkoitukseen. Erityisesti tietoturvan kannalta pohdittavaa riittää, sillä Adams ym. (2000, 98) arvelevat, että hierarkkiset PKI-järjestelmät tulevat olemaan seuraava tietomurtojen kohde ja toisaalta toimivien ja luotettavien verkostomaisten järjestelmien rakentaminen näyttää huomattavasti kalliimmalta ja hankalammalta kuin hierarkkisten.

Jonkun henkilön tuntemisella ja tämän sähköisen identiteetin tietämisellä on selvä ero. Tämä muodostaakin ongelman PKI-järjestelmissä, sillä niissä keskitytään vain jälkimmäiseen, mikä ei ole riittävää päätöksien tekemiseen esimerkiksi Internetissä tapahtuvissa, ehdotonta luottamusta vaativissa transaktioissa. Tämän vuoksi PKI:n käyttäjät tarvitsevat myös muunlaista tietoa toisesta osapuolesta. Tämä voi olla esimerkiksi lehdistä luettua, TV:ssä nähtyä, fyysistä kohtaamista tai puhelimessa juttelua. Ilman tällaista lisäinformaatiota PKI olisi merkityksetön ja kanssakäyminen luotettavasti autentikoidun WWW-sivuston kanssa vastaisi kanssakäymistä täysin tuntemattoman osapuolen kanssa. (Jøsang ym. 2001, 10)

Suurimpana ongelmana PKI:ssä sen yleistymisen kannalta on kuitenkin standardoinnin sekä yhteisten käytäntöjen ja politiikoiden puutteellisuus tai jopa niiden täydellinen puuttuminen. Esimerkiksi tällä hetkellä EU:n alueella käyttöön otetut PKI-ratkaisut ovat

keskenään täysin yhteensopimattomia. Tähän suurena syynä on useat laite- ja ohjelmistoalustat sekä lukuisat käyttöjärjestelmät eri versioineen. Edellä mainittu puolestaan johtuu pitkälti siitä, että PKI-järjestelmien on oltava myös kotoa käytettäviä, eikä tällöin ole mahdollista määritellä standardia käyttöympäristöä jota kaikki käyttäjät noudattaisivat. Nyt EU on kuitenkin alkanut panostaa PKI:hin ja pyrkimyksenä on luoda standardit ja käytännöt kattamaan kaikki EU-maat. Useita direktiivejä on jo määritelty koskien muun muassa digitaalisia allekirjoituksia, ristiinvarmennusta, elektronista liiketoimintaa, elektronista maksamista ja toimikortteja. Näillä laillisilla toimenpiteillä ja lisäksi aktiivisella osallistumisella tutkimus- ja kehityshankkeisiin EU aikoo saattaa toimintaan koko alueensa laajuisen PKI:n.

PKI nähdään monesti tekniikkana ja puhutaan PKI-järjestelmän hankkimisesta tai ostamisesta. Tämä on kuitenkin harhaanjohtavaa ja tällä tietämyksen tasolla PKI hankkeisiin ryhdyttäessä päädytään todennäköisesti epäonnistumiseen. PKI onkin nähtävänä prosessina, joka liittyy lähes kaikkiin organisaation toimintoihin. PKI:n onnistunut käyttöönotto vaatii uudenlaista ajattelua ja lähes kaikkien käytäntöjen uudelleen määrittelyä sekä kattavan koko organisaatiota koskevan tietoturvapolitiikan määrittelyn. Kuten aiemmin todettiin, PKI on vain yhtä vahva kuin sen heikoin lenkki ja siksi käytäntöjen ja politiikoiden on oltava tiukasti määriteltyjä ja niitä on myös noudatettava, jotta suunniteltu tietoturvan taso voitaisiin saavuttaa. Myös kaikkien käyttäjien perehdyttäminen kyseiseen järjestelmään ja tietoturvan merkitykseen yleensäkin on välttämätöntä hankkeen onnistumiseksi. Näiden toimenpiteiden laiminlyönti johtaa helposti huolimattomaan käyttöön ja virhetilanteisiin, jotka voivat vaarantaa koko järjestelmän tai jopa organisaation turvallisuuden.

4.6.1 Tietoturvanäkökohtia

PKI-järjestelmien, kuten muidenkin kryptografian sovellusten, uskotaan olevan turvallisia. Monet sovellukset voidaankin tiettyjen ehtojen täyttyessä todistaa turvallisiksi. Useimmissa tapauksissa takuu turvallisuudesta kestää kuitenkin vain niin kauan kuin salaisuudet, kuten salainen avain, pysyvät salassa. Kun salaisuus paljastuu, on salatun tiedon turvallisuus menetetty sen hetkisiltä ja myös aiemmilta salauksen

käyttökohteilta. Jos esimerkiksi digitaalisen allekirjoituksen salainen avain paljastuu, ei mihinkään kyseisellä avaimella luotuun allekirjoitukseen voi enää luottaa huolimatta siitä, milloin se on tehty. (Abdalla ja Reyzin 2000, 3)

Edellä mainitun ongelman lähestymiseen on esitetty muutamia eri keinoja. Esimerkiksi salaisuuden paljastumisen mahdollisuutta on pyritty pienentämään jakamalla salaisuus (salainen avain) osiin ja hajauttamalla se eri järjestelmiin. Tämä on kuitenkin varsin kallis ja monimutkainen menetelmä eikä siksi sovellu tavallisille käyttäjille. Lisäksi järjestelmät, joihin salaisuus on hajautettu, voivat olla alttiita samoille hyökkäyksille eikä varsinainen riski silloin juuri pienene. Eräs mahdollisuus on julkisen avaimen järjestelmissä usein tapahtuva salaisen avaimen vaihtaminen turvallisuuden parantamiseksi. Tämä ei kuitenkaan useinkaan tule kysymykseen siitä aiheutuvien suurten kustannusten vuoksi (Herzberg ym. 1997, 103). Abdalla ja Reyzin (2000, 3) esittävät tähän ratkaisuksi menetelmää, jolla pyritään pienentämään mahdollisia vahinkoja salaisuuden paljastuessa. Tästä käytetään nimitystä "forward security". Kantavana ideana tässä menetelmässä on, että salaista avainta käytetään vain lyhyen aikaa ja avaimen paljastuminen ei vaikuta mitenkään aiempiin salaisiin avaimiin eikä mahdollista niiden selvittämistä. Haasteena tällaisen menetelmän suunnittelussa on se, miten salainen avain voidaan vaihtaa tarvitsematta vaihtaa julkista tietoa, kuten julkista avainta.

PKI-järjestelmän turvallisuus riippuu monista eri tekijöistä ja ennen kaikkea kaikista sertifikaatteja käyttävän järjestelmän komponenteista. Näitä komponentteja ovat mm. järjestelmään kuuluvien tietokoneiden olinpaikan fyysinen turvallisuus, henkilöstö (esimerkiksi järjestelmän suunnittelijat, asentajat, käyttäjät ja ylläpitäjät), käyttöjärjestelmät, joiden päällä PKI-järjestelmää käytetään ja varmentajan turvallisuus. Minkä tahansa edellä mainitun komponentin pettäminen voi aiheuttaa koko järjestelmän turvallisuuden pettämisen. Ellisonin ja Schneierin (2000, 1) mukaan tietoturvan voidaankin ajatella olevan ketju, joka on vain yhtä vahva kuin sen heikoin lenkki. PKI-järjestelmissä näitä lenkkejä on paljon eivätkä ne kaikki ole kryptografiaa käyttäviä. Ihmiset ovatkin yleensä kaikkein heikoimpia lenkkejä ja siksi mikään järjestelmä jossa ihmiset ovat mukana ei voi olla niin turvallinen kuin sellainen teoreettinen, puhtaasti kryptografinen järjestelmä jollainen mielikuva PKI-järjestelmistä usein annetaan.

Ellison ja Schneier (2000, 1) esittävätkin kysymyksen: ovatko nykyiset PKI-järjestelmät suunniteltu maksimoimaan turvallisuutta vai niiden myynnistä saatavaa voittoa?

Adamsin ym. (2000, 99) mukaan etenkin hierarkkisissa PKI-järjestelmissä, kuten X.509, on suurena uhkana varmentajan murtaminen, jolloin koko järjestelmän tietoturva on murrettu. Huipputurvallisina pidettyihin järjestelmiin, kuten Pentagonin ja FBI:n tietojärjestelmät, on murtauduttu, joten ei voi ajatella, että mitkään varmentajajärjestelmät olisivat täysin turvallisia. Tässä tapauksessa heikoksi lenkiksi osoittautuvat yksittäiset tietokoneet, jotka eivät ole riittävän hyvin suojattuja hakkeroinnilta.

Luotettuun kolmanteen osapuoleen perustuvissa järjestelmissä on vielä ongelmana tietoturvan kannalta se, että hyökkäykset järjestelmää kohtaan voivat tulla sisältäpäin. Turvallisina pidetyt pankit tai muut varmenneorganisaatiotkaan eivät pysty takaamaan työntekijöidensä vilpittömyyttä, jolloin riski tietoturvan pettämiseksi kasvaa. Tietoturvaongelmien ratkominen onkin vielä ollut painottunutta ulkoapäin tuleviin hyökkäyksiin, mutta painotus saattaa muuttua lähitulevaisuudessa. (Ojala 1998, 53)

Luotettuun kolmanteen osapuoleen kohdistuvasta hyökkäyksestä on tuoreena esimerkkinä tapaus, jossa Microsoftin Active-X komponentille myönnetty sertifikaatti olikin valheellinen. Tapauksessa huijaava osapuoli esiintyi Microsoftina hakiessaan sertifikaattia VeriSigniltä Active-X komponentilleen. Tällöin on ollut mahdollista, että Internetin käyttäjät ovat voineet hyväksyä mahdollisesti viruksen tai muun haitallisen toiminnon sisältävän Active-X komponentin suorittamisen uskoen sen olevan Microsoftin tekemä. Vastuu virheestä kuuluu Verisignille, joka on myöntänyt sertifikaatin virheellisin tai riittämättömin tiedoin huijarille. (Patton ja Jøsang 2001, 7)

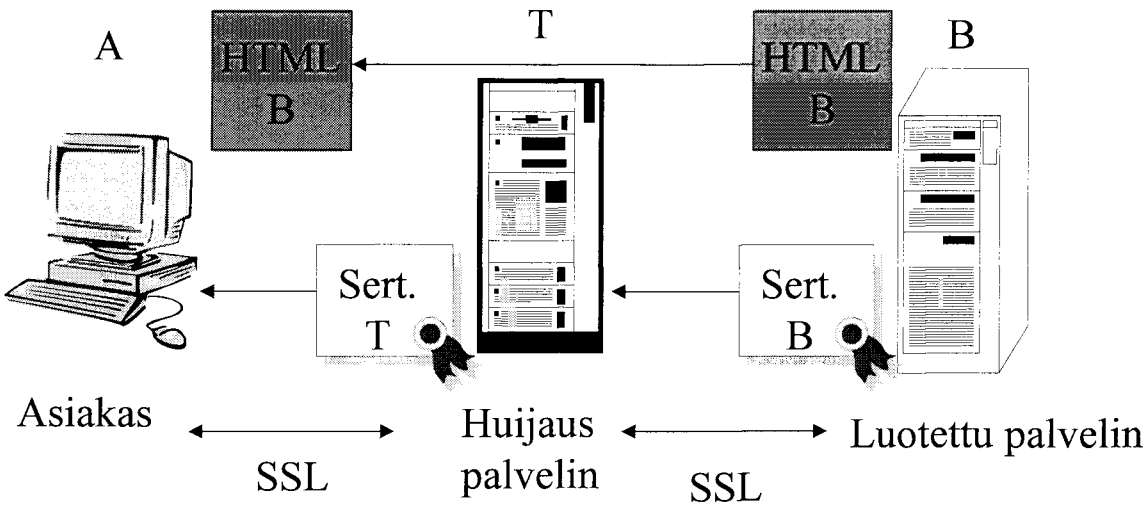
Juuri-sertifikaatit ja niiden eheys ovatkin tärkein turvallisen kommunikoinnin tekijä varmentaja-pohjaisissa PKI-järjestelmissä. Varsinkin kun puhutaan Internetissä toimivista PKI-järjestelmistä, tulee vastaan Jøsang ym. (2001, 7-8) mukaan seuraavanlainen tietoturvaongelma. Internet käytössä kaikki standardi juuri-sertifikaatit (kuten Verisign ja Thawte) on koodattu suoraan Netscapen ja Microsoftin selaimiin. Kun selain asennetaan, sertifikaatit kopioidaan koneelle Netscapen tapauksessa

tavalliseen tiedostoon ja Microsoftin tapauksessa rekisteriin (registry). Tiedostoissa ja rekisterissä olevat sertifikaatit ovat kuitenkin siinä määrin suojaamattomia, että niitä voidaan muuttaa esimerkiksi koneeseen tartutetun viruksen avulla. Tällöin voidaan luotettujen juuri-sertifikaattien tilalle vaihtaa väärennettyjä sertifikaatteja ja saada selain luottamaan valheellisiin sivustoihin.

Jøsang ym. (2001, 10) mukaan selainten mukana tulevia juurivarmentajien sertifikaatteja, jotka ovat itse allekirjoitettuja sertifikaatteja, ei pitäisi kutsua sertifikaateiksi ollenkaan. Tämä siksi, että niillä ei ole sertifikaattien semantiikkaa, koska juuri-sertifikaatin pätevyyttä ei voida mitenkään varmistaa. Jøsang ehdottaakin, että selaimen valmistaja allekirjoittaisi sertifikaatit, jotka tämän jälkeen koodattaisiin selaimeen, eikä missään vaiheessa kopioitaisi tiedostoon. Tällöin käyttäjä voisi varmistaa juuri-sertifikaattien pätevyyden digitaalisesta allekirjoituksesta, eikä edellä mainittu hyökkäys voisi toteutua. Toisena vaihtoehtona Jøsang ehdottaa, että käyttäjä allekirjoittaisi omalla salaisella avaimellaan kaikki juuri-sertifikaatit ja ikään kuin toimisi niiden yli varmentajana. Tässä tapauksessa juuri-sertifikaattien pätevyys on niin kauan turvattu kuin käyttäjän salainen avain pysyy suojassa.

Kuten myöhemmin tietoturvan käytettävyyden yhteydessä todetaan, ovat tietoturvan hallinnan käyttöliittymät puutteellisia. Tämä pitää paikkansa etenkin Internetin selainkäyttöliittymissä, mistä on esimerkkinä seuraavassa kuvassa esitetty Jøsangin (2000, 6-8) kuvailema tietoturvaongelma PKI:n yleisen sovelluksen, SSL:n käytöstä.

KUVA 3. Man In The Middle hyökkäys Jøsangia (2000, 7) mukaillen



Tässä tapauksessa käyttäjä A haluaa päästä käsiksi verkkopalveluihin luotetulta ja turvalliselta palvelimelta B, joka voisi olla esimerkiksi pankki, jonka maksupalveluja A haluaa käyttää. Normaalitapauksessa käyttäjä A ottaa selaimellaan (asiakas) yhteyden pankin B verkkosivuun. Palvelin B palauttaa tällöin sertifikaatin Sert.B A:n selaimelle, joka varmentaa sertifikaatin oikeellisuuden käyttämällä selaimelle ennalta tallennettua juuri-sertifikaattia, joka on myöntänyt palvelinsertifikaatin Sert.B. Kun sertifikaatti on varmennettu, jatkaa A:n selain yhteyttä B:hen turvallisessa SSL-moodissa. (Jøsang 2000, 7 - 9)

Huijauspalvelimella T on kuitenkin mahdollisuus saada sekä A että B uskomaan, että he keskustelevat toistensa kanssa, vaikka he kommunikoivatkin T:n kanssa. Tällöin T toimii HTML-sivujen välittäjänä A:n ja B:n välillä. Tällaisen hyökkäyksen onnistumiseksi A:n selaimella täytyy kuitenkin osoittaa alkuperäinen yhteydenotto T:hen B:n sijasta. Tähän on olemassa useitakin keinoja. Voidaan esimerkiksi asettaa väärä URL-osoite johonkin portaaliin ja odottaa kunnes joku ottaa yhteyden linkin kautta T:hen luullen kommunikoivansa B:n kanssa. Tähän on mahdollista käyttää myös aiemmin mainittua väärien sertifikaattien vaihtamista selaimen mukana tulleiden sertifikaattien tilalle. Tämä puolestaan voidaan suorittaa niin ikään aiemmin kuvatuilla valheellisilla Active-X komponenteilla. (Jøsang 2000, 7 - 9)

Kun A on ottanut yhteyden T:hen ja muodostanut SSL-yhteyden käyttäen T:n sertifikaattia Sert.T, muodostaa palvelin T SSL-yhteyden B:hen käyttäen B:n sertifikaattia Sert.B. Nyt huijauspalvelin T välittää viestejä A:n ja B:n välillä käyttäen kahta eri SSL-yhteyttä saaden molemmat uskomaan, että he todella kommunikoivat toistensa kanssa. Jos nyt A esimerkiksi suorittaa tilisiirron, on T:llä mahdollisuus muuttaa tilisiirron määrää ja kohdetta vaikka omalle tililleen. (Jøsang 2000, 7 - 9)

Kun SSL-yhteys muodostetaan, oletetaan, että asiakas autentikoi palvelimen, josta on osoituksena selaimen ikkunassa näkyvä lukko-kuvake. Itse asiassa se vain osoittaa, että jotakin on autentikoitu, mutta ei tarkemmin mitä. Käytännössä tämä tarkoittaa, että mitään ei ole autentikoitu. Lukko-kuvaketta napauttamalla voi kyllä tarkastella saatua sertifikaattia, mutta harva tekee niin. Ja vaikka sertifikaattia tutkii, on kokeneenkin käyttäjän usein vaikea arvioida onko sertifikaatti kelvollinen. Selain itse vertaa

palvelimen domain-nimeä sertifikaatissa olevaan, josta kokenut käyttäjä kyllä huomaa, mikäli sertifikaatti ei ole myönnetty sille palvelimelle, johon yhteyttä on yritetty ottaa. Useimmilta tämäkin jää kuitenkin huomioimatta tai sen merkitystä ei ymmärretä. Voidaan siis todeta, että selainkäyttöliittymä on helposti haavoittuva edellä kuvatuille hyökkäyksille, sillä se ei ole riittävän informatiivinen tietoturvan tarpeisiin nähden. (Jøsang 2000, 7 - 9)

4.6.2 Monen päätelaitteen ongelma

PKI:n käytön yleistyessä vastaan tulee monen päätelaitteen ongelma, kun sähköistä asiointia ja kauppaa aletaan käydä yhä useammanlaisilla päätelaitteilla. Jo nyt ostoksia voi tehdä tietokoneella ja puhelimella ja digi-TV sekä erilaiset PDA-laitteet ovat juuri astumassa kuvaan mukaan. Kun yhdellä käyttäjällä on useita erilaisia päätelaitteita, täytyisi sähköisessä asioinnissa vaadittavat sertifikaatit saada toimimaan kaikissa laitteissa joustavan ja käytännöllisen asioinnin saavuttamiseksi. Tällä hetkellä Suomessa on meneillään kokeiluita kaksi SIM-korttia sisältävien puhelinten käytöstä sähköisessä maksamisessa. Näissä kokeiluissa puhelimessa on operaattorin SIM-kortin lisäksi pankin SIM-kortti, jota käytetään maksamiseen. Tällaisella ratkaisulla olisi periaatteessa mahdollista toimia myös PKI:ssä, sillä SIM-kortillekin voidaan asentaa sertifikaatteja PKI-käyttöä varten. Yhtenä ratkaisuna voivat toimia myös toimikortit, joille tallennettuja sertifikaaatteja voidaan käyttää eri päätelaitteissa edellyttäen, että ne sisältävät toimikortin lukijan. Tällä hetkellä kortinlukijat ja itse toimikortitkin ovat kuitenkin sen verran suuria, että niiden käyttö pienissä päätelaitteissa, kuten matkapuhelimissa, ei ole järkevää.

Voidaankin sanoa, että monen päätelaitteen ongelmalle ei vielä toistaiseksi ole hyvää ratkaisua. BlueTooth teknologia vaikuttaa kuitenkin lupaavimmalta sen ratkaisemiseksi. Tässä ratkaisussa henkilön omistamat päätelaitteet voivat keskustella keskenään henkilökohtaisessa verkossa (Personal Area Network, PAN) eikä sertifikaatteja siksi tarvita kaikissa laitteissa erikseen asennettuna. Tämä on tosin vielä tulevaisuuden visio ja sen toteutumisen vaaditaan vielä monien teknisten ongelmien ratkaisuja.

4.6.3 Yhteenveto

Kuten tästä luvusta on ilmennyt, PKI-järjestelmät sisältävät lukuisia ongelmia. Mitkään ongelmista eivät kuitenkaan ole kriittisiä eikä niiden pitäisi olla esteenä PKI-järjestelmien käyttöönotolle. Näin monien ongelmien havaitseminen kuitenkin antaa helposti käsityksen, että PKI-järjestelmät eivät olisikaan tietoturvan kannalta riittävän kehittyneitä. Tosiasia kuitenkin on, että PKI-järjestelmiä voidaan pitää monin verroin turvallisempina kuin mitään aiemmin yleisessä käytössä ollutta menetelmää tietoturvan parantamiseksi. Patton ja Jøsang (2001, 7) toteavat myös, että oikein käytettyinä elektronisessa liiketoiminnassa salaustekniikat ja SSL yhdessä takaavat sellaisen turvallisuuden, joka on riittävä muissa kuin kaikkein korkeimmin motivoituneiden tietomurtajien tapauksessa, ja että ne ovat joka tapauksessa turvallisempia kuin esimerkiksi perinteinen luottokortteihin perustuva kaupankäynti.

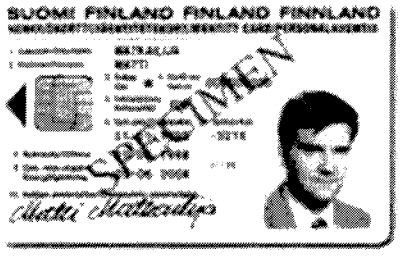
PKI-järjestelmien suurimpina uhkina voidaan sanoa olevan palvelinten heikko turvallisuus sekä ihmisten tietämättömyys tai välinpitämättömyys tietoturvasta yleensä. Sähköinen kaupankäynti perustuu pääasiassa palvelintekniikkaan ja tällöin salaiset avaimet, kuten monet muutkin luottamukselliset tiedot, ovat tallennettuna palvelimille. Koska palvelimet ovat käytännössä osoittautuneet melko helposti murrettaviksi, on suuri riski, että salaiset avaimetkin joutuvat tietomurtajan käsiin romahduttaen koko PKI:n tietoturvan. Kuten uutisiakin seuraamalla on voinut todeta, ovat lähes kaikki elektronista liiketoimintaa vastaan tehdyt hyökkäykset kohdistuneet juuri palvelimiin. Siirtotiehen kohdistetut hyökkäykset ovat harvinaisia ja ne ovat teknisestikin huomattavasti hankalampia toteuttaa. (Patton ja Jøsang 2001, 7)

Lopuksi voidaan todeta, että PKI-järjestelmissä on havaittavissa lukuisia ongelmia, joita voidaan kuitenkin jo ratkaista tämän hetkisillä tekniikoilla ja menetelmillä. Ratkaisun useisiin ongelmiin tarjoaa esimerkiksi toimikortit, joita käsitellään seuraavassa luvussa.

5 TOIMIKORTIT

Tässä luvussa käsitellään toimikortteja ja sitä, miten niillä voidaan ratkaista PKI-järjestelmien ongelmia elektronisessa kaupassa. Tällä tarkastelulla pyritään myös osoittamaan, että toimikorteilla vahvistetut PKI-järjestelmät täyttävät useimmat elektronisen liiketoiminnan tietoturvavaatimuksista. Yleisesti ottaen voidaan todeta, että toimikortteja käyttämällä päästään korkeammalle tietoturvan tasolle verrattuna ohjelmistopohjaisiin ratkaisuihin, kuten edellä esitetyt PKI-järjestelmät. Toimikortteja tarkasteltaessa PKI-järjestelmät voidaan nähdä periaatteessa lähinnä viitekehyksenä, jossa toimikortit toimivat. Tämän vuoksi elektronisen liiketoiminnan ongelmien ratkaisijaksi esitetäänkin toimikortteja, vaikka ne eivät sinällään voi olla ratkaisu ilman toimivaa PKI:tä. Tässä tutkielmassa toimikorteilla tarkoitetaan pääasiassa kortteja, jotka sisältävät prosessorin ja muistin. Tällaisia kortteja kutsutaan usein myös älykorteiksi.

Seuraavassa kuvassa on esimerkki toimikortista. Kuvan kortti on Suomen poliisilaitoksen myöntämä sähköinen henkilökortti, jota voidaan käyttää sekä tavallisen henkilökorttina että tunnistauduttaessa sähköisiin palveluihin. Sähköiset varmenteet kortille myöntää Väestörekisterikeskus, joka on niistä myös vastuussa. Sähköiseen henkilökorttiin ja varmenteisiin liittyvät standardit löytyvät esimerkiksi väestörekisterikeskuksen sivuilta. (Väestörekisterikeskus 2002)



KUVA 4. HST-kortti (Väestörekisterikeskus 2002)

5.1 Toimikortit osana PKI-järjestelmiä

Toimikorttien käyttö PKI:ssä voidaan jakaa karkeasti kahteen tapaan: off-line käyttö ja online käyttö. Off-line tavassa on mukana vain kaksi osapuolta, jotka ovat toimikortti ja esimerkiksi kaupan kassakoneen kortin lukija. Luotettu kolmas osapuoli ei siis osallistu tapahtumaan, eikä yhteyttä oteta mihinkään palvelimeen. Tässä järjestelyssä kortin lukijassa täytyy olla kryptografisesti suojattu moduuli, johon on tallennettuna kaikkien järjestelmässä käytettävien toimikorttien avaimet. Tämä moduuli on käytännöllisesti katsoen itsekin toimikortti. (Bakker 1999, 15)

Bakkerin (1999, 16) mukaan edellä mainittu off-line käyttö soveltuu kuitenkin ainoastaan pieniin ja suljettuihin järjestelmiin. Tähän on syynä muun muassa se, että järjestelmässä toisensa autentikoivat osapuolet vaativat saman jaetun salaisuuden ja helpoin tapa hallita järjestelmän avaimet on käyttää samaa organisaation laajuista salaista avainta kaikissa toimikorteissa ja lukijoissa. Tällainen järjestelmä on erittäin haavoittuva, sillä yhdenkin toimikortin tai lukijan murtaminen johtaa koko järjestelmän turvallisuuden murtamiseen. Vaikka off-line järjestelmät soveltuvatkin vain hyvin pieniin järjestelmiin ollen lisäksi varsin haavoittuvia, niin niitä on silti yleisesti käytössä organisaatioiden sisäisissä järjestelmissä. (Bakker 1999, 16)

Yleisesti ottaen online käytöllä voidaan saavuttaa parempi tietoturva kuin off-line käytöllä. Tähän on yksinkertaisena syynä se, että esimerkiksi toimikortin PIN-koodin murtoa yritettäessä ei off-line käytössä tarvitse olla reaaliaikaisessa yhteydessä muihin osapuoliin, jolloin voidaan käyttää enemmän aikaa ja laskentatehoa, eikä tällaista yritystä voida havaita niin helposti kuin online yhteydessä. Käytännössä toimikortit ovat kuitenkin niin hyvin suojattuja (tamper resistant) tällaisia hyökkäyksiä vastaan, että off-line käyttöä ei voida tämän seikan vuoksi pitää konkreettisena riskinä tietoturvalle. Toimikorttien off-line käyttöäkin voidaan siis perustella joissain tapauksissa, kuten esimerkiksi tilanteissa, joissa vaaditaan korkeaa tietoturvaa, mutta verkkoyhteyksiä ei ole järkevin kustannuksin saatavilla. Suurena ongelmana off-line käytössä tosin on korttien sulkeminen (revokointi), jonka toteuttamiseksi joudutaan erikseen päivittämään

kaikkien kortinlukijoitten tiedot. Myös tämän vuoksi off-line käyttö ei sovi kuin pieniin järjestelmiin.

Toimikorttien käyttöä PKI:ssä voidaan perustella tietoturvan kannalta esimerkiksi Halevin ja Krawczykin (1998, 122) mukaan seuraavasti. Jos käyttäjällä ei ole esimerkiksi palvelimelle tapahtuvaa autentikointia varten mukanaan mitään laskennallista laitetta, kuten salkkumikroa tai toimikorttia, on hänen tietoturvansa PKI:ssä ainoastaan heikon, käyttäjän muistinvaraisen salasanan varassa. Palvelimella voi puolestaan olla vahvaan salaukseen vaadittavat avaimet autentikointia varten. Tällainen epäsymmetria PKI:ssä heikentää sen tietoturvaa, sillä järjestelmän murtaminen mahdollistuu salasanaan kohdistuvilla hyökkäyksillä, jotka ovat varsin tehokkaita ja helposti toteutettavia kryptografisten menetelmien murtamiseen verrattuna. Toimikorteilla on siis selkeä merkitys PKI-järjestelmien tietoturvan kannalta.

Tällä hetkellä vallitsee tilanne, jossa markkinoilla on lukuisia toimikorttien valmistajia, joilla on valikoimissaan useita erilaisia toimikortteja. Jotta toimikortteja voitaisiin menestyksekkäästi käyttää osana PKI-järjestelmiä, vaaditaan selkeästi määriteltyjä standardeja, joita toimikorttien valmistajien tulisi myös noudattaa. Korttien standardointi on kuitenkin vielä kesken, mikä jarruttaa selvästi organisaatioiden halua lähteä ottamaan käyttöön toimikortein tuettuja PKI-järjestelmiä.

Toimikorttien käyttömahdollisuuksia ja käytön joustavuutta voitaisiin parantaa, mikäli kortille olisi mahdollista lisätä organisaatio- tai henkilökohtaisesti esimerkiksi sertifikaatteja, jotta kortteja voitaisiin hyödyntää erilaisia sertifikaatteja käyttävissä PKI-järjestelmissä. Tähän voi eräänä esteenä kuitenkin olla se, että erilaisten PKI-palvelujen tarjoajat ovat usein kilpailijoita keskenään, eivätkä siksi todennäköisesti hyväksyisi eri organisaatioiden sertifikaatteja tai sovelluksia korteilleen.

5.2 Toimikortit elektronisessa liiketoiminnassa

Hyvät perustelut sille miksi toimikortteja kannattaa yleensä käyttää elektronisessa liiketoiminnassa tarjoa esimerkki Ranskasta. Vuonna 1995 Ranskassa siirryttiin käyttämään toimikortteja magneettiraitakorttien sijasta kaikissa maan pankeissa, jonka seurauksena rahaliikenteeseen kohdistuvan rikollisuuden määrä laski jopa 90 prosenttia. Toimikorttien tuoma lisä tietoturvallisuuteen on siis selkeästi käytännössä todistettu.

On varsin todennäköistä, että toimikortit tulevat huomattavasti yleistymään elektronisessa liiketoiminnassa. Ojala (1998, 96) toteaa, että kunhan käyttäjät ymmärtävät toimikortin tarjoaman korkean tietoturvatason ja toisaalta helpon käytettävyyden, se tulee mahdollisesti saavuttamaan tilisiirtojen ja luottokorttien etumatkan maksukäytännön hyväksyttävyydessä.

PKI tarjoaa sähköiseen maksamiseen käytännössä vain yhden turvallisen ja käytössä olevan menetelmän, joka on SET (Secure Electronic Transaction) järjestelmä. Tämän heikkoutena on kuitenkin, että sitä voidaan käyttää vain kiinteältä työasemalta ja se vaatii asennettavaksi oman ohjelmistonsa. SET ei siis tue toimikortteja, eikä sitä ole siksi käsitelty tässä tutkielmassa tarkemmin. Toimikortteja hyödyntävään maksamiseen Internetissä on kehitetty EMV (Europay, Mastercard, Visa) standardi, joka kuvailee toimikorttimaksamiseen tarvittavan toiminnallisuuden. (Herreweghen ja Wille 1999, 1)

Dengin ym. (1997, 111) mukaan toimikorttien hyödyntäminen Internet käytössä taas saattaa muodostua liian kalliiksi ratkaisuksi eikä niitä heidän mukaansa välttämättä siinä tarvitakaan. Deng ym. (1997, 111) väittää myös, että julkisen avaimen operaatioihin perustuva toimikorttipohjainen maksaminen vaatii liikaa laskentatehoa, eikä siksi sovellu paljon pieniä maksuja vaativiin sovelluksiin. On kuitenkin osoittautunut, että toimikortit ovat yleistymässä ja niiden laskentateho ja muistikapasiteetti kasvaa jatkuvasti, joten toimikorttipohjaisen maksujärjestelmän käyttöönottoa ei voida enää pitää liian kalliina tai muuten soveltumattomana ratkaisuna. Kuten aiemmin on osoitettu, voidaan väittää, että toimikortteja todella tarvitaan Internet käytössä sen tietoturvan saattamiseksi yleisesti hyväksyttävälle tasolle.

5.3 Toimikorttien tuoma turvallisuus PKI:hin

Toimikorttien merkittävimpiä ominaisuuksia turvallisuuden kannalta on, että kortilla olevat salaiset avaimet eivät missään vaiheessa siirry kortin ulkopuolelle. Niinpä kortinkäyttäjä, kortinlukija tai kortilla olevat sovelluksetkaan eivät saa tietoonsa salaista avainta. Toimikortin käyttöjärjestelmä sallii sovellusten suorittavan ainoastaan tiettyjä komentoja, jotka käyttävät avainta ja tällöinkin kaikki toiminnot tapahtuvat kortin sisällä, ohjelmallisesti ja fyysisesti turvallisessa ympäristössä.

Toimikorteilla voidaan myös ratkaista PKI-järjestelmien ongelmien yhteydessä mainittu ongelmatilanne, joka syntyy ohjelmistovarmenteita käytettäessä. Tällöinhän PKI:n tietoturvan voidaan sanoa oleva vain yhtä vahva kuin yksittäisen päätelaitteen, jolla sertifikaattia säilytetään. Kun henkilökohtaiset sertifikaatit ja salaiset avaimet on tallennettu kryptografisesti suojatulle toimikortille, ei kenelläkään ulkopuolisella ole mahdollisuutta käyttää niitä hyväkseen tietämättä kortin PIN-koodia. Tämän vuoksi toimikortteja voidaan pitää huomattavasti turvallisempana kuin ohjelmistovarmenteita.

Ellisonin ja Schneier (2000, 2) väittävät, että toimikortille talletetut avaimet eivät ole turvassa, sillä heidän mielestään nykyiset toimikortit ovat heikkoja hyökkäyksiä vastaan. Tässä on syytä huomata, että kirjoittajat ovat erikoistuneita kryptografiaan ja lisäksi Schneier työskentelee yrityksessä, jonka tarkoituksena on murtaa kryptografiaan perustuvia tietoturvaratkaisuja. On totta, että kaikkien toimikorttien tietoturva on onnistuttu murtamaan, mutta toistaiseksi tämä on tapahtunut laboratorio-olosuhteissa huipputeknisillä ja kalliilla laitteistoilla. Siksi murtamisen kustannukset ainakin tällaisissa tapauksissa ylittävät saadut hyödyt. Ellisonin ja Schneierin väite pitää siis todennäköisesti paikkansa teoreettisesti ajateltuna, mutta käytännössä toimikortteja voidaan kuitenkin pitää erittäin turvallisina etenkin jos niitä verrataan muihin nykyisiin tietoturvaa parantaviin ratkaisuihin.

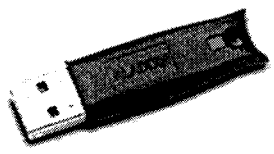
Toimikortteja on ehdotettu hyödynnettäviksi myös käyttöjärjestelmien turvaamisessa, kuten Clark ja Hoffman (1994) artikkelissaan. Heidän mukaansa yksittäisten tietokoneiden ja niiden käyttöjärjestelmien tietoturvaa voitaisiin parantaa merkittävästi,

mikäli kone käynnistettäisiin toimikortilta. Koska toimikorttia voidaan käyttää niin, että se vaatii käyttäjän autentikoinnin ennen kuin mihinkään sen dataan päästään käsiksi, se toimisi erinomaisena koneen tietoturvan parantajana. Näin voitaisiin suojautua myös koneiden käynnistyslohkoja muuttavilta viruksilta. Toimikortteja hyödyntäen voitaisiin siis suojata tehokkaasti suuriakin hajautettuja tietojärjestelmiä aina yksittäisten koneiden suojauksesta verkkoliikenteen suojaamiseen asti.

5.4 Toimikorttien mahdollisia turvallisuusuhkia

Toimikorttien hyödyntämisessä osana PKI:tä tietyn organisaation sisällä on syytä huomioida muun muassa seuraava seikka. Jos toimikorttia käytetään ainoastaan tietoteknisiin tarkoituksiin, kuten työasemiin kirjautumiseen ja turvallisen sähköpostin käyttöön voi käyttäjillä kasvaa houkutus jättää kortti työpaikalle saavuttuaan kortinlukijaan koko päiväksi. Tällöin menetetään hyöty salaisen avaimen pysymisestä vain käyttäjän itsensä hallussa, sillä kuka tahansa koneelle tulija voi nyt hyödyntää lukijaan jätettyä korttia. Tämä voidaan tietysti ratkaista esimerkiksi määrittelemällä aikaväli, jolloin kortin PIN-koodi on syötettävä uudelleen. Käytännöllisempi ratkaisu olisi kuitenkin käyttää toimikorttia myös fyysisessä kulunvalvonnassa, jolloin käyttäjän olisi pidettävä kortti aina mukanaan poistuessaan työpisteeltään. Tässä suhteessa seuraavan kuvan mukainen USB-token saattaisi olla käytännöllisempi kuin toimikortti, sillä USB-token on todennäköisimmin liitettynä käyttäjän avainnippuun, jota yleensä jokainen pitää aina mukanaan. USB-token on periaatteeltaan toimikorttia vastaava laite, joka ei tarvitse erillistä lukijaa, vaan sitä voidaan käyttää lähes kaikista uusista tietokoneista löytyvän USB-väylän kautta.

KUVA 5. USB-token



Vaikka toimikortteja on jo käytetty useita vuosia erilaisiin tarkoituksiin, ei niiden turvallisuusriskejä ole analysoitu paljoakaan huolimatta siitä, että toimikortteihin liittyy aivan erityinen riskiympäristö, jollaista ei aiemmissa tietoturvaratkaisuissa ole esiintynyt. Tämä riskiympäristö muodostuu pääasiassa toimikortin ominaispiirteisiin kuuluuvasta toiminnallisuuden jakamisesta tavalla, jota ei esimerkiksi kämmen- tai salkkumikroissa esiinny. Toiminnallisuuden jakautumista on kuvailtu tarkemmin seuraavassa kappaleessa.

Varsinkin liikemaailmassa toimikorteille halutaan yhdistää useita sovelluksia niiden käytön joustavuuden ja mahdollisten kustannussäästöjen vuoksi. Tämä kuitenkin vähentää toimikortteja hyödyntävän järjestelmän kokonaisturvallisuutta, kun järjestelmään liittyvien osapuolten määrä kasvaa. Useimmat seuraavissa kappaleissa mainituista uusista uhkista, jotka johtuvat niin toimikortin ominaispiirteistä kuin usean sovelluksen mallistakin, eivät ole mahdollisia "tavallisissa" toimikortittomissa tietokonejärjestelmissä. Toimikorttiympäristössä ne kuitenkin mahdollistuvat. Toimikorttiympäristöön kuuluvat yleensä seuraavat osapuolet: kortinhaltija, terminaali, datan omistaja, kortin myöntäjä, kortin valmistaja ja ohjelmiston kehittäjä.

Kortinhaltijalla tarkoitetaan henkilöä, joka fyysisesti hallitsee korttia pitämällä sitä mukanaan ja päättämällä koska sitä käytetään. Datan omistaja on osapuoli, joka kontrolloi kortilla olevaa dataa. Mikäli korttia käytetään digitaalisten sertifikaattien varastointiin, on kortinhaltija myös datan omistaja, mutta jos kortilla on esimerkiksi elektronisen rahan sovellus, ei kortinhaltija ole enää datan omistaja. Terminaalilla tarkoitetaan laitetta, joka mahdollistaa kortin kommunikoinnin muuhun maailmaan. Terminaali hallitsee kaikkea I/O liikennettä kortille (näppäimistö, jolla tieto syötetään) ja kortilta (näyttölaite, jossa kortilta tuleva data näkyy). Terminaali voi olla myös pankkiautomaatti tai matkapuhelin, mikäli puhutaan SIM-korteista. Kortin myöntäjällä tarkoitetaan osapuolta, joka kontrolloi toimikortin käyttöjärjestelmää ja kaikkea dataa, joka on sinne korttia alustettaessa tallennettu. Kortin valmistajalla taas tarkoitetaan osapuolta, joka valmistaa fyysisesti kortin sekä suunnittelee ja valmistaa sen mikrosirun. Ohjelmiston kehittäjä puolestaan suorittaa kortilla toimivien sovellusten ohjelmoinnin. Seuraavassa on kuvattu Schneierin ja Shostackin (1999) määrittelemiä mahdollisia hyökkäyksiä toimikorttijärjestelmää vastaan eri osapuolten kannalta.

- *Terminaalin hyökkäys kortinhaltijaa tai datan omistajaa vastaan.* Tällaiset hyökkäykset ovat helpoiten ymmärrettäviä ja vaikeasti kortinhaltijan havaittavissa. Esimerkiksi valepankkiautomaatti voi veloittaa kortinhaltijan tiliä.

- *Kortinhaltijan hyökkäys terminaalia vastaan.* Tässä tapauksessa kortinhaltija yrittää huijata terminaalia muutetulla tai valheellisella kortilla. Tällaisia hyökkäyksiä voi torjua tekemällä kortin fyysisistä ominaisuuksista vaikeasti kopioitavia, jolloin terminaalin omistaja voi valvoa sen käyttöä. Toinen keino on estää kortinhaltijan pääsy käsiksi kortin ohjelmistoon, mikä taas lisää yhden osapuolen toimikorttijärjestelmään, jossa huijausta voi tapahtua.

- *Kortinhaltijan hyökkäys datan omistajaa vastaan.* Useimmissa korteissa data on suojattu kortinhaltijalta ja joissain tapauksissa kortinhaltija ei saa edes tietää mitä dataa kortilla on. Esimerkiksi salaiset avaimet ovat sellaista dataa, mitä kortinhaltijan ei tarvitse saada tietoonsa. Kortteja on hankala suojata tällaisilta hyökkäyksiltä, sillä kortinhaltija voi teoriassa käyttää rajattomasti aikaa ja resursseja kortin murtamiseen. Korttien murtamiseen onkin löydetty monia onnistuneita murtomenetelmiä, kuten "reverse-engineering", virheanalyysi ja ajoitusanalyysi.

- *Kortinhaltijan hyökkäys kortin myöntäjää vastaan.* Monet hyökkäykset näyttävät kohdistuvan kortin myöntäjään, mutta kohdistuvatkin itse asiassa kortilla olevien ohjelmien ja datan eheyteen ja autenttisuuteen. Nämä hyökkäykset mahdollistuvat tapauksissa, joissa kortin myöntäjä päättää, että kortinhaltija voi hallita kortin myöntäjän omistamaa dataa tai ohjelmia. Mikäli kortille jätetään mahdollisuus sen ohjelmien hallintaan, voidaan olla varmoja, että niitä vastaan hyökätään.

- *Kortinhaltijan hyökkäys ohjelmiston kehittäjää vastaan.* Yleensä korttijärjestelmissä, joissa voidaan odottaa, että kortti myönnetään rikolliselle käyttäjälle, oletetaan että kortille ei asennetta uusia ohjelmia. Tämä perustuu siihen luottamukseen, ettei kortinhaltijan ja ohjelmiston kehittäjän väliin päästä hyökkäämään. On kuitenkin osoittautunut, että hyökkääjät ovat onnistuneet

saamaan haltuunsa laitteistoja kortin ohjelmien muuttamiseen, jotka auttavat tällaisen hyökkäyksen teossa.

- *Terminaalin omistajan hyökkäys kortin myöntäjää vastaan.* Avoimissa järjestelmissä (kuten elektroninen raha), joissa terminaalin omistaja ja kortin myöntäjä ovat eri osapuolia, voi terminaali toimia huijauksen välineenä. Terminaali hallitsee kaikkea tietoliikennettä kortin ja kortin myöntäjän välillä. Niinpä terminaali voi väärentää tai jättää kirjaamatta tapahtumia, joilla ei ole mitään tekemistä kortin kanssa. Terminaali voi myös jättää kesken tapahtumia, joissa korttia veloitetaan, huijaten näin kortin myöntäjää. Nämä hyökkäykset eivät suoraan liity toimikorttimaailman luonteeseen, sillä ne tapahtuvat terminaalin ja kortin myöntäjän välisessä suhteessa. Tällaisia hyökkäyksiä voidaan estää muodostamalla luotettava yhteys kortin ja taustajärjestelmän välille terminaalin kautta.

- *Kortin myöntäjän hyökkäys kortinhaltijaa vastaan.* Yleisesti ottaen kortin myöntäjän ajatellaan ajavan kortinhaltijan etua, mutta näin ei välttämättä ole. Kortin myöntäjän mahdolliset hyökkäykset koskevat lähinnä yksityisyyttä ja epärehellinen kortin myöntäjä voikin kerätä laittomasti tietoa kortin käyttäjästä. Kortin myöntäjä voi hyötyä tästä muun muassa rahakorttien tapauksessa, jolloin myöntäjä voi seurata vaikkapa kortinhaltijan ostokäyttäytymistä.

- *Kortin valmistajan hyökkäys datan omistajaa vastaan.* Joillain kortin valmistajan suunnitteluratkaisuillakin voi olla mahdollista aiheuttaa tietoturva-aukkoja toimikorttijärjestelmiin. Toimikorttiahan voidaan pitää monen käyttäjän ympäristönä eikä tavallistenkaan tietokoneympäristöjen tietoturvaongelmia ole vielä ratkaistu.

Edellä mainittujen hyökkäysten lisäksi voi olla myös hyökkäyksiä, joissa useampi kuin yksi osapuoli onkin rikollinen. Tällaisten hyökkäysten variaatioiden määrä luonnollisesti kasvaa osapuolten lukumäärän kasvaessa.

Toimikorttijärjestelmään kohdistuvia hyökkäyksiä vastaan on olemassa pelkistetysti kahdenlaisia suojautumismenetelmiä. Ensimmäinen on tehdä yksittäiset hyökkäykset hankalimmiksi esimerkiksi käyttämällä vahvempaa kryptografiaa tai parantamalla toimikorttien murron kestävyyttä (tamper-resistance). Schneier ja Shostack (1999) eivät kuitenkaan pidä tätä kovin tehokkaana vaan ehdottavat toisenlaista vaihtoehtoa, jolla voi tehdä kokonaisia hyökkäysmuotoja tehottomiksi. Heidän ehdotuksensa mukaan toimikorttijärjestelmän osapuolia vähentämällä tai osapuolten rooleja hämärtämällä voidaan vähentää erilaisten hyökkäysten määrää merkittävästi. Helpoin tapa tähän on roolien yhdistäminen. Jos esimerkiksi kortinhaltija on myös datan omistaja, ei kortinhaltijan hyökkäyksessä datan omistajaa vastaan ole enää järkeä. Lisäksi Schneier ja Shostack (1999) muistuttavat, että tekemällä järjestelmistä avoimia, voidaan niiden turvallisuutta kasvattaa julkisen arvioinnin, kritisoinnin ja kehityksen myötä.

Toimikortista tekee haavoittuvan sen kyvyttömyys kommunikoida ulkopuolisen maailman kanssa. Toimikorttihan tarvitsee aina näppäimistön, jolta sille syötetään PIN-koodi tai muuta tietoa ja jonkun näyttölaitteen kortilta tulevan tiedon esittämiseksi. Tämä seikka mahdollistaa erilaisia hyökkäyksiä korttia vastaan, sillä esimerkiksi näppäimistö on helposti muutettavissa siten, että se tallentaa näppäinpainalluksia, jolloin PIN-koodi saadaan varastettua. Vielä helpommaksi tämän tekevät kotitietokoneissa käytettävät kortinlukijat, koska ne on liitetty tietokoneeseen ja näin ollen näppäimistöltä tuleva PIN-koodi kiertää tietokoneen kautta kortinlukijalle ja avaa samalla taas yhden mahdollisuuden PIN-koodin varastamiselle. On tosin olemassa kortinlukijoita, jotka liitetään näppäimistön ja tietokoneen väliin siten, että PIN-koodi menee näppäimistöltä suoraan kortinlukijalle.

Yhteenvetona toimikorttien turvallisuudesta voidaan todeta, että on erittäin tärkeää, että toimikortin koko elinkaaren jokaisessa vaiheessa kiinnitetään riittävästi huomiota turvallisuusnäkökohtiin. Toimikorttimaailmassa on useita uusia uhkia, jotka kaikki on syytä ottaa vakavasti, mikäli halutaan saavuttaa ehdottoman turvallinen ympäristö sähköiselle asioinnille. Huolimatta mainituista uhkista ja mahdollisista hyökkäyksistä toimikortteja vastaan, voidaan sanoa, että käytännön tasolla toimikortteja hyödyntävät järjestelmät ovat merkittävästi parempi vaihtoehto tietoturvan kannalta kuin toimikortittomat. Mahdollisista heikkouksistaan huolimatta toimikortit kuitenkin

täyttävät riittävän hyvin tämän päivän elektronisen liiketoiminnan asettamat vaatimukset tietoturvalle.

6 TIETOTURVA JA TUNNISTUS KAUPANKÄYNTIPROSESSISSA

Tässä luvussa käsitellään tietoturvaa ja tunnistusta kaupankäyntiprosessin osaprosesseissa. Osaprosesseja käsitellään lähinnä kommunikointiprosessin kannalta. Tarkoituksena on selvittää millä edellisessä luvussa mainituista tietoturvan osa-alueista on eniten merkitystä kommunikoinnissa ja miten tämä ilmenee kussakin prosessissa. Näin voidaan selvittää mitä lisäarvoa kommunikoinnin parantamisella voidaan kaupankäynnin osaprosesseissa saavuttaa. Lisäksi selvitetään kuinka tunnistamisen perusratkaisut voidaan niitä vaativissa prosessissa toteuttaa ja mikä on niiden merkitys prosessien kannalta. Luvussa kolme todettiin mitä lisäarvoa PKI ja toimikortit tuovat tietoturvan eri alueisiin.

Koska kommunikointiprosessi liittyy kaikkiin kaupankäyntiprosessin osaprosesseihin, liittyy siihen myös kaikki tietoturvan osa-alueet. Kommunikoinnissahan olennaista on kommunikoivien osapuolten tunnistus ja siksi siihen pätee samat asiat kuin mitä tunnistusprosessin yhteydessä mainitaan. Voidaan kuitenkin sanoa, että PKI:llä ja toimikorteilla saavutetaan sellainen tietoturvan taso kommunikoinnissa, jota ei voida muilla keinoin sähköisessä maailmassa saavuttaa. Tärkeimpinä tietoturvan alueina, joihin PKI ja toimikortit tuovat lisäarvoa, voidaan mainita autentikoinnin lisäksi luottamuksellisuus, yksityisyys ja tiedon eheys.

6.1 Maksaminen

Sähköiseen maksuprosessiin liittyy läheisesti autentikointi, jossa sekä asiakkaan, että kauppiaan on aukottomasti tunnistettava toisensa tietoverkon välityksellä. Tyypillisesti autentikointi toteutetaan osapuolten kesken julkisen avaimen sertifikaatteja käyttäen. Toinen mahdollisuus on pelkkä digitaalinen allekirjoitus, jota ei tosin käytetä sen hitauden takia kuin yksittäisille sanomille. Autentikointiin on olemassa myös muita keinoja, kuten kryptografisesti suojatut laitteet (esimerkiksi toimikortit).

Myös luotettu kolmas osapuoli on keskeisessä asemassa maksuprosessissa. Aiemmin todettiin, että kolmannet osapuolet tarjoavat usein infrastruktuurin maksamiseen. Kolmansia osapuolia tarvitaan myös PKI:tä hyödyntävissä maksujärjestelmissä, joissa TTP voi varmentaa niin ostajan ja kauppiaan, kuin maksupalveluja tarjoavan organisaationkin identiteetin kaikkien osapuolten välillä lisäten näin maksuprosessin turvallisuutta ja käyttäjien luottamusta järjestelmään.

Maksuprosessia tarkasteltaessa tulee vastaan elektronisen liiketoiminnan vaatimus anonyymille asioinnille, joka asettaa suuria haasteita maksuprosessille, jossa yleisesti ottaen aina vaaditaan henkilön identiteetin selvittäminen. Tunnistuksen problematiikassahan todettiin, että maksaminen vaatii periaatteessa aina vahvan tunnistuksen, mutta PKI ja toimikortit tarjoavat myös mahdollisuuksia anonyymiin maksamiseen kuitenkin niin, että ongelmatilanteissa osapuolten identiteetit on voitava selvittää.

Tietoturvan vaatimuksista tiedon eheys ja luottamuksellisuus on syytä huomioida sähköisessä maksuprosessissa. Sekä maksajan, että maksun saajan on voitava varmistua siitä, että esimerkiksi maksutapahtumaan liittyviä tietoja ei voida muuttaa tiedon siirron tai sen säilytyksen aikana ja että ne pysyvät vain niihin liittyvien ospuolten tiedossa. Tietoa siirrettäessä tämä voidaan varmistaa tiedon salauksella ja digitaalisilla allekirjoituksilla. Myös tapahtumien jäljitettävyys on tärkeä osa tietoturvaa varsinkin maksuprosessissa. Perinteisessä kaupankäynnissä on tärkeää säilyttää kuitteja mahdollisten kauppatapahtumien jälkeisten epäselvyyksien ratkaisemiseksi. Sama pätee myös sähköiseen kaupankäyntiin, jossa on voitava ongelmatilanteen sattuessa selvittää maksutapahtuman vaiheet ja siihen liittyvät osapuolet.

6.2 Tunnistus

Kaupankäyntiprosessissa tunnistusta tarvitaan esimerkiksi henkilön iän varmistamiseen palveluissa, joihin on asetettu ikärajoja. Ilman kehittyneitä tunnistusmenetelmiä ikärajojen valvominen on lähes mahdotonta ja siksi esimerkiksi tupakan ja alkoholin myynti Internetin välityksellä on Suomessa kiellettyä.

PGP:llä ei voida saavuttaa elektronisen liiketoiminnan vaatimaa sähköistä tunnistusta, koska PGP:ssä tunnistus perustuu lähes pelkästään muihin kuin tietoverkosta saatuihin tietoihin (out-of-band). Tähän on suurimpana syynä PGP-sertifikaatit, joiden autenttisuutta ei voida sähköisesti varmistaa ja joissa henkilön tunnisteena on ainoastaan tämän sähköpostiosoite. TTP:tä hyödyntävissä varmentajajärjestelmissä osapuolten luotettava tunnistus on sen sijaan mahdollista.

Toisaalta edellä mainitusta syystä PGP:llä voidaan saavuttaa rajoitettu anonymiteetti sähköiseen asiointiin. Koska PGP:ssä käyttäjän identifioivana ominaisuutena on hänen sähköpostiosoitteensa, voidaan käyttää valesähköpostiosoitteita jonkin asteisen anonymiteetin saavuttamiseksi. Mutta koska PGP:n ei voida sanoa yleisesti soveltuvan sähköiseen kaupankäyntiin, ei tällä ole suurta merkitystä.

Kambil ja Van Heck (1998, 5) ovat määritelleet myös kiistämättömyyden tunnistusprosessiin kuuluvaksi. Sähköisessä kaupankäynnissä kiistämättömyydellä voidaan varmistaa se, että henkilö ei voi kiistää esimerkiksi ostaneensa jotain tuotetta elektronisesta kauppapaikasta. Tällä hetkellä sähköinen kauppa kuitenkin rinnastetaan lainsäädännön puolesta postimyyntiin. Tämä tarkoittaa sitä, että vaikka henkilö ei voi kiistää ostaneensa tuotetta, hänellä on kuitenkin oikeus perua kauppa määrätyn ajan sisällä kaupan teosta. Kuten aimmin todettiin, PKI:ssä vaaditaan kiistämättömyyden toteuttamiseen luotettuja kolmansia osapuolia eikä PGP:tä voida hyödyntää myöskään tästä syystä tunnistuksessa.

6.3 Laillistaminen

TTP:n läsnäolo helpottaa kaupan vahvistamista, kun asiakas esimerkiksi vahvistaa kaupan TTP:n varmentamalla sertifikaatilla tehdyllä digitaalisella allekirjoituksella. Näin myös laillistamisprosessin tietoturva paranee. Laillistamisprosessissa voidaan nähdä myös tapahtuman kiistämättömyydellä olevan merkitystä. Esimerkiksi digitaalisilla allekirjoituksilla voidaan sähköisessä kaupassa vahvistaa ostotapahtuma ja näin saavuttaa kyseisen tapahtuman kiistämättömyys. Digitaalinen allekirjoitus on myös

käytännöllisempi ja ennen kaikkea nopeampi ja turvallisempi keino vahvistaa kauppa kuin esimerkiksi paljon käytetyt sähköpostiviestit.

Kun puhutaan arvoltaan pienistä ostoksista Internetissä, ei asiakkaiden tunnistus ole usein kauppiaankaan näkökulmasta välttämätöntä vaan maksutapahtuman onnistumisen varmistus riittää. Siksi on mahdollista, että sellaistenkin varmentajajärjestelmin sertifikaatteja, joilta puuttuu viranomaistahon hyväksyntä, voitaisiin käyttää kauppatapahtuman laillistamisessa. Samalla tavoin voitaisiin käyttää PGP:tä. Tässä yhteydessä PKI toimisi siis vain luottamuksellisuuden, yksityisyyden ja tiedon eheyden varmistajana. Laillistamisprosessi ei siis välttämättä vaadi osapuolten vahvaa tunnistamista, mutta käytännössä vahvaa tunnistusta voidaan pitää edellytyksenä osapuolten luottamuksen saavuttamiseksi sähköisessä kaupankäynnissä.

6.4 Tuotteen esittely

Elektronisessa kaupankäynnissä voi syntyä tilanteita, joissa myös tuotteen esittelyssä vaaditaan jonkun prosessin osapuolen, tässä tapauksessa lähinnä asiakkaiden, luotettavaa sähköistä tunnistamista. Tällainen tilanne voi seurata esimerkiksi siitä, että kauppias haluaa esitellä tuotteitaan tai tehdä tarjouksia vain tietynlaisille asiakkaille. Tämä voi tulla esille vaikkapa sähköisessä kauppapaikassa, joissa yritysasiakkaat näkevät erilaisia ja erihintaisia tuotteita kuin tavalliset asiakkaat. Tällöin voidaan vaatia myös vahvaa tunnistamista riippuen tilanteesta. Yleisesti ottaen tuotteiden esittelyssä ei asiakkaita tarvitse tunnistaa. Asiakkaiden kannalta olisi kuitenkin toivottavaa, että he voisivat varmistua tuotteitaan esittelevän kauppapaikan oikeellisuudesta ja siksi esimerkiksi pelkkä palvelimen autentikoinnin mahdollistaman SSL-yhteyden muodostaminen asiakkaan ja verkkokaupan välille on tässä tapauksessa riittävä.

6.5 Kiistojen ratkaisu

Kiistojen ratkaisemiseksi elektronisessa liiketoiminnassa esiin tulevat selvimmin tapahtuman kiistämättömyys ja tapahtuman jäljitettävyys. Jotta ongelmatilanteissa

voidaan lakiin vedoten osoittaa, että henkilö on ollut osallisena johonkin tapahtumaan, täytyy taustalla olla PKI-järjestelmä, joka mahdollistaa lainvoimaisen tapahtuman kiistämättömyyden sekä tapahtumaan liittyvien osapuolten jäljitettävyyden. Tämän vuoksi PGP:hen perustuva PKI ei sovellu kaupankäyntiin, sillä esimerkiksi PGP-sertifikaatilla tehdyt digitaaliset allekirjoitukset eivät ole päteviä oikeudessa, koska ne eivät ole minkään viranomaisten hyväksymän luotetun kolmannen osapuolen varmentamia, eikä niillä voida tunnistaa henkilöä riittävän luotettavasti. Siksi varmentajapohjaisen PKI:n voidaan sanoa olevan ainut mahdollisuus sähköisessä liiketoimintaympäristössä. Kiistojen ratkaisu siis vaatii osapuolten vahvan tunnistuksen toimiakseen lainmukaisesti.

6.6 Arvotus

Arvotusprosessin käsittämässä hinnanmuodostuksessa tietoturvan osa-alueista esille nousee lähinnä henkilön sähköinen tunnistaminen. Hinnanmuodostus vaiheessa ei käyttäjien tarvitse välttämättä tietää toistensa identiteettiä, mutta järjestelmän, jossa hinnanmuodostus tapahtuu on pystyttyvä tunnistamaan sen käyttäjät pääasiassa väärinkäytösten estämiseksi. Tästä on esimerkkinä Huuto.net, jossa huutoja tehdäkseen käyttäjän on autentikoiduttava palvelulle. Käyttäjät eivät kuitenkaan tiedä myyjien, eikä toisten käyttäjien identiteettiä, vaan näkevät ainoastaan käyttäjien itsensä valitsemat käyttäjänimet, eli toisinsanoen käyttäjien pseudo-identiteetit. Vasta kaupan syntyessä järjestelmä paljastaa kaupan osapuolten oikeat identiteetit ostajalle ja myyjälle, jolloin he voivat keskenään sopia maksu- ja toimitusehdoista.

7 JOHTOPÄÄTÖKSET JA YHTEENVETO

Tässä luvussa esitellään tutkielman keskeisiä tuloksia ja johtopäätöksiä sekä lyhyt yhteenveto tutkielmasta.

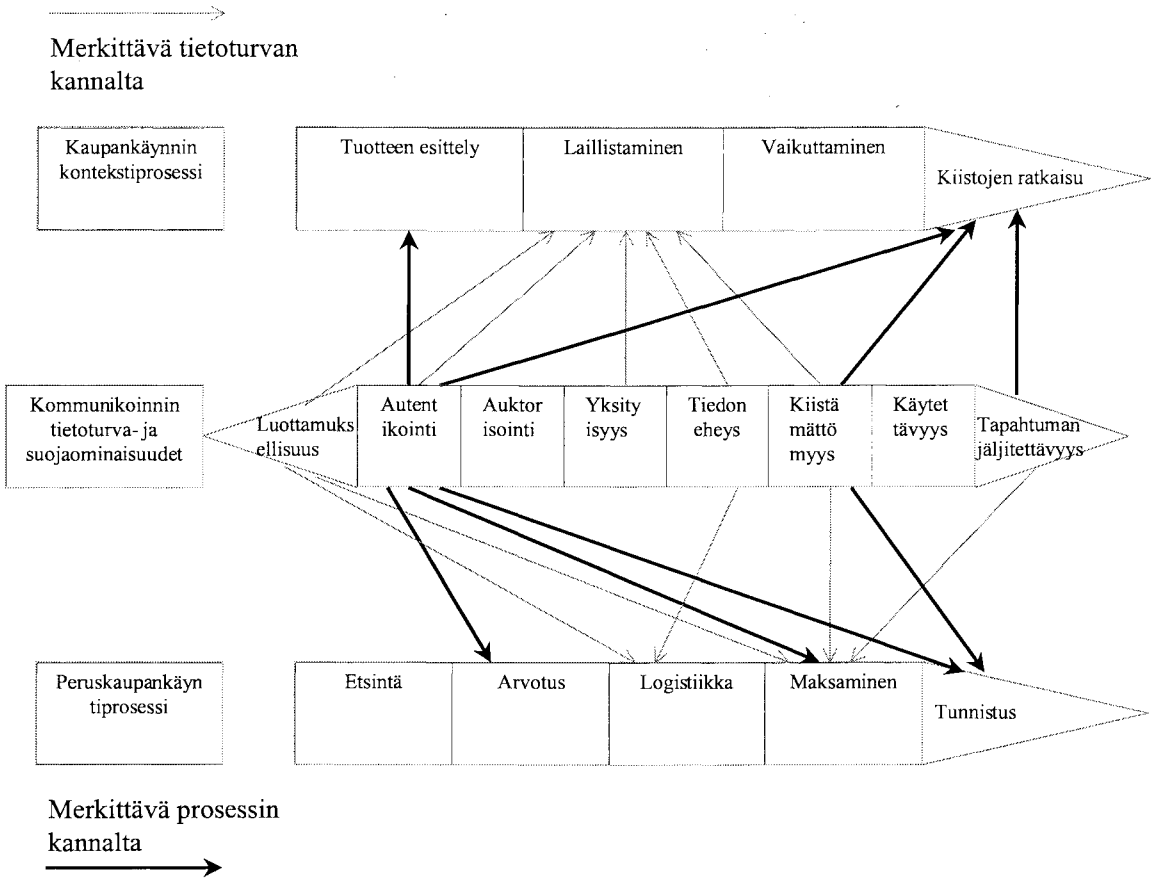
Otsikon kysymyksen asetteluun voidaan vastata, että toimikortit osana julkisen avaimen infrastruktuuria tarjoavat useita avaimia sähköisen kaupankäynnin ongelmiin, mutta osa ongelmista jää vielä ratkaisematta. PKI ja toimikortit eivät yhdessä eikä erikseen tarjoa lopullista ratkaisua elektronisen liiketoiminnan kaikkiin, tietoturvaan liittyviin ongelmiin, sillä tekniikat takaavat jo riittävän turvallisuustason. Ihmiset on koulutettava niiden käyttöön ja saatava ymmärtämään mitä ne käytännössä merkitsevät. Kuten on jo todettukin, mikään järjestelmä ei voi sinällään taata ehdotonta turvallisuutta, mikäli ihmiset eivät osaa sitä käyttää.

Voidaan kuitenkin osoittaa, että jo nykyisillä menetelmillä saavutetaan elektronisen liiketoiminnan asettamat vaatimukset tietoturvalle ja siksi toimikorttien ja PKI-järjestelmien yhdistelmää voidaankin pitää yhtenä ratkaisuna elektronisen liiketoiminnan tietoturvaongelmiin. Ja vaikka näihin uusiin tekniikoihin liittyykin uusia uhkia ja riskejä, on niillä saavutetut edut kuitenkin riskejä suurempia. Loppujen lopuksihan käyttäjät arvioivat sen, onko hyödyillä suurempi painoarvo kuin riskeillä. Historia on jo osoittanut esimerkiksi matkapuhelinten tapauksessa, että käyttäjän kokema hyöty syrjäyttää uudet riskit. Ensimmäisten matkapuhelinten (NMT) salakuuntelu oli nimittäin varsin helppoa, ja periaatteessa kenen tahansa suoritettavissa verrattuna lankapuhelimiin, mutta matkapuhelimet yleistyivät silti erittäin nopeasti. Matkapuhelinten myöhempi tekninen kehitys poisti laajamittaisen ja amatöörimäisen salakuuntelun mahdollisuuden tarjoten silti samat saavutetut hyödyt, ja samanlainen kehitys on todennäköistä PKI:n ja toimikorttienkin kohdalla.

Kaupankäyntiprosessin osalta voidaan tämän tutkielman perusteella todeta, että sähköiseen kauppaan siirryttäessä prosesseja on uudistettava nykyisten tietoturvavaatimusten täyttämiseksi. Tässä yhteydessä PKI:n ja toimikorttien merkitys

tulee selvästi esille, kuten tutkielmassa on osoitettukin. Kaupankäyntiprosessin tarkastelussa havaittiin, että tietoturva on huomioitava useissa osaprosesseissa. Kuten seuraavasta kuvasta ilmenee, kommunikointiprosessin voidaan ajatella sisältävän kaikki tietoturvan osa-alueet. Sen vuoksi myös PKI:n ja toimikorttien vaikutuksen voidaan nähdä olevan selkeintä juuri kommunikoinnissa. Kuvasta käy ilmi myös tapa, jolla kommunikointi yhdistää kaupankäynnin kontekstiprosessin ja peruskaupankäyntiprosessin, kun asiaa tarkastellaan tietoturvan näkökulmasta. Kuvassa on eroteltu tietoturvan osien merkitys kaupankäynnin osaprosesseissa sekä itse prosessin, että tietoturvan kannalta. Merkittävyys prosessin kannalta tarkoittaa sitä, että sähköisessä kaupankäynnissä koko prosessi on suunniteltava uudelleen tietoturvan vaatimusten täyttämiseksi. Merkittävyys tietoturvan kannalta tarkoittaa puolestaan sitä, että kyseistä prosessia voidaan parantaa huomioimalla siihen liittyvät tietoturvan osa-alueet.

KUVA 6. Tietoturvan rooli kaupankäyntiprosessin osien yhdistämisessä



Tietoturvan osa-alueita ja kaupankäyntiprosesssia tarkasteltaessa havaittiin, että monissa tilanteissa vaaditaan henkilöiden vahvaa tunnistamista, jota ei voida PGP:llä saavuttaa. Tämän vuoksi voidaankin todeta, että ainoastaan varmentajiin perustuvat PKI-järjestelmät soveltuvat sähköiseen kaupankäyntiin, sillä ne täyttävät suurimman osan sähköisen kaupankäynnin asettamista tietoturvavaatimuksista. On kuitenkin mahdollista, että PGP- ja varmentaja-järjestelmät yhdistyvät siten, että esimerkiksi joku viranomaistaho varmentaa PGP-sertifikaatin. Näin PGP:lläkin voitaisiin saavuttaa henkilön vahva tunnistaminen ja tapahtumien kiistämättömyys, joita PGP ei normaalisti voi taata. Tällaista menettelyä on jo kokeiltu käytäntöönkin, mutta mitään tuloksia ei vielä ole saatavilla.

Tutkielmassa todettiin, että sähköinen kauppa vaatii mahdollisuuden anonyymiin asiointiin saavuttaakseen samanlaisen luottamuksen kuin perinteiset kaupankäyntimenetelmät, joissa esimerkiksi anonyymi maksaminen on yleistä ja helposti toteutettavissa. Nykyiset luotettua kolmatta osapuolta hyödyntävät varmentaja-järjestelmät, joilla anonyymiys voidaan toteuttaa, ovat kuitenkin usein viranomaistahoja. Niiden tavoitteena on kuitenkin henkilöiden vahva tunnistaminen, eikä anonyymiys ole yleensä mahdollista. Siksi voidaankin olettaa, että sähköistä kauppaa varten kehittyy omat varmenteja-järjestelmänsä, joissa anonyymi asiointi on mahdollistettu. Tämä tulee kuitenkin vaatimaan sen, että viranomaisten on voitava selvittää henkilöiden todelliset identiteetit väärinkäytösten ehkäisemiseksi ja selvittämiseksi.

Tutkielmassa esiteltiin yleisellä tasolla nykyisin käytössä olevia PKI-järjestelmiä sekä niissä havaittuja ongelmakohtia. Lyhyesti yhteen vedettynä voidaan todeta, että PKI-järjestelmät ovat lupaava ratkaisu elektronisen liiketoiminnan vaatimuksiin, mutta niiden laajempi yleistyminen jokapäiväiseen käyttöön näyttää oleva vielä tulevaisuutta johtuen osittain esitellyistä ongelmakohdista. Näistä ongelmista johtuen käyttäjät eivät vielä ole vakuuttuneita PKI-järjestelmien toimivuudesta ja turvallisuudesta eikä yleisesti ottaen tietoturvan merkitystä tunnuta vielä täysin ymmärtävän.

Näyttää myös siltä, että toimivan ja kattavan PKI:n rakentaminen on useissa tapauksissa liian kallis ja raskas prosessi saavutettavaan hyötyyn nähden tai tarkemmin sanottuna käyttäjien kokemaan hyötyyn nähden. Siksi yrityksen on syytä harkita tarkkaan, ottaako se PKI:n käyttöön tässä vaiheessa, kun PKI-järjestelmät eivät vielä ole kehittyneet sille tasolle, että niitä voitaisiin myydä valmiina ratkaisuina. Lisäksi ongelmana on kesken oleva standardointi, mikä aiheuttaa suurta epävarmuutta päätettäessä PKI:n rakenteesta, luottamussuhteista ja ennen kaikkea käytettävien sertifikaattien muodosta. Koko ajan yleistyvät toimikortit ja muut kryptografiset laitteet näyttävät kuitenkin tarjoavan ratkaisun osaan PKI:n ongelmista ja niiden käytön nähdäänkin olevan merkittävä tekijä PKI:n yleistymisen kannalta.

PKI-järjestelmät, kuten lähes kaikki muutkin tekniikat, käyvät läpi useita kypsyysvaiheita ennen yleistymistään jokapäiväiseen ja tavallisia ihmisiä koskettavaan

käyttöön. PKI:n voidaankin nähdä olevan vasta melko alkuvaiheessa, vaikka teoria on jo kymmeniä vuosia vanha. Tietokoneiden laskentatehon kehityksen mukanaan tuomat vahvat salausalgoritmit ja PKI:n käytännön sovellusten suunnittelu on kuitenkin vasta viime vuosina mahdollistanut PKI:n vakavammin otettavan hyödyntämisen. Lähitulevaisuus kuitenkin näyttää, onko PKI hehkutuksensa arvoinen ja tuleeko se olemaan koko elektronisen liiketoiminnan kulmakivi niin kuin on ennustettu.

PKI:tä ja toimikortteja sekä niiden ongelmia tarkasteltaessa voidaan huomata, että useimmat ongelmat ovatkin pääosin asenteellisia ja "poliittisia". PKI ja etenkin toimikortit voidaankin nähdä teknisessä mielessä jo varsin kehittyneinä ja kypsinä laajaa käyttöönottoa ajatellen. Yhteiset standardit ja käytännöt ovat kuitenkin vielä niin puutteellisia, että nyt valmiina olevien ratkaisujen tulevaisuuden näkymät ovat hämärät, sillä ei voida vielä varmaksi sanoa mitkä tekniikat ja käytännöt tulevat saavuttamaan yleisen standardin aseman. PKI:n todellinen läpimurto vaatii siis vähintään valtioiden välisiä yhteisiä päätöksiä esimerkiksi EU:n sisällä, mutta ideaalista olisi jos saataisiin luotua koko maailman laajuisia PKI-rakenteita.

Tutkielmassa todettiin, että luottamus on oleellinen osa elektronista liiketoimintaa. Kun perinteisestä liiketoiminnasta siirrytään elektroniseen, ei luottamusta voidakaan välttämättä enää synnyttää totutuilla menetelmillä. Kaupankäynnin osapuolet eivät enää voi tunnistaa toisiaan konkreettisesti, eivätkä voi olla täysin varmoja saamiensa tietojen paikkansapitävyydestä. Tässä tutkielmassa on kuitenkin esitetty keinoja, joilla käyttäjien luottamusta elektroniseen liiketoimintaa voidaan vahvistaa. Tärkeimmäksi käsitteeksi on muodostunut tietoturva eri osa-alueineen. Tutkielmassa onkin määritelty tämän päivän elektronisen liiketoiminnan asettamat vaatimukset tietoturvalle ja etsitty ratkaisuja niiden saavuttamiseksi. Tärkeimpänä tietoturvaa parantavana menetelmänä on esitetty toimikorttien käyttäminen osana PKI-järjestelmiä, jolla voidaan täyttää varsin hyvin elektronisen liiketoiminnan vaatimukset. Tutkielmassa on myös esitelty lukuisia ongelmia, joita tähän menetelmään liittyy, mutta on todettu, että ongelmista huolimatta menetelmä on käytännön tasolla riittävän hyvä turvallisen sähköisen kaupankäynnin mahdollistamiseksi.

Tämä tutkielma on ensimmäinen yritys jäsentää teoriatasolla sähköistä kaupankäyntiprosessia tietoturvan näkökulmasta ja soveltaa PKI:tä ja toimikortteja vaaditun tietoturvan saavuttamiseksi. Tästä johtuen mitään tietoturvan osa-aluetta tai tiettyä kaupankäynnin osaprosessia ei ole käsitelty kovin tarkasti eikä perusteellisesti. Tutkielmasta käy kuitenkin ilmi, että kaikki mainitut seikat ovat merkityksellisiä sähköisten kaupankäyntiprosessien uudelleensuunnittelussa ja ne tulevat vaatimaan laajempia selvityksiä.

LÄHTEET

Kirjallisuus ja artikkelit

Abdalla M., Reyzin L., A New Forward-Secure Digital Signature Scheme, Advances in Cryptology – Asiacrypt 2000, Lecture Notes in Computer Science, vol. 1976, December 1, 2000, 1 – 18. [viitattu 10.7.2001]. Saatavilla WWW-muodossa <http://theory.lcs.mit.edu/~cis/pubs/reyzin/forwardsig.pdf>

Adams C., Burmester M., Desmedt Y., Reiter M., Zimmerman, P., Which PKI (Public Key Infrastructure) is the Right One? (panel discussion), in Proceedings of the 7th ACM conference on Computer and communication security, Athens, Greece, November 1 - 4, 2000, 98 - 101. [viitattu 18.5.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/proceedings/commsec/352600/p98-adams/p98-adams.pdf>

Anderson R., Why cryptosystems fail, Communications of ACM, Vol 37, Issue 11, 1994, 32 – 40. [viitattu 18.5.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/journals/cacm/1994-37-11/p32-anderson/p32-anderson.pdf>

Bakker B., A Portable Solution for Mutual Authentication, graduation report, faculty of information technology & systems, Harbinger BV, Rotterdam, Netherlands, January, 1999. [viitattu 23.5.2001]. Saatavilla WWW-muodossa <http://speeltuin.lifeline.nl/~bastiaan/smartcard/GraduationReport.doc>

Barton D., Moran A., O'Connor L., Design issues in PKI, Australia 1997. [viitattu 29.5.2001]. Saatavilla WWW-muodossa <http://security.dstc.edu.au/papers/PKIDesignIssues/PKIPaper.html>

Branchaud M., A Survey of Public-Key Infrastructures, Department of Computer Science, McGill University, Montreal, 1997. [viitattu 28.12.2001]. Saatavilla WWW-muodossa < http://home.xcert.com/~marcnarc/PKI/thesis/Thesis.doc>

Cooper D., A model of certificate revocation, In Proceedings of the Fifteenth Annual Computer Security Applications Conference, December, 1999, 256-264. [viitattu 7.11.2001]. Saatavilla WWW-muodossa <http://csrc.ncsl.nist.gov/pki/documents/acsac99.pdf>

Deng R., Han Y., Jeng A., Ngair T., A new on-line cash check scheme, In the proceedings of the 4th ACM conference on Computer and communication security, Zurich, Switzerland, April 1 – 4, 1997, 111 - 116. [viitattu 8.5.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/proceedings/commsec/266420/p111-deng/p111-deng.pdf>

Ellison C., Schneier B., Risks of PKI: Secure Email, Communications of ACM, Vol. 43, Issue 1, 2000, 160. [viitattu 18.5.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/journals/cacm/2000-43-1/p160-ellison/p160-ellison.pdf>

Ellison C., Schneier B., Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, Computer Security Journal, Vol. 16, No 1, 2000, 1-7. [viitattu 8.5.2001]. Saatavilla WWW-muodossa <http://www.counterpane.com/pki-risks.pdf>

Guthery S., Jurgensen T., 1998. Smart Card Developer's Kit. Indianapolis, USA: Macmillan Technical Publishing

Halevi S., Krawczyk H., Public-key cryptography and password protocols, in proceedings of the 5th ACM conference on computer and communication security, San Francisco, CA USA, November 2 – 5, 1998, 122 – 131. [viitattu 1.11.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/citations/proceedings/commsec/288090/p122-halevi/>

He Q., Sycara K., Finin T., Personal security agent: KQML - based PKI, in proceedings of the second international conference on Autonomous agents, Minneapolis, USA,

May 10 – 13, 1998, 377 – 384. [viitattu 8.5.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/proceedings/ai/280765/p377-he/p377-he.pdf>

Hendry M., 1997. Smart Card Security and Applications. Boston, London: Artech House.

Herreweghen E., Wille U., Risks and Potentials of Using EMV for Internet Payments, in the USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10 – 11, 1999. [viitattu 7.11. 2001]. Saatavilla WWW-muodossa <http://www.usenix.org/events/smartcard99/full_papers/herreweghen/herreweghen.pdf>

Herzberg A., Jakobsson M., Jarecki S., Krawczyk H., Young, M., Proactive Public Key and Signature Systems, In the proceedings of the 4th ACM conference on Computer and communication security, Zurich, Switzerland, April 1 – 4, 1997, 100 – 110. [viitattu 4.7.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/proceedings/commsec/266420/p100-herzberg/p100-herzberg.pdf>

Järvelä P., Tinnilä M., Elektronisesta kaupasta eLiiketoimintaan, Digitaalisen median raportti 1/2000, Tekes, Helsinki, 2000. [viitattu 5.10.2001]. Saatavilla WWW-muodossa <http://www.hkkk.fi/~lsaarine/1_00_ekauppa.pdf>

Jøsang A., Trust Management for e-Commerce, In Proceedings of the International Symposium on Information Theory Sorrento, Italy, June 2000. [Viitattu 29.10.2001]. Saatavilla WWW-muodossa <http://security.dstc.edu.au/papers/virtbank2k.pdf>

Jøsang A., Møllerud P., Cheung E., Web Security: The Emperor's New Armor, In the proceedings of the European Conference on Information Systems, (ECIS2001), Bled, Slovenia, June 2001. [viitattu 16.8.2001]. Saatavilla WWW-muodossa <http://security.dstc.edu.au/papers/websec.pdf>

Kambil A., Van Heck E., Reengineering the Dutch Flower Auctions: A Framework for Analyzing Exchange Organizations, Information Systems Research, Vol. 9, No.1,

March 1998. [viitattu 4.10.2001]. Saatavilla WWW-muodossa <www.hkkk.fi/~tuunaine/37d070/kambil_vanheck_isr.pdf>

Kerttula E., 1999. Tietoverkkojen tietoturva. Helsinki: Oy Edita Ab.

Kohlas R., Maurer U., Confidence Valuation in a Public-Key Infrastructure Based on Uncertain Evidence, In the proceedings of Public Key Cryptography 00, Lecture Notes in Computer Science, Vol. 1751, Jan 2000, 93 – 112. [viitattu 29.5.2001]. Saatavilla WWW-muodossa <ftp://ftp.inf.ethz.ch/pub/publications/papers/ti/isc/wwwisc/KohMau00.pdf>

Laine J., 2001. Verkkokauppaoikeus. Helsinki: WSOY

Maurer U., Modelling Public – Key Infrastructure, Proc. 1996 European Symposium on Research in Computer Security (ESORICS' 96), Lecture Notes in Computer Science, Springer-Verlag, vol. 1146, pp. 325-350, 1996. [viitattu 29.5.2001]. Saatavilla WWW-muodossa <ftp://ftp.inf.ethz.ch/pub/publications/papers/ti/isc/wwwisc/Maurer96b.pdf>

Menezes A., Oorschot P., Vanstone S., Handbook of applied Cryptography, 1999, Waterloo, Ontario, Canada. [viitattu 11.10.2001]. Saatavilla www-muodossa <http://cacr.math.uwaterloo.ca/hac/>

Ojala P., Sähköisen kaupankäynnin tietoturva ja sen vaikutukset maksukäytäntöjen käyttäjäystävällisyyteen, Working papers series B 57, University of Oulu, Infotech Research Center, Department of Information Processing Science, Oulun Yliopistopaino, 1998.

Patton M., Jøsang A., Technologies for Trust in Electronic Commerce, In the proceedings of the IFIP working conference on E-Commerce, Salzburg, Austria, June 2001. [viitattu 7.11.2001]. Saatavilla WWW-muodossa <http://security.dstc.edu.au/papers/technotrust.pdf>

Rankl W., Effing W., 1997. Smart card handbook. West Sussex, England: John Wiley & Sons Ltd.

Reiter M., Franklin M., Lacy J., Wright R., The key management service, In the proceedings of the 3rd ACM conference on Computer and communication security, New Delhi, India, March 14 – 15, 1996, 38 – 47. [viitattu 4.7.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/proceedings/commsec/238168/p38-reiter/p38-reiter.pdf>

Schneier B., Shostack A., Breaking up is hard to do: Modeling security threats for smart cards, USENIX Workshop on Smart Card Technology, USENIX Press, 1999, 175-185. [viitattu 29.5.2001]. Saatavilla WWW-muodossa <http://www.counterpane.com/smart-card-threats.pdf>

Steinauer D., Wakid S., Rasberry S., Trust and traceability in electronic commerce, StandardView, Vol. 5, Issue 3, 1997, 118 – 124. [viitattu 18.5.2001]. Saatavilla WWW-muodossa <http://www.acm.org/pubs/articles/journals/standardview/1997-5-3/p118-steinauer/p118-steinauer.pdf>

Whitten A., Why Johnny Can't Encrypt: A Usability Evaluation pf PGP 5.0, The 8th USENIX Security Symposium, Washington D.C., USA, August 23 – 26, 1999. [viitattu 31.12.2001]. Saatavilla WWW-muodossa <http://www-2.cs.cmu.edu/~alma/johnny.pdf>

Elektroniset julkaisut

Helsingin kauppakamari, Tietoyhteiskunta 2000+ projektin raportti, Selvitys PK-yritysten sähköisen liiketoiminnan tarpeista, Edita Oyj, elokuu 2001. [Viitattu 25.10.2001]. Saatavilla WWW-muodossa <http://www.helsinki.chamber.fi/asiakas/HKK/aloitus.nsf/273ecf27fbf309a6c225

6786003e2b14/b0be226160aa81e1c2256ab70027667b/$FILE/selvitys+tietoyhteiskunta.pdf>

Lange J., E-Commerce Audit Trails, UW-Madison Internal Audit, May 11, 1999. [Viitattu 26.10.2001]. Saatavilla WWW-muodossa <http://www.wisc.edu/architest/teams/ecommerce/e_commerce.html>

Leinonen H., Re-engineering Payment Systems for the E-world, Suomen Pankin keskustelualoitteita, Suomen Pankki, Helsinki, Finland 29.11.2001. [Viitattu 26.10.2001]. Saatavilla WWW-muodossa <http://www.fininter.net/payments/Bank%20of%20Finland.pdf>

Liikenneministeriö, TIVEKE - Liikenneministeriön kansallinen tietoverkkojen kehittämisohjelma, Tiveke 2 -työryhmä: Tietoturva tietoverkoissa, 18.3.1998. [viitattu 18.9.2001]. Saatavilla WWW-muodossa <http://palvelut.tieke.fi/arkisto/tiveke/turva.htm>

Väestörekisterikeskus, Sähköiseen henkilökorttiin ja varmenteisiin liittyviä standardeja, 2002. [viitattu 14.1.2002]. Saatavilla WWW-muodossa <http://www.fineid.fi/default.asp?path=4%2CTekniikka%2F8%2CStandardit&file=1%2CStandardit%2Ehtml&template=>

LIITE 1. Kryptografia

Tässä luvussa käsitellään kryptografiaa yleisellä tasolla historiasta ja perusteoriasta tämän hetkisiin sovelluksiin. Kryptografia on tämän tutkielman taustateoria, johon perustuvat niin PKI-järjestelmät kuin toimikortitkin. Kryptografian erilaisista sovelluksista käsitellään pääasiassa tutkielman kannalta oleellisinta julkisen avaimen kryptografiaa, mutta myös lyhyesti salaisen avaimen kryptografiaa, digitaalista allekirjoitusta ja Hash-funktioita.

Käsite kryptologia, joka tarkoittaa salakirjoitustiedettä, sisältää kryptografian ja kryptoanalyysin. Kryptografian ymmärretään usein tarkoittavan vain salakirjoitusta, mutta sillä on kuitenkin hieman laajempi merkitys. Kerttulan (1999, 23) mukaan käsitteellä kryptografia tarkoitetaan tietoturvaan liittyviä matemaattisia menetelmiä ja se on määritelty seuraavasti: "Kryptografia tarkoittaa tietoturvapalveluihin, kuten tiedon tai siirron luottamuksellisuuteen, tiedon eheyteen, olion autenttisuuteen tai tiedon alkuperän autenttisuuteen, liittyvien matemaattiseten menetelmien tutkimusta." Kryptoanalyysillä puolestaan tarkoitetaan kryptografian käänteisoperaatioita eli lähinnä koodien purkamista.

Kryptografia ei kuitenkaan ole ainoa keino tietoturvan saavuttamiseen, vaan lähinnä yksi kokoelma tekniikoita, joilla tietoturvaa voidaan rakentaa. Kryptografialle on määritelty neljä pääasiallista tavoitetta, jotka ovat luottamuksellisuuden, tiedon eheyden, tiedon ja henkilöiden autenttisuuden sekä kiistämättömyyden saavuttaminen. Näiden tavoitteiden täyttämisellä kryptografia pyrkii estämään ja havaitsemaan kaikenlaisen tietoon liittyvän väärinkäytön ja huijauksen.(Menezes 1996, 4)

Kryptografia on tekniikkana hyvin vanha ja sen juuret juontuvat Egyptiin neljän tuhannen vuoden taakse. Kryptografian pääasiallisin käyttö on ollut sodankäynnissä ja se on näytellyt merkittävää roolia muun muassa molempien maailmansotien lopputuloksessa. Suurimpia kehitysaskeleita kryptografian kehityksessä on ollut DES (Data Encryption Standard) algoritmi, joka kehitettiin 1970 luvun alussa ja otettiin

käyttöön ensi kertaa vuonna 1977. Siitä lähtien se on ollut käytössä ympäri maailmaa ja on tunnetuin kryptografinen mekanismi historiassa. Vaikka DES on onnistuttu murtamaan, voidaan sitä pitää yhä turvallisena, sillä murtamiseen ei ole mitään yksinkertaista metodia. Ainoa onnistunut murtotapa onkin ollut raan voiman (brute force) hyökkäys, joka on vaatinut kymmenien tuhansien koneitten kuukausien työn. Raan voiman hyökkäyksessä kokeillaan kaikkia mahdollisia avaimia tietyn salaviestin avaamiseen ja se on siksi erittäin raskas ja rikollisten ulottumattomissa oleva menetelmä. Tärkeän tiedon turvaamiseksi avaimia kannattaa silti vaihtaa usein ja suojata avaimet hyvin. Erittäin tärkeän tiedon pitkäaikaiseen turvaamiseen kuitenkin suositellaan jo Triple-Des:n käyttöä, jossa viesti salataan kolmeen kertaan DES-algoritmiä hyödyntäen.

Eniten tämän päivän kryptografiaan vaikuttanein kehitysaskel on kuitenkin julkisen avaimen kryptografia, jonka Diffie ja Helman esittelivät teoksessaan 'New Directions in Cryptography'. Vuonna 1978 Rivest, Shamir ja Adleman keksivät ensimmäisen käytännöllisen julkisen avaimen salaus- ja allekirjoitusmenetelmän, joka tunnetaan nykyisin nimellä RSA. (Menezes 1996, 1-2).

Kryptografiasta voidaan erottaa kaksi peruskomponenttia, jotka ovat algoritmi tai kryptografinen metodologia ja avain. Nykyisissä järjestelmissä algoritmit ovat monimutkaisia matemaattisia kaavoja ja avaimet bittijonoja. Kryptografian tyypillisimpiä sovelluksia tänä päivänä ovat avainten hallinta ja digitaaliset allekirjoitukset (Maurer 1996, 3). Tosin Reiterin ym. (1996, 38) mukaan juuri avainten hallintaan liittyvät ongelmat ovat suurimpana esteenä kryptografian laajemmalle hyödyntämiselle. Näitä ongelmia käsitellään tutkielman varsinaisissa luvuissa.

Vaikka kryptografia onkin jo vanhaa tekniikkaa ja se voidaan periaatteessa rinnastaa perinteisiin insinöörialoihin kuten lentokoneteollisuuten, niin siihen liittyy silti lukuisia ongelmia, joita ei enää perinteisillä aloilla esiinny. Tämä johtuu suurelta osin siitä, että kryptografia ei ole saavuttanut samanlaista kypsyystasoa kuin muut yhtä vanhat insinöörialat. Andersonin (1994, 32) mukaan tähän on suurimpana syynä se, että kryptografiaan perustuvat kryptosysteemit eivät ole käyneet läpi samanlaista "julkista oppimista" kuin monet muut insinöörialat. Kun esimerkiksi lentokone putoaa, niin

tapaus on lähes aina julkinen ja sitä tutkivat monien alojen asiantuntijat. Tulokset ja mahdollinen syy onnettomuuteen leviää ympäri maailmaa, jolloin lentokoneen valmistajat voivat oppia uutta ja varautua vastaaviin ongelmiin. Kryptosysteemit ovat sen sijaan olleet pääasiassa sotilaskäytössä ja siksi tarkkaan varjeltuja salaisuuksia. Tämän vuoksi samoja virheitä toistetaan jatkuvasti kaikkialla, koska "julkista oppimista" ei ole päässyt tapahtumaan ja kryptografiaa voidaankin siten pitää vasta varsin uutena, kypsymättömänä alana.

Kryptografian turvallisuutta on usein kyseenalaistettu perustuen siihen tosiasiaan, että vaikka tietokoneistettu systeemi olisi kuinka turvallinen tahansa, niitä suunnittelemassa, toteuttamassa ja käyttämässä ovat aina ihmiset. Tämä tuo mukaan inhimillisen tekijän, jonka jälkeen systeemin turvallisuutta on arvioitava uudelleen. Andersonin (1994, 37) mukaan kryptosysteemejä kehitellään pääasiassa "high-tech" hyökkäyksiä vastaan, mutta kuten todettiin, todelliset uhkat ovat paljon yksinkertaisempia ja inhimillisempiä.

Kryptografisten menetelmien yleistymistä on haitannut suuresti muun muassa USA:n vientirajoitukset ja kansainväliset patentit. USA:lla oli vuoden 1998 loppuun asti vientirajoitus, jonka mukaan vain 56-bittisiä tai sitä lyhyempiä DES-avaimia sai viedä ulos maasta. Tämän takia useimmat tietoturvaohjelmistot, joiden suurin tuottaja on USA, tarjosivat vain suhteellisen heikon tietosuojan. Nykyisin raja on nostettu jo 2048 bittiin, mutta rajoitukset ovat siis edelleen olemassa.

Vuonna 1998 33 keskeisintä teollisuusmaata allekirjoitti Wassenaar-sopimuksen, joka koskee vahvaa salausteknologiaa sisältävien tuotteiden maastavientiä. Tämän sopimuksen mukaisesti voidaan maasta yleensä viedä vain enintään 56 bitin symmetrisen avaimen ja 512 bitin asymmetrisen avaimen algoritmeillä varustettuja kryptojärjestelmiä. Wassenaar-sopimus onkin saanut kritiikkiä ympäri maailmaa, sillä sen pelätään hankaloittavan salaustuotteiden vapaata markkinakehitystä ja liiketoimintaa sekä rajoittavan vapaata vahvojen salausalgoritmien käyttöä ja rajoittavan siten myös yksilön suojaa. (Kerttula 1999, 57)

Myös patentit ovat haitanneet salausteknologian kehitystä, sillä lähes kaikki tietoturvaan liittyvät tuotteet ja etenkin kryptografiset algoritmit ovat patentoituja. Suurin osa

patenteista on kuitenkin 70-luvun lopulta ja 80-luvun alusta, joten ne ovat jo rauenneet tai lähiaikoina raukeamassa. Tärkeimpänä tapahtumana patenttien osalta viimeaikoina voidaan pitää RSA-patentin raukeamista syyskuussa 2000. Tämän uskotaan olevan merkittävin tapaus kryptografian yleistymisen kannalta. Mitään mullistuksia ei tosin ole vieläkään tapahtunut.

Kryptografian yhteydessä tulevat lähes poikkeuksetta esiin avaimet. Menezes (1997, 12) esittää kysymyksen: "Mihin avaimia yleensä tarvitaan, kun tietoa voitaisiin salata käyttämällä tiettyä kryptografista funktiota ja salauksen purkuun voitaisiin käyttää kyseisen funktion vastinetta?" Avainten käyttö on kuitenkin helposti perusteltavissa sillä, että käytettäessä avaimia ei jonkun tietyn kryptografisen funktioparin paljastumisen johdosta tarvitse suunnitella koko salausmenetelmää uudelleen, vaan pelkkä avainten vaihtaminen riittää tietoturvan säilyttämiseksi (Menezes 1997, 12). Seuraavissa alaluvuissa käsitelläänkin avaimiin perustuvaa kryptografiaa.

Salaisen avaimen kryptografia

Salaisen avaimen kryptografian, jota kutsutaan myös symmetrisen (salaus- ja purkuavain samat) avaimen kryptografiaksi, mallit perustuvat jaettuun salaisuuteen (shared secret), eli kumpikin osapuoli tietää jonkun salaisuuden, jota muut eivät tiedä ja he voivat siten varmistua toistensa antamista tiedoista tämän salaisuuden perusteella. Tällainen salaisuus on yleensä salainen avain, joka täytyy olla molempien osapuolien hallussa ja sen siirto on tapahduttava jotain turvallista menetelmää käyttäen. Turvalliseksi voidaan laskea vastapuolen kanssa kasvokkain tapahtuva avainten vaihto tai esimerkiksi kirjattu kirje, jolla on lain takaama suoja.

Salaisen avaimen menetelmät ovat vanhimpia kryptografian sovelluksia ja ne voidaan jakaa rakenteensa puolesta jonosalaajiin ja lohkosalaajiin. Klassiset salausmenetelmät ovat pääasiassa merkki kerrallaan toimivia jonosalaajia. Jonosalaajat ovat vielä nykyäänkin tärkeitä etenkin suurta nopeutta vaativassa reaaliaikaisessa salauksessa. (Kerttula 1999, 73-74)

Jonosalaajia ovat esimerkiksi korvaussalaajat ja sekoitussalaajat. Korvaussalaaja toimii siten, että selväkieli- ja salasanoman merkit saavat arvoja samasta merkkijoukosta. Kullakin salaisen avaimen valinnalla selväkielisanoman kukin merkki korvataan salasanoman kiinteällä "substituutilla". Tästä esimerkkinä on Julius Caesarin salaaja, jolla selväkielitekstin kirjain korvattiin siitä esimerkiksi kolmen merkin päässä olevalla toisella kirjaimella. Sekoitussalaajat toimivat puolestaan siten, että salasanoman lohko on kullakin salaisen avaimen valinnalla selväkielisanoman lohkon kiinteä permutaatio ja sala- ja selväkielisanoman merkkijoukot ovat samat. Klassisissa lohkosalaajissa salataan tekstiä vähintään kaksi merkkiä kerrallaan ja ne voivat toimia myös korvaussalaajina. (Kerttula 1999, 61,74, 76-78)

Edellämainittujen aakkosiin perustuvien salaajien lisäksi on tietokoneiden synnyttyä kehitetty binäärisiä salaajia, jotka ovat tehokkaampia ja monipuolisimpia kuin edeltäjänsä. Tosin tietokoneiden kehittyminen on helpottanut niiden murtamistakin. Tunnetuin binäärinen salausmenetelmä on vuonna 1918 kehitetty ns. Vernam-menetelmä. Tätä menetelmää käytettiin reikänauhakoneissa siten, että salattavan sanomareikänauhan kanssa syöttiin samanaikaisesti siihen synkronoitu avainreikänauha, joka salasi sanoman satunnaisesti bitti bitiltä. Vastaanotossa käytettiin identtistä avainreikänauhaa salasanoman purkamiseen. Tätä menetelmää kutsutaan myös nimellä "one-time system" koska jokaista avainta käytetään vain kerran. Menetelmä on teoriassa ainoa tunnettu täydellisesti salaava menetelmä, jota ei voida koskaan murtaa riippumatta murtautujan käyttämästä menetelmästä. Tämä kuitenkin pitää paikkansa vain silloin, kun seuraavat ehdot täyttyvät: Murtautuja ei tiedä bittiäkään salattavasta sanomasta, avaimen pituuden on oltava yhtä pitkä kuin salattavan sanoman, avaimen on oltava täysin satunnainen ja kutakin avainta saa käyttää vain kerran salaamiseen ja purkuun. Tällainen menetelmä on ollut käytössä Moskovan ja Washingtonin välisellä "kuumalla linjalla" 80-luvulla. Tällä hetkellä käytettävistä binäärisistä menetelmistä tunnetuin on DES. (Kerttula 1999, 78)

Salaisen avaimen menetelmiin kuuluvat myös tulosalaajat, jotka muodostuvat kahdesta tai useammasta yksinkertaisemman salaajan peräkkäin soveltamisesta. Useimmiten tulosalaajissa käytetään vuorotellen korvaus- ja sekoitussalaajia. Tulosalaajissa hyödynnetään involuutioita eli funktioita f(x), joissa funktio on kaikilla x:n arvoilla

itsensä käänteisfunktio eli f(f(x))=x. Korvaus- ja sekoitussalaaja voi olla involuutio, mikä on käytännöllistä, sillä jos kukin tulosalaajan komponentti on involuutio, salauksen purku voidaan toteuttaa samalla algoritmilla kuin salaaminenkin, mutta käänteisessä järjestyksessä. Tähän perustuu muun muassa DES-algoritmin käyttö sekä salaukseen että purkamiseen. (Kerttula 1999, 79)

Salaisen avaimen menetelmien suurimpana ongelmana on avainten hallinta ja jakelu. Jos otetaan esimerkiksi järjestelmä, jossa on n käyttäjää, ja missä kaikki haluavat lähettää salattuja sanomia kaikkien muiden kanssa, edellyttää N=n(n-1)/2 salaista avainta ja salaista kanavaa avainten jakeluun toisille käyttäjille. Jos käyttäjä aikoo vaihtaa avaimiaan, on hänen generoitava ja jaettava salaista kanavaa myöten n-1 uutta avainta. Ja jos verkkoon liittyy uusi käyttäjä, on hänen generoitava ja jaettava n uutta avainta. Salaisen avaimen järjestelmät eivät myöskään mahdollista digitaalisia allekirjoituksia luonnollisella tavalla. (Kerttula 1999, 157)

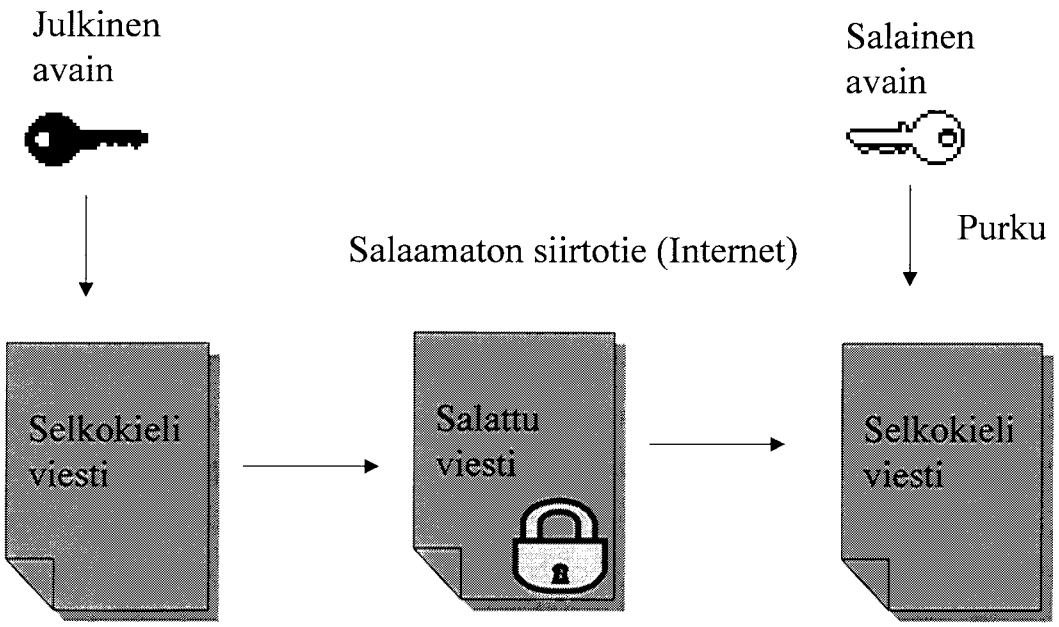
Edellämainittuihin ongelmiin löytyy ratkaisu julkisen avaimen kryptografiaan perustuvista järjestelmistä, joita käsitellään seuraavassa luvussa. Salaisen avaimen kryptografian järjestelmillä on kuitenkin paikkansa nykyaikaisissakin, julkisen avaimen kryptografiaan perustuvissa tietoturvaratkaisuissa, lähinnä tehokkuutensa ja lyhyempien avaintensa vuoksi. Salaisen ja julkisen avaimen tekniikoita käytetäänkin usein yhdessä. Koska julkisen avaimen kryptografia vaatii paljon enemmän laskentatehoa kuin salaisen avaimen kryptografia, käytetään julkisen avaimen kryptografiaa usein salaisten avainten vaihtamiseen, jolloin voidaan siirtyä salaisen avaimen kryptografiaan ja näin päästään pienempiin laskentatehovaatimuksiin ja säilytetään silti suuri turvallisuus.

Julkisen avaimen kryptografia

Julkisen avaimen kryptografia, josta käytetään myös nimitystä epäsymmetrisen avaimen kryptografia (salaus –ja purkuavain erilaiset), on tämän hetken tietoturvan

tärkein teknologia. Se on ensimmäinen tekniikka, joka mahdollisti salatun viestinnän ilman salaisen avaimen siirtoa lähettäjän ja vastaanottajan välillä. Tämä perustuu yksinkertaistetusti siihen, että viestin ja sen purkamiseen käytetyn avaimen perusteella ei voida selvittää viestin salaamiseen käytettyä avainta. Sama pätee myös toisinpäin.

KUVA 7. Julkisen avaimen kryptografia



Vaikka kryptografia onkin jo vanha tutkimusala, julkisen avaimen kryptografia on peräisin vasta 1970-luvun lopulta. Tämä johtuu osaltaan siitä, että salaisen avaimen kryptografiaa voitiin soveltaa ilman tietokoneita, kun taas julkisen avaimen kryptografia on laskennallisesti niin monimutkaista, että se vaati tietokoneiden kehittymistä. Asian uutuus selittää myös osaltaan sen, että vieläkään ei ole saatu kehitettyä täysin toimivaa julkisen avaimen kryptografiaan perustuvaa tietoturvajärjestelmää, joka olisi saavuttanut suurempaa suosiota ja käyttäjien yleistä hyväksyntää. Julkisen avaimen kryptografian teoria on melko yksinkertainen. Käytännön sovellukset ovat kuitenkin osoittaneet, että esimerkiksi täysin toimivien julkisten avainten infrastruktuurien rakentaminen onkin varsin monimutkainen ja monia ongelmia sisältävä tehtävä.

Julkisen avaimen kryptografia perustuu yksisuuntaisiin funktioihin, mikä tarkoittaa yksinkertaistetusti sitä, että funktio on helppo laskea yhteen suuntaan, mutta hankala selvittää toiseen suuntaan. Vaikka matemaattisesti todistettujen yksisuuntaisten funktioiden olemassaoloa ei ole todistettu, niin kuitenkin uskotaan (Kerttula 1999, 160).

Tunnetuin ja käytetyin julkisen avaimen algoritmi on 1977 kehitetty RSA (keksijöidensä Rivest, Shamir ja Aldeman mukaan). Julkisen avaimen tekniikka oli keksitty jo muutamaa vuotta aiemmin, mutta RSA oli ensimmäinen sitä hyödyntävä, toimiva salausmenetelmä. RSA perustuu yksinkertaiseen matemaattiseen totuuteen: kahden ison luvun kertominen keskenään on helppoa, mutta tämän ison luvun jakaminen tekijöihin on huomattavasti työläämpää. RSA:ssa kerrotaan keskenään alkulukuja, joiden tulona saatavaa suurta lukua on erittäin hankala jakaa takaisin tekijöihinsä. Salaisena avaimena toimii siis kaksi suurta alkulukua ja julkisena avaimena on niiden tulo.

Useasti ajatellaan, että julkisen avaimen kryptografia on turvallisempaa kuin salaisen avaimen. Esimerkiksi Kerttulan (1999, 157) mukaan kryptografisten algoritmien turvallisuus riippuu kuitenkin pelkästään avaimen pituudesta ja itse algoritmin laskennallisesta kompleksisuudesta. Niinpä riittävän pitkä symmetrinen avain voi olla turvallisempi kuin esimerkiksi asymmetrinen, turvallisena pidetty RSA-algoritmi.

Julkisen avaimen kryptografiaa hyödyntäviä ohjelmistoja ovat tällä hetkellä mm. Multipurpose Internet Mail Extensions (S/MIME), Transport Layer Security (TLS), Secure Socket Layer (SSL), Secure Shell (SSH) ja Internet Protocol Security (IPSec). Näistä kaikki ovat kuitenkin käytännössä hybridimenetelmiä eli ne käyttävät sekä julkisen- että salaisen avaimen kryptografiaa.

Herzbergin ym. (1997, 100) mukaan salaisen avaimen suojaaminen on julkisen avaimen kryptografian suurimpia turvallisuuden pullonkauloja etenkin tapauksissa, joissa samaa salaista avainta joudutaan säilyttämään muuttamattomana pitkiä aikoja. Tällaisten järjestelmien takana on usein tietoa, joka on arvokasta mahdollisille murtautujille, mikä lisää niihin kohdistuvien murtoyritysten määrää ja laatua. Edellä mainittu ei suinkaan ole ainoa julkisen avaimen kryptografiaan liitetty ongelma. Myös Adamsin ym. (2000,

98) mukaan julkisen avaimen kryptografiassa on selvästi havaittavissa kaksi autenttisuuteen liittyvää ongelmaa, jotka ilmenevät digitaalisten allekirjoitusten ja tiedon salauksen yhteydessä. Digitaalisten allekirjoitusten tapauksessa huijari voi tehdä valeavaimen ja saada viestin vastaanottajan uskomaan, että valeavain onkin jonkun muun julkinen avain. Tällöin vastaanottaja erehtyy luulemaan huijarin lähettämiä viestejä autenttisiksi ja jonkun muun lähettämiksi. Tiedon salauksen tapauksessa huijari voi vakuuttaa viestin lähettäjälle, että valeavain onkin vastaanottajan julkinen avain. Näin huijari pääsee avaamaan vastaanottajalle tarkoitettuja viestejä. Näihin ongelmiin on kuitenkin eräänä ratkaisuna julkisen avaimen sertifikaatit.

Digitaalinen allekirjoitus

Digitaaliselle allekirjoitukselle löytyy Kerttulan (1999) kirjasta ISO:n määritelmä (ISO 7498-2): "Sanoman digitaalinen allekirjoitus on sanomaan liitetty datalohko tai sanoman kryptografinen muunnos, mikä mahdollistaa sanoman alkuperän ja eheyden todentamisen sekä suojautumisen väärentämiseltä."

Digitaaliset allekirjoitukset ovat tällä hetkellä yksi tärkeimmistä tietoturvan osa-alueista ja siten myös tärkeä asia PKI-järjestelmissä. Niitä voidaan käyttää mm. sanoman kiistämättömyyteen, tiedon alkuperän varmistamiseen ja tiedon todistamiseen. Digitaaliset allekirjoitukset ovat merkittäviä erityisesti elektronisessa kaupankäynnissä ja sähköisissä viranomaispalveluissa, joiden perinteisissäkin muodoissa käsintehdyillä allekirjoituksillakin on ollut suuri painoarvo. Digitaalinen allekirjoitus on epäsymmetrisen kryptografian sovellus, sillä allekirjoitus muodostetaan eri avaimella kuin millä se todistetaan.

Jotta digitaalinen allekirjoitus olisi käytännöllinen, sen täytyy olla Menezesin (1997, 30) mukaan:

1. allekirjoittajan helposti laskettavissa eli allekirjoitusfunktion pitäisi olla helppokäyttöinen,

2. helposti kenen tahansa varmennettavissa eli varmennusfunktion tulisi olla helppokäyttöinen, ja

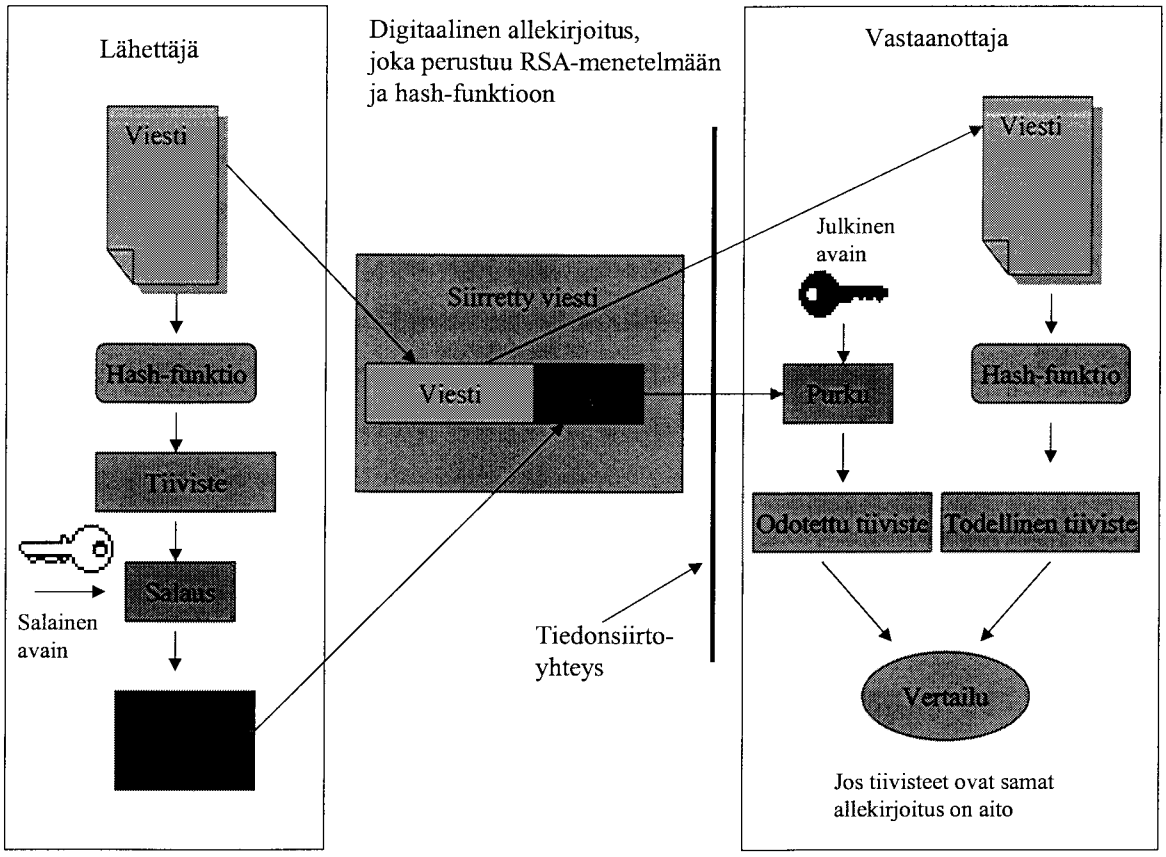
3. asiaan kuuluvan määräajan voimassa eli sen on oltava laskennallisesti turvallinen niin kauan, että allekirjoitus ei ole enää tarpeellinen alkuperäisessä yhteydessä.

Digitaalinen allekirjoitus toimii yksinkertaisimmillaan siten, että viestin lähettäjä salaa koko viestin salaisella avaimellaan ja julkaisee julkisen avaimensa. Nyt viestin voi avata kuka tahansa lähettäjän julkisella avaimella ja näin ollen varmistua siitä, että lähettäjä on juuri se kuka väittääkin olevansa, sillä salaukseen käytettävää avainta ei ole kenelläkään muulla. Tällainen menetelmä on kuitenkin raskas, koska koko viesti joudutaan salaamaan usein raskailla julkisen avaimen kryptografian avaimilla. Siksi digitaalisissa allekirjoituksissa käytetään lähes poikkeuksetta hash-funktioita, joilla saadut tiivisteet ovat ainoa salattava osa. Mikäli halutaan lisäksi varmistua siitä, että julkinen avain on autenttinen, tarvitaan varmenneinfrastruktuuria, missä luotettu kolmas osapuoli varmentaa käyttäjän ja hänen julkisen avaimen välisen yhteyden myöntämällään sertifikaatilla (Kerttula 1999, 292).

Digitaalisia allekirjoituksia voidaan tehdä myös käyttäen pelkkiä hash-funktioita. Tämä perustuu salaisten avainten käyttöön ja tapahtuu seuraavasti. Sekä sanoma että siihen liitetty salainen avain, joka on saatu varmentajalta, tiivistetään yhdessä hash-funktiolla ja lähetetään vastaanottajalle. Tiivistetty sanoman ja salaisen avaimen yhdistelmä toimii nyt digitaalisena allekirjoituksena. Vastaanottaja purkaa tiivisteen ja saa sekä sanoman että salaisen avaimen. Allekirjoitus voidaan nyt todentaa vertaamalla itsellä olevaa samaa salaista avainta vastaanotettuun purettuun avaimeen. Ongelmana on, että vastaanottajalla on oltava kopio salaisesta avaimesta. Salainen avain on siirrettävä jotain turvallista menetelmää käyttäen ja mikäli näin ei tapahdu, tämä menetelmä on periaatteessa helposti murrettavissa. Siksi sitä ei käytetä esimerkiksi elektronisessa kaupankäynnissä, jossa turvallisen avaimen siirtokanavan perustaminen asiakkaan ja kauppiaan on käytännössä lähes mahdotonta tai ainakin kannattamatonta. (Kerttula 1999, 292)

Yleisin ja turvallisin tapa käyttää digitaalisia allekirjoituksia on kuitenkin hash-funktioiden ja RSA-menetelmän yhdistäminen, joka on selvitetty myöhemmässä luvussa.

KUVA 8. Digitaalinen allekirjoitus



Digitaaliseen allekirjoitukseen käytettävää salaista avainta ei pitäisi koskaan varmuuskopioida tai muuten kahdentaa ja avain pitää tuhota aina käytöstä poistettaessa. Muuten väärien allekirjoitusten teko mahdollistuu. Digitaalisessa allekirjoituksessa käytettävän salaisen avaimen menetys ei kuitenkaan estä lukemasta allekirjoitettuja dokumentteja toisin kuin tiedon salaamiseen käytettävien avainten menetys. Salausavain onkin aina syytä olla varmuuskopioituna turvalliseen paikkaan. (Branchaud 1997, 7)

Hash-funktiot

Hash-funktioiden yleisimmät sovelluskohteet ovat digitaaliset allekirjoitukset ja tiedon eheyden varmistaminen. Menezes (1996, 33) on määritellyt hash-funktiot seuraavasti: Hash-funktio on laskennallisesti tehokas funktio, jolla voidaan tiivistää minkä tahansa mittainen binääriketju määrämittaiseksi binääriketjuksi, jota kutsutaan hash-arvoksi. Hash-funktioilla tai -algoritmeilla on muitakin nimiä, kuten kompressiofunktio tai kutistusfunktio. Hash-funktion käytön tuloksena syntyvästä hash-arvosta käytetään yleisimmin termiä sanoman tiiviste, mutta myös sormenjälki, kryptografinen tarkistussumma ja manipuloinnin ilmaisukoodi kuvaavat samaa asiaa (Kerttula 1999, 142).

Yleisimmät hash-algoritmit ovat MD5, joka käyttää 128 bitin mittaisia tiivisteitä ja SHA, jonka tiivisteen pituus on 160 bittiä ja jota voidaan siten pitää turvallisempana kuin MD5-algoritmia. SHA:ssa on myös parannettu MD5:ssä esiintyneitä heikkouksia, eikä sille tunnetakaan yhtään kryptografista murtomenetelmää. Molemmat algoritmit ovat toiminnaltaan samankaltaisia, nopeita ja tehokkaita toteuttaa ohjelmallisesti. Nykyisin laajassa käytössä on kuitenkin SHA-1 algoritmi, joka on vielä entisestään paranneltu. (Kerttula 1999, 142, 143)

Digitaalisissa allekirjoituksissa hash-funktioita käytetään seuraavasti. Allekirjoitettava viesti, joka on yleensä pitkä, tiivistetään määrämittaiseksi yleisesti saatavilla olevalla hash-funktiolla ja ainoastaan tuloksena saatu tiiviste allekirjoitetaan. Viestin vastaanottava osapuoli niin ikään tiivistää viestin samalla funktiolla, jonka jälkeen tiivisteiden allekirjoituksia voidaan verrata ja todeta viestin aitous ja muuttumattomuus. (Menezes 1996, 33)

Hash-funktioiden käytössä tulee huomata, että ainoastaan sellaiset hash-funktiot täyttävät tietoturvan vaatimukset, joissa on lähes mahdotonta löytää kahta erilaista viestiä, joiden tiivisteet ovat samanlaiset. Muuten olisi mahdollista, että viestin allekirjoittanut henkil, voisi myöhemmin väittää allekirjoittaneensa jonkun toisen viestin. Tämä taas sotisi kiistämättömyyden vaatimusta vastaan. Hash-funktion tulee myös olla sellainen, että tiivisteestä ei voi millään keinolla muodostaa alkuperäistä sanomaa. Tällaisia funktioita kutsutaan yksisuuntaisiksi hash-funktioiksi.

Hash-funktioiden toinen pääasiallinen käyttö, tiedon eheyden varmistaminen, toimii seuraavasti. Viestille lasketaan tiiviste tiettynä ajankohtana ja tiivisteen eheys varmistetaan jollain menetelmällä. Myöhempänä ajankohtana viestin muuttumattomuus voidaan varmistaa siten, että nykyiselle viestille lasketaan uusi tiiviste ja verrataan sitä alkuperäiseen tiivisteeseen. (Menezes 1996, 33)

Julkisen avaimen kryptografia tarjoaa aiemmista kryptografian sovelluksista selkeästi edukseen poikkeavan tavan salattuun ja turvalliseen viestintään. Julkisen avaimen kryptografian mahdollistamalla tiedon saluksella ja digitaalisilla allekirjoituksilla on jo nyt merkittävä rooli sähköisessä asioinnissa ja se tulee vielä kasvamaan tietoturvavaatimusten tiukentuessa. Nämä tulevatkin todennäköisesti olemaan merkittävimmät yksittäiset tekniikat tällä vuosikymmenellä elektronisen liiketoiminnan ja tietoturvan alueella.