Turvallinen kommunikaatioalusta: Ohjeita PKI-infrastruktuurin toteuttamiselle

Aapo Immonen,
Shiftec-tutkimusyksikkö, Kuopion yliopisto

Toimittanut Pekka Ruotsalainen

Osaavien keskusten verkoston julkaisuja 2/2004

ISBN 951-33-1569-X

Stakesin monistamo, Helsinki

Sisällysluettelo

ESIPUHE 4
1 Valtakunnallinen terveyshanke 6
1.1 Hanke 4.1.3, valtakunnallisen sähköisen potilaskertomuksen käyttöönotto 6
1.2 Tietoturvallinen tiedonvälitysympäristö osahanke 7
1.3 PKI –järjestelmän käyttöönotto –osaprojekti 8
2 Taustaa 9
3 Ohjeita PKI-järjestelmän käyttöönottoon ja tietojen salaukseen 11
4 Sairaanhoitopiirien tietoturvapolitiikka, PKI- tilanne ja toteutusaikataulu 14
4.1 Julkisen avaimen menetelmän käyttöönoton aikataulut 14
5 Paikallisen PKI-järjestelmän toteuttaminen - Shiftec-tutkimusyksikön toteutus 17
6 PKI-järjestelmä mobiilissa käyttöympäristössä 21
7 PKI-järjestelmän käytötönoton tuottamia muutospaineita potilastietojärjestelmälle 22
8 Julkisen avaimen menetelmän kuvaus alkaen tietoturvapolitiikasta tekniseen toteutukseen ja ylläpitoon 23
8.1 Yhteenveto kansainvälisistä terveydenhuollon PKI- hankkeista 23
8.2 Huomioitavat seikat julkisen avaimen menetelmän käyttöönotossa - terveydenhuollon erityispiirteet 24
9 Julkisen avaimen menetelmä terveydenhuollossa tietoturvallisuuden asiantuntijoiden näkökulmasta 25
9.1 Lainsäädännölliset vaatimukset 25
9.2 Toiminnalliset vaatimukset 25
9.3 Tekniset vaatimukset 26
9.4 Yhteenveto asiantuntijoiden näkemyksistä 26
10 Julkisen avaimen menetelmän kustannukset 27
11 Yhteenveto 29
Liite 1 Julkisen avaimen menetelmään liittyviä lyhenteitä ja käsitteitä 30
Liite 2 Perusteita tietoturvallisuudelle terveydenhuollossa 32
Lähteet 36

ESIPUHE

Valtioneuvoston terveydenhuollon turvaamista koskevana periaatepäätöksen (11.4.2002) mukaisesti "valtakunnallinen sähköinen sairauskertomus" otetaan käyttöön vuoden 2007 loppuun mennessä. Sosiaali- ja terveysministeriö asetti vuoden 2003 helmikuussa sähköisten potilasasiakirjojen käyttöönottoa ohjaavan työryhmän. Samalla käynnistettiin valtakunnalliset määrittelyhankkeet potilaskertomuksen ydintietojen ja yhteisten sanomien harmonisoimiseksi sekä tietoturvallisen tiedonvälityksen ohjeistuksen laatimiseksi.

Stakes ja STM solmivat sopimuksen, jonka mukaan Stakesin tietoteknologian osaamiskeskus (OSKE) tuottaa konkreettiset ohjeistukset/suositukset, jotka mahdollistavat potilasasiakirjojen ja -tiedon siirron ja/tai käytön terveydenhuollon sähköisissä tietojärjestelmissä tai niiden välillä. Hankkeessa määritellään mm.

- edellytykset tietojen luovuttamiselle
- sähköisen suostumuksen hyvät toimintatavat
- lokitietojen käyttö
- sähköisen allekirjoituksen hyvät toimintatavat
- sähköisen arkistoinnin hyvät periaatteet
- käytännön ohjeet PKI-infrastruktuurin toteuttamiselle
- potilaiden sekä terveydenhuollon ammattihenkilöiden ja palveluntuottajien nimeämisen hyvä käytäntö ISO-OID koodiston mukaan

Käytännön ohjeet PKI-infrastruktuurin toteuttamiselle - hankkeesta Stakes on solminut sopimuksen Kuopion yliopiston Terveyshallinnon ja -talouden laitoksen kanssa. Sopimuksen toteutuksesta on vastannut kyseisellä laitoksella toimiva Shiftec-tutkimusyksikkö. Kuopion yliopiston puolesta projektista on vastannut projektitutkija Aapo Immonen.

Projektille perustettuun tukiryhmään (ns. PKI-ryhmä) ovat kuuluneet Avain Technologies Oy'ltä myyntipäällikkö Tero Tammisalo, SSH Oy:ltä senior sales manager Peter Öhman, Medici Data Oy:stä tuotevastaava Jari Hurme sekä Fujitsu services Oy:ltä system architect Petri Heinilä. Projekti on saanut tukiryhmältä arvokkaita apua ja näkemyksiä.

Tämä raportti täydentää ja syventää OSKEn aikaisemmin julkaistun PKI-raportin (Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri, OSVE 4/2002) ehdotuksia. Tämä raportti paneutuu paikallisen PKI-järjestelmän käyttöönoton ongelmatiikkaan ja antaa ohjeita PKI-järjestelmän käyttöönoton suunnittelulle. Raportissa on myös esitetty arvioita paikallisen PKI- järjestelmän kustannuksia.

Projektin aikana on käynyt ilmeiseksi, että PKI-järjestelmä koetaan ennen kaikkea teknisenä järjestelmänä. Tällöin unohtuu se tosiseikka, että PKI-järjestelmä on yhdistelmä teknologiaa, toimintapolitiikkaa ja hallinnallisia menetelmiä. Teknisiä toteutuksia

voidaan ostaa, mutta toimintapolitiikka ja hallinnolliset toimenpiteet pitää toteuttaa organisaation tasolla.

Tämä raportti on yksi kansallisen terveysprojektin tietoturvallisen tiedonvälitysalustaprojektin osatuloksista. Tietoturvallisesta tiedonvälityksestä OSKE ja Osaavien keskusten verkosto ovat tuottaneet aikaisemmin seuraavat dokumentit ja selvitykset:

- Elektronisen potilaskertomuksen sisältömääritykset, K. Hartikainen, A. Kokkola ja R. Larjomaa, OSVE 4/2000
- Selvitys asiakas- ja potilasasiakirjojen sähköisestä säilytyksestä ja kiistämättömyydestä, A. Ensio ja P. Ruotsalainen, OSVE 1/2001
- Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri, OSVE 4/2002
- Sähköisen asiakas- ja potilasasiakirjojen säilytyksen ja kiistämättömyyden hyvä käytäntö, A. Ensio ja P. Ruotsalainen, OSVE 1/2003. Tämä dokumentti sisältää ehdotukset ammattilaisten, potilaiden, palveluntuottajien ja terveydenhuollon sähköisten dokumenttien yksikäsitteiseksi nimeämiseksi
- Selvitystyö sosiaali- ja terveysministeriölle "Lääkärin tunnistus sähköisen reseptin kokeilussa – vaihtoehtoisia tapoja koskeva selvitys", P. Ruotsalainen, Helsinki 28.03.2003.

Näiden raporttien lisäksi on OSKE ollut mukana valmistelemassa sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta annetun lain muuttamista. Eduskunta hyväksyi kyseisen lain vuoden 2003 lopulla. Uudistetun lain12 § antaa perustan terveydenhuollon asiakkaiden, ammattihenkilöiden ja organisaatioiden todentamiselle terveydenhuollon sähköisessä asioinnissa.

Tämän raportin luvut 1-3 on laatinut Pekka Ruotsalainen. Raportin muusta sisällöstä vastaa Aapo Immonen. Raportin on toimittanut Pekka Ruotsalainen. Kiitän lämpimästi kaikkia tämän raportin valmisteluun osallistuneita heidän tekemästään arvokkaasta työstä.

Pekka Ruotsalainen

Tietoturvallisen kommunikaatioalusta projektin vastuuhenkilö
Tutkimusprofessori

1 Valtakunnallinen terveyshanke

Valtioneuvoston terveydenhuollon turvaamista koskeva periaatepäätös annettiin 11.4.2002. Tavoitteena on, että väestö saa tarvitsemansa laadukkaan hoidon maan eri osissa. Periaatepäätökseen on kirjattu mm. seuraavat toimenpidealueet:

- toimiva perusterveydenhuolto ja ennaltaehkäisevä työ
- hoitoon pääsyn turvaaminen
- henkilöstön saatavuuden ja osaamisen turvaaminen
- toimintojen ja rakenteiden uudistaminen
- terveydenhuollon rahoituksen vahvistaminen

Toimintojen ja rakenteiden uudistamisen yhtenä kohteena on valtakunnallisen sähköisen sairaskertomuksen käyttöönotto ja terveydenhuollon tietojärjestelmien yhteensopivuuden turvaaminen. Edellä mainitun periaatepäätöksen mukaisesti "valtakunnallinen sähköinen sairauskertomus" otetaan käyttöön vuoden 2007 loppuun mennessä, samalla kun toimintojen sekä rakenteiden uudistushankkeet on saatettu loppuun vuoteen 2007 mennessä.

Sosiaali- ja terveysministeriö asetti 29.1.2003 sähköisten potilasasiakirjojen toteuttamista ohjaavan työryhmän. Samalla käynnistettiin sähköisen potilaskertomuksen käyttöönottoa tukevat valtakunnalliset määrittelyhankkeet mm. potilaskertomuksen ydintietojen, avointen rajapintojen ja tietoturvallisen tiedonvälityksen ohjeistuksen laatimiseksi.

1.1 Hanke 4.1.3, valtakunnallisen sähköisen potilaskertomuksen käyttöönotto

Hankkeen tavoitteena on tukea hyvän ja laadukkaan hoidon järjestämistä sekä yli organisaatiorajojen tapahtuvaa saumattoman hoidon ja palvelun järjestämistä. Pyritään tuottamaan entistä laadukkaampaa hoitoa tarjoamalla terveydenhuollon ammattihenkilölle tarvittaessa kokonaiskuva asiakkaan/potilaan aikaisemmasta hoito- ja sairaushistoriasta. Hankeen tavoitteena on siis ”saumatonta hoitoa tukeva saumaton tiedonkulku”.

Sähköisen potilaskertomuksen käyttöönottoprojektin konkreettiseksi tavoitteeksi on asetettu sähköisten kertomusjärjestelmien valtakunnan laajuinen käyttöönotto vuoteen 2007 mennessä, tietojärjestelmien yhteistoiminnallisuus ja terveydenhuollon kansallinen tietoturvallinen tiedonvälitysympäristö[1].

Sähköisen potilaskertomuksen käyttöönottoprojekti jakautuu kolmeen osahankkeeseen. Niiden toteuttamisesta vastaavat Suomen Kuntaliitto (potilaskertomuksen ydintiedot, jatkohoidon suunnitelma, sähköiset lomakkeet ja metadata), Stakes (tietoturvallinen kommunikaatioalusta) ja Suomen HL7 yhdistys (avoimet rajapinnat).

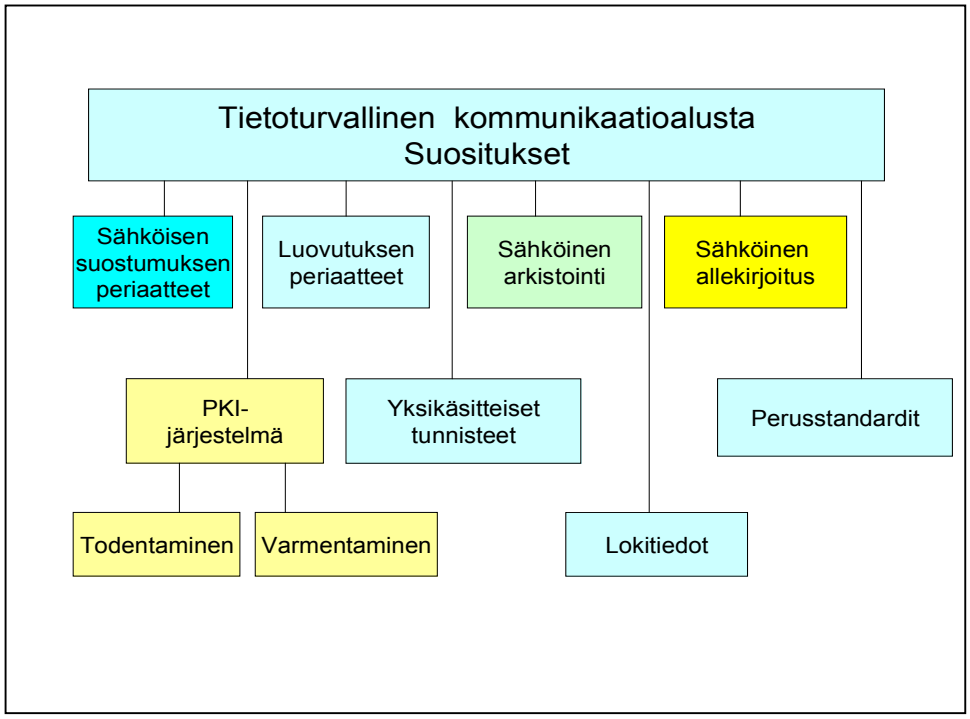
[1] Kansallisen terveydenhuoltoprojektin hanke 4.1.3, Valtakunnallisen sähköisen sairauskertomuksen käyttöönotto, Hankesuunnitelma 17.12.2002

1.2 Tietoturvallinen tiedonvälitysympäristö osahanke

Tietoturvallisen tiedonvälityksen lähtökohta on, että hoitotiedon luovutuksen tulee tapahtua siten, että tietoturva ja tietosuoja toteutuvat eettisten periaatteiden, lainsäädännön ja ministeriön antamien ohjeiden edellyttämällä tavalla.

Suomalaisessa terveydenhuollon palvelujärjestelmässä toimintayksiköt ovat hoitotietojen rekisterinpitäjiä. Rekisterinpitäjien välillä voidaan luovuttaa salassa pidettävää tietoa joko potilaan suostumuksella tai ilman suostumusta lainsäädännön määrittämin perustein. Potilaan suostumuksella voidaan luovuttaa hänen ongelmansa hoitamisen kannalta tarpeelliset hoitotiedot toiselle rekisterinpitäjälle hoitoon osallistuvien ammattihenkilöiden käyttöön. On syytä huomata, että terveydenhuollon toimintayksikkö päättää, ketkä ammattihenkilöt toimintayksikön sisällä osallistuvat potilaan hoitoon ja ketkä ovat sivullisia. Potilaan suostumusta tietojen käyttöön toimintayksikön sisällä ei siis edellytetä.

Tietoturvallinen kommunikaatioalusta -hanke tuottaa suosituksia tietoturvalliselle tiedonvälitykselle. Alla olevassa kuvassa 1 on esitetty kommunikaatioalustahankkeen osat.



Kuva 1 Tietoturvallinen kommunikaatioalusta -hanke

Laadittavia suosituksia voidaan hyödyntää niin organisaatioiden välisessä tiedonvaihdossa kuin toteutettaessa terveydenhuollon alueellisia tai seutukunnallisia sähköisiä palveluja.

Kommunikaatioalustahankkeessa tuotetaan mm. seuraavat suositukset:

- Ohjeita PKI-infrastruktuurin toteuttamiselle
- Potilaiden, ammattilaisten ja palveluntuottajien nimeämisen hyvä käytäntö
- Sähköisen suostumuksen periaatteet ja lokitiedot
- Sähköisen allekirjoituksen hyvät toimintatavat
- Sähköisen arkistoinnin hyvät periaatteet

1.3 PKI –järjestelmän käyttöönotto –osaprojekti

Osaprojektin tavoitteena on kuvata niitä tehtäviä, jotka tulevat vastaan kun terveydenhuollon toimintayksikkö harkitsee PKI-järjestelmän käyttöönottoa. Tulokset ja suositukset perustuvat tehtyihin selvityksiin, asiantuntijoiden näkemyksiin ja Kuopion yliopistossa PKI-testipenkin rakentamisesta saatuihin kokemuksiin.

Tämä raportti täydentää ja syventää OSKEn aikaisemman PKI-raportin (Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri, OSVE 4/2002) ehdotuksia.

2 Taustaa

Informaatioteknologia on tuonut uusia mahdollisuuksia julkisten palveluiden tuottamiseen ja jakeluun. Tämä edellyttää prosessien uudistamista myös terveydenhuollossa. Asiakkaiden tarpeista lähtevä prosessien uudistaminen on keskeinen tekijä palveluiden kustannus-laatusuhteen parantamisessa. Tietoverkot parantavat myös terveydenhuollon mahdollisuuksia tarjota laadukkaampaa palvelua tasapuolisesti riippumatta palvelujen tarjoajan ja sitä tarvitsevien fyysisestä välimatkasta [1].

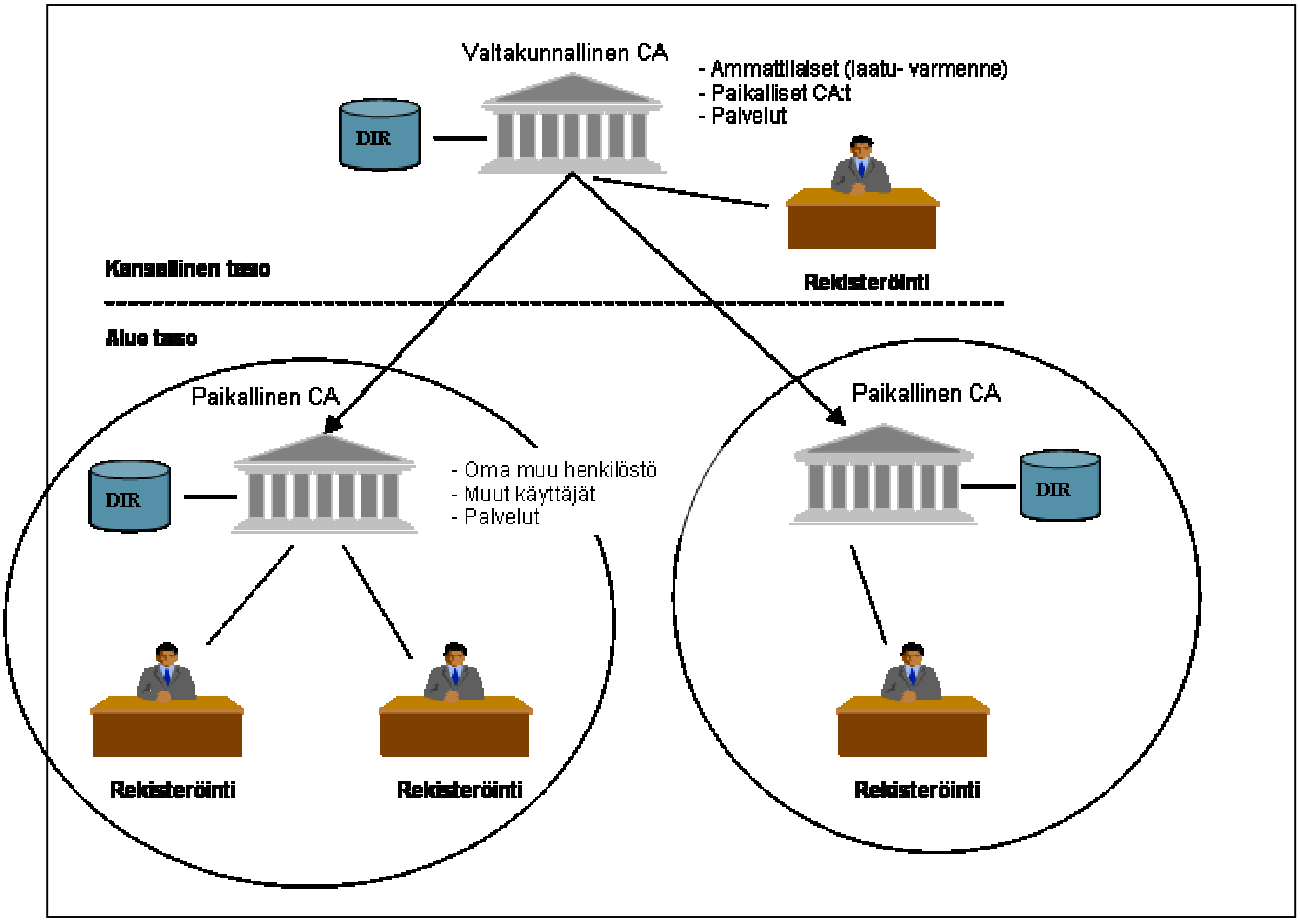
Tietoturvallisuudesta on tullut yksi keskeinen osa-alue terveydenhuollon informaatioteknologian käyttöönotossa. Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien ja palveluiden asianmukaista suojausta sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Tietoturvallisuussuunnitelmien tulee sisältyä paikallisiin/alueellisiin tietohallintostrategioihin. Merkittäväksi tietoturvainfrastruktuuriksi näyttää nousevan 'Julkisen avaimen menetelmä' (PKI menetelmä eli Public-Key Infrastructure). Se yhdistää digitaaliset sertifikaatit eli varmenteet, julkisen avaimen kryptografian eli salauksen ja sertifiointiauktoriteetit eli varmenneviranomaiset yhdeksi kokonaiseksi tietoturva-arkkitehtuuriksi [2,3,4,5].

PKI-järjestelmä on yksi kaikkein turvallisimmista menetelmistä turvata tiedonvälityksen luottamuksellisuus ja sähköisen viestinnän eheys. PKI:n tarjoamilla ratkaisuilla on mahdollista kattaa laajasti organisaatioiden välisen tiedonvälityksen tietoturvallisuuteen liittyvät tarpeet. Julkisen avaimen menetelmä mahdollistaa tiedon luottamuksellisuuden takaamisen, turvallisen tiedonvälityksen, käyttäjien ja tiedon todentamisen sekä tiedon muuttumattomuuden varmistamisen. Julkisen avaimen menetelmä ei muodostu pelkästään ohjelmista, laitteista ja tietotekniikasta vaan sen tulee olla osana käyttöön otettavaa perusinfrastruktuuria, jossa loppukäyttäjien asenteilla ja ennalta suunnitellulla tietoturvastrategialla on suuri merkitys [4,5,6]. PKI-järjestelmä onkin yhdistelmä teknologiaa, toimintapolitiikkaa ja hallinnollisia menetelmiä jotta mahdollistettaisiin arkaluontoisten tietojen vaihto turvattomassa tiedonkäsittely-ympäristössä.

PKI-järjestelmän käyttöönoton ydintavoitteita terveydenhuollossa ovat (kts. www.nhs.nhsia. co.uk/security):

- Henkilötietojen suojaaminen, kun niitä siirretään tietoverkoissa, niin ettei tietoja voida muuttaa tai lukea ulkopuolisten toimesta.
- Rekisterinpitäjien välisen tiedon vaihdon mahdollistaminen siten, että osapuolet voivat olla varmoja siitä, että vain juuri se vastaanottaja, jolle tiedot on tarkoitettu voi niitä lukea.
- Tarjota terveydenhuollon ammattihenkilöille ja organisaatioille keino luotettavaan todentamiseen.
- Tarjota terveydenhuollon ammattihenkilölle ja organisaatiolle menetelmä allekirjoittaa dokumentteja sähköisesti siten, ettei allekirjoitusta voida muuttaa ilman että tällainen muutos havaitaan.

Aikaisemmassa raportissaan (Ehdotus sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri, OSVE 4/2002) on tietoteknologian osaamiskeskus OSKE esittänyt mallin kansalliseksi terveydenhuollon PKI-järjestelmän arkkitehtuuriksi. Ehdotettu arkkitehtuuri perustuu kaksitasoiseen PKI-järjestelmään, jossa on sekä valtakunnan että aluetason varmennetoimintoja. Ehdotuksessa on keskitytty valtakunnan tason yhteisten PKI-palvelujen kuvaamiseen. Näitä ovat mm. lääkäreiden kansalliset varmennepalvelut, terveydenhuollon toimintayksiköiden varmentaminen sekä luotettujen arkistojen varmentaminen. OSKEn ehdottama arkkitehtuuri on kuvan 2 mukainen.



Kuva 2. Ehdotus kaksitasoiseksi terveydenhuollon PKI-arkkitehtuuriksi

3 Ohjeita PKI-järjestelmän käyttöönottoon ja tietojen salaukseen

Seuraavilla sivuilla esitetään ohjeen muodossa ne toimenpiteet, joita paikallisen/alueellisen PKI-järjestelmän käyttöönoton yhteydessä tulisi toteuttaa. Ohjeiden laadinnassa on käytetty hyväksi Englannin NHS Information Authorityn laatimia ohjeita. Tämän raportin editoija on sovittanut ne suomalaiseen terveydenhuollon toiminatympäristöön (kts. www.nhs.nhsia.co.uk/security).

PKI-infrastruktuurin käyttöönoton yhteydessä tulee PKI-järjestelmän toteuttamisesta vastaavan projektin toteuttaa seuraavat viisi tehtävää:

1. Terveydenhuollon palveluntuottajat, organisaatiot ja ryhmät tulee identifioida, rekisteröidä ja nimetä yksikäsitteisesti.
2. Tule varmistaa, että jokainen sertifikaatin omistaja allekirjoittaa sertifikaattisopimuksen.
3. Jokaiselle sertifikaatin omistajalle tulee generoida salausavainpari (ja optionaalinen digitaalisen allekirjoituksen avainpari).
4. Tulee huolehtia siitä, että yksityinen salausavain (ja yksityinen allekirjoitus avain) pysyy suojattuna siten, että vain rekisteröity sertifikaatin omistaja voi niitä käyttää.
5. Jokainen ainutlaatuinen nimi ja sitä vastaavat julkiset avaimet tulee julkistaa dokumentissa, jota kutsutaan digitaaliseksi sertifikaatiksi. Digitaalinen sertifikaatti on tehtävä todistusvoimaiseksi sertifioijan (Certification Authority, CA) allekirjoituksella.

Tunnistaminen ja rekisteröinti (tehtävä 1) tarkoittaa sitä, että terveydenhuollon ammattihenkilöt ja organisaatiot (mm. terveyskeskukset, lääkäriasemat ja sairaanhoitopiirit) tulee rekisteröidä. Näiden lisäksi voidaan organisaatioiden yksiköt ja tiimit rekisteröidä samoin kuin tietokonesovellutukset (esim. arkisto-ohjelmisto). Jokainen rekisteröity on ”sertifikaatin haltija (Certificate Holder).

Rekisteröintiä varten on luotava nimeämissäännöt (tehtävä 2). Rekisteröinti tulee tehdä huolellisesti, niin ettei kukaan voi esiintyä toisen puolesta. Rekisteröijä (esim. toimintayksikkö) voi tehdä rekisteröinnin itse tai delegoida tehtävän alemmalle tasolle (esim. organisaatiotasolle).

Sertifikaatin haltijan tulee sitoutua suojelemaan sertifikaattia. Tämä tarkoitta mm. sitä, että avainten hallintaan liittyvää PIN-koodia tai salasanaa ei saa antaa kenenkään ulkopuolisen käyttöön. Sertifikaatin haltijan tulee myös hyväksyä ja ymmärtää, että digitaalinen allekirjoitus vastaa perinteistä henkilökohtaista allekirjoitusta. Tästä seuraava laillinen vastuu tulee sertifikaatin haltijan ymmärtää.

Salausavaimella (tehtävä 3) ei salata tavallisesti suoraan dokumenttia, vaan tietojärjestelmä generoi symmetrisen avaimen, jolla dokumentin salaus tehdään. Tämä salausavain salataan sertifikaatin haltijan julkisella avaimella. PKI-järjelmän käyttöönotto edellyttää siis, että organisaatio sopii siitä, mikä on se salausmenetelmä, jota sen PKI-

ratkaisu tukee ja päättää siitä, mikä on salausmenetelmän tarjoama vähimmäissuojan hyväksyttävä taso. Nämä valinnat ovat osa organisaation sertifiointipolitiikkaa.

Yksityisiä avaimia ei tule tallettaa sellaisenaan esim. PC:n tiedostoon. Avaimen suojaamiseksi voidaan noudattaa seuraavia menetelmiä:

- Yksityinen avain talletetaan tiedostoon, joka on salattu sertifikaatin omistajan valitsemalla riittävän pitkällä salasanalla. Tämä vastaa ns. yhden tekijän perusteella tapahtuvaa todentamista, joka perustuu siihen mitä sertifikaatin omistaja tietää.
- Avain on tallennettu sertifikaatin omistajan ”tokeniin” (esim. sirukorttiin tai USB-laitteeseen). Laite on suojattu salasanalla, jonka käyttäminen aktivoi talletetut avaimet. Tämä on ns. kahden tekijän avulla tapahtuva todentaminen. Se perustuu siihen, mitä sertifikaatin omistajalla on (ts. token) ja siihen, mitä hän tietää (ts. salasana/PIN-koodi).
- Avain on tallennettu sertifikaatin omistajan sirukorttiin, joka voidaan aktivoida vain biometrisen tunnisteen avulla (esim. sormenjälki, silmänpohjakuva). Tämä vastaa ns. kolmen tekijän perusteella tapahtuvaa todentamista. Menetelmä perustuu siihen, mitä sertifikaatin omistaja tuntee (salasana), mitä hänellä on (token) ja mitä hän on (biometrinen ominaisuus). Tämä on suojauksen vaativin ja kallein aste.

Organisaation sertifiointipolitiikan laatimisen yhteydessä sen tulee valita yksityisen avaimen vähimmäissuojauksen taso. Lisäksi on varmistuttava, että jokainen sertifikaatin haltija tietää, miten yksityistä avainta tulee hallinnoida ja suojata.

Yksityistä avainta ja sitä vastaavaa sertifikaatin haltijan nimeä ei tule sijoittaa tietokoneen hakemistoon. Jos näin tehdään, voi tietojärjestelmään murtautuja korvata avaimen haltijan nimeen liittyvän yksityisen avaimen omalla avaimellaan ja esimerkiksi tämän jälkeen lukea sertifkaatin haltijan salaamia sähköposteja.

On huomattava, että se, että sertifikaatti tulee kiistämättömästi sitoa haltijan nimeen, edellyttää varmentajan (CA) perustamista. CA onkin jokaisen PKI-toteutuksen keskiössä. CA:n tehtävänä on varmistaa sertifikaatin ja nimen kytkös omalla sähköisellä allekirjoituksellaan. Sertifikaatti esitetään tavallisesti määrämuotoisena. Sertifikaatin muoto ja tietosisältö on määritelty mm. ITU X.509 standardissa, jonka myös IETF standardisointijärjestö on adaptoinut (IETF RFC 2459). Sertifikaattiin voi liittyä myös attribuutteja. Terveydenhuollon informatiikan standardisointikomitea ISO TC 215 on julkaissut terveydenhuollon PKI-standardin (ISO17090), jossa on kuvattu sertifikaattipolitiikkaa, hyviä PKI:n toteutustapoja ja esitetty esimerkkejä sertifikaateista.

PKI-järjestelmän implementointi edellyttää mm. seuraavia toimenpiteitä:

- CA:n perustamista. Se voi olla atk-osasto, yksityinen yritys tai valtakunnallinen julkinen organisaatio.
- Sertifiointipolitiikan laatimista.
- Sertifiointipolitiikan käyttöönottosuunnitelman laatimista
- Sertifikaattiprofiilin luomista. Tämä on dokumentti, joka spesifioi, mitä tietoja sertifikaatit sisältävät.

- Hakemiston perustamissa, josta sertifikaatit ovat niitä käyttävien haettavissa.
- Menetelmän jonka avulla sertifikaatti voidaan peruuttaa.

Sertifiointipolitiikan laatimisessa voidaan apuna käyttää seuraavia standardeja:

- IETF PKI X.509 RFC 2527 (Certification policy & Certification Practice Statement Framework)
- ISO TS 17090 (PKI in Healthcare)
- ISO 17799 standardi ja sitä vastaava englantilainen BS 7799 standardi

PKI- järjestelmä voidaan toteuttaa usealla eri tavalla. Seuraavassa on esitetty neljä tyypillistä tapaa toteuttaa terveydenhuollon PKI-järjestelmä. Rekisterinpitäjä voi:

1. Toteuttaa CA:n ja RA:n toiminnot omin toimin installoimalla tarpeellinen laitteisto ja ohjelmisto ja kouluttaa henkilöstö. Tämän raportin Shiftec-tutkimusyksikön PKI- installaatio on esimerkki tällaisesta toteutuksesta.
2. Ulkoistaa sekä CA:n että RA:n toiminnot. Palveluntuottajalle jää kuitenkin vastuu sertifiointipolitiikan valvonnasta ja sen implementoinnista. Toimittajan kanssa tehdyllä sopimuksella määritellään tässä tapauksessa sertifikaattien hallinnan ja palvelun tason ja osapuolten vastuut.
3. Ulkoistaa CA:n toiminnot ja toteuttaa RA:n toiminnot oman organisaation toimin. Tässä ratkaisussa CA:n toiminnot ulkoistetaan osapuolten välisellä sopimuksella. Palveluntuottajalla on vastuu sertifiointipolitiikasta ja rekisteröintiprosessista. Sillä on myös vastuu sertifikaattien peruutusmenettelystä ja sertifiointipolitiikan implementoinnista. Vastuut ja velvoitteet jaetaan sopimuksella palveluntuottajan ja toimittajan kesken.
4. Hankkia sertifikaatit kolmannelta luotetulta osapuolelta (ns. TTP). Tällöin TTP omistaa PKI-järjestelmän ja ylläpitää sitä. Se saattaa myös rajoittaa vastuitaan.

Toteuttamisvaihtoehdoista vaihtoehto 1 on kallein ja vaativin. Se soveltuu suurille organisaatioille. Vaihtoehto 3 on hyvä kandidaatti terveydenhuollon organisaatioille, koska ne joutuvat joka tapauksessa ylläpitämään omaa käyttöoikeuksien hallinnan tietojärjestelmää ja siihen liittyviä hakemistoja.

4 Sairaanhoitopiirien tietoturvapolitiikka, PKI- tilanne ja toteutusaikataulu

Saadakseen käsityksen vallitsevasta tilanteesta, tutki Kuopion yliopiston Shiftec-tutkimusyksikkö sairaanhoitopiirien ja kaupunkien sosiaalitoimen informaatioteknologian, tietoturvastrategian sekä julkisen avaimen menetelmän käyttöönoton aikatauluja. Kysely suoritettiin joulukuun 2003 ja tammikuun 2004 välisenä aikana. Tutkimuslupa saatiin 29:sta organisaatiosta. Näihin lähetettiin kyselylomakkeet elektronisessa muodossa, vastaukset saatiin 7 terveydenhuollon organisaatiosta ja 14 sosiaalitoimen organisaatioista, yhteensä 21 organisaatiolta. Kokonaisvastausprosentiksi tuli 72 %, terveystoimen osalta vastausprosentin ollessa 46 % ja sosiaalitoimen osalta vastausprosentin ollessa 88 %.

4.1 Julkisen avaimen menetelmän käyttöönoton aikataulut

Vastaajista 14 (70 %) ilmoitti, että heidän organisaatiossaan on käytössään asiakas- tai potilastietojärjestelmä ja kuusi (6)organisaatiota (28 %) on ottamassa asiakas- tai potilastietojärjestelmän käyttöönsä 24 kuukauden sisällä. Yksi organisaatio ilmoitti, ettei heillä ei oteta asiakas- tai potilastietojärjestelmää käyttöön.

Vastaajista 9 (40 %) ilmoitti, että organisaatiossa on tietohallintostrategia, 3 (15 %) ilmoitti strategiatyön olevan käynnissä, 2 (10 %) ilmoitti työn käynnistyvän 6 kuukauden kuluessa ja 6 (30 %) ilmoitti työn käynnistyvän 7-13 kuukauden kuluttua. Yksi organisaatio vastasi, ettei organisaatioon tehdä tietohallintostrategiaa.

Vastanneista terveydenhuollon organisaatioista 2 (33 %) ilmoitti, että organisaatiossa on tietohallintostrategia olemassa, yksi (17 %) ilmoitti strategiatyön olevan käynnissä, 2 (33 %) ilmoitti työn käynnistyvän 6 kuukauden kuluessa, yksi (16 %) ilmoitti työn käynnistyvän 7-13 kuukauden kuluttua. Vastanneista sosiaalitoimen organisaatioista 6 (43 %) ilmoitti, että organisaatiossa on tietohallintostrategia olemassa, 2 (14 %) ilmoitti strategiatyön olevan käynnissä, 5 (36 %) ilmoitti työn käynnistyvän 7-13 kuukauden kuluttua ja yksi organisaatio ilmoitti, ettei heidän organisaatiossaan tehdä tietohallintostrategiaa.

Vastaajista 12 (60 %) ilmoitti käyttävänsä tai käyttäneensä ulkopuolista apua asiakas- tai tietoturvastrategian suunnittelussa. Näistä terveydenhuollon organisaatioita oli 3 (50 %) ja sosiaalitoimen organisaatioita 9 (65 %).

Vastaajista 3 (15 %) ilmoitti että organisaatiossa on julkisen avaimen menetelmään perustuva tietoturvallisuusratkaisu käytössään. Kolme (15 %) ilmoitti ottavansa menetelmään perustuvan ratkaisun käyttöönsä 7-12 kuukauden kuluttua, 4 (20 %) ilmoitti ottavansa ratkaisun käyttöönsä 13 - 18 kuukauden kuluttua, 4 (20 %) ilmoitti ottavansa järjestelmän käyttöön 19 - 24 kuukauden kuluessa ja 4 (20 %) ilmoitti ottavansa

järjestelmän yli 25 kuukauden kuluttua. Yksi organisaatio ilmoitti, ettei se ota julkisen avaimen menetelmää käyttöönsä lainkaan.

Taulukko 1. Julkisen avaimen menetelmän käyttöönoton aikataulu

	Yhteensä		Sosiaalitoimi		Terveystoimi	
	n	%	n	%	n	%
PKI on käytössä	3	15	2	14	1	17
7-12 kk:n kuluttua	3	15	2	14	1	17
13-18 kk:n kuluttua	4	20	2	14	2	33
19-24 kk:n kuluttua	4	20	3	21	1	17
25 kk:n kuluttua tai myöhemmin	4	20	3	21	1	17
PKI infrastruktuuria ei oteta käyttöön	1	5	1	7	-	-
Puuttuu	1	5	1	7	-	-
Yhteensä	20	100	14	100	6	100

Vastaajista 17 (70 %) ilmoitti käyttävänsä tai käyttäneensä ulkopuolista apua julkisen avaimen menetelmän käyttöönoton suunnittelussa. Vastanneista terveydenhuollon organisaatioista 6 (100 %) ilmoitti käyttävänsä tai käyttäneensä ulkopuolista apua julkisen avaimen menetelmän käyttöönoton suunnittelussa. Vastanneista sosiaalitoimen organisaatioista 8 (57 %)ilmoitti käyttävänsä tai käyttäneensä ulkopuolista apua julkisen avaimen menetelmän käyttöönoton suunnittelussa.

Vastaajista 14 (70 %) ilmoittaa käyttävänsä tai, että on suunnitelmissa käyttää julkisen avaimen menetelmää tietojärjestelmän käyttäjän luotettavaan tunnistamiseen, 10 (50 %) sähköisen allekirjoittamisen toteuttamiseen ja 13 (65 %) tiedon luottamuksellisuuden takaamiseen. Vastanneista terveydenhuollon organisaatiosta 6 (100 %) ilmoittaa käyttävänsä tai tulee käyttämään julkisen avaimen menetelmää käyttäjän luotettavaan tunnistamiseen, 6 (100 %) sähköisen allekirjoittamisen toteuttamiseen ja 6 (100 %) tiedon luottamuksellisuuden takaamiseen. Vastanneista sosiaalitoimen organisaatiosta 8 (57 %) ilmoittaa käyttävänsä tai tulee käyttämään julkisen avaimen menetelmää käyttäjän luotettavaan tunnistamiseen, 4 (28 %) sähköisen allekirjoittamisen toteuttamiseen ja 7 (50 %) tiedon luottamuksellisuuden takaamiseen.

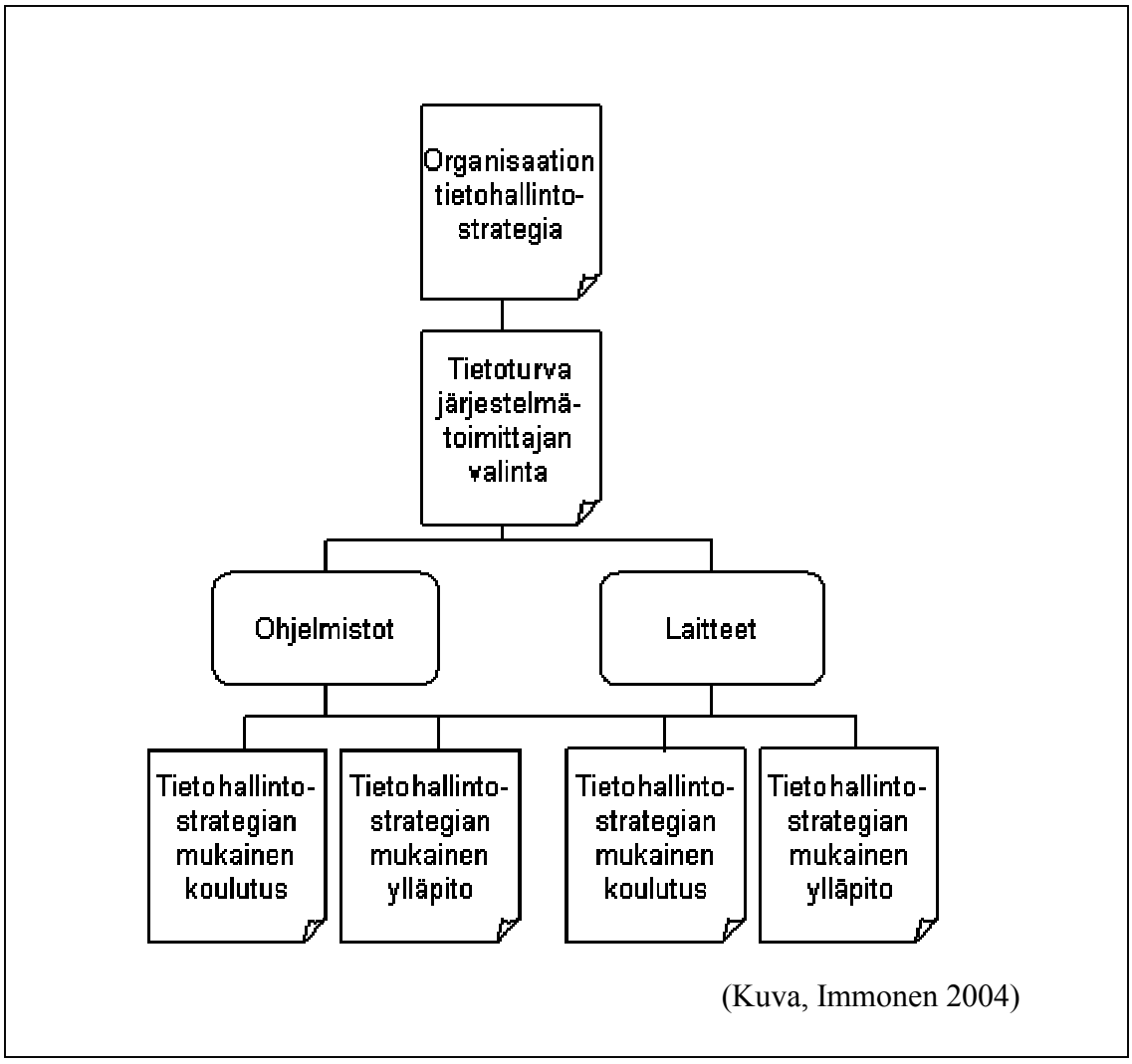
Vastaajista 17 (75 %) pitää luottamuksellisuutta ja 14 (70 %) eheyttä tärkeänä osaa tietoturvastrategiaa. Tiedon saatavuutta pitää 15 (75 %) vastaajaa tärkeänä osana tietoturvastrategia. Vahvaa tunnistautumista pitää 19 (95 %) vastaajista tärkeänä.

Vastauksista ilmenee, että 6 organisaatiota (30 %) tunnistaa luotettavasti henkilökuntansa heidän käyttäessään asiakas- tai potilastietojärjestelmiä. Kymmenen (50 %) ilmoittaa, että

potilasaineisto tai asiakastieto on heti saatavilla, kun sitä edellytetään. Yhdeksän organisaatiota (45 %) ilmoitti, että asiakirjat säilytetään niin, että vain aineistoon oikeutetuilla on niihin pääsy.

5 Paikallisen PKI-järjestelmän toteuttaminen - Shiftec-tutkimusyksikön toteutus

Ennen PKI-järjestelmän käyttöönoton aloitusta tulee organisaation suunnitella huolellisesti miten se hallinnoi tietoturvallisuutta. Kuvassa 3 on hahmoteltu tähän tehtävään liittyvät osatekijät.



(Kuva, Immonen 2004)

Kuva 3 Tietoturvallisuuden hallinnoinnin lohkokaavio

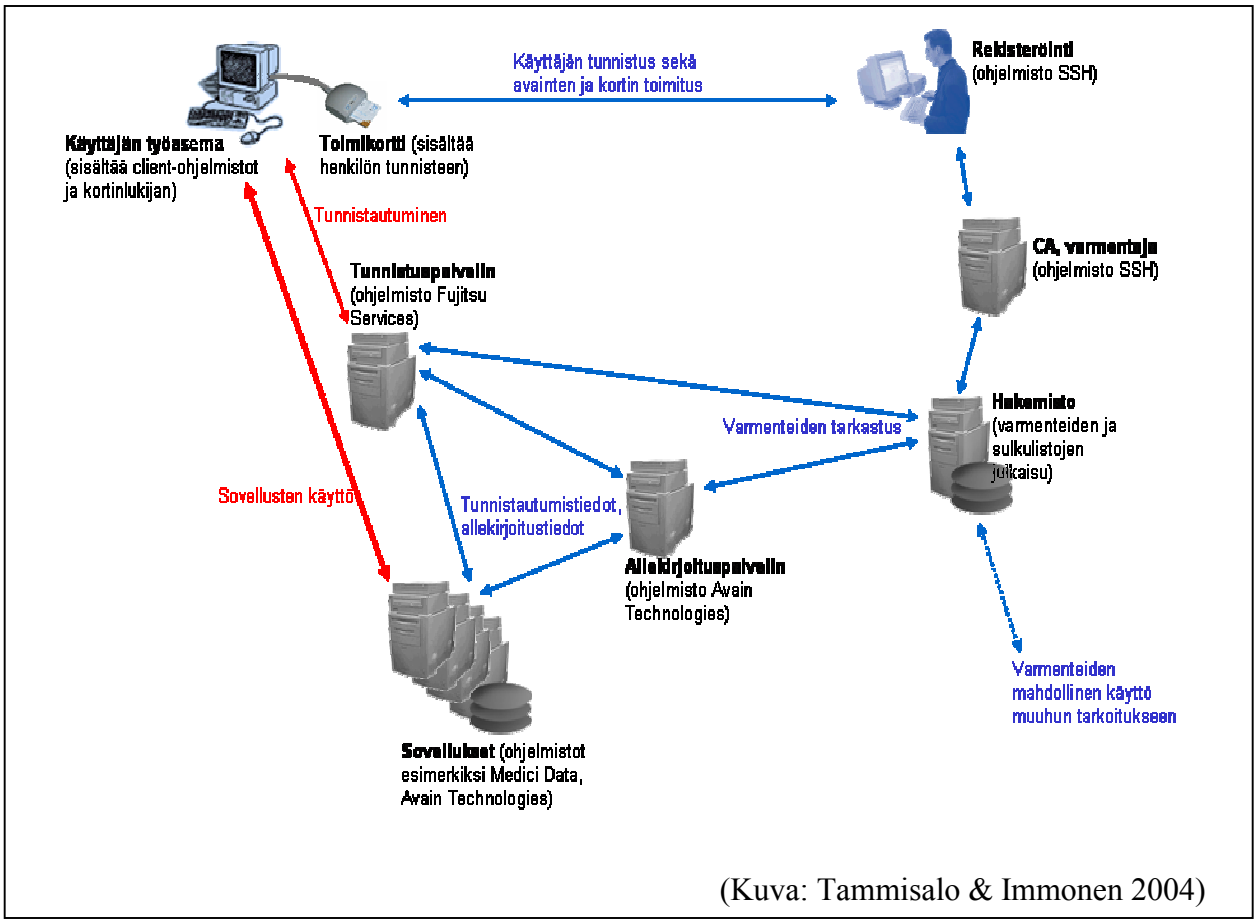
Organisaation saatua tietohallintostrategiansa valmiiksi voidaan aloittaa PKI-ympäristön laatimisen tekninen vaihe. Tämä sisältää ylimmällä tasolla laitteet ja ohjelmat, joiden valinta tapahtuu organisaation oman tietohallintostrategian perusteella. Tiedettäessä, mitä teknisiä vaatimuksia tietoturvaratkaisulta vaaditaan, voidaan valita järjestelmien toimittajat, jotka tulee kilpailuttaa. Koska kysymyksessä on kertaluonteisen investoinnin sijasta mahdollisesti pitkään kestävä yhteistyö, on järjestelmien toimittajien valinnassa kiinnitettävä erityistä huomiota mm. seuraaviin seikkoihin:

- kuinka vakavarainen yritys on
- noudattaako yrityksen käyttämä teknologia yleisesti hyväksyttyjä standardeja sek
- miten ylläpito, päivitys ja koulutukseen liittyvät seikat toteutetaan.

Varmenteella voidaan varmistaa, että osapuolet ovat heitä, keitä väittävät olevansa. Varmenne on edeltäkäsin yhteisesti sovitun luotettavan tahon, varmentajan, myöntämä sähköinen todistus, jolla todistetaan julkisen avaimen ja muiden varmenteen sisältämien tietojen vastaavan toisiaan. Varmentajan keskeinen tehtävä on varmentaa, mieluiten fyysisesti henkilötodistuksella, käyttäjän autenttisuus. Varmentaja luo myös elektroniset sertifikaatit, joiden autenttisuuden ja eheyden takaa varmenneviranomainen (CA). Varmenteessa on myös erityisesti mainittu varmentajan nimi sekä varmenteen voimassaoloaika. Varmenteen alkuperän ja eheyden takaa varmentajan digitaalinen allekirjoitus. Varmentaja toimittaa myöntämänsä varmenteet julkiseen hakemistoon, samoin mitätöityjen varmenteiden listan.

Julkisen avaimen menetelmän keskeinen toiminto on edellä kuvattu varmennejärjestelmä (kts. myös luku 3), jonka asennus ja ylläpito vaativat erittäin paljon erikoisosaamista. Varmennejärjestelmän asennukseen ja ylläpitoon liittyvien tehtävien suorittamiseksi on syytä harkita tarkkaan kahdesta vaihtoehdosta: suorittaako organisaatio itse asennuksen, konfiguroinnin sekä ylläpidon vai ulkoistaako organisaatio kyseisen palvelun. Tehtäessä kyseinen työ itse on huomioitava, että työ on korkeatasoista erikoisosaamista vaativaa ja osaajia on vähän vapailla työmarkkinoilla. Ulkoistettaessa varmennepalvelut on varmistettava yrityksen sitoutuminen myös asennuksen jälkeiseen ylläpitoon ja tekniseen tukeen.

Kuvassa 4 on esitetty ne tekniset laitteet ja ohjelmistot, joita tarvitaan terveydenhuollon PKI- ympäristön toteuttamiseksi. Kuvan esittämä toteutus on tehty Kuopion yliopiston Shiftec-tutkimusyksikössä.



Kuva 4. Esimerkki Shiftec- laboratorion tietoturvallinen PKI-ympäristö

Shiftec-tutkimusyksikössä suoritetuissa testeissä todettiin, että varmennejärjestelmät ovat kehitysvaiheen alussa olevia järjestelmiä, jotka vaativat vielä tuotekehitystä kypsyäkseen joustavasti asennettaviksi tuotteiksi. Testauksen aikana asennettiin kaksi erillistä kilpailevaa järjestelmää, jotka molemmat täyttivät julkisen avaimen asettamat tekniset vaatimukset tuotteille. Järjestelmien konfiguroiminen osoittautui niin vaativiksi, että ohjelmistojen toimittajien apu oli välttämätöntä. Molemmat järjestelmät asennettiin Linux-ympäristöön, joka omalta osaltaan lisäsi työn määrää. Asennusten jälkeen tuotteet ovat täyttäneet niille asetetut vaatimukset. Konfiguroinnin jälkeen ylläpitoon varattava aika on osoittautunut kohtuulliseksi. Varmennejärjestelmän käyttöönotossa on saatujen kokemusten valossa varattava huomattava määrä resursseja sekä asennukseen että järjestelmän konfigurointiin.

Testauksen tuloksena voidaan todeta, että vertaileva tutkimus suurimpien varmennejärjestelmän toimittajien kanssa olisi syytä suorittaa, jotta saadaan selvyys tuotteiden kehityksen realistisesta tilanteesta. Markkinoilla toimivat mm. seuraavat toimijat: SSH, Baltimore, Entrust, Smartrust, Verisign sekä RSA, muutamia mainitaksemme.

ITU X.509 -sertifikaatti sisältää tiedot yksilöllisestä sarjanumerosta, allekirjoitusalgoritmista, myöntäjästä, voimassaoloajasta, kohteesta, julkisesta avaimesta, myöntäjän yksilöllisestä tunnisteesta sekä käyttäjän yksilöllisestä tunnisteesta. Sertifikaatti sisältää myös tiedot myöntäjän sähköpostiosoitteesta, sertifioitavan nimestä, organisaatiosta ja sen yksiköstä, kaupungista ja maasta. Voimassaoloaika ilmoittaa sertifikaatin voimassaolon alkamispäivämäärän ja viimeisen voimassaolopäivämäärän.

Taulukko 2. X.509 ver.3 sertifikaatin rakenne

Sertifikaatin versio
Sertifikaatin sarjanumero
Varmentajan tunniste
Varmentajan allekirjoitus
Voimassaoloaika
Kohde tai käyttäjä
Kohteen tai käyttäjän julkisen avaimen informaatio
Kohteen tai käyttäjän tunniste
Laajennukset (esimerkiksi sähköpostiosoite)

Rekisteröintiviranomainen on se varmenneviranomainen tai rekisteröijä, joka rekisteröi käyttäjät ja tarjoaa mekaniikan ja rajapinnan varmenneviranomaisen myöntämien avaimien tunnistamiseen. Rekisteröintiviranomaisen tärkeimpänä tehtävänä on hoitaa käyttäjärajapinta. Se tunnistaa käyttäjän fyysisesti ja huolehtii varmennetietojen kirjaamisesta. Sen tehtävänä on myös luoda avaimet ja hoitaa koko varmennepolitiikka aina käyttäjän varmenteen tilaamisesta sulkulistojen ylläpitämiseen [6].

Tunnistuspalvelun tehtävänä on tunnistaa luotettavasti järjestelmän käyttäjä tarkistamalla sertifikaatin tiedot varmenteiden ja sulkulistan julkaisuhakemistosta. Varmennetallennin on yleensä LDAP (Lightweight Directory Access Protocol) määrittelyjen mukainen hakemisto.. LDAP itsessään on kevennetty versio X.500-hakemistostandardista, josta valisemalla joukko eniten käytettyjä piirteitä on aikaansaatu X.500 hakemistoa helpompi ja suorituskykyisempi protokolla, joka riittää useimpiin käytännön hakemistotarpeisiin [2,3,6,7,18].

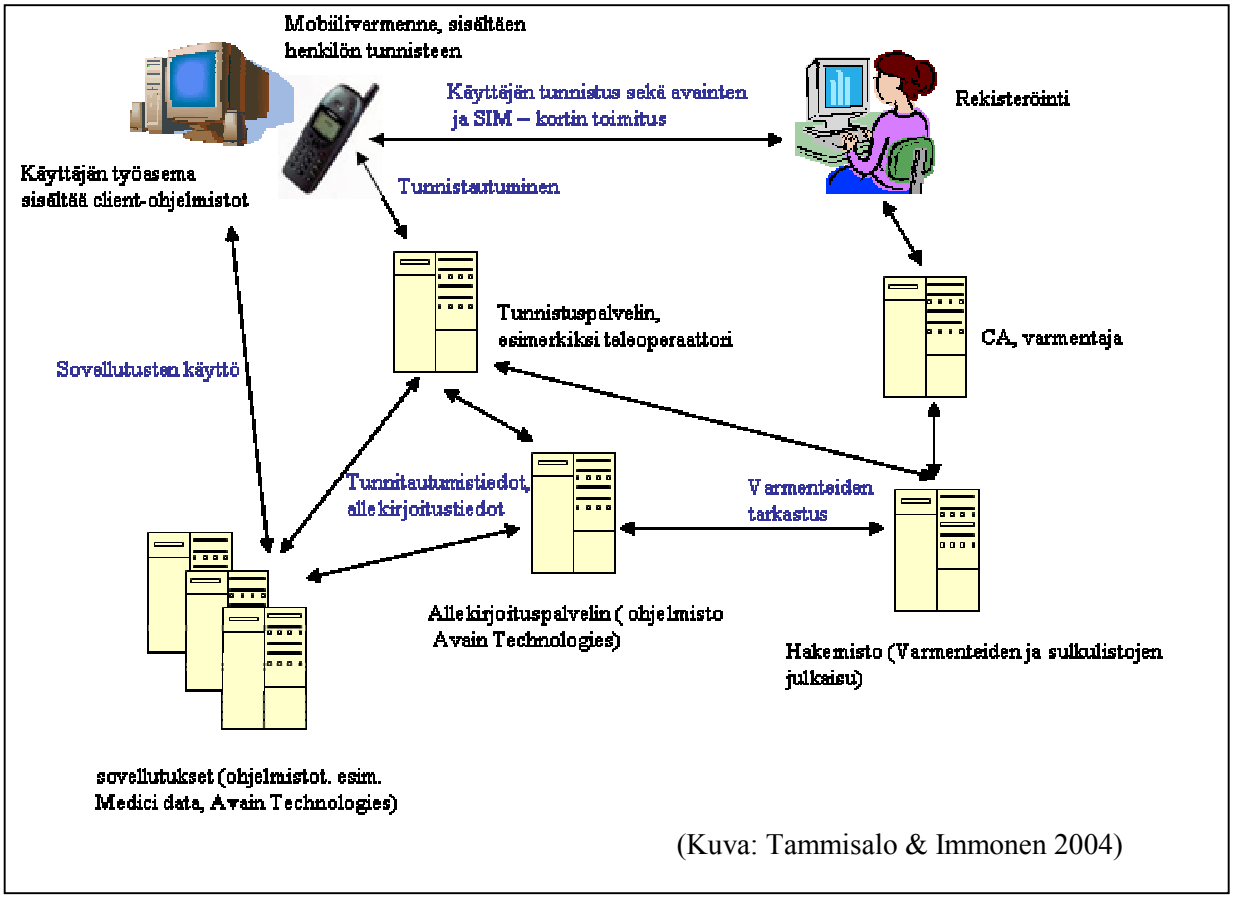
Rekisteröintiviranomainen asentaa sertifiointiviranomaisen luomat ja järjestelmien käyttäjän tarvitsemat tiedot joko toimikorttiin tai tokeniin. Kortin tai tokenin avulla käyttäjä kirjautuu luotettavasti järjestelmien käyttäjäksi.

Digitaalista allekirjoitusta varten on PKI-ympäristössä oltava allekirjoituspalvelin, jonka tehtävä on tarkistaa ja varmentaa allekirjoituksen oikeellisuus. Allekirjoituspalvelin voi toimia notariaattina, jolloin palvelin generoi aikaleiman allekirjoitustapahtumaan.

Varsinaisen asiakirjan allekirjoitus tapahtuu työasemilla käyttämällä joko toimikorttia tai tokenia sekä työasemille allekirjoitusta varten asennetulla allekirjoitusohjelmalla.

6 PKI-järjestelmä mobiilissa käyttöympäristössä

Kuvassa 5 on kuvattu tekniset laitteet ja ohjelmistot, joita tarvitaan terveydenhuollon mobilen PKI-ympäristöm toteuttamiseksi. Kuvan 5 ratkaisussa käytetään matkapuhelinta korvaamaan toimikortti tai token. Mobiilivarmentaminen eroaa kuvan 4 mallista siten, että järjestelemän pyytäessä joko tunnistautumista tai allekirjoitusta varten PIN-koodia, se syötetään matkapuhelimeen. Puhelimelta lähtee ensin viesti teleoperaattorin tunnistuspalvelimelle, joka tarkistaa tiedot hakemistopalvelimelta.



Kuva 5 Esimerkki terveydenhuollon turvallisesta käyttöympäristöstä hyödyntäen mobiilivarmennetta

7 PKI-järjestelmän käytötönoton tuottamia muutospaineita potilastietojärjestelmälle

PKI-järjestelmän käyttöönotolla on vaikutuksia terveydenhuollon toimintayksikön käytössä olevaan potilastietojärjestelmään ja erillisjärjestelmiin, jotka tulee sovittaa toiminnallisesti yhteen. Tämä sovitustyö edellyttää muutoksia nykyisin käytössä oleviin potilastietojärjestelmiin ja sitä, että palveluntuottajalla on organisatoriset PKI-valmiudet.

Palveluntuottajan organisatoriset edellytykset PKI-järjestelmän käyttöönotolle ovat seuraavat:

- Tarvitaan varmentaja, varmennepolitiikka ja sen mukaiset prosessit
- Tarvitaan PKI Infrastruktuuri ja mm.
    - Lukijalla varustetut työasemat ajureineen
    - Käyttäjän todentamispalvelu
- Tarvitaan yhteinen käyttäjätunnus, ns. geneerinen ID (ts. varmenteen sarjanumero –attribuutti)
- Tarvitaan varmenneympäristön hallinnoija.
- Tarvitaan käyttäjän varmennepohjainen todentaminen
    - palvelu, joka kytkeytyy palvelinpohjaisesti todentamispalveluun
    - sisäänkirjaus varmenteella ilman käyttäjätunnusta ja salasanaa
- Tarvitaan toiminnallisuus varmenteen poistoon, jotta sovellukset reagoivat poisvedettyyn varmenteeseen järkevällä tavalla.
- Sähköinen allekirjoitus ja arkistointi edellyttää :
    - palvelua, jolla sähköisesti allekirjoitetaan tietoja.
    - arkistoa, johon allekirjoitetut dokumentit varastoidaan pitkäaikaissäilytystä varten.

- Varmennettu tiedonsiirto organisaatioiden välillä edellyttää:
    - sovellusvarmenteita ja jopa sovellus – instanssivarmenteita
    - sovelluksiin varmenteita tukevia rajapintoja.

8 Julkisen avaimen menetelmän kuvaus alkaen tietoturvapolitiikasta tekniseen toteutukseen ja ylläpitoon

Euroopan komissio on viime vuosien aikana rahoittanut useita terveydenhuollon julkisen avaimen menetelmä -hankkeita. Ominaista näille hankkeille on ollut, että niissä on pääsääntöisesti kokeiltu yhtä tai kahta julkisen avaimen menetelmään liittyvää teknistä ominaisuutta. Yleisimmin käytössä ollut ominaisuus on ollut digitaalinen allekirjoitus ja tiedon salaus. Aktiivisimmin julkisen avaimen menetelmän käyttöä terveydenhuollossa ovat kokeilleet: Kreikka, Hollanti, Ranska, Tanska, Ruotsi, Belgia, Saksa, Itävalta, Iso-Britannia ja Norja. Suomi on ollut myös hankkeissa partnerina, mm. Pohjois-Karjalan sairaanhoitopiirin ollessa aktiivinen yhteistyökumppani useassa eri EU-projekteissa. Aktiivisimmin Suomessa on otettu julkisen avaimen menetelmä käyttöön Pohjois-Karjalan sairaanhoitopiirissä (PKSHP), Varsinais-Suomen sairaanhoitopiirissä (VSSHP), Helsingin ja Uudenmaan sairaanhoitopiirissä (HUS) sekä Pohjois-Pohjanmaan sairaanhoitopiirissä (PPSHP).

8.1 Yhteenveto kansainvälisistä terveydenhuollon PKI- hankkeista

Yhteenvetona kansainvälisistä tutkimuksista ja projekteista voidaan todeta, että ne ovat olleet varsin teknologialähtöisiä ja näin ollen myös niiden tulokset painottuvat teknologian toimivuuden tarkasteluun. Eurooppalaisissa hankkeissa on kiinnitetty vain vähän huomiota loppukäyttäjien omiin vaatimuksiin, kuten koulutukseen tai alueellisen lainsäädännön tietoturvallisuudelle asettamiin vaatimuksiin. Vaikka eurooppalaisten hankkeiden yhtenä viitekehyksenä mainitaan usein EU-lainsäädäntö, hankkeiden lopputuloksissa esitetään lähes poikkeuksetta teknisiä ratkaisuja [23]. Yhdysvalloissa säädetty HIPAA- lainsäädäntö on vaikuttanut mm. yritysten tuotekehitystyöhön. Leimaa-antavina piirteinä yhdysvaltalaisissa PKI-hankkeissa ovat olleet teknologialähtöisyys, alueelliset ratkaisut, luotetun kolmannen osapuolen aktiivinen hyödyntäminen [24].

Aiemmat kansalliset ja kansainväliset terveydenhuollon tietoturvallisuuteen liittyvät projektit ja tutkimukset osoittavat, ettei julkisen avaimen menetelmä ole pelkästään tuote, vaan sen tulee olla osa perusinfrastruktuuria, johon kuuluvat tilat, laiteet, ohjelmat ja käyttäjät. Tästä syystä käytössä olevien toimintamallin monistaminen paikasta toiseen johtaa huonoon ja usein kalliiseen lopputulokseen. Julkisen avaimen menetelmän käyttöönoton perusedellytys on huolellinen suunnittelu. Suunnittelussa on mm. analysoitava uhkien todennäköisyys, tunnistettava suojattavat kohteet, analysoitava suojauksen kustannus/ hyötysuhde ja ennen kaikkea todettava selkeästi, kenen vastuulla tietoturvan ylläpito ja päivitys organisaatiossa on. Suunnittelun lopputulos on organisaation tietohallintostrategia tai tietoturvapolitiikka, jota tulee noudattaa ja joka tulee olla kaikkien organisaatiossa työskentelevien tiedossa ja käytössä. Tehokkaan käytön peruslähtökohta on loppukäyttäjän kannalta järjestelmän läpinäkyvyys, joka merkitsee, ettei käyttäjän tarvitse ymmärtää, miten järjestelmä operoi avaimia ja sertifikaatteja salauksessa ja digitaalisessa allekirjoituksessa.

8.2 Huomioitavat seikat julkisen avaimen menetelmän käyttöönotossa - terveydenhuollon erityispiirteet

Tietoturvan luotettavuus on kiinni siitä, miten loppukäyttäjät tiedostavat tietosuojaan ja -turvaan liittyvät riskit, miten he hyväksyvät tietoturvaan liittyvät teknologiat, ja miten onnistutaan luomaan helppokäyttöinen ja hyväksyttävä rajapinta loppukäyttäjän ja teknologian välille. Ratkaisujen käyttöönoton tulee muodostua alueelliseksi, yhteensopivaksi, läpinäkyväksi sekä käyttäjäystävälliseksi. Näin taataan järjestelmien yleinen hyväksyntä loppukäyttäjien keskuudessa.

Terveydenhuollon ollessa muutoinkin poikkeuksellinen toimiala, on julkisen avaimen menetelmän käyttöönotossa kiinnitettävä eritystä huomiota loppukäyttäjien koulutukseen, tekniseen tukeen ja järjestelmän ylläpitoon. Tämä vaatii saumatonta yhteistyötä järjestelmän toimittajan ja niiden organisaatioiden välillä, jotka ottavat julkisen avaimen menetelmän käyttöönsä. Koska yhteistyö tulee jatkumaan vielä pitkään järjestelmän käyttöönottopäätöksen jälkeen, on varmistuttava, että yhteistyölle on olemassa toimintaedellytykset. Käyttöönotossa koulutuksen lisäksi on huolehdittava teknisestä tuesta ja siitä, että ylläpidosta vastaa asiantunteva tekninen henkilökunta.

9 Julkisen avaimen menetelmä terveydenhuollossa tietoturvallisuuden asiantuntijoiden näkökulmasta

Vuoden 2003 aikana Shiftec-tutkimusyksikkö käynnisti laadullisen tutkimuksen, johon valittiin haastateltaviksi yhdeksän asiantuntijaa terveydenhuollon tietotekniikan tai julkisen avaimen menetelmän toimialoilta. Nämä asiantuntijat ovat kirjoittaneet aiheesta tieteellisiä artikkeleja, johtaneet alan tutkimuksia, toimineet organisaatioissa tutkimus- ja kehittämisjohtajana, toimineet aktiivisesti kansainvälisessä terveydenhuollon tietoturvan standardoimistyössä tai olleet suunnittelemassa valtakunnallista tietoturvainfrastruktuuria, johon henkilön sähköinen tunnistamismenetelmä tukeutuu. Kertyneen aineiston pohjalta tulokseksi saatiin kolme toisiaan täydentävää kokonaisuutta: lainsäädännölliset, toiminnalliset ja tekniset vaatimukset julkisen avaimen menetelmässä terveydenhuollossa [25].

9.1 Lainsäädännölliset vaatimukset

Lainsäädännölliset vaatimukset kohdistuvat käyttäjään, ohjelmistoon ja tietoturvaan. Lainsäädäntö on peruste julkisen avaimen menetelmän käyttöönotolle. Kaikki haastateltavat viittasivat lakiin sähköisistä allekirjoituksista. Hallituksen esitys muutoksesta lakiin sähköisestä allekirjoituksesta annettiin tämän tutkimuksen aikana [26].

Lainsäädännön vaatimuksista nousi esiin terveydenhuollon ammattilaisten asema käyttäjinä, ohjelmiston sisällölliset vaatimukset ja tietosuoja ja -turva. Tietoturvan parantamiseksi ja sen hallinnoinnin helpottamiseksi jokainen asiantuntija pohti valtakunnallisen yhteisen arkkitehtuurin merkitystä. Voidaankin todeta, että yhteiselle julkisen avaimen menetelmän arkkitehtuurille on tarvetta. Teknisten vaatimusten toteutukseen ja ylläpitoon tulee kiinnittää huomiota [26].

9.2 Toiminnalliset vaatimukset

Terveydenhuollossa käyttäjät kuuluvat eri ammattiryhmiin, mutta tämän lisäksi he saattavat toimia eri tilanteissa eri rooleissa. Roolit oikeuttavat erilaisiin toimintatapoihin ja tietoihin. Terveydenhuollossa ovat tyypillistä useat toimijat ja sidosryhmät, joilla on erilaisia tietotarpeita lainsäädännön ja työtehtävien perusteella [26].

Käytettäessä digitaalista aineistoa, terveydenhuollon ammattihenkilöt voivat hyödyntää aikaansa tehokkaammin keskeiseen tehtäväänsä, joka on potilaiden hoito. Helppokäyttöisyys, koulutus ja selkeät ohjeet ovat vaatimuksia, jotka vähentävät muutosvastarintaa, sitouttavat käyttäjiä ja lisäävät digitaalisen aineiston käyttöä [26].

9.3 Tekniset vaatimukset

Haastatellut asiantuntijat esittivät useita teknisiä vaatimuksia. Yhteiseksi teemaksi teknisille vaatimukselle nousi PKI-järjestelmän toteutus ja ylläpito. PKI:n tekninen toteutus terveydenhuoltossa toi esille jotain erityispiirteitä, jotka näyttäisivät olevan tyypillisiä juuri kyseiselle toimialalle. Näistä voidaan mainita mm. toimikorttien hallinnointi, jossa joudutaan toimimaan normaalista käytännöstä poikkeavasti. Jos joku hoitohenkilökuntaan kuuluva hukkaa korttinsa, on se kyettävä mitätöimään välittömästi ja ennen kaikkea on kyettävä luomaan uusi, varmenteeet sisältävä kortti saman tien. Muita teknisiä toimialakohtaisia erityispiirteitä ovat mm. käytettävyys, sulkulistat, roolit sekä alueelliset järjestelmät [26].

Ohjelmistojen tulee pystyä toimimaan suurilla käyttäjämäärillä reaaliajassa. Terveydenhuollossa on varsin paljon henkilöstöä määräaikaisissa ja lyhytkestoisissa työsuhteissa ja ohjelmistojen tulee pystyä hallitsemaan käyttöoikeudet sujuvasti. Lisäksi ohjelmistojen tulee olla helppokäyttöisiä. Ohjelmisto on syytä paitsi pilotoida niin myös ottaa käyttöön hallittuina osaprojekteina. Lainsäädäntö asettaa ohjelmistoille tiukkoja edellytyksiä, jotta tiedot pysyvät muuttumattomina, eheinä ja kiistämättöminä. Tekniikassa on hyödynnettävä jo toimiviksi ja turvallisiksi todettuja toimintatapoja [26].

9.4 Yhteenveto asiantuntijoiden näkemyksistä

Vastausten perusteella voidaan todeta, että asiantuntijoiden käsitysten mukaan lainsäädäntö ohjaa toiminnallisia vaatimuksia ja toiminnalliset vaatimukset voidaan toteuttaa teknisillä toimenpiteillä. Ainoastaan yksittäisinä kommentteina haastateltavat toivat esille johdon sitouttamisen sekä suunnitelmallisen tietosuojastrategian merkityksen. Vertailtaessa tutkimustulosta kansainvälisiin tieteellisiin artikkeleihin ja tietoturvan teoreettisiin lähtökohtiin, voidaan tutkimusta pitää luotettavana. Tutkimustulosten perusteella tulisi tarkentaa terveydenhuollon tietotekniikkaan liittyvään tietoturvakoulutuksen sisältöä [26].

Asiantuntijahaastattelujen perusteella voidaan todeta, että julkisen avaimen menetelmän käyttöönotto terveydenhuollossa on perusteltua ja ajankohtaista. Tämän vuoksi tulisi luoda selkeä valtakunnallinen ohjeistus ja menettelytavat, joita kaikkein tulisi noudattaa. Terveydenhuollossa tulee määritellä, miten hallinnoidaan ja auditoidaan tietoturvapolitiikkaa. Julkisen avaimen menetelmän käyttöönotossa on huomioitava toiminnalliset, lainsäädännön ja tekniset vaatimukset. Julkisen avaimen menetelmän käyttöönotto terveydenhuollossa edellyttää uusien toimintaprosessien huolellista suunnittelua. On varauduttava käyttäjien mahdolliseen muutosvastarintaan, joten tekniikan on oltava toimintavarmaa ja ohjelmistojen helppokäyttöisiä. Lisäksi koulutuksen on oltava hyvin suunniteltua, laadukasta ja riittävää, jotta käyttäjien sitoutuminen varmistetaan [26].

10 Julkisen avaimen menetelmän kustannukset

Merkittäväksi julkisen avaimen menetelmän käyttöönoton esteeksi voi muodostua teknologian ja palveluiden hinta. Koska kyseessä on merkittävä taloudellinen sijoitus, järjestelmän käyttöönotolle on syytä varata riittävästi aikaa ja myös mahdollisuus jakaa julkisen avaimen menetelmän käyttöönotto useampaan osa-projektiin.

Varmenneviranomainen voi olla joko organisaation itse tai varmennepalvelut voidaan hankkia ostopalveluna. Tehtäessä päätös varmenneviranomaisen valinnasta, on huomioitava, että toiminnot hankitaan organisaatiosta, jossa on asiantuntemusta, johon luotetaan ja joka on vakavarainen (ei mahdollisuutta konkurssiin tai ei ole odotettavissa, että palvelua tarjoava yritys myydään).

Organisaatiossa päädyttäessä ratkaisuun, jossa julkisen avaimen menetelmä asennetaan ja sitä ylläpidetään omasta organisaatiosta käsin, voidaan kustannukset jakaa pääpiirteittään seuraaviin segmentteihin: suunnittelu ja tietohallintostrategian tekeminen, toteutus ja loppukäyttäjäkoulutus, ylläpito ja tekninen tuki. Kustannukset voidaan suunnitella jaettavaksi tasan kaikkien segmenttien välillä.

Taulukko 3. Julkisen avaimen menetelmän kustannukset organisaation toteuttamana

Tietoturvastrategian luominen		**henkilöresursseja**
Varmennejärjestelmä	Alkaen 100 000€	Lisenssi
Rekisteröintijärjestelmä	Alkaen 5 000€	Lisenssi
Client- ohjelma	Alkaen 100€/työasema	lisenssi / työasema
Käyttäjien kortit tai token tunnistautumiseen, avaimiin, sertifikaatin sekä digitaaliseen allekirjoittamiseen	noin 200-1 000€/työasema	lisenssit / työasema lukulaiteet/ työasema ajurit/ työasema
Allekirjoitusjärjestelmä palvelimelle	Alkaen 20 000€	Lisenssi
Palvelimet	Alkaen 2 500€, riippuen resursseista	Laite
Käyttöjärjestelmät palvelimille	Alkaen 1 000€	Lisenssi
Konesali	Riippuen mitä on määritelty tietohallintostrategiaan	infrastruktuuri
Tietoliikenne		infrastruktuuri
Ylläpito		henkilöresursseja
Tekninen tuki		henkilöresursseja
Koulutus		henkilöresursseja

Organisaation ulkoistaessa PKI-palvelut syntyvät kustannukset aiheutuvat taulukossa 2 kuvattujen tekijöiden palvelu- ja konsultaatiomaksuina, joiden suuruutta on vaikea ennakoida. Tästä syystä tietoturvallisuuspalvelujen ulkoistamisessa on syytä kiinnittää erityistä huomiota palveluntuottajien kilpailuttamiseen. Tilaajan on myös kiinnitettävä erityistä huomiota siihen, että tietohallintostrategia on sen itsensä tekemä ja että palveluntarjoaja kykenee vastaamaan kaikkiin strategian asettamiin haasteisiin.

11 Yhteenveto

Lainsäädännön lisäksi tietoturvaratkaisujen käyttöönoton yhtenä motiivina on säilyttää terveydenhuollon asiakkaiden **luottamus** siihen, ettei potilaiden **yksityisyyden suoja** ole vaarassa missään hoidon vaiheessa. Tietoturvaratkaisujen tavoitteena tulee olla myös potilaan hoidon saumattomuuden edistäminen niin, että potilastietojärjestelmien joustava käyttö toteutuu. Tietoturvan huomioiminen terveydenhuollon tietotekniikan käyttöönotossa merkitsee luotettavampaa ja tehokkaampaa sähköistä asiointia tietoverkoissa.

Maassamme on tarve luoda terveydenhuoltoon menettelytapa, joka mahdollistaa turvallisen sähköisen asioinnin. Tätä varten tulee terveydenhuollon henkilökunnan sekä asiakkaiden käyttöön tarjota mm. vahvan tunnistamisen ja pääsyvalvonnan, tiedon salauksen ja luottamuksellisuuden sekä tiedon ja tapahtumien kiistämättömyyden ja eheyden takaavat palvelut. Julkisen avaimen menetelmään perustuva tietoturvallinen ympäristö mahdollistaa henkilön sähköisen tunnistamisen kiistämättömästi. Varmenteiden avulla toteutettu sähköinen allekirjoitus on laillisesti pätevä. Julkisen avaimen menetelmän avulla voidaan salata asiakirjoja ja tiedostoja, eikä salattua sähköistä aineistoa voi muuttaa. Digitaalisesti allekirjoitettu aineisto voidaan myös aikaleimata.

Tässä työssä on noussut esille terveydenhuollon organisaatioiden varsin kirjavat menettelytavat tietojärjestelmien käyttöönotoille sekä tietoturvaan liittyvälle koulutukselle. Organisaatioiden tulisi huomioida että tietoturvaratkaisuihin liittyy olennaisena osana sekä tietoturvapolitiikan luonti että erilaiset hallinnolliset menettelyt. Tietoturvassa ei ole kyse pelkästään teknologiasta, vaan sen tulee olla osaa perusinfrastruktuuria, johon kuuluvat tilat, laiteet, ohjelmat ja käyttäjät. Tästä syystä yhdessä paikassa käytössä olevan toimintamallin monistaminen toiseen paikkaan johtaa huonoon ja usein kalliiseen lopputulokseen. Tietoturvan perusedellytys on huolellinen suunnittelu. Suunnittelussa on mm. analysoitava uhkien todennäköisyys, tunnistettava suojattavat kohteet, analysoitava suojauksen kustannus/hyötysuhde ja ennen kaikkea todettava selkeästi, kenen vastuulla tietoturvan ylläpito ja päivitys organisaatiossa on. Koska kyseessä on merkittävä taloudellinen sijoitus, järjestelmän käyttöönotolle on syytä varata riittävästi aikaa ja myös mahdollisuus aktiiviseen koulutukseen.

Tietotototurvan peruslähtökohtana on loppukäyttäjän kannalta järjestelmän läpinäkyvyys. Käyttäjän ei siis tarvitse ymmärtää, miten järjestelmät esimerkiksi operoivat julkisia ja salaisia avaimia sekä sertifikaatteja salauksessa ja digitaalisessa allekirjoituksessa. Terveydenhuollon ollessa muutoinkin poikkeuksellinen toimiala, on tietoturvassa kiinnitettävä eritystä huomiota loppukäyttäjien koulutukseen, tekniseen tukeen ja järjestelmän ylläpitoon. Tämä vaatii saumatonta yhteistyötä järjestelmän toimittajan ja niiden organisaatioiden välillä. Koska organisaatioiden ja järjestelmäntoimittajan yhteistyö tulee jatkumaan vielä pitkään järjestelmän käyttöönottopäätöksen jälkeen, on varmistuttava, että yhteistyölle on olemassa toimintaedellytykset [27].

Liite I

Julkisen avaimen menetelmään liittyviä lyhenteitä ja käsitteitä

Yksi tietoturvan näkyvimmistä piirteistä on käsitteistön ja lyhenteiden suuri määrä. Julkisen avaimen menetelmän ollessa uutta teknologiaa on käytössä oleva terminologia varsin vaikeaselkoista eikä kaikille termeille löydy luontevaa suomenkielistä vastinetta. Lisäksi julkisen avaimen menetelmälle on ominaista valtava määrä eri teknologisia lyhenteitä, joita on hankala tulkita. Seuraavassa määritellään tässä tutkimuksessa esiintyviä keskeisiä tietoturvaan liittyviä teknisiä käsitteitä.

Julkisen avaimen menetelmällä (PKI-järjestelmä) tarkoitetaan asymmetrisen avainparin ja varmenteiden ja sähköisen allekirjoituksen käyttöön perustuvaa menetelmää, jonka avulla käyttäjät voidaan luotettavasti todentaa. Menetelmässä yhdistyy korkea tietoturva ja helppo hallittavuus. Julkisen avaimen menetelmä mahdollistaa vahvan tunnistuksen, digitaalisen allekirjoituksen, kiistämättömyyden, tiedon eheyden ja salauksen [5,6,7]. PKI-järjestelmä on yhdistelmä teknologiaa, toimintapolitiikkaa ja hallinnollisia menetelmiä jotta mahdollistettaisiin arkaluontoisten tietojen vaihto turvattomassa tiedonkäsittely-ympäristössä.

Pääsynvalvonnalla (access control) tarkoitetaan järjestelmän tai resurssien käytön estämistä tai rajoittamista [2,3,6,7].

Digitaalisella allekirjoituksella tarkoitetaan dokumenttiin liitettyä merkkijonoa, joka mahdollistaa tiedon alkuperän ja tiedon eheyden todentamisen. [2,3,6,7].

Tiivisteellä (Hash-arvo) muodostetaan sanomasta kiinteän pituinen merkkijono (tiiviste), jonka muuttumattomuutta vertaamalla on mahdollista todentaa, onko viesti pysynyt alkuperäisessä muodossaan vai onko tietoja muutettu esimerkiksi tiedonsiirron aikana [2,3,6,7].

Varmentajalla tarkoitetaan luotettua organisaatiota, joka luo, jakaa ja varmentaa sertifikaatteja niin että eri osapuolet voivat luottaa varmennetiedon kuuluvan asianomaiselle [7,8]. Varmentajan keskeisenä tehtävänä on varmistaa, että käyttäjä, jolle varmenne myönnetään, on tunnistettu sovitulla tavalla. Varmentaja huolehtii myönnettyjen varmenteiden hallinnasta sekä varmistaa, että yksityisten ja julkisten avainten käsittely on ollut turvallista niiden luomisen ja käyttäjälle toimittamisen välisenä ajanjaksona [4].

Varmenteella, sertifikaatilla tarkoitetaan varmentajan myöntämää elektronista dokumenttia, jolla todistetaan, että henkilön tai organisaation varmenteen sisältö kuuluu asianomaiselle käyttäjälle [2,3,6,7].

Rekisteröijän (Registration Authority) tehtävänä on kerätä tarvittavat käyttäjätiedot ja varmistua käyttäjän henkilöllisyydestä tunnistamalla käyttäjä esimerkiksi virallisesta henkilödokumentista [2,3,4,5,6].

Laatuvarmenteella tarkoitetaan korkeat kansainväliset turvallisuusvaatimukset täyttävää varmennetta. EU-direktiivi sähköisistä allekirjoituksista edellyttää, että jäsenvaltiot hyväksyttävät lainsäädäntöönsä direktiivin mukaisen lain sähköisistä allekirjoituksista. Siinä asetetaan varmenteelle vaatimukset, jotka sen on täytettävä ollakseen hyväksytty laatuvarmenne [4].

Sulkulistapalvelulla julkaistaan vanhentuneet, perutut ja kuoletetut tai määräaikaisesti käytöstä poistetut varmenteet. Sulkulistapalvelu on osa rekisteröijän tehtäviä [2,3,4,5,6,7].

Liite 2

Perusteita tietoturvallisuudelle terveydenhuollossa

Tietoturvallisuuden hyvä taso ja laatu ovat tärkeitä niin kansalaisten kuin hallinnon kannalta. Puutteellinen tietoturvallisuus vaarantaa kansalaisten turvallisuutta, yksityisyyden suojaa ja taloudellisia etuja sekä aiheuttaa vahinkojen ja tiedonmenetysten takia lisätyötä ja -kustannuksia sekä heikentää viranomaisten uskottavuutta.

Luottamus yksityisyyden suojan säilymisestä on yksi laadukkaan hoidon edellytys [10,11,12,13]. Laadukas hoito edellyttää, että potilaat voivat hakeutua luottamuksellisesti tarkastuksiin ja hoitoihin. Hyvän hoidon perustana on potilaan ja hoitohenkilökunnan välille muodostuva luottamus, joka korostuu potilas-hoitosuhteessa [10,11,12]. Esimerkiksi potilas-lääkäri suhteessa kysymys on luottamuksellisesta viestinnästä, jota suojaavat salassapitosäännökset ja johon lääkäri on ammatillisen etiikkansa myötä sitoutunut vahvasti [13].

Hoitohenkilökunta-potilas suhteissa on kysymys luottamuksellisesta viestinnästä, jota suojaavat salassapitosäännökset. Hoitosuhteen luottamuksellisuus konkretisoituu hoitohenkilökunnan vaitiolovelvollisuutena, asiakirjasalaisuutena, hyväksikäyttökieltona sekä tietojen suojaamisena [11]. Potilaan tai asiakkaan on voitava luottaa siihen, että terveydenhuollossa työskentelevät ammattilaiset osaavat ja pystyvät huolehtimaan kyseisestä arkaluotoisesta aineistosta lain edellyttämällä tavalla. Potilas luovuttaa pääsääntöisesti omalla suostumuksellaan, jolla tarkoitetaan henkilötietolain mukaan *”kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.”*, yksityisyytensä suojaan kuuluvan perusoikeuden, omat terveys- ja sairaustietonsa toiselle olettaen, että terveydenhuollon ammattilaiset huolehtivat kertyneestä ja syntyvästä uudesta aineistosta lain edellyttämällä tavalla [11, 14]. Yksityisyys ja yksilöllisyys ovat avainkäsitteitä määriteltäessä henkilöoikeuden keskeisintä lähtökohtaa eli itsemääräämisoikeutta [14]. Kyse ei ole ensisijaisesti tietojen suojaamisesta vaan potilaan yksityisyyden suojaamisesta sekä luottamuksellisesta potilassuhteesta [11,14].

Yksi lähtökohta on henkilötietolain huolellisuusvelvoite, jonka mukaan terveydenhuoltoyksiköiden velvollisuus on pitää asiallista huolta potilaista syntyvästä aineistoista niin, ettei rekisteröidyn, tässä tapauksessa henkilön joka on rekisteröity potilaaksi tai terveydenhuollon asiakkaaksi, yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rikota [15].

Tietosuoja tarkoittaa tietosuojalainsäädäntöön kirjoitetussa merkityksessä sitä, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Henkilötiedot on lain mukaan pidettävä salassa asiattomilta ja ulkopuolisilta, henkilötietojen oikeellisuus on varmistettava, henkilötietoja ei saa tuhota tai käsitellä asiattomasti ja merkittävien henkilötietojen on oltava käytettävissä. Tietosuoja voidaan määritellä henkilörekisterilainsäädäntöön sisältyvien säännösten kokonaisuudeksi, jonka tarkoituksena on henkilötietoja kerättäessä, tallennettaessa, käytettäessä ja luovutettaessa, arkistoitaessa ja hävitettäessä henkilön yksityisyyden sekä hänen etujensa ja oikeuksiensa suojeleminen, valtion turvallisuuden varmistaminen samoin kuin hyvän rekisteritavan toteuttaminen. Valtionhallinnon tietoturvallisuuden johtoryhmän laatimassa käsitteistössä tietosuoja on määritelty perusoikeudeksi, joka on tarkoitettu turvaamaan kansalaisen yksityisyys suojaamalla henkilötiedot oikeudettomalta tai henkilöä vahingoittavalta käytöltä [10,14,16].

Tietoturva on määritelty tietoriskien hallinnaksi. Tietoturvan toteuttaminen tapahtuu teknisin tai organisatorisin menetelmin. Tietoturvallisuudessa on kysymys kokonaisuuden hallinnasta, jossa kokonaisuuden heikoin rengas määrää tietoturvan kestävyyden. Tietoturvallisuus perustuu kahdeksaan toimenpidealueeseen. Tietoturvan hallinta sisältää suunnitelmien lisäksi myös toteutuksen seurannan [6,16,17]

Tietoturvallisuuden päätavoite on hyvän tietojenkäsittelytavan ja asianmukaisen perusturvallisuuden luominen [18,19,20]. Parhaimmillaan tietoturvan toteutuminen tarkoittaa hallittua informaation käyttöä, jossa luotettavasti tunnistettu henkilö hyödyntää eri tilanteessa juuri oikeaa aineistoa, johon hänellä on ammatilliseen rooliinsa perustuen oikeus.

Koska terveydenhuollon informaatioteknologia on uutta, ei sille löydy yksiselitteistä käsitemallia. Gritzalis määrittelee tietoturvaohjeistuksen muodostuvan neljästä tasosta. Yleiset toimintamallit, jotka ohjaavat tietojen suojaamista. Pääperiaatteet eri hallinnonaloille, joista terveydenhuolto on yksi. Ohjeistukset, jotka sisältävät yksityiskohtaisia tietoturvaan liittyviä toimenpidemalleja hyödynnettäessä uutta informaatioteknologiaa. Konkreettiset toimenpiteet, jotka sisältävät tietoturvaan liittyviä teknisiä toimenpiteitä. Nämä tulee määritellä hyvissä ajoin ennen tietojärjestelmien käyttöönottoa ja niiden tulee olla keskeinen ohjaava ominaisuus tietotekniikan käytössä [21].

Tämän raportin viitekehys perustuu henkilötietolakiin, joka määrittelee yksityisyyden suojan sekä geneeriset tietoturvapalvelut, joita ovat **luottamuksellisuus, eheys, oikeellisuus** ja **kiistämättömyys,** jotka ovat tiedon käytön mahdollistamisen ja sen turvaamisen tärkeimpiä vaatimuksia [2,3,4,5,6,17,18,19,22].

Luottamuksellisuudella (confidentiality) varmistetaan, että tiedot ovat vain niihin oikeutettujen henkilöiden ja organisaatioiden saatavilla eikä tietoja paljasteta muille. Valtionhallinnon tietoturvallisuuskäsitteistössä luottamuksellisuus määritellään seuraavasti: ”Tietojen säilyminen luottamuksellisena ja tiedostoihin tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkauksilta.” [20]. Henkilötieto- ja julkisuuslaeissa on nimenomaisia kohtia, jotka turvaavat potilaan

tiedonsaantioikeudet sekä edellyttävät, että potilasrekisteriin sisältyvät tiedot ovat virheettömiä käsittelyn kaikissa vaiheissa [6,7,11].

Luottamuksellisuus merkitsee sitä, että kukaan ei pääse oikeudettomasti käyttämään tietoja, jotka eivät ole tarkoitettu hänelle. Luottamuksellista tietoa voivat lukea tai muokata vain ne, joilla on tähän tietoon oikeus. Se on ensimmäinen ja tärkein tietoturvan peruspilari. Tällä tarkoitetaan asiakirjojen ja dokumenttien sekä niiden sisältämien tietojen olemista vain ja ainoastaan niitä tarvitsevien henkilöiden ja tahojen käytettävissä. Niitä pyritään suojaamaan luvatonta käyttöä vastaan. Tarkastelukulmasta riippuen voi luottamuksellisuus tarkoittaa joko yksittäisen henkilön tietoja tai kyseessä voivat olla kaikki organisaation toiminnassaan käyttämät tiedot. Olennaisen tärkeää luottamuksellisuus on erityisen arkaluontoisten asiakirjojen kohdalla. Näitä ovat mm. potilas, asiakas- ja henkilötiedot sekä organisaation suunnitteludokumentit. Koska tietojen tulee olla niihin oikeutettujen henkilöiden käytössä, edellyttää tämä tietojen luokittelua koko organisaation tasolla sekä tietojen käyttöoikeuksien määrittelyä ammatillisten roolien perusteella [5,20].

Eheydellä (integrity) tarkoitetaan, etteivät tiedot muutu tai tuhoudu aiheiston käsittelyn missään vaiheessa [2,3,6,16,17,19]. Valtionhallinnon tietoturvallisuuskäsitteistössä eheys määritellään seuraavasti: ”Tietojen tai tietojärjestelmien aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus. Ominaisuus, että tietoa tai viestiä ei ole valtuuttomasti muutettu ja että mahdolliset muutokset voidaan todentaa kirjausketjussa.”[20].

Eheys tarkoittaa, ettei tietoa ole muutettu ilman valtuuksia ja mahdolliset muutokset voidaan todentaa. Aineisto on voitava varmistaa aitona ja väärentämättömänä. Aineiston sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus on myös kyettävä varmistamaan. Järjestelmien tiedot ja palvelut tulee olla niihin oikeutettujen käytettävissä etukäteen määritellyn vasteajan puitteissa. Eheyden vaatimuksina on, etteivät tiedot muutu eivätkä häviä laitteisto-, ohjelmisto- ja tiedonsiirtovirheiden, inhimillisten virheiden tai minkään luvattoman toimenpiteen seurauksena. Tiedon muuttamisella tarkoitetaan sitä, että esimerkiksi tietoja tuhotaan tai niihin tulee asiattomia muutoksia. Tiedon eheydellä pyritään tiedon ja sen käsittelytapojen täydellisyyteen ja virheettömyyteen. Eheys voi särkyä tahattomasti tai tahallisesti [3,4,5,6,18,19].

Eheys voidaan taata eri kryptografisilla menetelmillä. Ennen kuin kryptografia voidaan ottaa laajemmalti käyttöön organisaatioissa, on organisaation henkilökunnan ymmärrettävä tietoturvakäytäntö ja sen merkitys. Kryptografialla salataan tai muunnetaan tietoja siten, että sen sisältö pysyy salassa [3,4,5,6,18,19].

Oikeellisuudella (authentity) tarkoitetaan sekä oliota tai toimijaa itseään että sen sisältämän informaation luotettavaa tunnistamista. Tiedon oikeellisuuden varmistaminen on tärkeää, jotta voidaan varmistaa siirretyn tiedon säilymisestä muuttumattomana lähettäjältä vastaanottajalle. Oikeellisuudella varmistetaan tiedon muuttumattomuus syötön, varastoinnin, käsittelyn ja tiedonsiirron aikana. Lisäksi on varmistuttava, etteivät

tiedot muutu eivätkä häviä laitteisto-, ohjelmisto- ja tiedonsiirtovirheiden eivätkä minkään luvattoman toimenpiteen seurauksena [2,3,5,6,18,19].

Valtionhallinnon tietoturvallisuuskäsitteistössä oikeellisuus määritellään seuraavasti: ”Virheettömyys, yhtäpitävyys todellisen asiantilan kanssa. Vrt. eheys” (Valtionvarainministeriö 2000). Sama dokumentti määrittelee virheen seuraavasti ”Suureen lasketun tai mitatun arvon ja todellisen tai teoreettisesti oikean arvon välinen ero. Vrt. oikeellisuus. Ihmisen tai tietokoneen suorittama, joka tai jonka tulos ei ole sovittujen sääntöjen tai tarkoituksen mukainen”[20].

Kiistämättömyys (non-repudiation) on keskeinen tekijä erityisesti luottamuksellisessa sähköisessä asioinnissa ja tarkoittaa, että käyttäjä voidaan todentaa pitävästi. Viestin aitouden ja eheyden avulla voidaan toteuttaa kiistämättömyys, joka tarkoittaa tietoverkossa eri menetelmin saatavaa varmuutta siitä, että tietty henkilö on lähettänyt tai vastaanottanut tietyn viestin tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi. Kiistämättömyyttä tarvitaan, kun muut aineiston käyttäjät haluavat varmistua osapuolen sitoutumisesta tiettyyn viestiin tai asiaan, esimerkiksi lausuntoon. Yksi kiistämättömyyden hyödyntäjä onkin sähköinen allekirjoitus, jolla siirretään kynällä tehdyn allekirjoituksen oikeudellinen muotovaikutus tietoverkossa tapahtuvaan toimintaan. Kiistämättömyydellä käsitetään myös tietoverkossa eri menetelmin saatavan varmuus siitä, että tietty henkilö on lähettänyt tietyn viestin tai vastaanottanut tietyn viestin tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi. Kiistämättömyydellä estetään lähettäjän ja vastaanottajan kiistely sanoman siirrosta ja sisällöstä. Tarkoituksena on siis antaa kiistämättömät todisteet, että lähetys on tapahtunut ja vastaanotettu. Kiistämättömyydellä osoitetaan myös, ettei tiedon lähettäjä voi kiistää lähettäneensä tietoa ja olleensa jossakin tapahtumassa osapuolena. Kiistämättömyys on tietolähteen todennuksen vahva muoto ja se toteutetaan sähköisellä allekirjoituksella. Tällä voidaan varmistaa tiedon eheys ja lähettäjän alkuperä [2,3,4,5,6, 18,19].

Kiistämättömyyttä käytetään todistamaan jälkeenpäin tapahtunut tapahtuma. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin. Viestin lähettäjä ei pysty jälkeenpäin kiistämään lähettäneensä viestiä. Kiistämättömyys on ehdoton edellytys monien palvelujen ja toimintojen toteuttamiselle tietoverkkojen kautta.

Lähteet

[1] Kinnunen Juha 1999 ’Etälääketieteen terveystaloudelliset vaikutukset.’ Teoksessa Mattila Matti (toim.) ‘Telelääketiede’ Recallmed , Klaukkala.

[2] Adams Carlisle Lloyd Steve 1999: Understanding Public-Key Infrastructure. Macmillan Technical Publishing. Indianapolis, USA.

[3] Nash Andrew, Duane William, Celica Joseph Brink Derec 2001 ‘ PKI- Implementing and Managing E -security.’ Osborne / MCGraw-Hill, California, USA.

[4] Ruotsalainen Pekka (toim.) 2002 ’Ehdotus Sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi -terveydenhuollon PKI- arkkitehtuuri’ Sosiaali- ja terveydenhuollon sähköisen tietoverkkopalvelujen ja -asioinnin kansallinen yhteistoiminnallinen arkkitehtuuri projektin osaraportti 1.

[5] Linden Mikael 2003 ’Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatioissa’ Lisensiaattitutkimus. Tampereen tekninen korkeakoulu.

[6] Kerttula Esa 2000 ’ Tietoverkkojen tietoturva.’ Oy Edita Ab, Helsinki

[7] Järvinen Petteri 2003 ’Salausmenetelmät’ Docendo, Jyväskylä.

[8] Ensio Antero, Ruotsalainen Pekka, 2001’ Selvitys asiakas- ja potilasasiakirjojen sähköisestä säilytyksestä ja kiistämättömyydestä.’ Osaavien keskusten verkoston julkaisuja 10/2001, STAKES. Helsinki.

[9] Jokinen Yrjö 1999 ’Tietoturvallisuus.’ Teoksessa Saranto Kaija & Korpela Mikko (toim.). Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa. WSOY, Helsinki

[10] Kleemola Maija, Tervo-Pellikka Raija 1998 ’Tietosuoja’ Suomen ATK kustannus, Espoo.

[11] Ylipartanen Arto 2001 ’Tietosuoja terveydenhuollossa’ Hakapaino Oy, Helsinki.

[12] Lehtonen Lasse 2001 ’Potilaan yksityisyyden suoja’ Suomalaisen lakimiesyhdistyksen julkaisuja A – sarja N:o 230, Vammalan kirjapaino Oy, Vammala.

[13] Lääkärin etiikka 1999. Suomen lääkäriliitto, Helsinki.

[14] Korhonen Rauno 2003 ’Perusrekisterit ja henkilötietojen suoja’ Acta Universitatis Lapponiensis, Rovaniemi.

[15] Henkilötietolaki 22.4.1999 /523, http//www.finlex.fi.

[16] Tähtinen Heikki 1997 ’ Terveydenhuollon tietoturvan ja tietosuojan toteutuksen hyviä käytäntöjä.’ Suomen kuntaliitto, Helsinki.

[17] Valtionvarainministeriö, 2000 ’Valtionhallinnon tietoturvallisuuskäsitteistö’ Valtionhallinnon tietoturvallisuuden johtoryhmä 1/2000.

[18] Housley Russ, Polk Tim 2001 ’ Planning for PKI ’ Willey Computer Publishing , New York.

[19] Paavilainen Juhani 1998 ’ Tietoturva.’ Suomen Atk-kustannus Oy. Jyväskylä.

[20] Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämiseksi valtionhallinnossa, VM 0024:00/02/99/1998.

[21] Gritzlis Dimitri, Kokolakis, S. 2003 ’ Seurity Policy Development for Healthcare Information Systems Teoksessa Blöbel Bernad, Pharlow Peter ‘Advanced Health Telematics and Telemedicine’ IOS press, Amsterdam.

[22] Spanhi Stephane, Weber Patrick 2002 ‘Secure exchange of medical data: requirements and solutions’ Teoksessa Surjan György (toim.) ‘ Health data in the information society. ‘ Proceedings of MIE2002. IOS press, Amsterdam.

[23] http:// www.cordis.lu

[24] http://www.hhs.gov/ocr/hipaa/

[25] Hallituksen esitys eduskunnalle laeiksi sähköisistä allekirjoituksista ja viestintähallinnosta annetun lain 2 §:n muuttamisesta. 12.11.2002.

[26] Immonen Aapo, Hannula Anu, Klami Päivi, Von Fieandt Noora, Saranto Kaija, Turunen Pekka 2002 ’ Julkisen avaimen menetelmän käyttöönotto terveydenhuollossa teknisten asiantuntijoiden näkökulmasta. PKI- asiantuntijoiden haastattelu’ Teoksessa Saranto Kaija, Häyrinen Kristiina (toim.): SoTeTiTe2003 - Sosiaali- ja terveydenhuollon tietotekniikan ja tiedonhallinnan tutkimuspäivät. Osaavien keskusten verkoston julkaisuja 1/2003.

[27] Immonen Aapo, Mauranen Kari, Saranto Kaija 2003 ‘A study design to measure the outcomes of education in data security issues among the health care professionals’ Teoksessa Baud Robert (toim.) “The new navigators: from professionals to patients, proceedings of MIE2003”, IOS press. Amsterdam.