

JULKISEN AVAIMEN JÄRJESTELMÄ OSANA  
TERVEYDENHUOLLON TIETOTURVAA

Minna Porali  
Pro gradu -tutkielma  
Tietojenkäsittelytiede  
Kuopion yliopisto,  
tietojenkäsittelytieteen laitos  
Joulukuu 2005

PORALI, M.: Julkisen avaimen järjestelmä osana terveydenhuollon tietoturva  
Pro gradu -tutkielma, 65 s.

Pro gradu -tutkielman ohjaajat: FT, professori Anne Eerola ja  
TtT, tutkimusjohtaja Anneli Ensio

Joulukuu 2005

---

Avainsanat: tietoturva, varmentaja, varmenne, sähköinen potilaskertomus, PKI

Sähköinen potilaskertomus, mukaan lukien potilastietojen sähköinen luovutus terveydenhuollon toimintayksikköjen välillä, on asettanut uusia vaatimuksia tietoturvan toteuttamiselle. Tietoja saavat käyttää vain ne, joilla on siihen oikeus. Tietoja siirrettäessä ne eivät saa joutua sivullisten käsiin ja tietojen tulee säilyä muuttumattomina. Yhtenä tietoturvan vaatimusten toteuttajana nähdään julkisen avaimen järjestelmä eli PKI.

Tässä tutkielmassa käsitellään tietoturva ja tietosuojaa sekä yleisellä tasolla että terveydenhuollon näkökulmasta. Salausmenetelmiä sivutaan lyhyesti, samoin turvallisuusinfrastruktuurin käsitettä. Molemmat edellä mainitut toimivat hyvänä johdantona julkisen avaimen järjestelmään. Julkisen avaimen järjestelmää kuvataan laajemmin, käsittäen muun muassa siihen kuuluvat osapuolet, joista tärkeimpinä mainittakoon varmentaja ja varmenne, ja sen tarjoamat ydinpalvelut. Tutkielmassa käsitellään julkisen avaimen järjestelmää terveydenhuollossa ja esitellään tilanteet, joissa PKI osaltaan mahdollistaa tietojen tietoturvallisen käytön.

Sähköisen potilaskertomuksen käyttäminen edellyttää käyttäjien todentamista. Se myös mahdollistaa tietojen luovutuksen, joka edellyttää potilaan suostumusta, jonka tulisi olla sähköisessä muodossa. Edelleen se mahdollistaa tietojen sähköisen arkistoinnin. Tietoturvaan liittyvät asiat ovat sähköisessä maailmassa erittäin tärkeitä ja voidaan edellyttää, että tietoturvan osalta kaikki noudattaisivat samoja, yhdessä sovittuja standardeja ja suosituksia.

## **Esipuhe**

Tämä tutkielma on tehty Kuopion yliopiston tietojenkäsittelytieteen laitokselle Tekesin FinnWell-tekniologiaohjelmaan kuuluvassa Avointa-hankkeessa vuoden 2005 aikana. Muita hankkeen rahoittajia olivat ohjelmistoyritykset ja sairaanhoitopiirit. Tutkielman ohjaajat olivat FT, professori Anne Eerola ja TtT, tutkimusjohtaja Anneli Ensio.

Kuopiossa 15.12.2005

---

Minna Porali

# Sisällysluettelo

1	JOHDANTO .....	6
2	TIETOTURVA JA TIETOSUOJA .....	8
2.1	Tietoturvan perustavoitteet .....	8
2.1.1	Luottamuksellisuus (confidentiality) .....	9
2.1.2	Eheys (integrity).....	9
2.1.3	Saatavuus (availability) .....	10
2.1.4	Todentaminen eli autentikointi (authentication).....	10
2.1.5	Pääsynvalvonta (access control) .....	10
2.1.6	Kiistämättömyys (non-repudiation) .....	11
2.2	Terveydenhuollon tietoturva ja tietosuojaja .....	11
2.2.1	Henkilötietojen käsittely terveydenhuollossa .....	12
2.2.1.1	Potilasasiakirjojen laatiminen, säilyttäminen ja arkistointi .....	12
2.2.1.2	Tietojen salassapito ja suojaaminen .....	14
2.2.1.3	Potilasrekisteritietojen luovuttaminen.....	14
2.2.1.4	Henkilörekisteritietojen tarkastusoikeus .....	14
2.2.2	Tietoturvapoliittika.....	15
2.3	Sähköinen potilaskertomus .....	16
2.3.1	Käyttäjän ja asiakkaan sähköinen todentaminen .....	18
2.3.2	Sähköisten potilasasiakirjojen säilytyksen hyvä käytäntö.....	18
2.3.3	Sähköisen suostumuksen periaatteet .....	19
2.3.4	Luovutusten ja luovutuslokin hallinnan suositukset .....	20
2.3.5	Tietoturvan ja tietosuojan standardit .....	21
3	JULKISEN AVAIMEN INFRASTRUKTUURI (PKI) .....	23
3.1	Salausmenetelmistä .....	23
3.1.1	Symmetrinen salausmenetelmä.....	24
3.1.2	Epäsymmetrinen salausmenetelmä .....	25
3.2	Turvallisuusinfrastruktuuri .....	27
3.2.1	Turvallisuusinfrastruktuurin tarkoitus.....	27
3.2.2	Turvallisuusinfrastruktuurin toimittamia palveluja .....	28
3.2.2.1	Turvallinen sisäänkirjautuminen.....	28
3.2.2.2	Huomaamattomuus käyttäjälle .....	29
3.2.2.3	Kokonaisvaltainen turvallisuus.....	29
3.3	Taustaa julkisen avaimen järjestelmän käytön tarpeellisuudelle .....	30
3.4	PKI:n osapuolet .....	32
3.4.1	Varmenne (certificate).....	32
3.4.2	Varmentaja (certification authority, CA) .....	34
3.4.3	Rekisteröijä (registration authority, RA).....	34
3.4.4	Varmennehakemisto (certificate repository) .....	35
3.4.5	Varmennearkisto .....	35
3.4.6	Varmenteen haltija .....	36
3.4.7	Varmenteeseen luottava osapuoli .....	36
3.5	Varmennepoliittika (certificate policy, CP) .....	38
3.6	Varmenteen elinkaaren hallinta.....	38
3.6.1	Varmenteen luominen .....	39
3.6.2	Varmenteen käyttäminen.....	40
3.6.3	Varmenteen mitätöinti.....	41
3.7	PKI:n tekninen toteutus .....	42
3.8	Luottamus .....	43

3.8.1	Hierarkkinen luottamusmalli .....	43
3.8.2	Ristiinvarmennus .....	45
3.9	PKI:n tarjoamat ydinpalvelut .....	45
3.9.1	Todentaminen .....	45
3.9.2	Eheys .....	47
3.9.3	Luottamuksellisuus .....	48
3.9.4	Kiistämättömyys .....	49
4	PKI TERVEYDENHUOLLOSSA .....	50
4.1	Terveydenhuollon PKI-arkkitehtuuri .....	50
4.1.1	Varmennepalvelut .....	52
4.1.2	Kortinhallinta .....	52
4.1.3	Rekisteröintipalvelut .....	53
4.1.4	Hakemistopalvelut .....	53
4.1.5	Lisäpalvelut .....	53
4.2	Sähköinen allekirjoitus .....	55
4.2.1	Kokemuksia sähköisestä allekirjoituksesta .....	56
4.2.2	Sähköisen allekirjoituksen pitkäaikaissäilytys .....	57
5	POHDINTA.....	59
	LÄHTEET.....	62

# 1 JOHDANTO

Terveydenhuollossa ollaan vähitellen siirtymässä pois perinteisestä paperisesta potilaskertomuksesta. Vuonna 2003 perusterveydenhuollon puolella 93,6 % kunnista tai kuntayhtymistä käytti sähköistä potilaskertomusta. Yksityisistä klinikoista 82 % oli ottanut käyttöönsä sähköisen potilaskertomuksen. Erikoissairaanhoidon sairaaloista 62 %:ssa sähköinen sairauskertomus oli jossain määrin käytössä. [ELS05]

Siirtyminen sähköiseen potilaskertomukseen on tuonut mukanaan monenlaisia haasteita. Yksi niistä on tietoturvan perustavoitteiden huomioiminen, joka ei sähköisessä maailmassa aina ole yksinkertaista. Lisäksi henkilötietojen käsittelyä säätelevät monet lait ja ne tulee ottaa huomioon tietoturvan toteutuksessa. Terveydenhuollossa avainasemassa on potilaiden tietosuojat. Potilasasiakirjat sisältävät arkaluontoisia tietoja, jotka eivät saa joutua väärin käsiin. Tietojärjestelmän käyttäjät pitää todentaa ja järjestelmän käyttäjän oikeus käyttää tietoja tulee olla rajattu hänen työtehtäviensä mukaisesti; lääkärin ja sairaanhoitajan käyttöoikeudet ovat erilaiset.

Laki potilaan asemasta ja oikeuksista määrittelee potilasasiakirjoihin liittyvät tiedot salassa pidettäväksi. Potilaan hoidon kannalta tarpeelliset tiedot tulee kuitenkin olla potilasta hoitavien käytettävissä. Sähköinen potilaskertomus mahdollistaa tietojen käytön siellä missä tietoa tarvitaan. Potilastietojen luovuttaminen terveydenhuollon toimintayksiköstä toiseen edellyttää potilaan suostumusta, lukuun ottamatta laissa määriteltyjä erikoistapauksia, esimerkiksi tietojen luovuttaminen tapauksissa, joissa potilas on tajuton.

Luovutettaessa tietoja avoimissa tietoverkoissa tulee taata tietojen muuttumattomuus ja se, että tiedot eivät joudu sivullisten käsiin. Lisäksi verkossa asioivien osapuolten on varmistuttava toistensa henkilöllisyydestä. Tietoverkoissa asioivien osapuolten välinen luottamus on siis erittäin tärkeää. Ongelmana on ollut kuinka osapuolten välinen riittävä luottamus on saavutettavissa. Julkisen avaimen infrastruktuuri (PKI = Public Key Infrastructure) tarjoaa ongelmaan yhden ratkaisumallin. Julkisen avaimen infrastruktuurissa luottamus perustuu varmenteeseen. Varmenteen myöntää luotettu kolmas osapuoli, joka allekirjoituksellaan todistaa, että tietty yksityinen avain kuuluu tietylle henkilölle [Lin02].

Julkisen avaimen infrastruktuurin tarjoamien palvelujen avulla kukin osapuoli voi todistaa olevansa se, joka väittääkin olevansa, varmistua siitä, että tieto ei ole muuttunut matkalla ja vakuuttua siitä, että toiselle osapuolelle lähetettävä tieto on vain vastaanottajan luettavissa. PKI on turvallisuusinfrastruktuuri, jonka palvelut on tuotettu ja jaettu käyttäen julkisen avaimen käsitettä ja tekniikoita. PKI perustuu kryptografiaan eli salakirjoitustieteeseen. [AdL99]

Mikael Linden Tampereen teknillisestä yliopistosta on tarkastellut julkisen avaimen järjestelmää liseniaatintutkimuksessaan. Tutkimuksessaan hän on perehtynyt palveluihin, joita julkisen avaimen järjestelmä tarjoaa tietoverkossa.

Terveydenhuollon tietoturva on erittäin ajankohtainen aihe. Meneillään oleva kansallinen terveyshanke edellyttää, että vuoden 2007 loppuun mennessä potilaan tiedot kirjataan sähköisesti yhdenmukaista rakennetta käyttäen ja potilaan tietoja voidaan potilaan suostumuksella siirtää terveydenhuollon toimintayksiköstä toiseen. Stakes on viime vuosina julkaissut useita suosituksia aiheeseen liittyen. Yksi suositus sisältää ehdotuksen valtakunnallisesti toteutettavasta terveydenhuollon PKI-arkkitehtuurista, joka esitellään tässä tutkielmassa.

Ennen PKI-arkkitehtuurin esittelyä tässä tutkimuksessa tarkastellaan tietoturvan perustavoitteita, joita ovat esimerkiksi luottamuksellisuus ja todentaminen. Lisäksi tarkastellaan tietoturvan toteuttamiseen liittyviä asioita, jotka tulee ottaa huomioon terveydenhuollossa. Tutkielmassa esitellään julkisen avaimen infrastruktuuri: esitellään taustoja sen käytön tarpeellisuudelle, esitellään sen osapuolet ja sen tarjoamat ydinpalvelut. Johdatuksena julkisen avaimen infrastruktuuriin esitellään lyhyesti salausmenetelmät ja turvallisuusinfrastruktuuri. Tutkielman avulla lukija saa kuvan siitä, miten julkisen avaimen infrastruktuurin avulla voidaan toteuttaa tietoturvan perustavoitteet.

Tutkielman toisessa luvussa määritellään tietoturva ja tietosuoja. Lisäksi tarkastellaan terveydenhuollon tietoturvaan ja tietosuojaan liittyviä asioita. Luvussa 3 esitellään aluksi lyhyesti salausmenetelmiä ja turvallisuusinfrastruktuuria, niiden jälkeen perehdytään julkisen avaimen järjestelmään. Luku 4 esittelee PKI:n soveltamista terveydenhuollossa. Sen lisäksi luvussa käsitellään sähköistä allekirjoitusta. Luvussa 5 pohditaan käsiteltyjä asioita ja mietitään mahdollisia ongelmakohtia.

## 2 TIETOTURVA JA TIETOSUOJA

*Tietoturvan* (usein puhutaan myös *tietoturvallisuudesta*) avulla suojataan tietoa, tietojärjestelmiä ja palveluja niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvilta uhilta. Tietoturvaan kuuluu myös lainsäädäntö ja ne toimenpiteet, joiden avulla tietoturva varmistetaan. Tietoturvallisuuden toteuttamisessa erotetaan kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus. *Tietosuojaan* kuuluu ihmisten yksityiselämän suoja ja sen turvaaminen henkilötietojen käsittelyssä [VM03]. Tietosuojaa kutsutaan myös yksityisyyden suojaksi ja se on tietoturvaa uudempi käsite. Terveydenhuollon tietosuojassa ihmisen yksityisyyden suoja ja potilassuhteen luottamuksellisuus korostuvat [Yli01].

Tietoturva ja tietosuojat liittyvät läheisesti toisiinsa. Tietoturvan toteuttaminen jo sinällään parantaa myös tietosuojaa. Esimerkiksi varmistamalla tietojen luottamuksellisuus estetään tiedon käyttö luvattomilta tahoilta [Jär02]. Tietoturvan toteuttaminen ei kuitenkaan yksinään riitä parantamaan tietosuojaa.

Tietoturva on käyttäjistä riippumatonta. Tietoturvatavoitteet ovat sovittuja ja sovellusta käyttävien osapuolten tulee olla vakuuttuneita siitä, että tavoitteet myös täyttyvät. Tietoturvatavoitteita ovat esimerkiksi: tunnistaminen, allekirjoitus, pääsynvalvonta ja yksilönsuoja. Tietoturvallisuuden tavoitteisiin päästään käyttämällä matemaattisia kaavoja ja ennalta sovittuja käytäntöjä eli protokollia. Niiden lisäksi tarvitaan teknisiä menettelytapoja, tietoturvalakeja ja hyviä käytäntöjä. [Ker98]

Luvussa 2.1 esitellään tietoturvan perustavoitteet. Luku 2.2 tarkastelee tietoturvaa ja tietosuojaa terveydenhuollossa. Sähköiseen potilaskertomukseen tutustutaan luvussa 2.3.

### 2.1 Tietoturvan perustavoitteet

Seuraavissa aliluvuissa esitellään tietoturvan kuusi perustavoitetta. Tavoitteet ovat: luottamuksellisuus, eheys, saatavuus, todennus, pääsynvalvonta ja kiistämättömyys. Luku perustuu pääosin lähteeseen [Jär02].

### **2.1.1 Luottamuksellisuus (confidentiality)**

Internetissä siirretty tieto on usein suojaamatonta. Esimerkiksi sähköpostiviestit liikkuvat verkossa, niitä käsittelevät useat verkot ja laitteistot. Henkilöt, joilla on oikeus käyttää näitä järjestelmiä, voivat lukea sähköpostiviestejä. [Ker98]

*Luottamuksellisuudella* pyritään takaamaan, että tiedot ovat vain niiden käytettävissä, joilla siihen on oikeus. Lisäksi tulee määrittellä jokaisen käyttäjän valtuudet tietojen käyttöön. Valtuuksien määrittely edellyttää tietojen luokittelua, käyttäjien tunnistamista ja todennusta, valtuuksien määrittelyä ja käsittelytapojen ja -sääntöjen määrittelyä. Valtiovarainministeriön tekemässä valtionhallinnon tietoaaineistojen käsittelyn tietoturvallisuusohjeessa viranomaisen tieto on luokiteltu julkiseen ja salaiseen tietoon. Salassa pidettävä tieto on lisäksi jaettu erittäin salaiseen, salaiseen ja luottamukselliseen tietoon. Käyttäjien tunnistamista ja todentamista on käsitelty luvussa 3.9.1. Henkilöiden valtuudet määritellään henkilöiden työtehtävien mukaisesti. Tiedon käsittelytavat pitävät sisällään asiakirjan luomisen, muuttamisen ja tuhoamisen. [Tam05]

Ei kuitenkaan riitä, että tietoihin pääsy on turvattu. Luvattomat henkilöt voivat murtautua esimerkiksi tietokantaan tai salakuunnella tietoliikennettä. Tämän vuoksi tieto pitää olla salattu. Näin estetään tietojen paljastuminen. Salausmenetelmiin tutustutaan luvussa 3.1.

### **2.1.2 Eheys (integrity)**

Tiedon *eheydellä* tarkoitetaan tietojen tai tietojärjestelmän aitoutta, sen lisäksi eheys on ominaisuus, joka tiedolla on, jos sitä ei ole valtuudettomasti muutettu ja mahdolliset muutokset voidaan todentaa kirjausketjusta. [VM03] Tiedon eheyden voivat rikkoa muun muassa virukset. Eheys voi murtua myös vahingossa esimerkiksi käyttökatkon tai levyille tulleen vika-alueen takia. Eheyden turvaamiskeinoja ovat: tarkistussummien, lokitiedostojen, tiedonsiirron protokollien ja virustentorjuntaohjelmien käyttäminen. Tietojen eheyttä suojataan myös tietojen salaamisella. Arkistoitaessa jotain erittäin tärkeää ja salaista tietoa on erityisen tärkeää, että tieto säilyy eheänä. Tällaisia tietoja ovat esimerkiksi yrityksen taloustiedot. [Ker98]

Eheysvaatimuksen toteutuminen ja etenkin eheyden palauttaminen on erittäin vaikeaa. Eheyden rikkoutumista pidetään yhtenä vakavimmista tietoturvaloukkauksista [Tam05]. Eheyden vaatimukset tulee ottaa huomioon jo tietojärjestelmien suunnitteluvaiheessa, muuten järjestelmän käytön aikaiset ongelmat voivat olla suuria [Paa98].

### 2.1.3 Saatavuus (availability)

Ei riitä, että pääsy muuttumattomiin tietoihin on rajoitettu vain tietyille käyttäjille. Tieto pitää myös olla *saatavilla* silloin, kun sitä halutaan käyttää. Tämä tarkoittaa sitä, että verkkoyhteyksien ja koneiden pitää toimia. Jos kyseessä on verkkopalvelu, on sen saatavuus oltava jatkuva. Käytännössä se tarkoittaa 24 tuntia vuorokaudessa seitsemänä päivänä viikossa. Toimistojärjestelmien saatavuus on sidoksissa toimiston henkilökunnan työaikoihin. Henkilöt, jotka haluavat häiritä palvelun toimintaa voivat tarkoituksellisesti ylikuormittaa sitä. Tätä kutsutaan *palvelunestohyökkäykseksi*. [Ker98]

Saatavuutta voidaan parantaa tiedostojen palvelimien mitoituksella, varmuuskopioinnilla ja tekniikalla, joka turvaa laitteiden toiminnan (UPS-laite sähkökatkojen varalta). Lisäksi laitteet tulee sijoittaa lukkojen taakse ja varustaa palomureilla. [Ker98]

### 2.1.4 Todentaminen eli autentikointi (authentication)

*Todentamisella* varmistutaan siitä, että käyttäjä on se kuka väittää olevansa. Käyttäjän lisäksi voidaan todentaa myös laite tai nettipalvelu. Päätepalvelussa todentaminen tulee olla molemminpuolista eli sekä päätteen että palvelutietokoneen tulee olla vakuuttuneita toistensa autenttisuudesta. Samalla tulee varmistaa ettei kolmas osapuoli häiritse yhteyttä naamioitumalla jommaksi kummaksi [Ker98]. Käyttäjät todennetaan useimmiten salasanan perusteella. Oletuksena on, että salasana on vain ja ainoastaan sen henkilön tiedossa, jolle se oikeasti kuuluu. Tätä ei aina muisteta. Organisaatiossa voi esimerkiksi olla tapana säilyttää salasanvoja muistilapulla, joka on kiinnitetty tietokoneen näyttöön. Todennuksen keinoja käsitellään luvussa 3.9.1.

### 2.1.5 Pääsynvalvonta (access control)

Tietoturvan tavoitteista vanhin ja samalla tärkein on pääsynvalvonta [Ker98]. *Pääsynvalvonnan* tehtävänä on pitää huolta siitä, että ainoastaan ne henkilöt, jotka on asianmukaisesti todennettu, pääsevät käyttämään järjestelmän tietoja. Lisäksi pääsynvalvonta huolehtii lokitiedoista. Lokitietojen avulla voidaan jäljittää mahdollisia tietoturvarikkomuksia. Sen lisäksi, että pääsynvalvonnan kuuluu huolehtia siitä, että tietoja pääsevät käyttämään vain ne henkilöt, joilla siihen on oikeus, se ottaa kantaa myös siihen käytetäänkö järjestelmää paikallisesti vai etänä [Ker98].

## 2.1.6 Kiistämättömyys (non-repudiation)

*Kiistämättömyydellä* tarkoitetaan

"tietoverkossa eri menetelmin saatavaa varmuutta siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi" [VM03].

Kiistämättömyyden avulla varmistutaan siitä, että jälkikäteen ei voida kiistää tehtyä tekoa. Kiistämättömyys sitoo siis teon ja teon tekijän toisiinsa [Ker98]. Kiistämättömyyttä tarvitaan erityisesti sähköisessä tietojen vaihdossa ja kaupankäynnissä, jossa tilauksen tekemisen ja vastaanoton sekä tuotteen toimittamisen todistaminen on erittäin olennaista. Eheyden ja todennuksen avulla voidaan varmistaa myös kiistämättömyys. Sähköisessä kaupankäynnissä olennainen osa kiistämättömyyttä on lisäksi tapahtumiin liittyvät aikaleimat.

Tietoturvan saavuttaminen koetaan usein hyvinkin vaikeaksi. Yhtenä syynä tähän pidetään tietoturvaan liittyvien tekijöiden (koneet, ihmiset) muodostamaa ketjua. Ketjussa jokainen siihen kuuluva lenkki edustaa yhtä tekijää. Lopullisen tietoturvan katsotaan olevan niin vahva kuin on sen heikoin lenkki. Tietoturvallisuuden ja sitä vaarantavien tekijöiden tutkimukset ovat osoittaneet ihmisen toiminnan, tahallisen tai tahattoman, olevan suurin yksittäinen tekijä, joka vaarantaa tietoturvallisuuden. Tekniset toimet eivät voi korvata ihmisen osaamista, asenteita ja suhtautumista tietoturvallisuuteen liittyen. [Tam05]

## 2.2 Terveydenhuollon tietoturva ja tietosuoja

Terveydenhuollossa henkilötietojen käsittelyllä ja muulla tiedonhallinnalla on keskeinen asema. Sähköisten asiankäsittelyjärjestelmien ja sähköisen tiedonsiirron käyttö ovat yleistyneet terveydenhuollossa [Yli01]. Terveydenhuollon organisaatioiden toiminta ja päätöksenteko perustuvat pitkälti sähköisessä muodossa olevaan tietoon [Tam05].

Sähköiseen asiakirjojen käsittelyyn ja tiedonsiirtoon siirtyminen asettavat haasteita tietoturvan toteuttamiselle. Sähköisesti säilytettävä tieto on paperilla säilytettävää tietoa arempi erityyppisille tietoturvaloukkauksille [Tam05]. Tietosuojan ja tietoturvallisen

potilastietojen käsittelyn perustana ovat eettiset periaatteet, lait, asetukset ja Sosiaali- ja terveysministeriön (STM) laatimat ohjeet.

Stakesin tietoteknologian osaamiskeskuksen (OSKE) tietoturvallista kommunikaatiota koskevassa hankkeessa on määritelty suositukset koskien potilaan sähköisessä muodossa olevien tietojen tietoturvallista käyttöä terveydenhuollon eri tietojärjestelmien välillä. [Säh04b]

Luvussa 2.2.1 tutustutaan henkilötietojen käsittelyyn vaikuttaviin asioihin terveydenhuollossa. Luvussa 2.2.2 esitellään tietoturvapoliitikkaa.

## **2.2.1 Henkilötietojen käsittely terveydenhuollossa**

Terveydenhuollossa potilaasta syntyy suuri määrä asiakirjoja, jotka sisältävät potilaan kannalta joskus hyvin arkaluonteisia tietoja, jotka eivät saa joutua sivullisten käsiin. Tässä luvussa tutustutaan lainsäädäntöön, jossa on annettu ohjeet potilasasiakirjojen laatimisesta, säilyttämisestä ja arkistoinnista, tietojen salassapidosta ja suojaamisesta, potilasrekisteritietojen luovuttamisesta ja henkilörekisteritietojen tarkastusoikeudesta.

### **2.2.1.1 Potilasasiakirjojen laatiminen, säilyttäminen ja arkistointi**

Laissa potilaan asemasta ja oikeuksista *potilasasiakirjat* määritellään seuraavasti:

"potilaan hoidon järjestämisessä ja toteuttamisessa käytettäviä, laadittuja tai saapuneita asiakirjoja taikka teknisiä tallenteita, jotka sisältävät hänen terveydentilaansa koskevia tai muita henkilökohtaisia tietoja" [PotL92].

Potilasasiakirjoista muodostuvaa kokonaisuutta kutsutaan *potilasasiakirja-järjestelmäksi*. Potilasasiakirjajärjestelmästä löytyy jokaisesta potilaasta kaikki hoitoon liittyvät tiedot [Säh04a]. Potilasasiakirjoihin tulee merkitä tiedot, jotka ovat potilaan hoidon kannalta tarpeellisia. Tiedot ovat salassapidettäviä. Potilasasiakirjoihin saavat tehdä merkintöjä terveydenhuollon ammattihenkilöt, jotka osallistuvat potilaan hoitoon. Merkintöjen tulee olla selkeitä, ymmärrettäviä ja virheettömiä. Merkintöjä korjatessa sekä alkuperäisen että korjatun merkinnän tulee olla luettavissa. [STM01]

Potilasasiakirjojen tietoja ei saa ilman potilaan suostumusta luovuttaa sivulliselle, lukuun ottamatta laissa säädettyjä poikkeustapauksia. Yksi poikkeustapaus on esimerkiksi tietojen luovuttaminen omaisille, kun potilas on tajuton. *Sivullisella* tässä tapauksessa tarkoitetaan henkilöä, joka ei osallistu potilaan hoitoon [PotL92].

Potilasasiakirjojen laatimisesta ja säilyttämisestä säädetään tarkemmin sosiaali- ja terveysministeriön asetuksella [Yli01].

Potilasasiakirjojen sähköisen säilyttämisen ja arkistoinnin perusvaatimuksina pidetään käyttäjien vahvaa tunnistamista, tietojen muuttumattomuutta, tietoturvaa, saatavuutta, vastuullisuutta ja luotettavuutta. Tietojen luovuttaminen arkistosta tapahtuu ainoastaan määrättyjen ehtojen täytyessä; esimerkiksi tietoja pyytävän tulee osoittaa, että hänellä on hoitosuhde potilaaseen, jonka tietoja ollaan luovuttamassa. Lokitiedostosta tulee voida tarkastaa tietojen käyttö ja luovuttaminen [Ruo02]. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus (jatkossa Stakes) hankkeessa laaditaan sähköisestä arkistoinnista kansalliset määräykset. [Säh04b]

Terveydenhuollon toimintayksikkö ja itsenäisesti ammattiaan harjoittava terveydenhuollon toimintayksikkö ovat *rekisterinpitäjiä*, joiden vastuulla on potilasasiakirjajärjestelmän suunnittelu ja toteuttaminen, niin että se vastaa potilasasiakirjojen käyttötarkoitusta. Lisäksi on otettava huomioon tietoihin liittyvät käyttöoikeudet ja tietojen siirtämis- ja luovuttamistarpeet. Potilasasiakirjojen laatimiseen ja säilyttämiseen käytettävien välineiden ja menetelmien käytössä on huomioitava tietojen eheys- ja käytettävyyksivaatimus tietojen säilytysaikana. [STM01]

Potilasasiakirjojen säilyttäminen on sen rekisterinpitäjän vastuulla, jonka toiminnassa ne ovat syntyneet. Potilasasiakirjoja tulee säilyttää vähintään sosiaali- ja terveysministeriön asetuksessa olevassa liitteessä mainittu aika [STM01]. Terveydenhuollon potilasasiakirjojen säilytysajat ovat pitkiä, vaihteluväli on kymmenestä vuodesta 110 vuoteen. Tästä poikkeuksena on 18. ja 28. päivänä syntyneiden potilasasiakirjat, jotka säilytetään pysyvästi arkistolaitoksen 22.12.2000 tekemän päätöksen mukaisesti. Rekisterinpitäjien tietojärjestelmien tulee ottaa huomioon erilaiset säilyttämisaajat [Yli01]. Arkistolaitos määrää pysyvästi säilytettävistä asiakirjoista. Pysyvästi säilytettävät asiakirjat tulee laatia ja niiden sisältämät tiedot on tallennettava käyttäen pitkäaikaista säilytystä kestäviä materiaaleja ja säilyvyyden turvaavia materiaaleja. Asiakirjat tulee säilyttää siten, että ne eivät pääse tuhoutumaan, vahingoittumaan, eikä niihin pääse käsiksi asiattomat henkilöt. [ArkL94]

Asiakirjat tulee olla allekirjoitettuja. Tämä edellyttää sähköisen allekirjoituksen käyttämistä [Ruo02]. Sähköistä allekirjoitusta tarkastellaan luvussa 4.2.

### **2.2.1.2 Tietojen salassapito ja suojaaminen**

Potilasasiakirjojen sisältämät tiedot ovat *salassa pidettäviä* [PotL92].

"Salassa pidettävää asiakirjaa tai sen kopiota tai tulostetta siitä ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi" [JulkL99].

Myös sairauskertomustietojen jättäminen tietokoneen näytölle tulkitaan tiedon paljastamiseksi ulkopuoliselle, jos on mahdollista, että sivullinen pääsee näytöltä tietoja lukemaan [Yli01].

Henkilötietolain mukaan rekisterinpitäjän velvollisuutena on suojata henkilötietoja käyttämällä tarpeellisia teknisiä ja organisatorisia toimenpiteitä. Suojaaminen on ensiarvoisen tärkeää silloin, kun käsiteltävät tietomäärät ovat suuria tai tietojen siirto tai käsittely tapahtuu tietoverkoissa. Asiaton pääsy tietoihin ja vahingossa tai laittomasti tapahtuva tietojen hävittäminen, muuttaminen, luovuttaminen, siirtäminen tai muu laitton käsittely on estettävä [HetL99]. Suojaamalla tiedot varmistetaan siitä, että tiedot ovat vain niiden käytettävissä, joilla on oikeus tietoja käyttää. Siinä vaiheessa kun tietojärjestelmiä suunnitellaan ja rakennetaan, pitää ottaa huomioon tietosuojan asettamat vaatimukset järjestelmälle. [Täh97]

### **2.2.1.3 Potilasrekisteritietojen luovuttaminen**

Potilaasta hänen hoitonsa aikana kertyneitä tietoja saa luovuttaa vain niissä tapauksissa, kun potilaalta on saatu suostumus tietojen luovuttamiseen tai tietojen luovuttaminen perustuu lakiin. Suostumus pitää pääsääntöisesti olla kirjallinen, mutta joissain tapauksissa myös suullinen suostumus on riittävä. Avoimessa verkossa tapahtuva tietojen luovuttaminen ei täytä tietosuojavaatimuksia. Potilastietojen luovuttaminen suojaamattomasti on mahdollista ainoastaan silloin, kun kyseessä on kiireellinen tapaus [Yli01]. Luovutuksen laillisuudesta ja riittävästä tietosuojasta vastaa tietojen luovuttaja. Tietojen luovutuspyynnön tulee pääsääntöisesti olla kirjallinen. [Pot01]

### **2.2.1.4 Henkilörekisteritietojen tarkastusoikeus**

Henkilötietolain mukaan jokaisella on oikeus tarkastaa henkilörekisteriin talletettuja häntä itseään koskevia tietoja [Yli01]. Halutessaan tarkastaa itsestään talletettuja tietoja henkilön tulee tehdä pyyntö siitä terveydenhuollon ammattihenkilölle. Ammattihenkilö

hankkii tiedot ja antaa tiedot henkilölle, joka niitä pyysi [HeTiL99]. Potilasasiakirjojen tarkastamisessa tulee pyrkiä siihen, että tarkastus tapahtuu henkilökohtaisesti. Mahdollisuus tutustua omiin potilasasiakirjoihinsa tulee tarjota mahdollisimman nopeasti sen jälkeen, kun potilas on pyynnön esittänyt. Jos potilas niin haluaa, on tiedot saatava kirjallisesti. Jokaisella on oikeus tarkastaa tietonsa veloitus kerran vuodessa. Tietojen tulkintaan pitää tarjota asiantuntija-apua. [Pot01]

### **2.2.2 Tietoturvapoliittika**

Organisaation ja sen johdon käytännön toimenpiteet tietoturvan toteuttamiseksi terveydenhuollon toimintayksikössä kuvataan *tietoturvapoliitikassa*. *Tietosuojapolitiikka* kuvaa henkilötietojen lainmukaisen käsittelyn organisaatiossa [Säh04b]. Stakesin 2005 julkaisema raportti Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt sisältää ohjeita sosiaali- ja terveydenhuollon organisaatioille ja toimintayksiköille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi. Ohje suosittaa, että kaikissa terveydenhuollon toimintayksiköissä tulee olla dokumentoituina tietoturva- ja tietosuojapolitiikat. Ohjeen mukaisesti toteutettu tietoturvallisuus on standardien ja lakien mukainen. [Tam05]

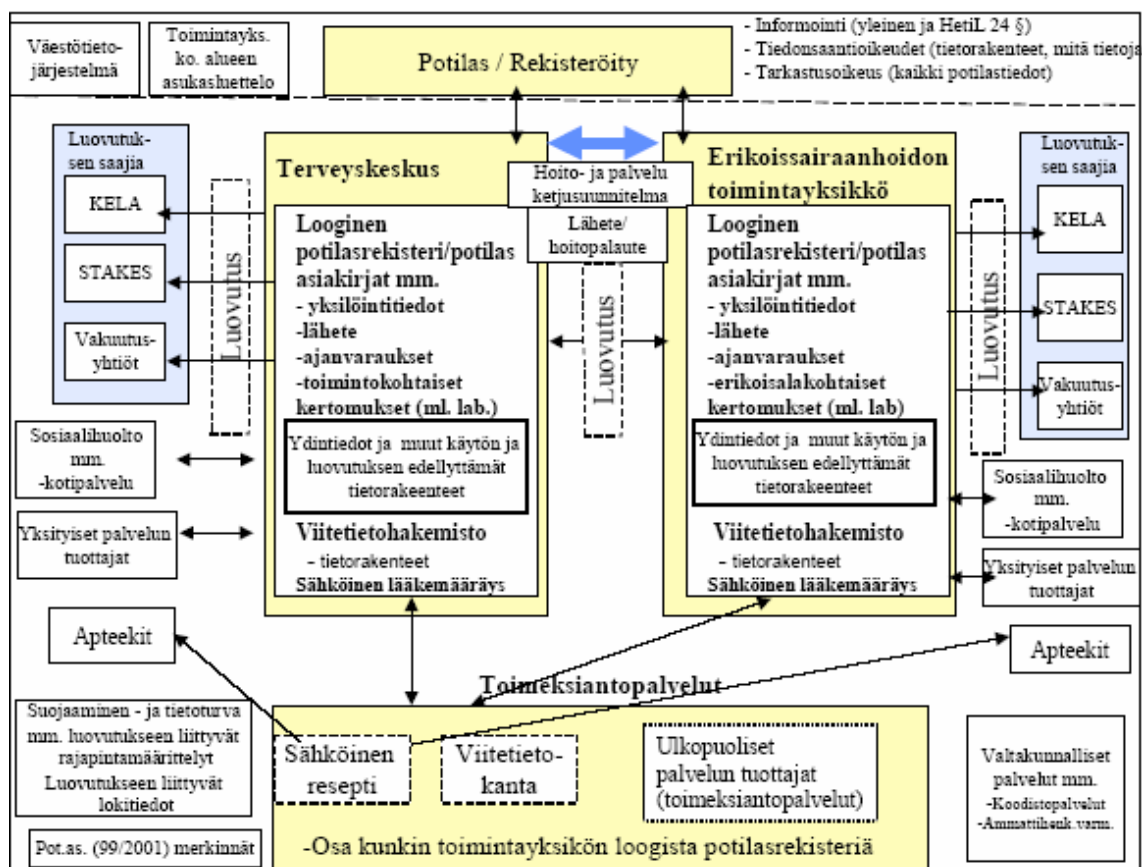
Tietojen turvaamisen perustana on tunnistettu riski. Jos riski toteutuu, tietojen käyttö häiriintyy tai estyy kokonaan. Tietojen turvaamisen tarkoituksena on tunnistaa erilaiset riskit ja varautua niihin. Mitä yksityiskohtaisemmin uhkat ja riskit tunnistetaan, sitä paremmin niiden mahdollisia seurauksia voidaan yksilöidä ja niitä vastaan varautua. Organisaation tulee suojata tietonsa niihin kohdistuvilta uhkilta. Kehitettäessä tietoturvaa pitää vastata seuraaviin kysymyksiin [Tam05]:

- mitkä tiedot pitää suojata ja minkä takia,
- miltä tiedot pitää suojata (esimerkiksi muuttuminen, paljastuminen),
- mitkä ovat riskit, jotka johtavat tietoturvaloukkauksiin ja
- miten estetään riskien toteutuminen?

## 2.3 Sähköinen potilaskertomus

Valtioneuvoston 11.4.2002 tekemän periaatepäätöksen pohjalta käynnistyi vuoden 2007 loppuun jatkuva kansallinen terveyshanke. Yhtenä hankkeen tavoitteena on sähköisen potilaskertomuksen vakiintunut käyttö vuoden 2007 loppuun mennessä kaikissa terveydenhuollon organisaatioissa. Tämä koskee sekä yksityistä että julkista sektoria. [Säh04a]

Sähköisen potilaskertomuksen käyttäminen mahdollistaa sähköisessä muodossa olevien potilastietojen luovuttamisen terveydenhuollon eri rekisterinpitäjien välillä. Terveydenhuollossa *rekisterinpitäjiä* ovat terveydenhuollon toimintayksiköt (esimerkiksi terveyskeskukset) ja itsenäisesti ammatiaan harjoittavat terveydenhuollon ammattihenkilöt [Yli01]. Kuvassa 1 on kuvattu yleisellä tasolla terveyskeskuksen ja erikoissairaanhoidon toimintayksiköiden potilasrekistereitä, jotka muodostuvat sähköisistä asiakirjoista; potilasrekistereiden välistä tiedonsiirtoa sekä keskeiset yhteistyö-, toimija- ja luovutuksensaajatahot.



Kuva 1. Esimerkki potilasasiakirjoista muodostuvasta loogisesta potilasrekisteristä, sen toimintaympäristöstä sekä keskeisistä toimija- ja yhteistyötahoista [Säh04b]

Jotta tietojen luovuttaminen olisi mahdollista, sähköisten potilasasiakirjajärjestelmien täytyy olla yhteensopivia. Käytännössä tämä tarkoittaa sitä, että eri järjestelmien rakenteiden, sisältöjen, terminologioiden, avoimien rajapintojen ja tietoturvallisen tiedon luovutuksen osalta täytyy tehdä kansallisia määrittelyjä ja ohjeistuksia. Lisäksi tarvitaan valtakunnallisia tukipalveluja. [Säh04a]

Sosiaali- ja terveysministeriö asetti kansalliselle hankkeelle työryhmän, jonka tehtävänä oli vuoden 2003 aikana valmistella strategia siitä, miten sähköiset potilasasiakirjajärjestelmät tulee valtakunnallisesti määritellä ja toimeenpanna. Strategia julkaistiin 2004 tammikuussa. Se sisältää sähköisten potilasasiakirjajärjestelmien vähimmäisvaatimukset. Lisäksi siinä on esitetty toimenpiteet, joita strategian toimeenpano edellyttää sekä strategian aikataulu ja vastuutahot. Määrittelytyö koostuu useista eri osahankkeista. Kaikkien hankkeiden yhteisenä tarkoituksena on sähköisten potilasasiakirjajärjestelmien sisällöllisten ja teknisten määrittelyjen tekeminen, niin että ne tukevat potilaan laadukasta hoitoa, yksityisyyden suojaa ja kustannustehokkuutta palvelujen järjestämisessä. [Säh04b]

Tietoturvaan liittyviä asioita on määritelty Tietoturvallinen kommunikaatioalusta - osahankkeessa, jonka on toteuttanut Stakes. Teknologian tuomat ratkaisut tekevät mahdolliseksi saada tarpeelliset tiedot käyttöön ajasta ja paikasta riippumatta. Potilastietojen käytössä ja siirtämisessä tulee muistaa lain asettamat vaatimukset, tietoturva ja potilaan yksityisyys. Tietoturvallisuuden ja tietosuojan toteutusten tulee olla valtakunnallisesti samantasoisia. Tämä edellyttää tietoturva-arkkitehtuuria ja sen sisältämien tietoturvapalvelujen toteuttamista. Stakesin hankkeessa on tehty suosituksia, joissa on kuvattu potilasta koskevien tietojen tietoturvallista käyttöä sähköisten potilastietojärjestelmien välillä [Säh04b]. Seuraavissa luvuissa tarkastellaan hankkeen tuottamia suosituksia.

Luku 2.3.1 käsittelee käyttäjän sähköistä todentamista. Luvussa 2.3.2 aiheena on sähköisen asiakas- ja potilasasiakirjojen säilytyksen hyvä käytäntö, luku 2.3.3 käsittelee sähköistä suostumusta, luvussa 2.3.4 tutustutaan luovutusten ja luovutuslokin hallinnan suosituksiin ja luvussa 2.3.5 kerrotaan tietoturvaan ja tietosuojaan liittyvistä standardeista.

### 2.3.1 Käyttäjän ja asiakkaan sähköinen todentaminen

Kun terveydenhuollossa siirretään tai käytetään salassa pidettävää tietoa, vaatimuksena on asioivien osapuolten luotettava tunnistaminen ja todentaminen. Lähtökohtana voidaan pitää ammattilaisen todentamista toimikortin avulla. [Ruo02]

Sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilulaki (22.9.2000 / 811) on mahdollistanut käyttäjän ja asiakkaan sähköisen todentamisen kokeilun. Stakes on tehnyt vuonna 2005 kyselyn, jonka avulla on koottu tietoa kokeilussa mukana olevien kokemuksia kokeilulaista. Kokeilulain mukaan asiakas voidaan todentaa henkilökorttilain mukaisen henkilökortin sisältämällä varmenteella tai vastaavalla muulla varmenteella. Ammattihenkilö sen sijaan voidaan todentaa riittävän tasoisella varmenteella. Hallituksen esityksen mukaan voidaan edellyttää, että käytetty varmenne täyttää laatuvarmenteelle asetetut vaatimukset. [HHP05]

Asiakkaan sähköistä todentamista on pilotoitu yhdellä kokeilualueella. Ammattihenkilön todentamista pilotoidaan yhdeksällä alueella ja käytetään kolmella kokeilualueella. Todentamiseen käytetyt varmenteet olivat Terveydenhuollon oikeusturvakeskuksen (jatkossa TEO) varmenteita, sairaanhoitopiirin omia varmenteita ja avainlukulistoja. Todentamisen välineiden taso vaihtelee. Laissa ei ole säädetty tapaa, jolla todentaminen tulee suorittaa. Kyselyn mukaan todentamista koskevat säädökset tulee tarkistaa. [HHP05]

### 2.3.2 Sähköisten potilasasiakirjojen säilytyksen hyvä käytäntö

Asiakirjojen säilymisen ja olemassaolon perusteita ovat: niiden fyysinen säilyminen, käytettävyyden eheys, luotettavuus ja aitous. Tässä yhteydessä *käytettävyydellä* tarkoitetaan tietojen säilymistä ymmärrettävänä erilaisista konversioista, dokumentointitavoista ja ohjelmistoista huolimatta. [EnR03]

Asiakirjojen säilytysajat vaihtelevat. Asiakirjan säilytysaika tulee merkitä asiakirjan kuvailutietoihin eli metatietoihin. Säilytettävillä potilasasiakirjoilla tulee olla yksikäsitteinen tunniste eli kahdella eri asiakirjalla ei voi olla samaa tunnistetta. Yksilöinti toteutetaan käyttämällä ISO-standardin mukaisia OID-tunnuksia (object identifier). *OID-tunnus* on yksilöllinen esitysmuoto tietylle objektille. Se ilmaistaan kokonaislukusarjana, jossa luvut on eroteltu pilkulla tai pisteellä. OID-tunnukset ovat hierarkkisia ja ne rekisteröidään kansainvälisen, kansallisen tai organisaatiokohtaisen

rekisteröijän toimesta; näin taataan, että tietyille objektille myönnetty OID-tunnus on ainutkertainen [AdL99]. [EnR03]

Potilastiedot muodostuvat perus- eli aktiivikäytön järjestelmässä, *peruskäytön* järjestelmällä tarkoitetaan asiakirjojen käsittelyjärjestelmiä, kuten Effica ja Pegasos. Perusjärjestelmä huolehtii potilaan hoitamistarpeen edellyttämästä säilytyksestä. Perusjärjestelmässä syntyneet tiedot siirretään arkistoon joko välittömästi niiden muodostumisen jälkeen tai sen jälkeen, kun aktiivikäyttö on päättynyt. *Arkisto* on organisaatio tai organisaatioyksikkö, joka vastaanottaa, hankkii ja säilyttää arkistoaineistoa tai arkistoja. Arkiston tulee taata arkistossa säilytettävien asiakirjojen alkuperäisyys ja kiistämättömyys [EnR03]. Arkisto voi olla tuotekohtainen, paikallinen, alueellinen tai kansallinen [ELS05].

### **2.3.3 Sähköisen suostumuksen periaatteet**

Potilaan hoitotietojen luovutus kahden rekisterinpitäjän välillä on mahdollista vain siinä tapauksessa, kun potilas on antanut suostumuksen tietojen luovutukseen tai kun luovutus perustuu lainsäädäntöön. *Suostumus* on vapaaehtoinen, yksilöity, informoitu ja tietoinen tahdonilmaisu, jolla asiakas antaa luvan henkilötietojensa käsittelyyn [KokL00]. Suostumusasiakirja sisältää muun muassa luovutuksen saajan, luovutettavat tiedot ja suostumuksen voimassaolon [ELS05]. Tavoitteena on, että suostumukset ovat tulevaisuudessa sähköisessä muodossa. Jotta suostumuksia voitaisiin hallita sähköisesti, tulisi olla käytössä asiakkaan sähköinen allekirjoitus. Siinä tapauksessa suostumusta ei enää tarvitsisi tulostaa, allekirjoittaa manuaalisesti eikä arkistoida paperimuodossa. [MSR04]

Suostumus kuuluu hoitotietoihin ja sen säilyttämisessä tulee noudattaa niitä ohjeita, mitä sähköisissä arkistointivaatimuksissa määrätään. Suostumusten arkistointiaika on 10 vuotta, alkaen suostumuksen päättymispäivästä. Kun hoitotietoja luovutetaan suostumuksen perusteella, pitää voida jälkikäteen selvittää, mihin suostumukseen tietojen luovutus on perustunut. Suostumuksia tulee hallita lokitietojen avulla. [MSR04]

Stakesin julkaisemassa selvityksessä sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilulain toimeenpanosta kokeilualueilla selvitettiin kokeilualueiden kokemuksia myös asiakkaiden suostumusten hallinnasta. Suostumuksen hallintaa pidettiin tärkeänä asiana. Kymmenellä alueella kahdestakymmenestä toteutui suostumusten hallinta jollain tasolla. Suostumukset olivat sähköisiä neljällä alueella.

Samasta selvityksestä kuitenkin käy ilmi, että potilaan sähköinen allekirjoitus ei ole vielä käytössä millään kokeilualueella. Tästä voidaan päätellä, että täydellistä sähköistä suostumusta ei vielä ole käytössä. Suostumuslomake on sähköisessä muodossa, se tallennetaan sähköisesti, mutta allekirjoittamista varten se pitää vielä tulostaa. [HHP05]

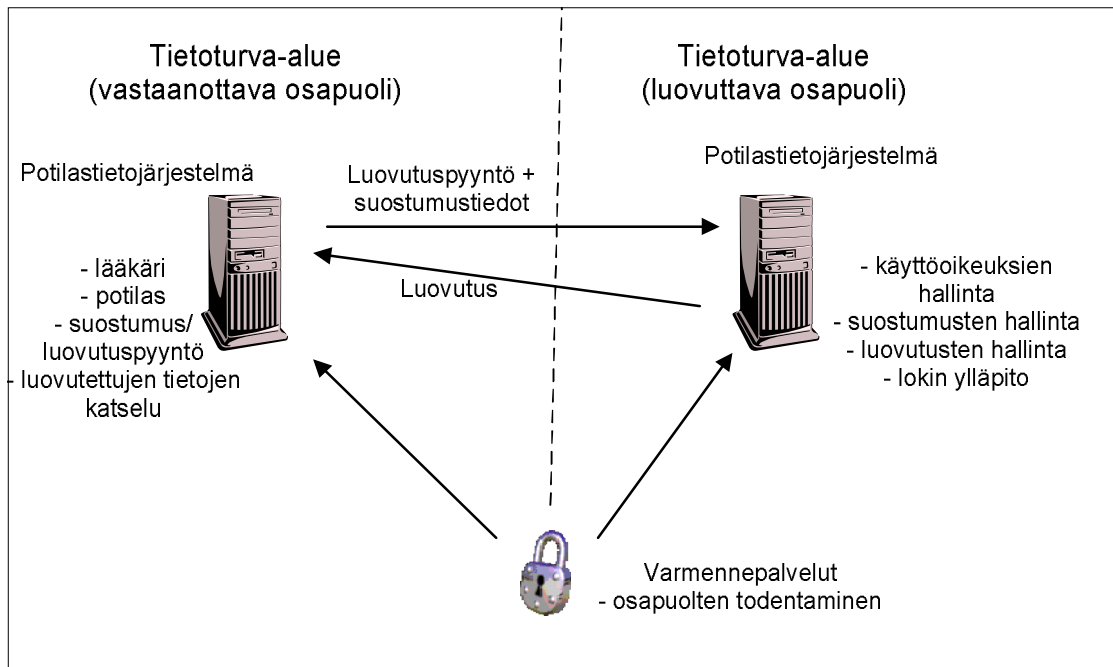
### **2.3.4 Luovutusten ja luovutuslokin hallinnan suositukset**

Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta vuodelta 2000 mahdollisti ensimmäisen kerran potilasta koskevan tiedon luovuttamisen sähköisesti organisaatioiden välillä. Tietojen luovuttamisen nopeuttamiseksi otettiin käyttöön viitetietokanta [Säh04b]. *Viitetietokannalla* tarkoitetaan "viitetietojen ja niiden luovuttamista koskevien suostumusten muodostamaa sosiaali- tai terveydenhuollon asiakasrekisterin osarekisteriä, johon talletetaan myös lokitiedot." *Viitetiedolla* puolestaan tarkoitetaan

"tietoa siitä, että mainitussa sosiaali- tai terveydenhuollon toiminnallisen yksikön sähköisessä asiakasrekisterissä tai osarekisterissä on tiettyä ajankohtana tallennettua rekisterinpitäjän toiminnassa syntyneitä kyseessä olevaa asiakasta koskevia henkilötietoja". [KokL00]

*Tietojen luovuttamisella* tarkoitetaan hoitotietojen luovuttamista kahden tai useamman rekisterinpitäjän välillä. Tietojen luovutuksen periaatteita ovat muun muassa: asiakkaalta pitää olla suostumus tietojen luovuttamiseen tai luovutuksen tulee perustua lainsäädäntöön, luovutuksen saajalla ja asiakkaalla tulee olla hoitosuhde tai muu asiallinen yhteys ja hoitotietojen luovutuksesta on tehtävä merkintä luovutuslokiin luovuttavassa toimintayksikössä sekä tiedot saaneessa vastaanottavassa yksikössä [MSR04].

Tietojen luovutuksen perusmalli on esitetty kuvassa 2. Sanomapohjaisen tiedonvälitystekniikan käyttö tietojen välityksessä on hyvin yleistä. Tietoliikenneyhteys tietojärjestelmien välillä toteutetaan käyttämällä esimerkiksi VPN-yhteyttä (VPN = virtual private network) tai avointa tietoverkkoa ja vahvaa salausta. [ItR04]



Kuva 2. Tietojen luovutus potilastietojärjestelmien välillä, mukailtu [ItR04]

Sekä luovuttavalla että vastaanottavalla rekisterinpitäjällä on omat tietoturva-alueensa. Kummallakin tietoturva-alueella on oma tietoturvapoliittikka, suostumusten, luovutusten ja käyttöoikeuksien hallinta. Tietoturva-alueiden välillä pitää vallita luottamus. Luottamus voi perustua esimerkiksi osapuolten tekemään sopimukseen tietojen vaihdosta. [ItR04]

Saumattoman palveluketjun kokeilualueilla tietojen luovutusta on seurattu lokitietojen ja arkistoitavien suostumusten avulla ja valvojan toiminnolla. Yksi alue ilmoitti, ettei seuranta ole järjestetty. [HHP05]

### 2.3.5 Tietoturvan ja tietosuojan standardit

Yhteistoiminnallisten ja tietoturvallisten sosiaali- ja terveydenhuollon tietojärjestelmien perusteena käytetään standardeja. Standardointityötä tehdään sekä *de jure* että *de facto* tasolla. *De jure* -standardien tuottajat ovat virallisia standardointiorganisaatioita (esimerkiksi eurooppalaiset CEN-standardit), *de facto* -standardien tuottajat ovat vapaaehtoisryhmiä (esimerkiksi HL7-standardit). Osallistuminen standardointityöhön on vapaaehtoista, samoin standardien käyttöönotto, ellei niitä ole määrätty pakollisiksi viranomaisten taholta [Säh04b, EnR04]. Standardin vahvistaminen edellyttää, että tärkeimmät intressipiirit hyväksyvät standardiehdotuksen. Suomen virallinen standardointielin on Suomen standardoimisliitto eli SFS. Tietojärjestelmien

yhteentoimivuutta parannetaan standardoinnilla ja standardien käytöllä, samalla säästetään myös kustannuksia. Myös käyttäjä hyötyy standardien käytöstä; toimintatavat yksinkertaistuvat ja vakiintuvat. [EnR04]

Terveydenhuollon tietojenkäsittelyn standardit liittyvät muun muassa seuraaviin osa-alueisiin: tiedonsiirtoon, tietojen säilytykseen ja tietoturvaan. Stakesin vuonna 2004 julkaisemassa suosituksessa kansallisesti noudatettaviksi standardeiksi ehdotetaan, että standardit jaetaan kolmeen ryhmään. Ehdotetut ryhmät ovat: pakolliset, suositeltavat ja ohjaavat standardit. Pakollisia standardeja ovat ne, jotka liittyvät tietojen siirrettävyyteen, käytettävyyteen, säilyvyyteen ja tietoturvaan. Terveydenhuollon tietoturvan toteuttamiseen käytetään pääasiallisesti yleisiä standardeja, joista esimerkkinä mainittakoon: ISO 17799 (BS7799) Part 1 Code for practise for information security management, ISO-7816 toimikorttistandardit ja ISO TS 17090, joka on kolmiosainen terveydenhuollon PKI-standardi, jossa kuvataan sertifikaattipolitiikka, PKI:n toteutustapoja ja annetaan esimerkkejä sertifikaateista. [EnR04]

### 3 JULKISEN AVAIMEN INFRASTRUKTUURI (PKI)

*Julkisen avaimen infrastruktuuri* eli *julkisen avaimen järjestelmä* (yleisesti käytetään myös lyhennettä *PKI*) sisältää laitteiston, ohjelmistoja ja menettelytapoja. Se mahdollistaa turvallisen kommunikaation turvattomassa ympäristössä toisilleen tuntemattomien osapuolien välillä [Hun01]. PKI on turvallisuusinfrastruktuuri, minkä palvelut on toteutettu ja jaettu käyttäen julkisen avaimen käsitteitä ja tekniikoita [AdL99]. Lisäksi PKI voidaan nähdä alustana, jonka päälle voidaan rakentaa sähköisen asioinnin palveluita ja sovelluksia [Ruo02]. *Sähköisellä asioinnilla* tarkoitetaan asioiden hoitoa Internetin tai sähköpostin välityksellä. Asiointi on asiakkaan ja viranomaisen välistä tietojen vaihtoa sekä viranomaisten välistä tietojen vaihtoa. Laissa on esitetty velvollisuuksia asioiville osapuolille sähköisiin asiakirjoihin liittyen. Sähköiset asiakirjat tulee olla liitettävissä niissä mainittuun lähettäjään tai vastaanottajaan. Tämä on mahdollista viranomaisten ja asiakkaiden hallussa olevan varmenteen avulla. [Paj05]

Luvussa 3.1 tutustutaan salausmenetelmiin. Luku 3.2 esittelee turvallisuusinfrastruktuurin. Luvussa 3.3 esitellään perusteluja julkisen avaimen käytölle. PKI:n osapuolet esitellään luvussa 3.4. Varmennepoliikkaan tutustutaan luvussa 3.5. Varmenteen elinkaaren hallintaan paneudutaan luvussa 3.6. Luvussa 3.7 esitetään PKI:n tekninen toteutus. Luottamusta käsitellään luvussa 3.8. PKI:n tarjoamat ydinpalvelut esitetään luvussa 3.9.

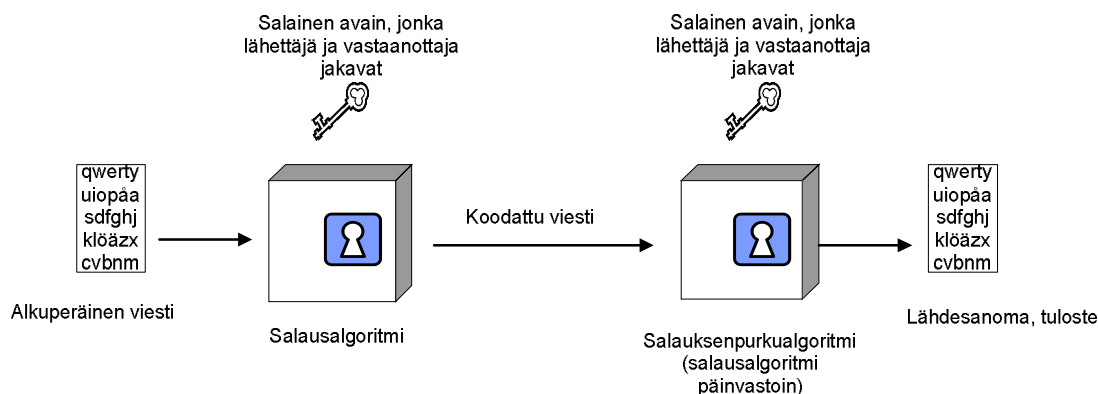
#### 3.1 Salausmenetelmistä

Tiedon salaamisen ja kätkemisen välineitä ja menetelmiä ja niiden käytön osaamista kutsutaan *kryptografiaksi* [VM03]. Kryptografian pääasiallisena tavoitteena on joko a) salata sanoma tai sanoman lähettäjä ja/tai vastaanottaja tai b) autentikoida (= todistaa aidoksi) sanoma tai sanoman lähettäjä ja/tai vastaanottaja [Ker98].

Internet on avoin tietoverkko. *Avoimella tietoverkolla* tarkoitetaan verkkoa, joka on kaikkien käytettävissä [VM03]. Kun avoimessa tietoverkossa lähetetään sanomia, ei voida olla varmoja siitä, että vain sanoman aiottu vastaanottaja pystyy viestin lukemaan. Kryptografia tarjoaa vastauksen tähän ongelmaan. Sanoma salataan sellaisella periaatteella, että vain vastaanottaja tietää miten salaus puretaan. Salausmenetelmä voi olla joko symmetrinen tai epäsymmetrinen [Lin02]. Symmetrinen salausmenetelmä esitellään luvussa 3.1.1 ja epäsymmetrinen luvussa 3.1.2.

### 3.1.1 Symmetrinen salausmenetelmä

*Symmetrisessä salausmenetelmässä* (puhutaan myös perinteisestä salauksesta ja yhden avaimen salauksesta [Sta03]) samaa salausavainta käytetään sekä viestin salaamiseen että salauksen purkamiseen. Perinteisen salauksen yksinkertaistettu malli on esitetty kuvassa 3.



Kuva 3. Symmetrisen salauksen yksinkertaistettu malli, mukailtu [Sta03]

Kuvassa on esitetty symmetrisen salauksen viisi tekijää, jotka ovat [Sta03]:

- Alkuperäinen viesti: Tämä on salattava viesti tai tieto, joka on algoritmin syöte.
- Salausalgoritmi: Salausalgoritmi suorittaa lähdesanomalle erilaisia korvauksia ja muunnoksia.
- Salainen avain: On myös salausalgoritmin syöte. Viestin koodaus ja koodatun viestin purku tehdään avaimella. Avain on lähdesanomasta riippumaton. Algoritmin suorittamat tarkat korvaukset ja muunnokset ovat avaimesta riippuvaisia.
- Koodattu viesti: Salattu viesti, joka on riippuvainen alkuperäisestä viestistä ja salaisesta avaimesta.
- Salauksenpurkualgoritmi: Tämä on salausalgoritmi, joka on käänteisalgoritmi salausalgoritmile. Syötteenä sillä on koodattu viesti ja salainen avain ja tulosteena alkuperäinen viesti.

Vain viestin vastaanottaja pystyy purkamaan salatun viestin. Edellytyksenä tälle on, että vastaanottaja tietää käytetyn avaimen ja algoritmin. [Jär96]

Salaus perustuu salausalgoritmin käyttöön [Lin02]. Valtionhallinnon tietoturvakäsitteistössä *salausalgoritmi* määritellään seuraavasti: "sarja ohjelmitavia matemaattisia toimituksia, joita käyttäen tieto salakirjoitetaan tai salakirjoitettu tieto avataan" [VM03]. Salausalgoritmia ei tarvitse pitää salassa, ainoastaan salainen avain. Tämä piirre mahdollistaa symmetrisen salauksen laajan käytön [Sta03]. Piirre tunnetaan myös nimellä *Kerckhoffin periaate*, "jonka mukaan järjestelmä on varma (salainen), vaikka kaikki sen salaus- ja purkuprosessien yksityiskohdat julkistetaan lukuunottamatta salaista avainta" [Ker98].

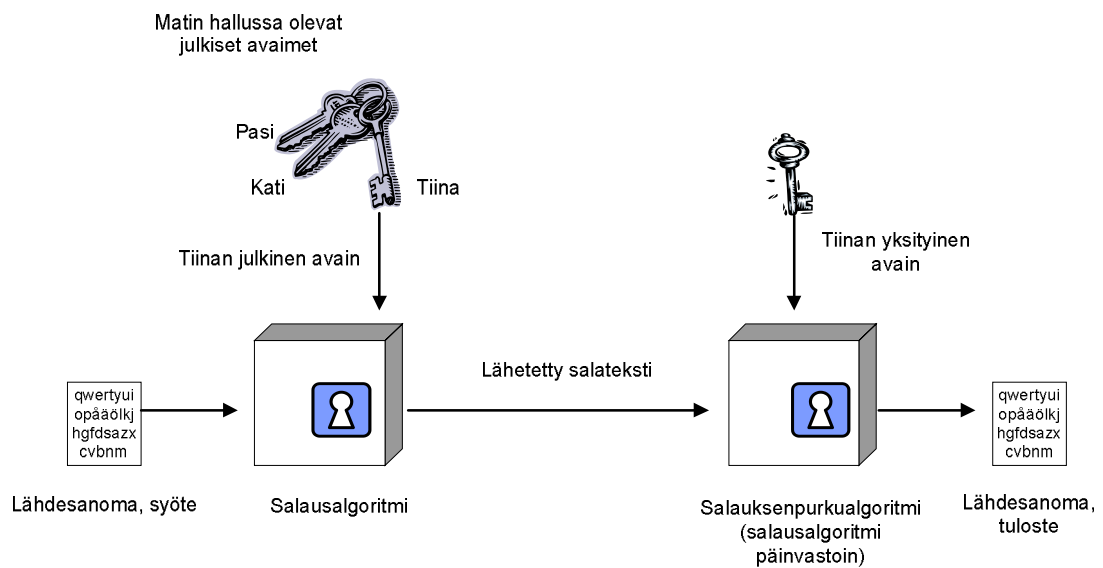
Symmetrisiä salausalgoritmeja on useita erilaisia. Osa salausalgoritmeista on helposti murrettavissa, kun taas osa algoritmeista voidaan murtaa ainoastaan käyttämällä väsytyksen menetelmää (brute force attack). *Väsytyksen menetelmä* tarkoittaa kaikkien mahdollisten avainten kokeilemistä, kunnes oikea avain löytyy. Symmetrisiä salausalgoritmeja ovat muun muassa: DES (Data Encryption Standard), joka on yksi tunnetuimmista symmetrisistä salausalgoritmeista, IDEA ja Blowfish. [Lin02, Sta03]

Perinteisen salauksen ongelmana on: salaisen avaimen välittäminen viestin vastaanottajalle, skaalautuvuuden ongelmat ja kommunikointiongelmat entuudestaan tuntemattomien välillä. Symmetrisen salaus perustuu täysin siihen, että viestin lähettäjä ja vastaanottaja jakavat keskenään salaisen avaimen ennen varsinaisen viestin lähettämistä. Avaimen kuljettaminen vaatii erillistä turvallista kommunikointia ennen varsinaista salatun viestin lähettämistä. Tämä vaihe on tavallaan ylimääräinen ja joissain tapauksissa erittäin vaikea toteuttaa. Jos henkilön täytyy lähettää salattuja viestejä useiden eri henkilöiden kanssa, on hänellä oltava jokaisen kanssa eri salainen avain. Tämä johtaa salaisten avainten määrän kasvuun ja salaisten avainten varastointi ja hallinta vaikeutuu. Erillinen salaisen avaimen jakamisvaihe on vaikeaa, kun ollaan tekemisissä entuudestaan tuntemattoman henkilön kanssa. [AdL99]

### **3.1.2 Epäsymmetrisen salausmenetelmä**

Epäsymmetrisen salausmenetelmä (tunnetaan myös julkisen avaimen salausmenetelmänä) kehitettiin 1970-luvulla. *Epäsymmetrisessä salausmenetelmässä* käytetään kahta eri avainta: *julkista avainta* (public key) viestin salaamiseen ja *yksityistä avainta* (private key) viestin purkamiseen. Julkinen avain voi olla julkisesti saatavilla esimerkiksi julkisessa avainhakemistossa, sen sijaan yksityinen avain pitää säilyttää huolella, sillä se on tarkoitettu ainoastaan omistajansa käyttöön. Yksityinen avain voidaan tallettaa esimerkiksi toimikortille [Lin02]. "*Toimikortti* on suorittimen ja

muistia muodostavia mikropiirejä sisältävä luottokortin kokoinen muovikortti" [VM03].  
Kuvassa 4 on esitetty epäsymmetrisen salauksen periaate.



Kuva 4. Epäsymmetrisen salauksen periaate, mukailtu [Sta03]

Erona symmetriseen salaukseen on salausavainten määrä. Epäsymmetrisessä salauksessa käytössä on kaksi eri avainta; yksityinen ja julkinen avain. Avaimet muodostavat avainparin ja niiden välillä on matemaattinen yhteys. Epäsymmetrisen salauksen turvallisuus perustuu siihen tosiasiaan, että yksityistä avainta ei voida johtaa julkisesta avaimesta. Teoriassa se on mahdollista, mutta käytännön tasolla se vaatii erittäin paljon aikaa, muistia ja laskentatehoa [AdL99]. Epäsymmetrisen salauksen keskeiset vaiheet ovat:

1. Jokainen käyttäjä luo avainparin, jota käytetään viestien salaamiseen ja purkamiseen.
2. Jokainen käyttäjä laittaa julkisen avaimensa julkiseen rekisteriin tai johonkin muuhun muiden käytettävissä olevaan tiedostoon. Avaimen pari pidetään yksityisenä. Kuten kuvassa 2 on esitetty, jokaisella käyttäjällä on kokoelma muiden käyttäjien julkisia avaimia.
3. Jos Matti haluaa lähettää luottamuksellisen viestin Tiinalle, salaa Matti viestin Tiinan julkisella avaimella.

4. Kun Tiina saa viestin, hän purkaa sen yksityisellä avaimellaan. Kukaan muu ei pysty purkamaan viestiä, koska vain Tiina tietää Tiinan yksityisen avaimen. [Sta03]

Julkisen avaimen salauksen hitaudesta johtuen, se on monissa tilanteissa epäkäytännöllistä. Tämän takia käytännössä salaus on usein kaksivaiheinen: ensin tieto salataan käyttäen sattumanvaraisesti luotua symmetristä avainta. Tämän jälkeen symmetrinen avain salataan käyttäen viestin vastaanottajan julkista avainta. [AdL99]

Epäsymmetrisiä salausalgoritmeja ovat muun muassa RSA (Rivest-Shamir-Aldeman), joka on yksi tunnetuimmista ja Diffie-Hellman. [Lin02, Sta03]

## **3.2 Turvallisuusinfrastrukturi**

Tässä luvussa esitellään turvallisuusinfrastruktuurin tarkoitus (luku 3.2.1) ja turvallisuusinfrastruktuurin toimittamia palveluita (luku 3.2.2). Luku perustuu pääosin lähteeseen [AdL99].

### **3.2.1 Turvallisuusinfrastruktuurin tarkoitus**

*Infrastruktuurin* periaatteena on, että erilaiset itsenäiset kokonaisuudet voivat käyttää sitä hyödykseen; se toimii ikään kuin kaikkialle leviävänä alustana. Esimerkkinä mainittakoon sähkövoima-infrastrukturi. Sähkövoiman avulla suuri määrä sähkölaitteita saa jännitteen ja sähkövirran, joita ne tarvitsevat toimiakseen. Myös turvallisuusinfrastruktuurin tulee noudattaa samaa periaatetta.

Turvallisuusinfrastrukturi tarjoaa turvallisuusperustan koko organisaatiolle. Infrastruktuurin tulee olla kaikkien turvallisuutta tarvitsevien sovellusten käytettävissä. Turvallisuusinfrastruktuurin liittymiskohtien tulee olla tarkoituksenmukaisia ja samanlaisia (vertaa: sähköpistorasiat seinässä).

Turvallisuusinfrastruktuurin päätavoitteena on toimia sovellusten käytön mahdollistajana. Sähkövoimainfrastrukturi mahdollistaa "sovellusten", kuten leivänpaahtimien ja lamppujen, oikean toiminnan. Turvallisuusinfrastruktuurin avulla sovellukset lisäävät turvallisuutta omaan tietoonsa ja kanssakäymiseen muun tiedon kanssa. Turvallisuuden lisäämisen täytyy olla helppoa ja nopeasti toteutettavissa. Infrastruktuuriin pääsyn tulee olla yhtä helppoa kuin sähkölaitteen töpselin paneminen pistorasiaan:

- täytyy olla olemassa helppokäyttöinen rajapinta
- infrastruktuurin toimittaman palvelun täytyy olla odotettu ja hyödyllinen
- infrastruktuuria käyttävän laitteen ei tarvitse tietää kuinka infrastruktuuri toteuttaa palvelun.

Leivänpaahtimelle on aivan sama kuinka sähkö kulkee voimalaitokselta taloon ja talon eri pistorasioihin. Tärkeää on vain se, että kun leivänpaahtimen töpseli pannaan mihin tahansa pistorasiaan, se saa sieltä tarvitsemansa palvelun eli sähkön. Samalla tavalla myös turvallisuusinfrastruktuurilla täytyy olla tunnetut "sisäänmenokohdat", jotka toimittavat turvallisuuspalvelun sitä tarvitseville laitteille. Laitteiden ei tarvitse tietää, kuinka tämä tapahtuu. Olennaista on se, että se tapahtuu yhdenmukaisesti ja oikein.

### **3.2.2 Turvallisuusinfrastruktuurin toimittamia palveluja**

Turvallisuusinfrastruktuurin toimittamia palveluja ovat tässä luvussa tarkasteltavat: turvallinen sisäänkirjautuminen, huomaamattomuus käyttäjälle ja kokonaisvaltainen turvallisuus.

#### **3.2.2.1 Turvallinen sisäänkirjautuminen**

Sisäänkirjautumis-tapahtumassa käyttäjä tunnistetaan käyttäjätunnuksen avulla ja todennetaan salasanalla. Oletuksena on, ettei kukaan muu kuin laillistettu käyttäjä tunne käyttäjätunnusta ja salasanaa. Sisäänkirjautumisprosessi on tunnettu, samoin siihen liittyvät ongelmat. Jos sovellus, johon käyttäjän pitää kirjautua, sijaitsee esimerkiksi toisella tietokoneella, suojattomissa tietoverkoissa kulkevat salasanat ovat salakuunneltavissa.

Turvallisuusinfrastruktuuri mahdollistaa paikallisen sisäänkirjautumisen. Eli käyttäjä sisäänkirjautuu laitteeseen, jota hän fyysisesti käyttää. Onnistunut tulos tarjotaan turvallisesti etäsovellukselle, kun sitä tarvitaan. Turvallisuusinfrastruktuuria käyttämällä poistetaan salasanoihin yleisimmin liittyvä ongelma eli niiden kuljettaminen turvattomissa tietoverkoissa.

Sisäänkirjautumiseen liittyvät ongelmat vaikeutuvat, kun käyttäjän täytyy päästä useisiin sovelluksiin, joihin jokaiseen pitää erikseen sisäänkirjautua. Saman salasanan käyttäminen kaikkiin sovelluksiin vähentää turvallisuutta ja eri salasana jokaiseen eri sovellukseen vähentää käyttömukavuutta. Turvallisuusinfrastruktuuri mahdollistaa onnistuneen sisäänkirjautumistapahtuman välittämisen toiselle laitteelle, joka

normaalisti vaatii sisäänkirjautumista. Tämä ominaisuus on laajennettavissa niin, että onnistunut sisäänkirjautumistapahtuma voidaan välittää usealle etälaitteelle. Näin poistetaan usean sisäänkirjautumisen tarve, puhutaan kertakirjautumisesta. *Kertakirjautuminen* (single sign-on) mahdollistaa pääsyn useisiin palveluihin ja verkkoihin samalla kertaa [VM03].

Turvallinen kertakirjautuminen on palvelu, jonka turvallisuusinfrastruktuuri voi toimittaa kaikille sitä käyttäville sovelluksille ja laitteille. Infrastruktuuri sisältää mekanismin, jonka avulla autentikointi-informaatio välitetään turvallisesti sinne, missä sitä tarvitaan. Tämä infrastruktuurin palvelu helpottaa käyttäjää, koska hänen ei tarvitse kirjautua monta kertaa. Hyvin suunniteltu infrastruktuuri voi varmistaa, että käyttäjä kirjautuu vain koneelle, jolla hän työskentelee. Näin ollen salasanat eivät liiku suojaamattomassa tietoverkossa.

### **3.2.2.2 Huomaamattomuus käyttäjälle**

Yksi infrastruktuurin piirteistä on sen lähes totaalinen huomaamattomuus käyttäjälle. Sama pätee myös turvallisuusinfrastruktuuriin. Käytännöllisesti katsoen turvallisuuden tulee olla käyttäjältä piilossa. Käyttäkseen palveluita käyttäjä ei tarvitse lisäoppaita eikä hänen tarvitse tietää mitään avaimista ja algoritmeista. Käyttäjien tekemien virheiden vaikutus turvallisuuteen on pieni. Turvallisuus ei myöskään saa hankaloittaa käyttäjän tekemää työtä. Turvallisuus ei vaadi käyttäjältä mitään erityistä tietoa tai toimenpiteitä eikä se myöskään saa kuormittaa käyttäjää erityisillä viivytyksillä. Sisäänkirjautumis-tapahtumaa lukuun ottamatta, infrastruktuurin tulee suorittaa turvallisuuteen liittyvät tehtävät, niin ettei käyttäjä niitä huomaa.

Vaikka turvallisuuteen liittyvien tehtävien tulee olla käyttäjälle huomaamattomia, sääntöön on olemassa kaksi poikkeusta. Ensimmäinen poikkeus: käyttäjä pitää tehdä tietoiseksi infrastruktuurista, kun hän ensimmäistä kertaa on sen kanssa tekemisissä (käyttöönottovaiheen yhteydessä). Toinen poikkeus: käyttäjää pitää informoida, jos turvallisuusinfrastruktuuri ei pysty toimittamaan palvelujaan. Esimerkiksi, kun tunnistautuminen epäonnistuu tai etäpalvelimeen ei pysytä muodostamaan turvallista yhteyttä.

### **3.2.2.3 Kokonaisvaltainen turvallisuus**

Turvallisuusinfrastruktuurin tärkein etu on sen takaama yksi, luotettu turvallisuusteknologia, joka on kaikkien siihen liittyvien osapuolten saatavilla. Rajaton

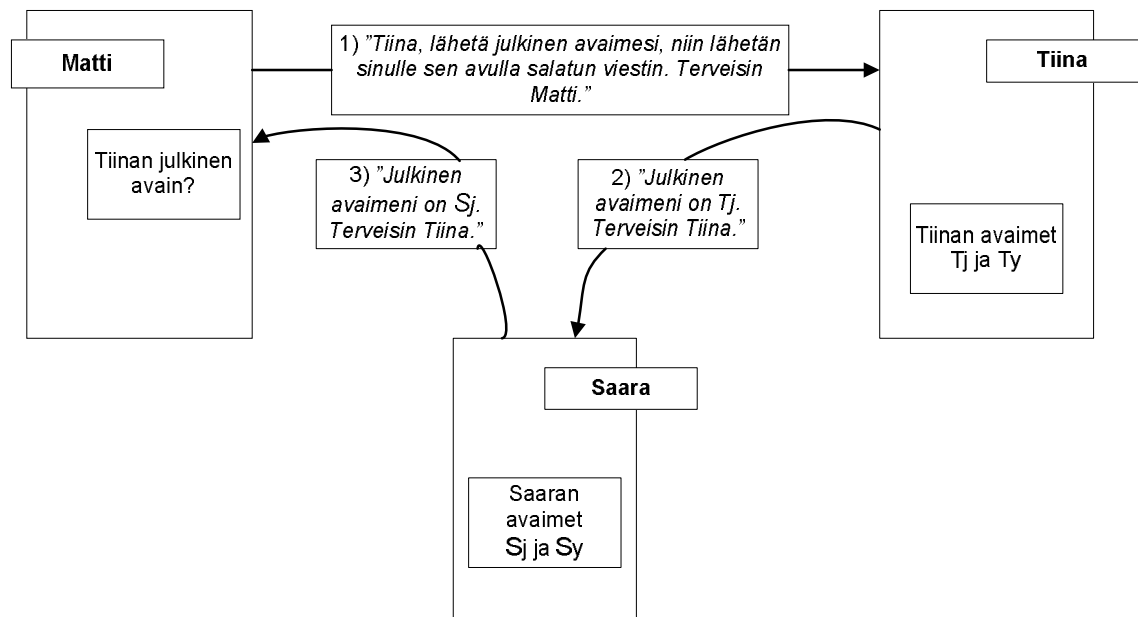
määrä sovelluksia, laitteita ja palvelimia voi työskennellä yhdessä saumattomasti turvataksien tiedon kuljetuksen, varastoinnin ja haun. Sähköpostisovellukset, web-selaimet ja palomuurit ymmärtävät ja pystyvät hyödyntämään turvallisuusinfrastruktuuria yhtenäisellä tavalla. Tämä helpottaa loppukäyttäjän kanssakäymistä eri laitteiden ja sovellusten kanssa. Myös laitteiden ja sovellusten turvallisuustason noudattamisen varmistaminen on näin yksinkertaisempaa.

Infrastruktuurin puitteissa kokonaisvaltainen turvallisuus saavutetaan varmistamalla avainten käytön, ymmärtämisen ja käsittelyn yhdenmukaisuudesta kaikkien organisaatiokokonaisuuksien ja laitteiden suhteen. Ilman kaikkialle leviävää turvallisuusinfrastruktuuria, on mahdotonta saavuttaa samantasoinen toiminnallinen yhdenmukaisuus.

### **3.3 Taustaa julkisen avaimen järjestelmän käytön tarpeellisuudelle**

Luvussa 3.1.2 esitettiin julkisen avaimen salauksen periaate. Siinä lähetettävä viesti salataan vastaanottajan julkisella avaimella. Herää kysymys: Mistä viestin lähettäjä on saanut vastaanottajan julkisen avaimen ja kuinka hän voi olla varma, että julkista avainta vastaavan yksityisen avaimen omistaja on viestin oikea vastaanottaja [Lin02]? Kuvassa 5 on esitetty tilanne, jossa viestin lähettäjä (Matti) pyytää viestin vastaanottajalta (Tiina) tämän julkista avainta sähköpostitse ja sähköpostiliikennettä salakuuntelee Saara. Tilanne kuvastaa niin sanottua *välimeshyökkäystä* (man-in-the-middle attack) eli verkossa tapahtuvaa hyökkäystä,

"jossa kahden viestijän väliin tunkeutuu näiden huomaamatta kolmas osapuoli, joka sieppaa viestit ja saattaa aiheuttaa vahinkoa muuttamalla tai poistamalla viestejä, urkkimalla salausavaimia tai korvaamalla pyydetyn julkisen avaimen omalla julkisella avaimellaan [VM03]."



Kuva 5. Yksi välimieshyökkäyksen tekotapa, mukailtu [Lin02]

Kuvasta nähdään, että Mattin ja Tiinan välistä sähköpostiliikennettä salakuuntelee Saara. Tiina luulee lähettävänsä julkisen avaimensa Matille, mutta Tiinan viestin (viesti 2) nappaa Saara. Hän korvaa Tiinan avaimen omalla julkisella avaimellaan ja lähettää sähköpostiviestin Matille (viesti 3). Matti vastaanottaa viestin, jonka luulee olevan Tiinalta. Seuraavaksi Matti salaa lähetettävän viestin saamallaan julkisella avaimella, jonka luulee kuuluvan Tiinalle. Todellisuudessa julkinen avain on Saaran, joka salakuuntelee liikennettä. Saara saa haltuunsa salatun viestin ja pystyy avaamaan sen omalla yksityisellä avaimellaan. Tiina ei välttämättä saa koskaan viestiä ja vaikka saisikin, ei hän pysty sitä avaamaan. [Lin02]

Välimieshyökkäystä voidaan ajatella väärinkäyttötapauksena. "*Väärinkäyttötapa*us on käyttötapaus, jossa toimija haluaa käyttää systeemiä tahallaan väärin." Väärinkäyttötapaukset tulee ottaa huomioon muun muassa vaatimusten etsimisessä ja analyysissä. Väärinkäyttötapausten aikainen havaitseminen etenkin turvallisuuteen liittyvissä asioissa on tärkeää. [Lin04]

Julkinen avain julkistetaan hakemistopalvelimella. Haettaessa avainta hakemistosta, joku voi väärentää sen matkan varrella. Hakemistoon voidaan myös murtautua tai hakemiston ylläpitäjä ei välttämättä ole rehellinen [Lin02]. Julkisen avaimen voi myös julkaista Internetissä omalla kotisivullaan. Myös www-palvelimelle voidaan murtautua ja korvata siellä oleva avain omalla avaimella. [Jär96]

Matin tulee siis jotenkin varmistua siitä, että julkista avainta vastaava yksityinen avain on nimenomaan Tiinan hallussa. Julkisen avaimen järjestelmän avulla on mahdollista yhdistää tietty julkinen avain sitä vastaavan yksityisen avaimen haltijan nimeen. Käyttämällä julkisen avaimen järjestelmää, estetään edellä kuvattu välimieshyökkäys. [Lin02]

Julkisen avaimen järjestelmässä avainasemassa on julkisten avainten jakelu. Luotettava tapa on hakea julkinen avain sen haltijalta henkilökohtaisesti. Jos osapuolet tuntevat toisensa äänen perusteella, voidaan julkinen avain antaa myös puhelimitse. Entä, jos osapuolet asuvat kaukana toisistaan tai eivät tunne toisiaan? Julkisen avaimen järjestelmän ratkaisu julkisten avainten jakeluun on niin sanotun luotetun (kolmannen) osapuolen (trusted third party, TTP) käyttö [Lin02]. *Luotettu osapuoli* on usein viranomainen tai tunnettu yritys, jolle uskotaan erityistä luottamusta vaativia tehtäviä [VM03]. Tämä luotettu taho allekirjoittaa julkiset avaimet omalla yksityisellä avaimellaan. Tällä allekirjoituksella varmistetaan tietyn julkisen avaimen kuuluminen tietylle henkilölle tai esimerkiksi palvelimelle. Allekirjoitettuja julkisia avaimia kutsutaan varmenteiksi ja luotettua osapuolta varmentajaksi. Allekirjoitetut varmenteet ovat haettavissa julkisesta varmennehakemistosta. [Lin02]

### 3.4 PKI:n osapuolet

Tässä luvussa tarkastellaan julkisen avaimen järjestelmän osapuolia. Osapuolet ovat: varmenne, varmentaja, rekisteröijä, varmennehakemisto, varmennearkisto, varmenteen haltija ja varmenteeseen luottava osapuoli. Luku perustuu pääosin lähteeseen [Lin02].

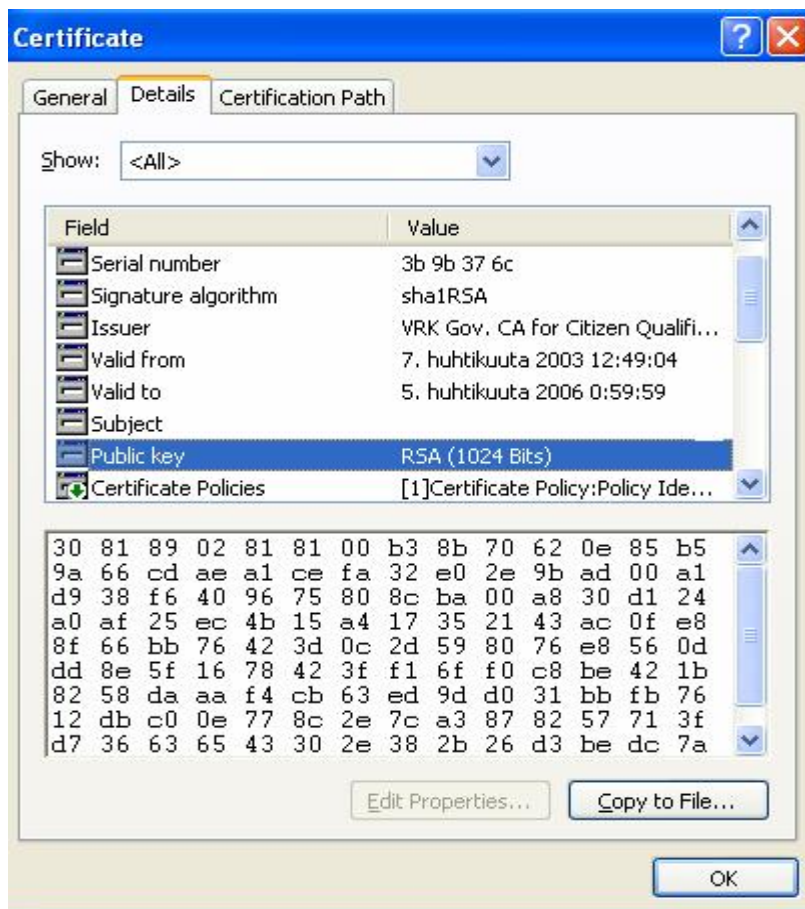
#### 3.4.1 Varmenne (certificate)

Varmenne on PKI:n keskeinen komponentti. Se yhdistää tietyn julkisen avaimen ja tietyn henkilön tai esimerkiksi palvelimen toisiinsa [Hun01, Lin02]. *Varmenne* on

"konekoodinen aitoustodistus, jonka ulkopuolinen luotettu taho (varmentaja) on myöntänyt palveluverkossa asiakkaana, palveluntuottajana, varmentajana tai muussa ominaisuudessa toimivalle. Varmenne on julkinen, mutta allekirjoitettu varmentajan omalla yksityisellä avaimella, jolloin sen aitouden voi todeta avaamalla varmenteen varmentajan julkisella avaimella" [VM03].

Jotta varmenne on kaikkien sitä tarvitsevien osapuolten luettavissa, on varmenteen muodon oltava standardoitu. ITU-T (International Telecommunication Union) on standardoinut X.500-hakemiston, jonka yhteydessä on määritelty varmenteen esitystapa nimeltään X.509. Tämän hetken käytetyimmät varmenteet Internetissä ovat X.509v3-varmenteita eli kolmannen version mukaisia varmenteita. X.509-varmenteeseen sisältyy kenttiä, joita on määritelty noin 30. Kenttiä on sekä pakollisia että vapaaehtoisia. Varmenne sisältää muun muassa varmenteen haltijan julkisen avaimen, varmenteen haltijan nimen ja varmentajan nimen. Vapaaehtoinen kenttä on esimerkiksi varmennetta myönnettäessä käytetyn varmennepoliitikan tunnus.

Kuvassa 6 on osa yhdestä Väestörekisterikeskuksen varmennehakemistosta haetusta kansalaisvarmenteesta. Varmenteen omistajan nimi on pyyhitty pois, mutta osa hänen julkisesta avaimestaan on näkyvissä. Varmennehakemistosta löytyvät kaikki Väestörekisterikeskuksen myöntämät, yleisesti käytössä olevat varmenteet. Varmennehakemisto löytyy Internetistä sivulta: <http://www.fineid.fi/vrk/fineid/home.nsf/suomi/varmennehakemisto>.



Kuva 6. Väestörekisterikeskuksen myöntämä kansalaisvarmenne

### 3.4.2 Varmentaja (certification authority, CA)

Yksi olennainen osa julkisen avaimen järjestelmää on varmentaja. *Varmentaja* on

"julkisen avaimen järjestelmässä luotettu taho, joka tuottaa järjestelmän käyttäjille avainparit ja tuottaa, allekirjoittaa ja jakelee varmenteet ja tallettaa ne julkiseen hakemistoon sekä tarvittaessa peruuttaa varmenteet" [VM03].

Allekirjoituksellaan varmentaja takaa tietyn yksityisen avaimen kuulumisen tietylle henkilölle. Lisäksi varmentaja takaa, että myös muut varmenteissa olevat tiedot ovat oikein.

Jos yksityinen avain jostain syystä häviää, paljastuu tai joutuu väärin käsiin, pitää siitä mahdollisimman nopeasti ilmoittaa varmentajalle. Varmenne asetetaan tällöin *sulkulistalle* (*certification revocation list, CRL*), joka on käytöstä poistettujen varmenteiden luettelo, jonka varmentaja on digitaalisesti allekirjoittanut. Myös varmenteen tietojen muuttuessa tai varmenteen käytössä tarpeettomaksi se on asetettava sulkulistalle.

Varmentajan tehtävät voidaan automatisoida ja ne hoitaa sisäinen palvelin tai luotettu kolmas osapuoli, esimerkiksi VeriSign. Kun organisaatio toteuttaa PKI:n, se voi itsenäisesti toteuttaa varmennepalvelut tai käyttää kaupallisen varmentajan palveluja. Kaupallisia toteutuksia on olemassa kahta eri mallia. Ensimmäisessä mallissa organisaatio hankkii käyttöönsä koko PKI-systeemin (esimerkiksi Entrust's PKI 4.0), joltain PKI-ratkaisuja toimittavalta yritykseltä. Tässä tapauksessa organisaatiosta tulee oma varmentajansa ja se on itse vastuussa varmenteiden myöntämisestä ja hallinnasta. Toisessa mallissa varmenteita ostetaan varmenneorganisaatiolta tarpeen mukaan (esim. VeriSign). [Hun01]

Varmentajalla on kokonaisvastuu varmentamistoiminnasta. Osa tehtävistä voidaan kuitenkin delegoida alihankkijoille. Yksi alihankkijoista on rekisteröijä.

### 3.4.3 Rekisteröijä (registration authority, RA)

Varmennetta hakevan rekisteröinnin voi hoitaa varmentaja, mutta joskus on järkevää siirtää rekisteröintitehtävä erilliselle taholle, jota kutsutaan *rekisteröijäksi*. Joissakin

tapauksissa tiettyyn PKI-alueeseen liittyvien loppukäyttäjien määrä kasvaa tai loppukäyttäjät sijaitsevat maantieteellisesti laajalla alueella. Näissä tapauksissa on järkevää käyttää useita paikallisia rekisteröijä. Osa varmentajan tehtävistä voidaan siirtää rekisteröijälle; näin parannetaan skaalautuvuutta, lisätään palvelun tehokkuutta ja vähennetään operationaalisia kuluja. [AdL99]

Rekisteröijän tehtäviä ovat muun muassa: varmennetta hakevan henkilöllisyydestä varmistuminen ja yksityisen avaimen sisältävän laitteen, esimerkiksi toimikortin, luovuttaminen varmenteen hakijalle. Esimerkiksi nämä ovat paikallisen poliisilaitoksen tehtävät, kun kansalainen hakee Väestörekisterikeskukselta kansalaisvarmennetta. *Kansalaisvarmenne* on "väestörekisterikeskuksen tuotteistama ja ylläpitämä varmenne" [VM03].

#### **3.4.4 Varmennehakemisto (certificate repository)**

*Varmennehakemisto* on "julkinen hakemisto, joka sisältää tietyn varmennehallinnon puitteissa myönnetyt, varmentajan allekirjoittamat varmenteet" [VM03]. Myös sulkulista sijaitsee usein varmennehakemistossa. Sovellukset hakevat varmenteet hakemistosta käyttäjälle [Ker99]. Varmennehakemisto on useasti julkinen, mutta se voi myös olla ainoastaan organisaation sisäiseen käyttöön tarkoitettu.

Varmentaja ja rekisteröijä ovat luotettuja tahoja, mutta varmennehakemiston ylläpitäjän ei tarvitse olla luotettu taho. Varmenteita ei voida enää muokata, koska ne sisältävät digitaalisen allekirjoituksen. Varmennehakemiston ylläpitäjän vastuulla on taata palvelun saatavuus. Asiointi varmennehakemiston kanssa tapahtuu LDAP-protokollan välityksellä. *LDAP* (Lightweight Directory Access Protocol) on "X.500-hakemiston kanssa yhteensopiva yksinkertainen saantikäytäntö" [VM03]. LDAP-protokolla määrittelee tietoliikenneprotokollan sekä tietojen esittämisen hierarkkisen rakenteen.

#### **3.4.5 Varmennearkisto**

*Varmennearkistoon* varastoidaan myönnetyt varmenteet ja sulkulistat. Kun varmenteen voimassaolo päättyy, varmenne siirretään varmennehakemistosta varmennearkistoon. Varmennearkistoa tarvitaan tapauksissa, joissa varmenteen voimassaolon päättyttyä halutaan selvittää, oliko varmenne aito ja voimassaoleva tiettyä ajankohtana.

### **3.4.6 Varmenteen haltija**

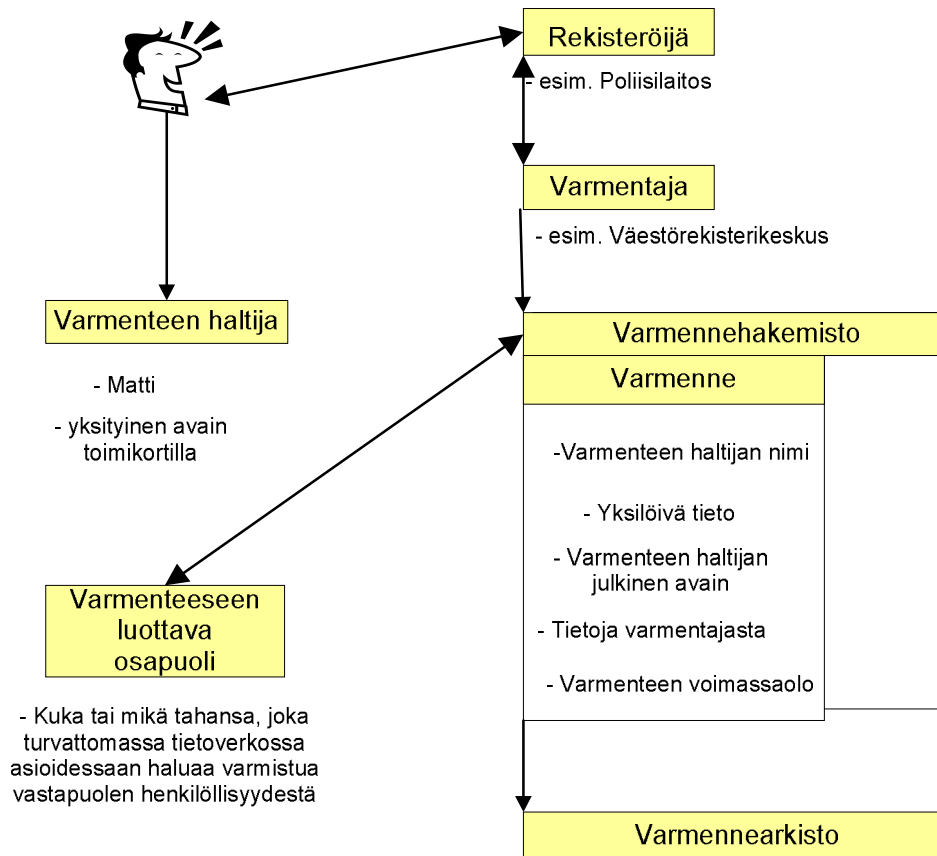
*Varmenteen haltijan* nimi on kirjattu varmenteessa kohtaan varmenteen kohde. Varmenteen haltija on luonnollisesti se, jonka hallussa on varmenteeseen liittyvä yksityinen avain, joka sijaitsee esimerkiksi toimikortilla. Julkisen avaimen järjestelmä on rakennettu varmenteen haltijan todentamista varten. Varmenteen haltijan vastuulla on suojella yksityistä avainta, niin ettei se häviä. Jos varmenteen haltija hukkaa yksityisen avaimensa, hänen tulee ilmoittaa siitä heti varmentajalle, jonka vastuulla on varmenteen laittaminen sulkulistalle.

### **3.4.7 Varmenteeseen luottava osapuoli**

Julkisen avaimen järjestelmä on olemassa *varmenteeseen luottavaa osapuolta* varten. Julkisen avaimen järjestelmän avulla varmenteisiin luottava osapuoli voi varmistua, että osapuoli, jonka kanssa hän turvattomassa tietoverkossa asioi, on se, kuka hän väittää olevansa.

Ensimmäiseksi varmenteeseen luottavan osapuolen tulee hankkia varmentajan *juurivarmenne*, joka on "tietyn varmenneorganisaation ylimmän varmentajan varmenne, jonka se on itse allekirjoittanut", tämän jälkeen alkaa varmenneketjun todentaminen. (Varmentajan juuresta lisää kappaleessa 3.8.1). Varmenneketjua rakentaessaan varmenteeseen luottavan osapuolen tulee todentaa ketjun jokainen lenkki aina varmenteen haltijan varmenteeseen saakka. Varmenteeseen luottavan osapuolen on myös tarkistettava, että varmenteen allekirjoitukset on tehty ketjun edellisen varmenteen yksityisellä avaimella. Lisäksi varmenteeseen luottavan osapuolen tulee tarkistaa, että varmenne on voimassa, eikä se ole sulkulistalla.

PKI:n osapuolet on esitetty kuvassa 7.



Kuva 7. PKI:n osapuolet

Kuvassa esiintyvä Matti haluaa hankkia itselleen sähköisen henkilökortin, joka sisältää kansalaisvarmenteen. Korttia haetaan paikalliselta poliisilaitokselta, jonka tehtävänä on todentaa Mattin henkilöllisyys esimerkiksi passista. Hakemus lähetetään Väestörekisterikeskukselle, joka toimii varmentajana. Varmentaja toimittaa varmenteen ja yksityisen avaimen sisältävän henkilökortin takaisin poliisilaitokselle, josta Matti voi sen noutaa. Korttia noutaessaan hänen pitää todistaa henkilöllisyytensä. Varmentaja toimittaa varmenteen myös varmennehakemistoon. Kun Matilla on sähköinen henkilökortti, voi hän asioida esimerkiksi KELA:n sähköisessä asiointipalvelussa, joka edellyttää asiakkaan sähköistä tunnistamista. KELA on tässä tapauksessa varmenteeseen luottava osapuoli.

### 3.5 Varmennepolitiikka (certificate policy, CP)

*Varmennepolitiikka* on "varmentajan julkaisema asiakirja, jossa kuvataan, miten varmennepalveluja tuotetaan niiden käyttäjille" [VM03]. Varmennepolitiikan avulla varmentaja esittää perusteet sen myöntämien varmenteiden turvallisuudelle ja julkisten avainten aitoudelle ja eheydelle. Varmennepolitiikassa kuvattavia asioita ovat [Ruo02]:

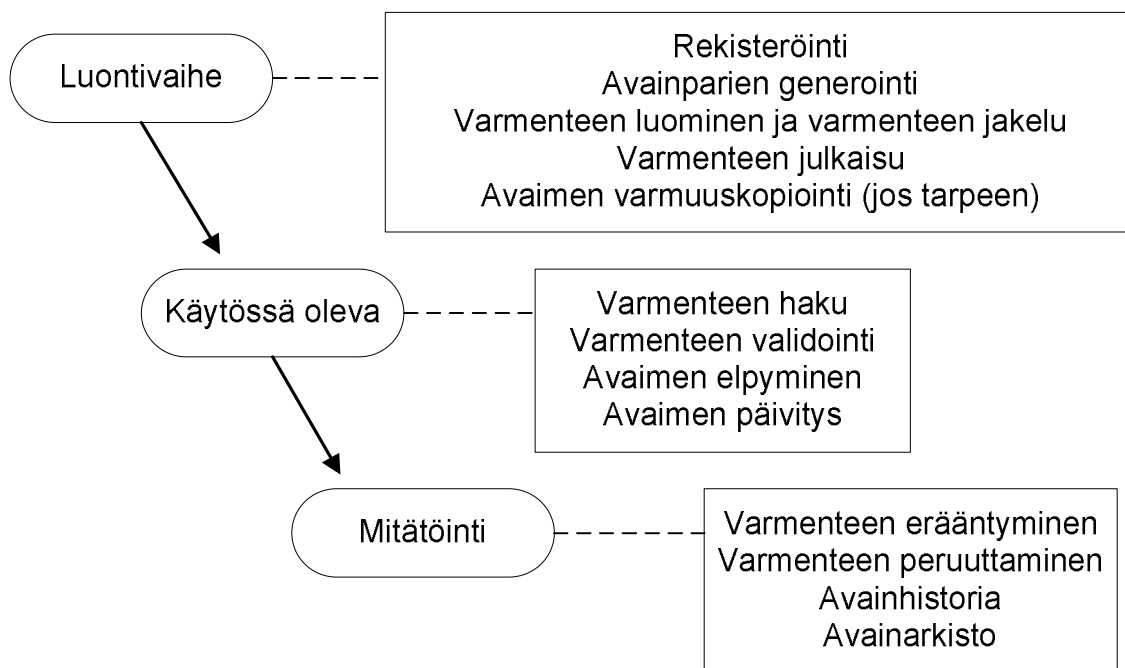
- osapuolten vastuut ja velvollisuudet,
- varmentajan, rekisteröijän ja varmennehakemiston toiminta ja
- varmennejärjestelmän ylläpito ja hallinnointi.

Varmennepolitiikassa kuvataan varmentajan toiminta yleisellä tasolla. Varmennepolitiikkaan tutustumalla varmenteeseen luottava osapuoli voi arvioida varmentajan myöntämien varmenteiden luotettavuutta [Lin03]. Jokaisella varmennepolitiikalla on oma OID-tunniste, jonka avulla ne erotetaan toisistaan [AdL99].

*Varmennekäytäntölausuma* tai *varmennuskäytäntö* (certificate practises statement, CPS) sisältää varmennepolitiikan käytännön toteutuksen. Se sisältää yksityiskohtaisia tietoja käytännöistä ja toimintatavoista. Näiden yksityiskohtaisten tietojen takia varmennekäytäntölausuma on hyvä pitää salaisena, jotta sen sisältämiä tietoja ei voida käyttää luvattomiin tarkoituksiin [Lin03]. Myös varmennuskäytännöllä on oma yksilöivä OID-tunniste.

### 3.6 Varmenteen elinkaaren hallinta

Julkinen avain jaetaan yleensä varmenteen muodossa. Sen sijaan yksityinen avain on erillinen tietorakenne, joka tulee aina suojella paljastumiselta. Sekä varmenne että yksityinen avain voivat sijaita toimikortilla. Varmenteen elinkaaren hallinta pitää sisällään toiminnot, jotka liittyvät avainparien ja niihin liittyvän varmenteen luontiin, käyttöön ja mitätöintiin. Nämä vaiheet on esitetty kuvassa 8. Luku perustuu lähteeseen [AdL99].



Kuva 8. Varmenteen elinkaaren hallinta

Kokonaisvaltaiseen varmenteen elinkaaren hallintaan liittyy seuraavat oletukset:

- ei ole käytännöllistä, että loppukäyttäjä hallinnoisi varmenteen elinkaarta,
- varmenteen elinkaaren hallinnan tulisi olla niin automatisoitua kuin mahdollista,
- varmenteen elinkaaren hallinnan tulee olla loppukäyttäjälle niin huomaamatonta kuin mahdollista ja
- varmenteen elinkaaren hallinta edellyttää turvallista kanssakäymistä luotettujen osapuolten, kuten rekisteröijän ja varmentajan kanssa, sen lisäksi pitää olla olemassa loppukäyttäjän ohjelmisto, joka kommunikoi näiden komponenttien kanssa, kun tarpeellista.

Seuraavissa aliluvuissa tarkastellaan varmenteen elinkaaren jokaista vaihetta erikseen.

### 3.6.1 Varmenteen luominen

Ennen kuin loppukäyttäjät voivat käyttää PKI:n tarjoamia palveluja, heidät täytyy liittää osaksi PKI:ää. Varmenteen luominen koostuu: loppukäyttäjän rekisteröinnistä, avainparin luomisesta, varmenteen luomisesta ja varmenteen jakamisesta, varmenteen julkaisemisesta ja avaimen varmuuskopiointista (jos tarpeen).

*Loppukäyttäjän rekisteröinti* on prosessi, jossa käyttäjä tai prosessi ilmoittautuu joko rekisteröijälle tai varmentajalle. Ilmoittautumisen vastaanottaja todentaa ilmoittautujan. Rekisteröinti voi tapahtua henkilökohtaisesti tai sähköisesti.

*Avainparin luominen* koostuu julkisen avaimen ja yksityisen avaimen luomisesta. Avaimet luodaan etukäteen tai loppukäyttäjän rekisteröinnin yhteydessä. Kokonaisvaltaisessa PKI-mallissa on mahdollista generoida avaimet loppukäyttäjän asiakassysteemissä, rekisteröijän tai varmentajan toimesta. Avainparin generointipaikkaan vaikuttavat muun muassa suorituskyky ja avainten aiottu käyttö.

*Varmenteen luominen* on ainoastaan valtuutetun varmentajan vastuulla. Jos julkisen avaimen on generoinut joku muu kuin varmentaja, täytyy julkinen avain kuljettaa turvallisesti varmentajalle, jotta se voidaan panna varmenteeseen.

Kun avainpari ja siihen liittyvä varmenne on generoitu, ne pitää asianmukaisesti *jakaa* loppukäyttäjille. Myönnetty varmenne jaetaan suoraan sen omistajalle, hakemistoon tai molempiin.

*Varmenteen julkaisemisella* tarkoitetaan sitä toimenpidettä, jolla varmenne saadaan muiden sitä tarvitsevien käyttäjien saataville. Varmenteet julkaistaan esimerkiksi yleisessä hakemistossa, josta ne ovat helposti saatavilla.

Luomisvaihe voi myös sisältää *avaimen varmuuskopioinnin* luotetun kolmannen tahon toimesta. Se ei kuitenkaan ole pakollinen toimenpide.

### **3.6.2 Varmenteen käyttäminen**

Kun avainpari ja varmenne on tehty, alkaa varmenteen käyttövaihe. Tähän vaiheeseen kuuluu: varmenteen haku, varmenteen todentaminen, avaimen elpyminen ja avaimen päivitys.

*Varmenteen haulla* tarkoitetaan sitä, kun varmenteeseen luottava osapuoli käyttää varmennetta. Varmennetta tarvitaan tilanteessa, jossa joko halutaan salata tietylle käyttäjälle tarkoitettua tietoa tai halutaan varmistua sähköisen allekirjoituksen aitoudesta.

*Varmenteen todentamisella* tarkoitetaan varmenteen laillisuuden arviointia. Varmenteen todentaminen täytyy suorittaa ennen varmenteen käyttöä. Vähimmillään todentamiseen kuuluu:

- varmenteen eheyden todentaminen,
- varmistuminen siitä, että varmenteen on myöntänyt luotettu varmentaja,
- varmistuminen varmenteen voimassaolosta ja
- varmistuminen siitä, että varmennetta käytetään politiikan mukaisesti.

On ensiarvoisen tärkeää, että kokonaisvaltaisessa PKI:ssä on automaattinen avaimen varmuuskopiointi ja *elpymispalvelu*. Ennemmin tai myöhemmin jotkut käyttäjät hävittävät yksityisen avaimensa. Ilman varmuuskopiointia ja kykyä elpyä, yksityisen avaimen häviäminen saattaa johtaa tärkeiden tietojen lopulliseen häviämiseen.

Varmenteet myönnetään tietyksi ajaksi. Kun varmenteen erääntymispäivä lähenee, pitää myöntää uusi avainpari ja siihen liittyvä varmenne. Tätä toimenpidettä kutsutaan *avaimen päivitykseksi*.

### **3.6.3 Varmenteen mitätöinti**

Varmenteen elinkaaren hallinnan päättää varmenteen mitätöinti. Mitätöintivaiheeseen kuuluu: varmenteen erääntyminen, varmenteen peruuttaminen, avainhistoria ja avainarkisto.

Varmenteet myönnetään tietyksi ajanjaksoksi. Lopulta varmenteen voimassaolo lakkaa.

*Varmenteen erääntymistä* seuraa jokin seuraavista toimenpiteistä:

- ei toimenpidettä - loppukäyttäjä ei ole enää kirjoilla PKI:ssä,
- varmenteen uudistaminen - sama varmenne saa uuden voimassaoloajan tai
- varmenteen päivitys - luodaan uusi avainpari ja myönnetään uusi varmenne (tämä voi tapahtua ennen kuin varmenne erääntyy, kuten avaimen päivitys - kohdassa on kerrottu).

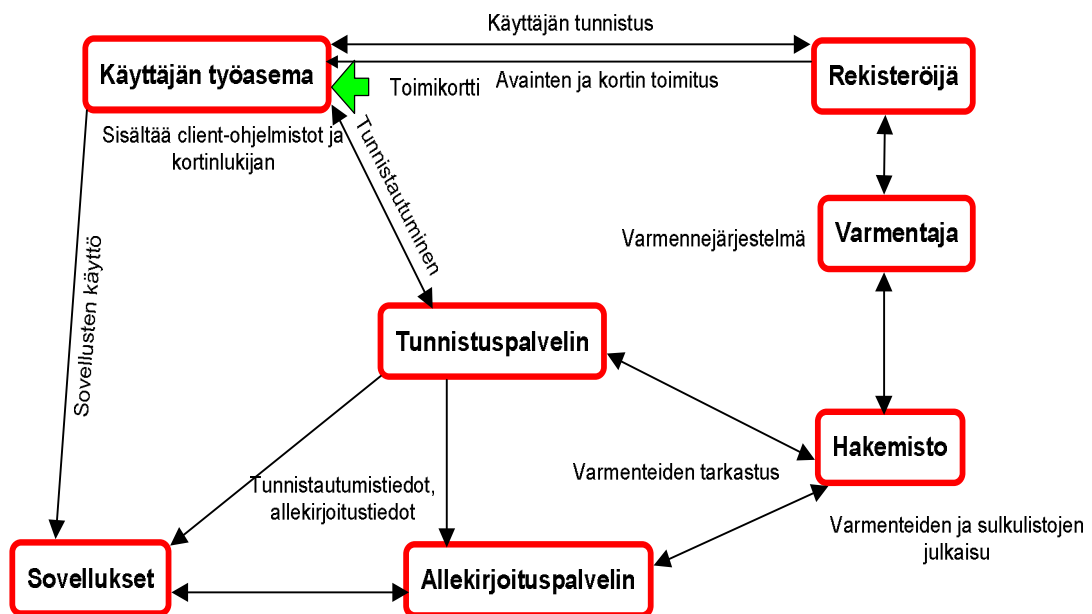
Varmenne voidaan *peruuttaa*, ennen kuin sen voimassaoloaika on mennyt umpeen. Varmenteen peruuttamiseen johtava syy voi olla: epäily yksityisen avaimen paljastumisesta, muutos työtehtävissä tai työsuhteen päättymisen. Varmenteen peruuttamispyyntö tulee tehdä välittömästi, kun siihen ilmenee aiheutta. Ilmoitus tehdään joko rekisteröijälle tai varmentajalle.

*Avainhistoria* mahdollistaa, että salausavainten erääntyessä käyttäjä saa salatut tiedot luettavaan muotoon. Käyttäjän viisi vuotta sitten salaamaa tietoa ei voida purkaa hänen nykyisellä salaisella avaimellaan. Voidakseen purkaa salauksen hän tarvitsee avainhistoriaa. Avainhistorian avulla käyttäjä voi luotettavasti ja turvallisesti varastoida avaimet, vaikka ne ovat erääntyneet. Avainhistoria säilytetään tyypillisesti paikallisesti avaimen omistajan toimesta, jotta se on helposti saatavilla.

*Avainarkisto* huolehtii avainten ja varmenteiden pitkäaikaissäilytyksestä. Avainarkisto eroaa avainhistoriasta siinä, että avainarkistoa käytetään auditointitarkoitukseen sekä kiistojen selvittämiseen, erityisesti, kun ne liittyvät luotettuihin aikaleima- ja notariaattipalveluihin.

### 3.7 PKI:n tekninen toteutus

Kuvassa 9 on esitetty Kuopion yliopiston terveyshallinnon ja -talouden laitoksella toteutettu tietoturvallinen PKI-ympäristö.



Kuva 9. PKI-ympäristön toteutus, mukailtu [Imm04]

PKI-ympäristö sisältää sekä teknisiä laitteita että ohjelmistoja. PKI:n keskeisin toiminto on *varmennejärjestelmä*, johon kuuluu varmentaja ja sen myöntämät varmenteet. Varmennejärjestelmän toimittajia on useita, esimerkiksi SSH ja Smartrust. [Imm04]

Kirjautuessaan järjestelmään tunnistuspalvelin tunnistaa käyttäjän tarkistamalla tämän varmenteen tiedot hakemistosta. Kirjautuminen tapahtuu toimikortin avulla eli käyttäjän työasemalla täytyy tätä varten olla kortinlukija. Allekirjoituspalvelin puolestaan varmentaa allekirjoituksen oikeellisuuden. Lisäksi palvelin voi tarvittaessa generoida allekirjoitukseen aikaleiman. *Aikaleima* on "tapahtumatietoon tai viestiin liitetty tieto lähetys-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista". [VM03] Allekirjoituksen tekemistä varten työasemaan täytyy olla asennettuna allekirjoitusohjelma. [Imm04]

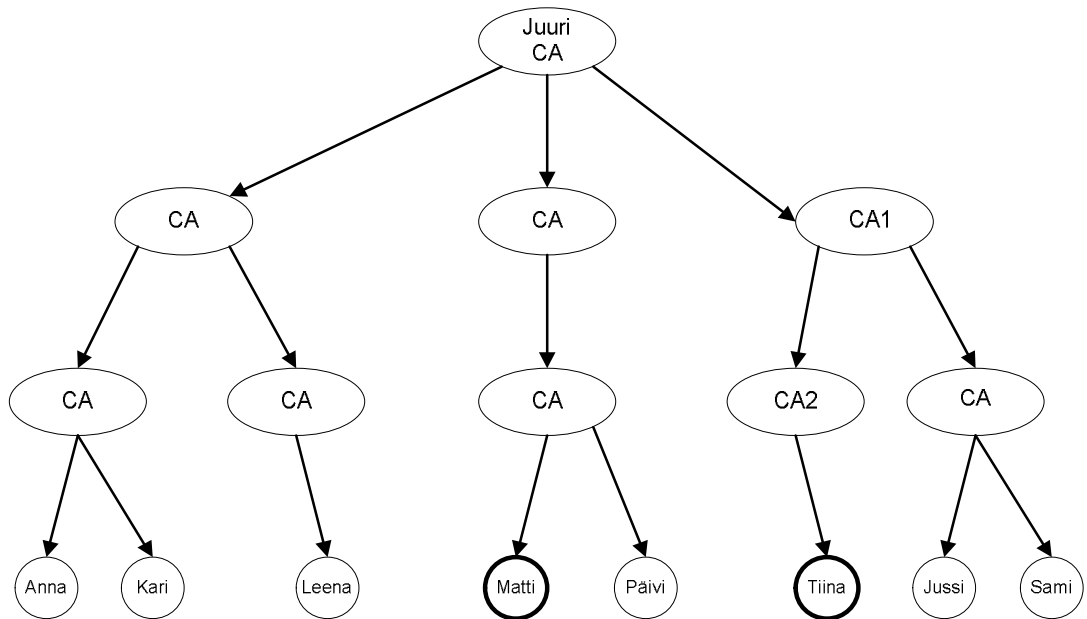
## **3.8 Luottamus**

Luku 3.8.1 käsittelee hierarkkista luottamusmallia. Luvussa 3.8.2 tutustutaan ristiinvarmennukseen. Luku perustuu pääosin lähteeseen [AdL99].

### **3.8.1 Hierarkkinen luottamusmalli**

Varmenteeseen luottavan osapuolen tulee varmentaa varmenneketjun jokainen lenkki. Luottamus täytyy perustua johonkin järjestelmään. Standardissa X.509 luottamus perustuu hierarkkiseen luottamusmalliin [BuD04]. *Hierarkkisessa luottamusmallissa* luottamuksen lähtökohtana on varmentajan julkinen avain [Lin02]. Jokaisella hierarkiaan kuuluvalla on hallussaan kopio juurivarmentajan julkisesta avaimesta. *Juurivarmentaja* on kaikkien PKI:n käyttäjien luottamusankkuri [PHM03]. Juurivarmentaja varmentaa alivarmentajat, joita voi olla useassa tasossa. *Alivarmentaja* on juurivarmentajan alainen varmentaja. Muut varmennehierarkian varmenteet on allekirjoitettu joko varmentajan juureen liittyvällä yksityisellä avaimella tai yksityisellä avaimella, joka liittyy alivarmentajan varmenteeseen.

Hierarkkinen luottamusmalli esitetään tyypillisesti ylösalaisin olevana puuna: juuri ylhäällä, oksat lähtevät alaspäin ja lehdet ovat alimmaisina. Lehdet edustavat loppukäyttäjiä. Hierarkkinen luottamusmalli on esitetty kuvassa 10.



Kuva 10. Hierarkkinen luottamusmalli, mukailtu [AdL99, PHM03]

Tässä mallissa hierarkia muodostuu niin, että juurivarmentaja varmentaa välittömästi alapuolellaan olevat varmentajat ja nämä varmentajat varmentavat välittömästi niiden alapuolella olevat varmentajat. Nämä varmentajat varmentavat loppukäyttäjät.

Ennen kuin varmenteeseen luottava osapuoli käyttää varmenettä, tulee hänen todentaa varmenneketju juuresta alkaen. Varmenteeseen luottava osapuoli Matti voi varmentaa Tiinan varmenteen seuraavalla tavalla:

1. Matti todentaa juurivarmentajan julkista avainta käyttämällä CA1:n varmenteen. Näin hän saa poimittua käyttöönsä kopion CA1:n julkisesta avaimesta.
2. Käyttämällä CA1:n julkista avainta Matti voi todentaa CA2:n varmenteen. Näin hän saa käyttöönsä kopion CA2:n julkisesta avaimesta.
3. CA2:n julkista avainta käyttämällä Matti voi todentaa Tiinan varmenteen. Nyt Matilla on hallussaan kopio Tiinan julkisesta avaimesta.

Hierarkkiseen luottamusmalliin perustuvat PKI:t ovat erittäin tehokkaita, mutta toiminnallisuus vähentää turvallisuutta [ABD00]. Juurivarmenteen tai sitä hierarkkisesti lähellä olevan varmenteen salaisen avaimen paljastuminen olisi katastrofi koko varmenneketjulle [Ruo02].

### 3.8.2 Ristiinvarmennus

*Ristiinvarmennuksessa* muodostetaan luottamusketjuja eri varmentajien välille [BoP03]. Ristiinvarmennuksessa varmentaja A allekirjoittaa varmentajan B julkisen avaimen omalla allekirjoitusavaimellaan ja varmentaja B allekirjoittaa varmentajan A julkisen avaimen omalla allekirjoitusavaimellaan [Lin02]. Jos molemmat varmentajat kuuluvat samaan alueeseen (esimerkiksi organisaation sisäisessä varmennehierarkiassa varmentaja varmentaa alemmalla tasolla olevan varmentajan), puhutaan *sisäisestä ristiinvarmentamisesta*. Sisäinen ristiinvarmentaminen on yksipuolista, eli ainoastaan varmentaja A ristiinvarmentaa varmentajan B. Jos varmentajat kuuluvat eri alueisiin (esimerkiksi organisaation X varmentaja varmentaa organisaation Y varmentajan), puhutaan *alueiden välisestä varmentamisesta*. Alueiden välisessä varmentamisessa ristiinvarmennus on molemminpuolista, eli varmentaja A ristiinvarmentaa varmentajan B ja päinvastoin.

Ristiinvarmentamisen yhteydessä varmentajien tulee tutustua toistensa varmennepolitiikkoihin. Varmennepolitiikoissa voi olla eroja ja on varmentajien asia päättää, voivatko he hyväksyä toistensa varmennepolitiikat ja ovatko niiden sisällöt molemmille riittävät [Ruo02]. Ristiinvarmentamisen toteutumisen esteenä eivät ole tekniset ongelmat, vaan huomio keskittyy nimenomaan varmennepolitiikoiden vertailemiseen [Lin02].

## 3.9 PKI:n tarjoamat ydinpalvelut

PKI tarjoaa neljä turvallista palvelua, jotka ovat: todentaminen, eheys, luottamuksellisuus ja kiistämättömyys.

### 3.9.1 Todentaminen

Järjestelmän käyttäjän, palvelun ja palvelimen vahva todentaminen on perustoiminto, joka kuuluu kaikkiin PKI-sovelluksiin. Kirjautumisen yhteydessä järjestelmä ensin tunnistaa käyttäjän esimerkiksi käyttäjätunnuksen perusteella. Tämän jälkeen järjestelmän on todennettava, että käyttäjä on se, kuka hän väittää olevansa. [Ruo02]

Todentamiseen on olemassa kolme mahdollisuutta [Jär02, Lin02]:

1. Yksilölliset ominaisuudet eli jotain, mitä olet. Vain elävät olennot tunnistetaan yksilöllisten ominaisuuksien perusteella. Kun todentamiseen käytetään

esimerkiksi sormenjälkeä, ääntä tai käsialaa, puhutaan *biometrisestä tunnistuksesta*.

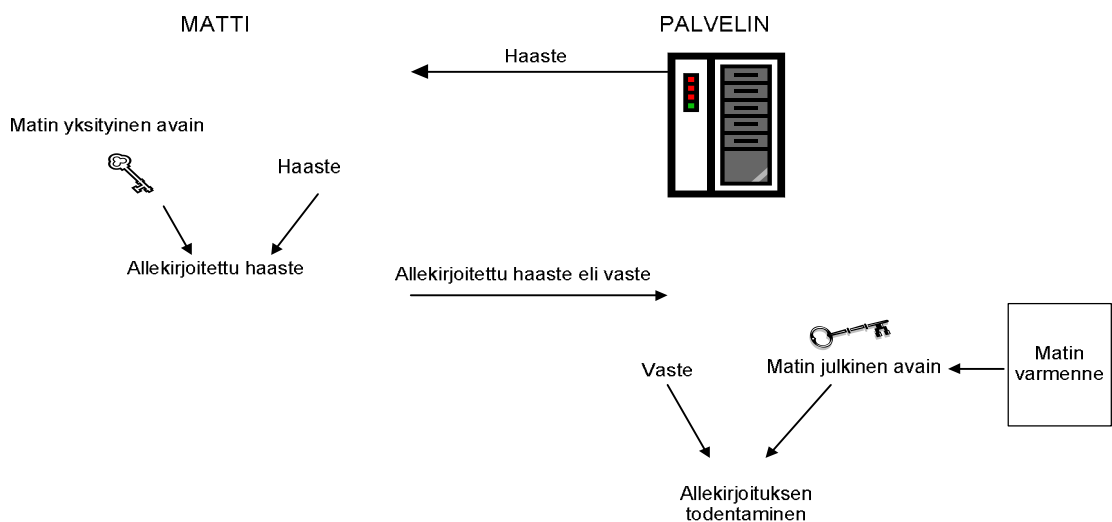
2. Esine eli jotain, mitä sinulla on, esimerkiksi älykortti.
3. Tieto eli jotain, mitä tiedät, esimerkiksi salasana tai PIN-koodi (PIN=Personal Identification Number). Tieto ei saa olla muiden tiedossa.

*Heikosta todentamisesta* puhutaan, kun todentaminen perustuu salasanan tai vastaavan käyttöön. *Vahva todentaminen* perustuu joko siihen, ettei salasanoja lähetetä verkon yli, esimerkiksi PKI, tai vähintään kahteen todentamisen keinoon, esimerkiksi älykortti yhdessä PIN-koodin kanssa [Soh03]. *Luotettavasta todentamisesta* puhutaan, kun molemmat asioivat osapuolet käyttävät tunnettujen varmentajien myöntämiä varmenteita [Ruo02].

Julkisen avaimen järjestelmää käytetään, kun tarvitaan todentamista etäsovelluksiin. Julkisen avaimen järjestelmän etu on, ettei salasanaa tarvitse koskaan lähettää turvattomissa tietoverkoissa.

Esimerkki julkisen avaimen järjestelmään perustuvasta todentamisesta on *haaste/vaste-todentaminen* (kuva 11). Siinä

"kutsuttu palvelin tai viestin saaja pyrkii varmistumaan kutsujan tai lähettäjän aitoudesta ottamalla tähän uuden yhteyden tai esittämällä tälle kysymyksen (haaste), johon vain oikea taho osaa vastata oikein (vaste)" [VM03].



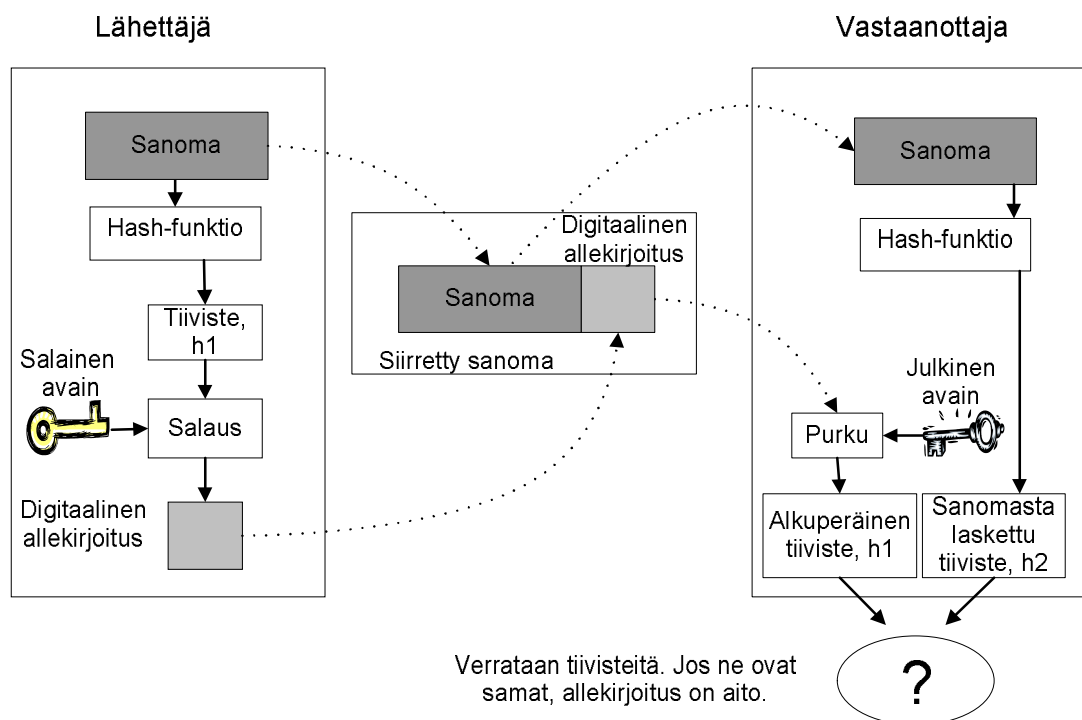
Kuva 11. Haaste/vaste -todentaminen, mukailtu [AdL99]

Haaste/vaste -todentamisessa palvelimella on kopio käyttäjän julkisesta avaimesta. Palvelin lähettää haasteen, joka voi olla esimerkiksi arvottu pitkä satunnaisluku, jonka käyttäjä allekirjoittaa omalla yksityisellä avaimellaan ja palauttaa allekirjoitetun haasteen palvelimelle. Palvelin todentaa käyttäjän lähettämän vastauksen käyttäjän julkisella avaimella. Palvelin saa julkisen avaimen varmenteesta, joka on varastoituna hakemistoon [AdL99]. Pankit käyttävät haaste/vaste -todennusmenetelmää verkkoasioinnissa. Verkkopankin käyttäjä antaa joka kerta muuttuvan tunnusluvun, joka on vain hänen tiedossaan [VM03].

Julkisen avaimen järjestelmän tuoma etu todentamiseen on kertakirjautumisen mahdollisuus julkisen avaimen järjestelmän palveluihin. Käyttäjä kirjautuu ensin paikalliseen ympäristöön. Näin hän pääsee käyttämään yksityistä avaintaan. Yksityistä avainta käytetään käyttäjän automaattiseen todentamiseen muihin sovelluksiin, joko paikallisiin tai etäsovelluksiin. Käyttäjä voi liikkua sekä paikallisissa että etäsovelluksissa, mutta hänen ei tarvitse syöttää salasanaa uudestaan. [AdL99]

### **3.9.2 Eheys**

Tiedon eheys on vakuutus tiedon muuttumattomuudesta sen kuljetuksen tai varastoinnin aikana. Julkisen avaimen järjestelmän tarjoama eheyspalvelu perustuu digitaaliseen allekirjoitukseen (kuva 12) [AdL99]. *Digitaalinen allekirjoitus* on "sähköinen allekirjoitus, jonka tuottamiseen on käytetty varmennetta", se yksilöi lähettäjän, todistaa viestin ja lähettäjän aitouden ja viestin eheyden [VM03].



Kuva 12. Digitaalinen allekirjoitus, mukailtu [Ker98]

Digitaalisen allekirjoituksen periaate on seuraava: sanoman kirjoittaja laskee kirjoittamastaan sanomasta *tiiviste*,  $h_1$ , joka on "tiedosta jonkin säännön mukaan muodostettu lyhyempi uusi tieto varmisteen muodostamiseksi" [VM03], jos sanoma muuttuu, myös tiiviste muuttuu. Tämän jälkeen tiiviste salataan toimikortilla olevalla yksityisellä avaimella. Näin saadaan digitaalinen allekirjoitus. Sanoma lähetetään tiivistämättömänä yhdessä digitaalisen allekirjoituksen kanssa sanoman vastaanottajalle. Vastaanottaja lukee sanoman ja laskee siitä tiiviste,  $h_2$ . Hän myös purkaa allekirjoituksen lähettäjän julkisella avaimella, näin hän saa selville lähettäjän salaaman tiiviste  $h_1$ . Tämän jälkeen hän vertaa tiivistettä  $h_1$  tiivisteeseen  $h_2$ . Jos tiivisteet ovat samat, on viesti säilynyt muuttumattomana. [Lin03]

### 3.9.3 Luottamuksellisuus

Luottamuksellisuus on vakuutus tiedon yksityisyydestä. Tietoa voivat lukea ainoastaan ne, joilla on siihen oikeus. Luottamuksellisuutta vaaditaan, kun [AdL99]:

- tietoa säilytetään välineessä (esimerkiksi tietokoneen kovalevyllä), jota voi lukea luvaton henkilö,
- tiedosta otettu varmuuskopio voi joutua luvattoman henkilön käsiin tai
- tietoa lähetetään suojaamattomissa tietoverkoissa.

Julkisen avaimen järjestelmän tarjoama luottamuksellisuuspalvelu perustuu salaukseen. Salaus voi tapahtua esimerkiksi seuraavasti [AdL99]:

- Matti luo symmetrisen eli salaisen avaimen.
- Matti käyttää symmetristä avainta tiedon salaamiseen.
- Matti lähettää salatun viestin Tiinalle. Viestin mukana hän lähettää symmetrisen avaimen, joka on salattu Tiinan julkisella avaimella.

Tiedon salaaminen riittävän turvallisella menetelmällä takaa sen, ettei tieto paljastu, vaikka joku salakuuntelisi tietoliikenneyhteyttä tai tallennuksessa käytetty kone joutuisi luvattomiin käsiin [Jär02].

### **3.9.4 Kiistämättömyys**

Kiistämättömyys toteutetaan viestin eheyden avulla. Kiistämättömyys on hyödyllinen, kun tietoverkossa halutaan varmistaa osapuolten sitoutuminen, esimerkiksi sopimukseen. [Lin02]

Kiistämättömyys edellyttää myös tapahtumien aikaleimaamista [Jär02]. *Aikaleimapalvelu* on "verkossa luotetun osapuolen tarjoama palvelu, joka liittää aikaleiman viestiin" [VM03]. Aikaleiman ei välttämättä tarvitse edustaa aikaa. Yksinkertainen järjestysnumero, joka osoittaa, että dokumentti X on syntynyt ennen dokumenttia Y ja dokumentin Z jälkeen, on riittävä. [AdL99]

## 4 PKI TERVEYDENHUOLLOSSA

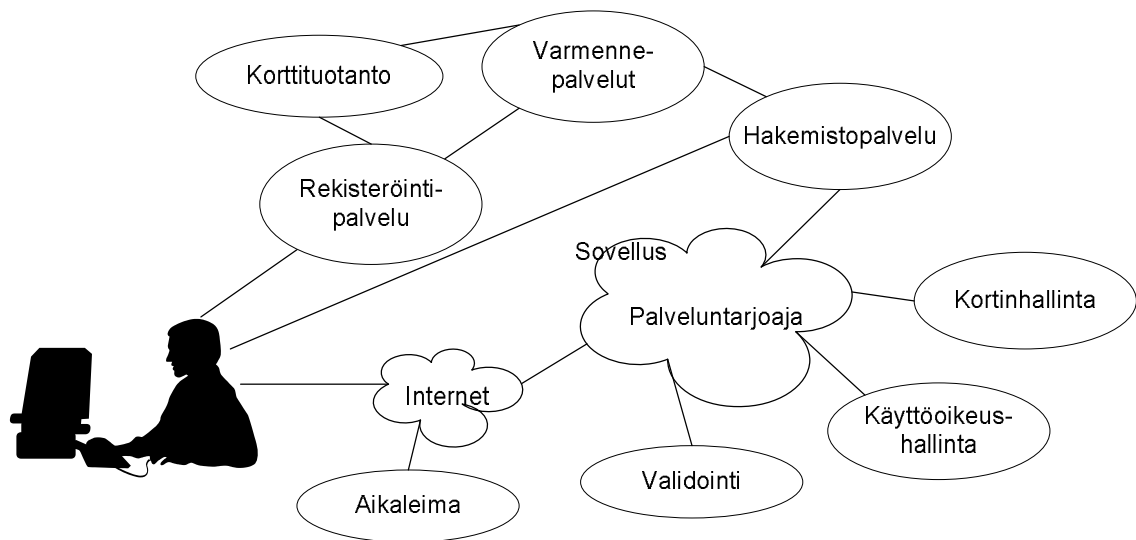
Sähköisen potilaskertomuksen käyttö, mukaan lukien tietojen luovutus terveydenhuollon toimintayksiköiden välillä, asettaa vaatimuksia tietoturvan toteuttamiselle. Tiedot saavat olla vain niihin oikeutettujen käytettävissä ja tiedonsiirron aikana tiedot eivät saa joutua sivullisten käsiin ja tietojen tulee pysyä muuttumattomina. Lisäksi järjestelmän käyttäjien todentaminen tulee olla toteutettu luotettavasti. Julkisen avaimen järjestelmän palveluiden avulla voidaan toteuttaa terveydenhuollon tietoturvalle asetetut vaatimukset.

PKI-järjestelmän avulla tunnistetaan luotettavasti henkilöt, toimintayksiköt ja palvelimet. Se mahdollistaa sähköisen allekirjoituksen ja yhteisen tietoturvapoliitikan muodostamisen. PKI takaa potilasasiakirjojen muuttumattomuuden, se tukee digitaalista arkistointia ja sen avulla hallinnoidaan sähköisiä suostumuksia. [Ruo02]

Luvussa 4.1 esitellään terveydenhuollon PKI-arkkitehtuuri ja luvussa 4.2 tutustutaan tarkemmin sähköiseen allekirjoitukseen.

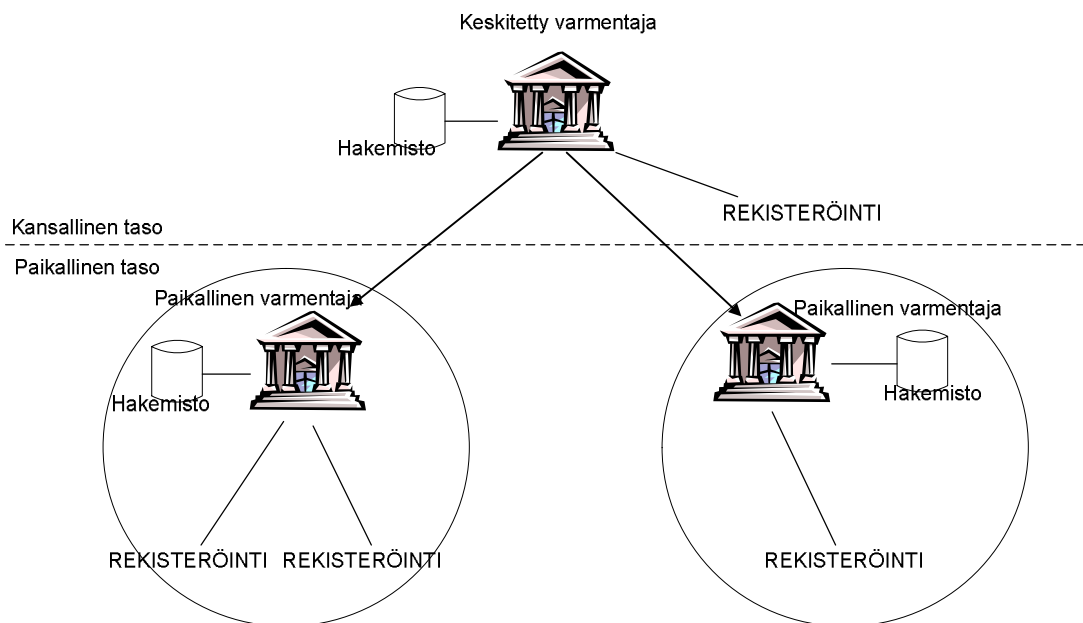
### 4.1 Terveydenhuollon PKI-arkkitehtuuri

Samojen standardien ja periaatteiden noudattaminen helpottaa järjestelmien yhteentoimivuutta. PKI-infrastruktuuri koostuu karkeasti katsottuna kolmesta peruskomponentista. Nämä peruskomponentit ovat luvussa 3.4 kuvatut varmentaja, rekisteröijä ja hakemisto. Lisäksi infrastruktuuri pitää sisällään useita muita osakomponentteja. *PKI-arkkitehtuuri* kuvaa infrastruktuuriin kuuluvien komponenttien ja toimintojen välisiä suhteita. Terveydenhuollon PKI-arkkitehtuurin tärkeänä vaatimuksena nähdään koko maan kattavat yleiset standardit ja yhteisesti hyväksytyt periaatteet [Ruo02]. Kuvassa 13 on esitetty PKI-arkkitehtuurin osakomponentit. Luku perustuu lähteeseen [Ruo02].



Kuva 13. PKI-arkkitehtuurin osakomponentit, mukailtu [Ruo02]

Stakesin tietoteknologian osaamiskeskus (OSKE) on arvioinut kolmea eri arkkitehtuurivaihtoehtoa terveydenhuollon PKI-arkkitehtuuriksi. Vaihtoehdot olivat: keskitetty vaihtoehto, jossa varmennepalvelujen hoitamisesta vastaisi yksi kansallinen varmentaja; osittain keskitetty vaihtoehto ja hajautettu vaihtoehto, jossa kaikki toiminnot hoidettaisiin paikallisesti. Vuonna 2002 julkaistussa raportissa sosiaali- ja terveydenhuollon kansalliseksi arkkitehtuurimalliksi ehdotetaan kaksitasoista osittain hajautettua mallia. Malliin kuuluu yksi valtakunnan tason varmentaja ja alueellisen tason varmentajia. Kuvassa 14 on kuvattu ehdotettu malli.



Kuva 14. Esitys terveydenhuollon kansalliseksi arkkitehtuurimalliksi, mukailtu [Ruo02]

Arkkitehtuurille asetettuja määräyksiä on kuvattu seuraavissa aliluvuissa: varmennepalvelut, kortinhallinta, rekisteröintipalvelut, hakemistopalvelut, lisäpalvelut.

#### **4.1.1 Varmennepalvelut**

Ehdotetussa arkkitehtuurissa terveydenhuollossa olisi yksi juurivarmentajaorganisaatio, joka varmentaa laillistetut ammattihenkilöt ja paikalliset varmentajat. Juurivarmentajaksi on kaavailtu Terveydenhuollon oikeusturvakeskusta (jatkossa TEO). *Laillistettuja ammattihenkilöitä* ovat: "henkilöt, joille on lain nojalla myönnetty ammatinharjoittamisoikeus, esimerkiksi lääkärit, sairaanhoitajat, terveydenhoitajat ja fysioterapeutit, yhteensä nimikkeitä on 17." Valtakunnallisena varmentajana TEO olisi tulevaisuudessa vastuussa kaikkien terveydenhuollon ammattihenkilöiden varmentamisesta (edellisten lisäksi esimerkiksi lähihoitaja, perushoitaja ja mielisairaanhoitaja) [Säh04b]. Voidakseen myöntää varmenteita laillistetuille ammattihenkilöille, varmentajan on täytettävä laatuvarmentajalle asetetut vaatimukset. Laillistetuille ammattihenkilöille myönnettyjen varmenteiden tulee olla laatuvarmenteita. Laatuvarmentajaa ja laatuvarmenteita käsitellään luvussa 4.2.

Paikalliset varmentajat, joita voivat olla esimerkiksi sairaanhoitopiirit, myöntävät varmenteita niille omaan henkilökuntaan kuuluville, jotka eivät tarvitse laatuvarmennetta. Lisäksi paikalliset varmentajat myöntävät varmenteita omille palvelimilleen. Paikallisten varmentajien varmenteita käytetään lähinnä käyttäjän todentamiseen.

#### **4.1.2 Kortinhallinta**

Potilaiden ja ammattilaisten varmentamiseen voidaan käyttää toimikorttia. Juurivarmentajaorganisaatio huolehtii korttien tuotannosta ja korttien jakelusta laillistettujen ammattihenkilöiden osalta yksityisille toimijoille. Tarvittaessa myös niille organisaatioille, jotka eivät kykene tai halua toteuttaa paikallisia toimintoja itse. Paikalliset varmentajat pääsääntöisesti vastaavat itse oman alueensa korttien tuotannosta.

On mahdollista, että kortti joskus esimerkiksi unohtuu kotiin. Näissä tilanteissa tarvitaan tilapäiskorttia. Tilapäiskorttien käyttämisessä pitää kuitenkin olla tarkkana.

Niitä voidaan käyttää järjestelmään todentautumiseen, mutta allekirjoittamiseen niitä ei voi käyttää.

### **4.1.3 Rekisteröintipalvelut**

Rekisteröintipalvelun tehtävänä on varmistaa, että henkilöt saavat juuri hänelle tarkoitetun varmenteen sisältävän toimikortin. Rekisteröijän tehtävänä on todentaa varmennetta hakevan henkilöllisyys, toimittaa varmennehakemus varmentajalle ja valmis kortti kortin omistajalle. Kun ammattilaisille myönnetään varmenteita, tulee ammattilaisstatus tarkistaa rekisteristä, jota TEO ylläpitää. Juurivarmentaja toteuttaa yksityisten laillistettujen ammattihenkilöiden rekisteröintipalvelut sekä niiden organisaatioiden, jotka eivät pysty tai halua toteuttaa rekisteröintiä itse.

Rekisteröijän ja varmentajan yhteinen tehtävä on sulkulistapalvelu. Sulkulistapalvelusta vastuussa olevien henkilöiden käyttöoikeuksiin kuuluu ainoastaan varmenteen peruminen. Varmenteen peruuttamista voi pyytää joko puhelimitse tai kirjallisesti ja se pitää olla mahdollista 24 tuntia vuorokaudessa. Jokaisella varmentajalla on oma sulkulistansa ja se julkaistaan varmennehakemistossa. Sulkulista päivitys tapahtuu esimerkiksi kerran tunnissa.

### **4.1.4 Hakemistopalvelut**

Jokainen varmentaja perustaa oman julkisen hakemistonsa, jossa julkaistaan varmenteet ja sulkulistat. Tarvittaessa ammattihenkilöiden varmenteet kopioidaan keskitetystä hakemistosta paikallisiin hakemistoihin. Tämä voi olla tarpeen käyttöoikeuksien hallintaa varten.

### **4.1.5 Lisäpalvelut**

Lisäpalveluita ovat: aikaleimapalvelu, varmenteen validointipalvelu ja käyttäjä- ja käyttöoikeushallinta. Aikaleimapalvelun avulla taataan tapahtumien voimassaolo varmenteiden voimassaolon umpeuduttua. Aikaleiman avulla voidaan esimerkiksi varmistua allekirjoitetun dokumentin aitoudesta. Aikaleiman tulee olla varmennettu, jäljitettävissä ja tarkistettavissa jälkikäteen. Aikaleimapalvelu voi olla kolmannen luotettavan osapuolen järjestämä. Näin varmistutaan aikaleiman objektiivisuudesta.

Varmenteen validointipalvelun avulla PKI:tä hyödyntävät organisaatiot validoivat varmenteet ja allekirjoitukset. Validointipalvelu on luotettavat palvelu, joka tarkistaa

halutun tietoelementin pyydetyn profiilin mukaisesti ja antaa vastauksen validoinnin onnistumisesta sitä pyytäneelle. Validointipalvelu toteutetaan joko keskitetysti tai paikallisesti.

Käyttäjä- ja käyttöoikeushallinta on jokaisen organisaation oma toiminto.

Valtakunnallisen varmentajat tehtävät ovat:

- muodostaa tietoturvapoliittika [Tam05],
- varmentaa alueelliset varmentajat,
- varmentaa ammattihenkilöt niissä tapauksissa, kun tarvitaan laatusertifikaattiin perustuvaa sähköistä allekirjoitusta,
- varmentaa julkiset ja yksityiset palveluntuottajat,
- varmentaa turvalliset arkistot,
- huolehtia kansainvälisestä ristiinsertifioinnista,
- tuottaa valtakunnalliset hakemisto- ja varmennepalvelut ja
- huolehtia ammattihenkilöiden, palveluntuottajien ja notariaattiarkistojen avainten pitkäaikaissäilytyksestä.

Paikallisen- tai alueorganisaation tehtävät ovat:

- varmistaa, että alueellinen varmennepoliittika on kansallisten määritysten mukainen,
- käyttöoikeuksien ja työsuhteiden hallinta ja niiden tarvitsemien tunnistamis- ja varmennepalvelujen tuottaminen,
- paikallisten, ei laatuvarmentamista edellyttävien, allekirjoitus- ja varmennepalvelujen tuottaminen,
- dynaamisten roolien hallitseminen ja
- alueellisten varmenne- ja hakemistopalvelujen ylläpitäminen.

Esitetyn mallin vahvuutena nähdään sen keskittyneisyys. Palveluntuottajille annetaan suuntaviivat, joiden mukaisesti he voivat itse toteuttaa palvelunsa melko itsenäisesti. Palvelujen käyttöönotossa voi noudattaa omaa aikatauluaan. Palveluntuottajat käyttävät järjestelmien toteutuksessa haluamiaan välineitä. Lisäksi malli tukee niitä organisaatioita, jotka eivät pysty itse toteuttamaan tarvittavia toimintoja. Muita mallin vahvuuksia ovat: varmennepolun muodostamisen ja validoinnin yksinkertaisuus, selkeä laatuvarmenteiden ja niitä vastaavien sulkulistojen arkistoinnin järjestäminen sekä kustannusten hallinta organisaation omassa hallinnassa.

Raportissa on arvioitu, että vuoden 2004 aikana tulisi käyttöön valtakunnallinen varmennepalvelu terveydenhuollon ammattilaisille [Ruo02]. Vuoden 2005 lokakuussa ei vielä ole käytössä valtakunnallista varmennepalvelua.

## **4.2 Sähköinen allekirjoitus**

Julkisen avaimen järjestelmän tarjoama eheys ja kiistämättömyys perustuvat sähköiseen allekirjoitukseen.

Laki sähköisistä allekirjoituksista määrittelee *sähköisen allekirjoituksen* seuraavasti: "sähköisessä muodossa oleva tieto, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan todentamisen välineenä" [SähL03]. Digitaalinen allekirjoitus, joka kuvattiin luvussa 3.9.2, on yksi sähköisen allekirjoituksen muoto. Digitaalinen allekirjoitus on kehittynyt sähköinen allekirjoitus. *Kehittynyt sähköinen allekirjoitus* liittyy yksiselitteisesti sen allekirjoittajaan, joka voidaan yksilöidä. Se on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan. Lisäksi kehittynyt sähköinen allekirjoitus on liitetty muuhun sähköiseen tietoon siten, että tietoon mahdollisesti tehdyt muutokset ovat havaittavissa [SähL03]. Sosiaali- ja terveysministeriö on asettanut tavoitteen, jonka mukaan vuoteen 2010 mennessä kaikki potilastieto pitää voida allekirjoittaa sähköisesti [www1].

Asiakirjan laatijan omakätinen tai sähköinen (varmennettu) allekirjoitus pitää olla ainakin seuraavissa potilasasiakirjoissa: lähetteet, hoidon loppulausunto, yhteenveto annetusta hoidosta, leikkaus- ja muu toimenpidekertomus, lomake- ja vapaamuotoiset lausunnot ja todistukset [Pot01]. Varmennettu allekirjoitus tarkoittaa käytännössä sitä, että allekirjoitus on tehty varmennetta hyväksikäyttäen. Varmenteen avulla liitetään

allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistetaan allekirjoittajan henkilöllisyys [SähL03].

Sähköisestä allekirjoituksesta puhuttaessa esiintyvät usein termit laatuvarmentaja ja laatuvarmenne. *Laatuvarmenne* on: "Euroopan Unionin sähköisen allekirjoituksen direktiivin mukaiset vaatimukset täyttävä varmenne" [VM03]. *Laatuvarmentaja* on varmentaja, joka saa myöntää laatuvarmenteita. Laatuvarmentajalle on laissa määrätty useita velvollisuuksia. Voidakseen myöntää laatuvarmenteita, on varmentajan tehtävä kirjallinen ilmoitus Viestintävirastolle. Laatuvarmenteita myöntävistä varmentajista ylläpidetään rekisteriä. Rekisterin ylläpidosta vastaa Viestintävirasto [SähL03]. Tutkielman tekohetkellä, vuonna 2005, ainoa laatuvarmenteita myöntävä taho Suomessa on Väestörekisterikeskus.

Luvussa 4.2.1 kerrotaan sähköisen allekirjoituksen käytännön kokemuksista ja luvussa 4.2.2 tutustutaan sähköisen allekirjoituksen pitkäaikaissäilytykseen.

#### **4.2.1 Kokemuksia sähköisestä allekirjoituksesta**

Sähköisten allekirjoitusten käyttötavoista annetaan ohjeet vuonna 2006 uudistettavassa potilasasiakirja-asetuksessa. Uudistuksessa hyödynnetään alueellisista piloteista saatavia kokemuksia [Säh04b]. Sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilulain alueilla ammattihenkilön sähköistä allekirjoitusta ollaan kokeilemassa 13 alueella. Asiakkaan sähköistä allekirjoitusta ei ole vielä käytössä tai edes pilotoitavana missään. Kyselyn mukaan kokeilulain tärkeimmäksi osa-alueeksi koettiin sähköinen allekirjoitus ja nimenomaan terveydenhuollon ammattihenkilön sähköinen allekirjoitus. Muutamat alueet olivat sitä mieltä, että tulisi tarkemmin määritellä ne tilanteet ja dokumentit, joiden sähköisessä allekirjoittamisessa pitää noudattaa standardia ja toisaalta missä tapauksissa riittää kevyempi menettely. Toiveena oli myös useamman dokumentin samanaikainen allekirjoitus. Kokeilualueilla käytössä olevat varmenteet ovat TEO:n varmenteita, sairaanhoitopiirien omia varmenteita ja avainlukulistoja. TEO:n varmenteet ovat käytännössä Väestörekisterikeskuksen myöntämiä varmenteita ja ne täyttävät laatuvarmenteele asetetut vaatimukset. Sen sijaan sairaanhoitopiirien varmenteet ja avainlukulistat eivät vaatimuksia täytä. [HHP05]

Sähköisen allekirjoituksen välineiden taso vaihtelee alueittain. Kokeilulaissa ei määritellä, millä tavalla allekirjoitukseen liittyvä varmentaminen tulee suorittaa.

Säännökset sähköisen allekirjoituksen tietoturvan tasosta puuttuvat. Hallitus on kuitenkin esittänyt, että sähköisessä allekirjoituksessa voidaan edellyttää laatuvarmenteen käyttöä. Tästä huolimatta alueilla kuitenkin on käytössä sähköisen allekirjoituksen välineitä, jotka eivät täytä laatuvarmenteele asetettuja vaatimuksia. [HHP05]

#### **4.2.2 Sähköisen allekirjoituksen pitkäaikaissäilytys**

Potilasasiakirjojen säilytysajat ovat yleensä erittäin pitkiä. Arkistoitujen dokumenttien arvo riippuu sähköisen allekirjoituksen olemassaolosta. Sähköinen allekirjoitus on se, joka takaa asiakirjan eheyden. Sähköisen dokumentin pitkäikäisyys riippuu sen luettavuuden säilyttämisestä. Sähköisen allekirjoituksen pitkäikäisyys riippuu monista tekijöistä. Näitä tekijöitä ovat [LeG05]:

- Avaimilla, joita käytetään allekirjoituksen luomiseen ja todentamiseen, tulee olla rajoitettu elinaika. Näin vältetään pitkäaikainen altistuminen salauksen ratkonnalle ja muille uhille. Varmentajien yleinen käytäntö on rajoittaa varmenteiden elinaika yhteen tai kahteen vuoteen. Tekniikan kehittymistä ei voida ennustaa. Ongelmaan, joka nyt on ratkaisematta, löytyy ratkaisu muutamassa vuodessa. Pitkään käytössä olevat avaimet todennäköisesti häviävät tai tulevat varastetuiksi.
- Allekirjoitusavaimet voivat paljastua ennen elinajan päättymistä. Allekirjoitukseen käytettävä algoritmi voidaan myös murtaa. Molemmat altistavat dokumentin allekirjoituksen hyökkäyksille.
- Sähköisen allekirjoituksen todentamiseen tarvittava tieto, kuten varmenteen voimassaolo, ei ole käytettävissä tulevaisuudessa.
- Luotettu kolmas osapuoli ei välttämättä ole tulevaisuudessa luotettu. Esimerkiksi sen takia, että se on lopettanut toimintansa tai se ei täytä enää tarpeellisia vaatimuksia.

Täytyy siis olla jokin keino, jonka avulla sähköinen allekirjoitus on todennettavissa myös sen jälkeen, kun allekirjoitukseen käytettävä avain ei enää ole saatavilla. Yksi ratkaisu ongelmaan on järjestelmä, jossa allekirjoituksen varmentamisprosessi perustuu varmentamisen hetkellä saatavilla olevaan luottamussuhteeseen, tietoon ja teknologioihin. Tästä käytetään termiä *kumulatiivinen notaarisointijärjestelmä*.

(PKI:ssä *notarisointi* on luotetun tahon eli *notariaatin*, todistus sille, että tieto on voimassa olevaa tai oikeaa. Tämä tapahtuu notariaatin sähköisen allekirjoituksen avulla. Notariaatti liittää allekirjoitukseensa aikaleiman [AdL99].) Kumulatiivisessa notarisointijärjestelmässä aiemmin allekirjoitettu tai notarisoitu tieto todennetaan ja allekirjoitetaan sähköisesti notariaatin toimesta, joka sillä hetkellä on luotettu taho. Näin muodostettua sähköistä allekirjoitusta kutsutaan *kumulatiiviseksi notarisointimerkiksi*. Kumulatiivisen notarisointimerkin varmennusprosessissa tarvitaan vähintään [LeG05]:

- alkuperäinen dokumentti tai sen tiivistearvo,
- alkuperäisen allekirjoituksen tekijän henkilötiedot,
- metadata, joka kuvaa alkuperäistä dokumenttia ja edellisen notariaatin allekirjoitusprosessia ja
- edellinen kumulatiivinen notarisointimerkki ja tieto, jonka avulla se on todennettavissa, kuten esimerkiksi varmenteen luottamusketju.

PKI:ään perustuva allekirjoitus riippuu allekirjoitukseen käytettävän avaimen elinajasta, luottamussuhteista ja teknologioista. Kumulatiivinen notarisointi riippuu ainoastaan päivitetystä luottamussuhteesta. [LeG05]

## 5 POHDINTA

Tässä tutkimuksessa on kuvattu tietoturvaä yleisellä tasolla. Tarkemmin on paneuduttu terveydenhuollon tietoturvaan. Tutkimuksessa on käsitelty symmetrisen ja epäsymmetrisen salauksen periaatteet pääpiirteissään. Varsinaisia salausalgoritmeja ei ole käsitelty. Yhtenä osana terveydenhuollon tietoturvan toteuttamista on esitelty julkisen avaimen infrastruktuuri eli PKI. Johdatuksena PKI:hin on lyhyesti esitelty turvallisuusinfrastruktuurin periaatteet.

Terveydenhuollossa keskeisessä asemassa on potilaan tietosuojaja: sivullisella ei ole oikeutta potilastietoihin ilman potilaan suostumusta. Kun otetaan huomioon tietoturvan periaatteet, parannetaan samalla tietosuojaä. Tietoturvan toteuttaminen on saanut uusia ulottuvuuksia sähköisen potilaskertomuksen myötä. Ennen potilaan kaikki tiedot olivat paperilla. Nyt potilastiedot ovat suurelta osin sähköisessä muodossa. Käyttöoikeuksien avulla määritellään ne tiedot, joihin kullakin ammattihenkilöllä on oikeus päästä. Osastolla a töissä oleva hoitaja ei ole oikeutettu näkemään osastolla b hoidossa olevan potilaan tietoja.

Potilastietojärjestelmät mahdollistavat myös potilaan tietojen siirron terveydenhuollon toimintayksiköiden välillä. Tämä lisää tietoturvalle asetettuja vaatimuksia. Ei enää riitä, että huolehditaan siitä, että tiedot ovat paikallisesti vain niihin oikeutettujen saatavilla. Lisäksi on varmistuttava siitä, että tietoa siirrettäessä se ei joudu sivullisten käsiin, tieto säilyy eheänä ja kiistämättömyyden periaate toteutuu. Tiedon siirron edellytyksenä on potilaan suostumus (lukuunottamatta laissa määriteltyjä tapauksia, jolloin suostumusta ei tarvita).

Julkisen avaimen salaukseen perustuvan julkisen avaimen infrastruktuurin avulla voidaan toteuttaa käyttäjän todentaminen, tiedon luottamuksellisuus, eheys ja kiistämättömyys. Jokaisella PKI:hin liitettyllä käyttäjällä on hallussaan avainpari: julkinen ja yksityinen avain. Julkinen avain sijaitsee varmenteessa, joka sitoo tietyn julkisen avaimen tiettyyn käyttäjään. Varmenteet julkaistaan hakemistossa, sen lisäksi varmenne sijaitsee käyttäjän hallussa olevalla toimikortilla. Toimikortilla sijaitsee myös käyttäjän yksityinen avain. Varmenteet myöntää luotettu kolmas osapuoli eli varmentaja.

Terveystieteiden tutkimuskeskuksen PKI-arkkitehtuuriksi on vuonna 2002 esitetty kaksitasoista, osittain hajautettua arkkitehtuuria, jossa valtakunnallinen varmentaja varmentaa terveydenhuollon ammattihenkilöt. Ehdotettua PKI-arkkitehtuuria ei ole toteutettu. Saumattoman palveluketjun alueilla varmentajana on käytännössä Väestörekisterikeskus. Yhteistyötahona sillä on TEO, joka varmistaa henkilöiden ammattistatuksen. Samanaikaisesti varmentajana toimii myös yksi sairaanhoitopiireistä eli Varsinais-Suomen sairaanhoitopiiri, joka on vuonna 2003 toteuttanut oman varmennejärjestelmän. Sairaanhoitopiirin varmenteet eivät kuitenkaan täytä laatuvarmenteelle esitettyjä vaatimuksia. Todennäköistä on, että ammattihenkilöiden varmenteiden tulee olla laatuvarmenteita. Tulevaisuus näyttää miten varmentaminen käytännössä tullaan valtakunnallisesti toteuttamaan.

Käyttäjän todentaminen, potilasasiakirjojen sähköinen arkistointi, luovutusten ja luovutuslokin hallinta ja sähköinen suostumus ovat kokonaisuuksia, joiden toteuttamiseen on panostettu, ainakin suositusten muodossa. Käytännön kokemukset tuntuvat olevan vielä aika vähissä. Saumattoman palveluketjujen kokeilualueille tehdyn kyselyn perusteella näyttää siltä, että tietoturvaan liittyvät määrittelyt ovat vielä osittain keskeneräisiä ja puutteellisia.

Ammattihenkilön sähköisen todentamisen suhteen puuttuu selkeät ohjeet: tarvitaanko laatuvarmenne vai ei? Ja jos tarvitaan, niin missä tilanteissa? Samoin asiakkaan todentamisen suhteen ei ole yksiselitteisesti määritelty, miten se tulee toteuttaa.

Sähköistä allekirjoitusta on kokeiltu jo muutaman vuoden ajan. Sähköisen allekirjoituksen käytännöistä vaaditaan vielä tarkennuksia. Mitä allekirjoitetaan ja minkä tasoisella varmenteella? Suosituksia sähköisten allekirjoitusten käyttötavoista on luvassa vuonna 2006. Asiakkaan sähköinen allekirjoitus herättää paljon keskustelua. Epäselvää näyttää olevan, miten käytännössä onnistuu se, että kaikilla kansalaisilla olisi esimerkiksi toimikortti, jolla allekirjoituksen voisi tehdä? Olisiko mahdollista uudistaa Kela-korttia, joka on jokaisella kansalaisella? Uusi Kela-kortti sisältäisi tarvittavat avainparit. Siirtymisaika uuteen korttiin voisi olla vaikka viisi vuotta.

PKI:n tarjoama eheyspalvelu perustuu sähköiseen allekirjoitukseen, joten sähköisen allekirjoituksen toimintatapojen suhteen tulee päästä nopeasti yksimielisyyteen. Esimerkiksi sähköinen suostumus ei voi olla täydellisesti sähköinen ennen kuin asiakas allekirjoittaa suostumuksen sähköisesti.

Paljon on tehty sen eteen, että potilastietojärjestelmien toteutuksessa otetaan huomioon tietoturvalle asetetut vaatimukset. On tehty erilaisia määrityksiä ja suosituksia. Toteutuksissa kaikkia näitä asioita ei ole otettu huomioon. Syitä tähän voi olla esimerkiksi tietämättömyys ja määrittelyjen puutteellisuus. PKI:n suhteen vaikuttaa siltä, että tekniikka kyllä on hallussa, mutta vielä puuttuu selkeät pelisäännöt, joiden mukaan käytännössä toteutetaan PKI:n mahdollistamat palvelut.

Ohjelmistoyritysten, kuten myös terveydenhuollon organisaatioiden tulee olla valppaana uusien suositusten suhteen. Organisaatioiden osuutta tulee korostaa. Organisaatiot ovat kuitenkin loppukädessä vastuussa siitä, että organisaatiossa käytössä olevat järjestelmät ovat määräysten mukaisia.

Pitää myös muistaa, että julkisen avaimen järjestelmä on vain yksi osa terveydenhuollon tietoturvan toteutusta. Organisaation ja yksittäisten ihmisten toimintatavat vaikuttavat myös tietoturvan toteutumiseen tai toteutumattomuuteen. Tekniikan sanotaan olevan vain apukeino. Inhimillisten tekijöiden osuutta tietoturvan toteutumisessa ei pidä unohtaa.

## LÄHTEET

- [ABD00] Adams, C., Burmester, M., Desmedt, Y., Reiter, M., Zimmermann, P.: Which PKI (Public Key Infrastructure) is the right one? *Proceedings of the 7th ACM conference on Computer and communications security*, ACM Press, NY, USA, 2000. [ONLINE] Viitattu 3.6.2005, saatavilla <http://delivery.acm.org>
- [AdL99] Adams, C., Lloyd, S.: *Understanding Public-Key Infrastructure*, Macmillan Technical Publishing, Indianapolis, USA, 1999.
- [ArkL94] *Arkistolaki*, 23.9.1994 / 831.
- [BoP03] Bourka, A., Polemi, D.: Interoperability among healthcare organizations acting as certification authorities, *IEEE transactions on information technology in biomedicine*, vol. 7, no. 4, December 2003. [ONLINE] Viitattu 1.9.2005, saatavilla <http://ieeexplore.ieee.org/Xplore/dynhome.jsp>
- [BuD04] Burmester, M., Desmedt, Y.: Is hierarchical Public-Key Certification the next target for hackers? *Communications of the ACM*, Vol. 47, No. 8, 2004, s. 68–74. [ONLINE] Viitattu 3.6.2005, saatavilla <http://delivery.acm.org>
- [ELS05] Ensio, A., Laine, M., Saranummi, N., Nykänen, P., Ruotsalainen, P., Hartikainen, K., Rahkila-Bergström, R., Vuolasto, J.: *Kansallinen terveysterveysprojekti - sähköinen potilaskertomus. Ehdotus sähköisen potilaskertomuksen viranomaismääräyksiksi*, 2005.
- [EnR03] Ensio, A., Ruotsalainen, P.: *Sähköisen asiakas- ja potilasasiakirjojen säilytyksen ja kiistämättömyyden hyvä käytäntö*, Osaavien keskustien verkoston julkaisu 2 / 2003, Stakesin monistamo, Helsinki, 2003.
- [Hetil99] *Henkilötietolaki*, 22.4.1999 / 523.
- [HHP05] Hyppönen, H., Hämäläinen, P., Pajukoski, M., Tenhunen, E.: *Selvitys sosiaali- ja terveydenhuollon saumattoman palveluketjun kokeilulain (22.9.2000 / 811) toimeenpanosta kokeilualueilla*. Loppuraportti, Stakesin monistamo, Helsinki, 2005.

- [Hun01] Hunt, R: *PKI and digital certification infrastructure*, New Zealand, 2001. [ONLINE] Viitattu 1.9.2005, saatavilla <http://ieeexplore.ieee.org/Xplore/dynhome.jsp>
- [Imm04] Immonen, A: *Turvallinen kommunikaatioalusta: ohjeita PKI-infrastruktuurin toteuttamiselle*, osaavien keskusten verkoston julkaisuja 2 /2004, Stakesin monistamo, Helsinki 2004. Saatavilla myös <http://www.oskenet.fi/>
- [ItR04] Itälä, T., Ruotsalainen, P.: *Tietoturvallinen kommunikaatioalusta: luovutuksen ja luovutuslokin hallinnan suositukset*, Osaavien keskusten verkoston julkaisuja 6 / 2004, Stakesin monistamo, Helsinki, 2004.
- [Jär02] Järvinen, P.: *Tietoturva ja yksityisyys*, Docendo, Jyväskylä, 2002.
- [Jär96] Järvinen, P.: *Internet-muutostekijä*, 1996. [ONLINE] Viitattu 1.6.2005, saatavilla <http://www.pjoy.fi/kirjat/imuutos/>
- [JulL99] *Laki viranomaisten toiminnan julkisuudesta*, 21.5.1999 / 621.
- [Ker98] Kerttula, E.: *Tietoverkkojen tietoturva*, Oy Edita Ab, Helsinki, 1998.
- [KokL00] *Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta*, 22.9.2000 / 811.
- [LeG04] Lekkas, D., Grizalis, D.: *Cumulative notarization for long-term preservation of digital signatures*, Athens, Greece. Viitattu 25.10.2005, saatavilla <http://www.sciencedirect.com>
- [Lin02] Linden, M.: *Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiossa*, liseniaatintutkimus, Tampereen teknillinen yliopisto, 2002.
- [Lin04] Lintula, H.: *Vaatimusten validointi ja verifiointi*, Pro gradu -tutkielma, Kuopion yliopisto, 2004.
- [MSR04] Mikola, T., Sorvari, H., Ruotsalainen, P.: *Turvallinen kommunikaatioalusta: suositukset sähköisen suostumuksen periaatteiksi*, Osaavien keskusten verkoston julkaisuja 3 / 2004, Stakesin monistamo, Helsinki, 2004.

- [Paa98] Paavilainen, J.: *Tietoturva*, Gummerus Kirjapaino Oy, Jyväskylä, 1998.
- [Paj05] Pajukoski, M.: *Sähköinen asiointi sosiaali- ja terveydenhuollossa. Lainsäädännön rajat ja mahdollisuudet*. Stakes, Raportteja 283, Gummerus Kirjapaino Oy, Saarijärvi, 2005.
- [PHM03] Polk, W.T., Hastings, N.E., Malpani, A.: Public key infrastructure that satisfy security goals, *IEEE Internet Computing*, Vol. 7, No. 4, 2003, s.60–67. [ONLINE] Viitattu 3.6.2005, saatavilla <http://ieeexplore.ieee.org/>
- [Pot01] *Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen*, Sosiaali- ja terveysministeriön oppaita 2001:3.
- [PotL92] *Laki potilaan asemasta ja oikeuksista*, 17.8.1992 / 785.
- [Ruo02] Ruotsalainen, P.: *Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri*, Osaavien keskusten verkoston julkaisuja, Stakesin monistamo, Helsinki, 2002. Saatavilla myös <http://www.oskenet.fi/>
- [Säh04a] *Sähköisten potilasasiakirjajärjestelmien valtakunnallinen määrittely ja toimeenpano*, Sosiaali- ja terveysministeriön työryhmämuistioita 2003:38, Helsinki 2004.
- [Säh04b] *Sähköisten potilasasiakirjajärjestelmien toteuttamista ohjaavan työryhmän loppuraportti*, Sosiaali- ja terveysministeriön työryhmämuistioita 2004:18, Helsinki 2004.
- [SähL03] *Laki sähköisistä allekirjoituksista*, 24.1.2003 / 14.
- [Soh03] Sohlman, T.: *Käyttäjän autentikointimekanismit*, Mediatekniikan seminaari, kalvosarja, 2003. [ONLINE] Viitattu 2.6.2005, saatavilla [http://pww.evitech.fi/courses/mts03/users/teemuis/autentikointi\\_mekanismit.ppt#1](http://pww.evitech.fi/courses/mts03/users/teemuis/autentikointi_mekanismit.ppt#1)
- [Sta03] Stallings, W.: *Cryptography and network security*, Prentice Hall, New Jersey, USA, 2003.

- [STM01] *Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä*, 19.1.2001 / 99.
- [Täh97] Tähtinen, H: *Terveydenhuollon tietoturvan ja tietosuojan toteutuksen hyviä käytäntöjä*, Suomen Kuntaliitto, Helsinki 1997.
- [Tam05] Tammisalo, T: *Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt*, Stakes, Helsinki, 2005.
- [VM03] Valtiovarainministeriö, *Valtionhallinnon tietoturvakäsitteistö*, Valtionhallinnon tietoturvallisuuden johtoryhmä, 2003. [ONLINE] Viitattu 31.5.2005, saatavilla <http://www.vm.fi/tiedostot/pdf/fi/50902.pdf>
- [www1] *Kaikki potilaskertomusjärjestelmät sähköisiksi vuoteen 2007 mennessä*. [ONLINE] Viitattu 21.11.2005, saatavilla <http://websrv2.tekes.fi/opencms/opencms/OhjelmaPortaali/Kaynnissa/FinnWell/fi/system/uutinen.html?id=2100&nav=Uutisia&arkisto=true>
- [Yli01] Ylipartanen, A.: *Tietosuoja terveydenhuollossa*, Hakapaino Oy, Helsinki, 2001.

