Ehdotus Sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri

Sosiaali- ja terveydenhuollon sähköisen tietoverkkopalvelujen ja –asioinnin kansallinen yhteistoiminnallinen arkkitehtuuri projektin osaraportti 1

Toimittanut:

Pekka Ruotsalainen

Osaavien keskusten verkoston julkaisuja 4/2002

ISBN 951-33-1358-1

Stakesin monistamo
Helsinki

Sisällys

ESIPUHE

Stakesin tietoteknologian osaamiskeskus (OSKE) edistää ratkaisuja ja toimenpiteitä, joilla lisätään sosiaali- ja terveydenhuollon tietojärjestelmien yhteistoiminnallisuutta. OSKE käynnisti keväällä 2001 *Sosiaali- ja terveydenhuollon sähköisen tietoverkkopalvelujen ja -asioinnin kansallisen yhteistoiminnallisen arkkitehtuurin* määrittelyprojektin. Nyt käsillä oleva raportti on määrittelyprojektin ensimmäinen osaraportti. Myöhemmin julkaistavat dokumentit käsittelevät tietoturvallista arkkitehtuuria sosiaali- ja terveydenhuollon tietojärjestelmien yhteistoiminnallisuuden näkökulmasta, yhteistoiminnallisuutta loppukäyttäjän kannalta, suostumuksen merkitystä ja hallintaa sosiaali- ja terveydenhuollossa sekä digitaalisen arkistoinnin hyviä toimintamalleja. Projekti on saanut rahoitustukea sosiaali- ja terveysministeriöltä.

Sähköisten palvelujen ja asioinnin lisääntyessä on välttämätöntä luoda sekä menettelytavat että tekniset ratkaisut, joiden avulla osapuolten välinen luottamus, luotettava asiointi voidaan toteuttaa sinänsä turvattomassa tietoverkkoympäristössä. Yhteisten toimintamallien ja ratkaisujen synnyttäminen on edellytys toimintayksikköjen ja ammattilaisten väliselle lisääntyvälle yhteistoiminnalle. Asiakkaiden ja potilaiden yksityisyyden suoja ja ammattilaisten oikeusturva edellyttävät luotettavien tunnistamisen ja tiedonsalauksen menetelmien käyttöä asioitaessa tietoverkkoympäristössä. Toimintayksiköiden ja organisaatioiden muuttuessa entistä alueellisimmiksi joudutaan luotettava sähköinen asioinnin infrastruktuuri ulottamaan myös organisaatioiden ja toimintayksiköiden sisälle.

Julkisen avaimen järjestelmään perustuvan arkkitehtuurin (ns. PKI-järjestelmän) palveluilla pystytään takaamaan riittävän luottamuksen syntyminen osapuolten välillä, jotta arkaluontoisia henkilötietoja sisältävä sähköinen asiointi olisi mahdollista toteuttaa sosiaali- ja terveydenhuollossa. PKI-pohjaiset palvelut tarjoavat ratkaisun, joka takaa etteivät tiedot voi joutua ulkopuolisten käsiin, ja että osapuolten tunnistaminen ja todentaminen on tehty kiistämättömästi ja asianmukaisesti. Yhteisesti sovittava PKI-arkkitehtuurimalli luo mahdollisuudet kaikille alueellisille organisaatioille ja potilaille saada tasalaatuiset pelisäännöt. Arkkitehtuuri sopii sekä perinteisille tietoverkkoratkaisuille että mobiiliympäristöön.

Tämä dokumentti sisältää ehdotuksen kansalliseksi sosiaali- ja terveydenhuollon tietoturva-arkkitehtuuriksi. Ehdotus perustuu kaksitasoiseen PKI-arkkitehtuuriin (aluetaso ja kansallinen taso), jossa valtakunnan tason palvelut on pyritty minimoimaan. Tässä raportissa on PKI-arkkitehtuurin soveltamista tarkasteltu erityisesti terveydenhuollon näkökulmasta. Ehdotettu ratkaisu on kuitenkin yleinen ja soveltuu sosiaalihuollolle. Myöhemmissä raporteissa tullaankin keskittymään sosiaalihuollon tietoverkkoasiointiin ja sosiaali- ja terveydenhuollon tietojärjestelmien yhteistoiminnallisuutteen. Ehdotuksesta on pyydetty asiantuntijalausuntoja väestörekisterikeskukselta, yliopistollisilta sairaanhoitopiireiltä ja yhdeltätoista alan yritykseltä.

Projektin johtoryhmän jäseninä ovat toimineet projektipäällikkö Ralf Ekebom sosiaali- ja terveysministeriöstä, tietohallintopäällikkö Simo Pietilä Helsingin ja Uudenmaan sairaanhoitopiiristä, tietoteknologian osaamiskeskuksen päällikkö Pekka Ruotsalainen Stakesista ja osastopäällikkö Björn-Eric Svensson ICL Inviasta. Kristiina Luokomaa ICL Inviasta on toiminut johtoryhmän sihteerinä. Johtoryhmä on osallistunut aktiivisesti tämän raportin suositusten ja johtopäätösten tekemiseen

Raportin toimituksellisen työn ja lopullisen editoinnin on tehnyt Pekka Ruotsalainen. Raportin lukujen 1 - 8 sisällön ovat tuottaneet Ari Hakala, Sirkku Helasterä ja Kristiina Luokomaa ICL Inviasta, kappaleen 7.1.2 (potilaskertomuksen arkistointi) on kirjoittanut Pekka Ruotsalainen Stakesista. Yhteenvedon (luku 9) tekijät ovat Ari Hakala, Sirkku Helasterä, Kristiina Luokomaa ja Pekka Ruotsalainen yhdessä. Raportin ehdotukset on hyväksytty projektin johtoryhmässä.

Helsingissä 9.10.2002

Pekka Ruotsalainen

Tietoteknologian osaamiskeskuksen päällikkö

1. JOHDANTO

Tässä raportissa kuvataan julkisen avaimen järjestelmää (PKI-järjestelmä) yleisesti sekä siihen perustuvia sosiaali- ja terveydenhuollon tarpeisiin soveltuvia arkkitehtuurimalleja. Lopputuloksena on ehdotus kansalliseksi sosiaali- ja terveydenhuollon tietoturvalliseksi PKI-arkkitehtuuriksi. Raportissa selvitetään ja valotetaan julkisen avaimen järjestelmän yleispiirteitä, kuten varmennepolitiikan osatekijöitä. Koska terveydenhuollossa parhaillaan keskustellaan ja suunnitellaan PKI-toteutuksia, on raportin esimerkeissä keskitetty erityisesti terveydenhuoltoon. PKI-järjestelmä samoin kuin esitetty arkkitehtuuriratkaisu eivät ole kuitenkaan yksinomaan terveydenhuoltoon soveltuvia, vaan PKI-arkkitehtuuri on yleinen ratkaisu, joka on käyttökelpoinen myös sosiaalihuollossa.

Raportin alussa on yleinen kuvaus PKI-järjestelmistä ja -menetelmistä. Arkkitehtuurimalleja käsitellään luvusta 7 alkaen.

1.1 Hankkeen tausta

Stakes toimii sosiaali- ja terveysministeriön hallinnonalalla asiantuntijakeskuksena, jonka ydintoimintoja ovat tutkimus, kehittäminen ja tietovarannot. Stakesin strategian tavoitteena on, että Suomi on vuonna 2007 dynaaminen ja monisärmäinen tietoyhteiskunta, jossa Stakes edistää hyvinvointia ja terveyttä, kestävää kehitystä ja tasa-arvoa. Stakes luo uudenlaisia tutkimuksen, kehittämisen ja tietovarantojen yhdistelmiä ja tiedon hyödyntämisen käytäntöjä.

Stakesin tietoteknologian osaamiskeskuksen (OSKE) tavoitteena on osaltaan kehittää ja luoda hyviä käytäntöjä sosiaali- ja terveydenhuollon turvallisille sähköisille palveluille ja edistää alan asiakastietojärjestelmien yhteistoiminnallisuutta.

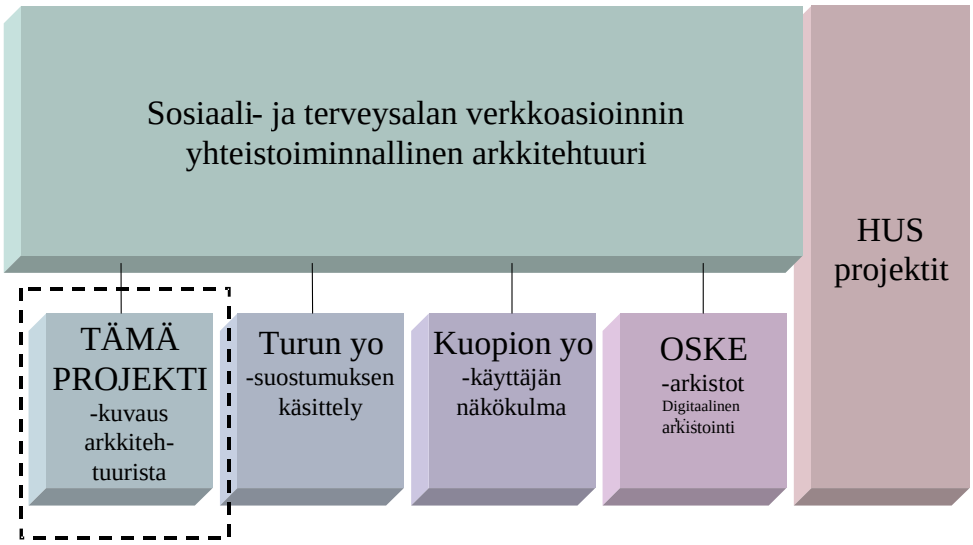
Sosiaali- ja terveydenhuollon tietoteknologian hyödyntämisstrategia (Sosiaali- ja terveysministeriön työryhmämuistioita 1995:27) ja saumaton hoito- ja palveluketjutyöryhmä (Sosiaali- ja terveysministeriön työryhmämuistioita 1998:8) asettivat valtakunnallisiksi tavoitteiksi mm. siirtymisen digitaalisten asiakas- ja potilasasiakirjojen käyttöön, tietoverkkojen käytön, tietosuojan- ja tietoturvan kehittämisen ja tietojärjestelmien yhteistoiminnallisuuden.

Sosiaali- ja terveysministeriön ohjeet potilasasiakirjojen laatimisesta (Sosiaali- ja terveysministeriö (Sosiaali- ja terveysministeriö, Oppaita 2001:3) merkitsevät mm. sitä, että sähköisessäkin (digitaalisessa) muodossa käsiteltäviin potilasasiakirjoihin tulee ammattilaisen allekirjoitus. Lisäksi potilasasiakirjoja on säilytettävä muuttumattomana ja kiistämättömänä kymmeniä vuosia (jopa yli 100 vuotta). Koko arkistointiajan tulee ammattilaisten tarvitsemien potilastietojen olla helposti käytettävissä ajasta ja paikasta riippumatta.

Suomessa kunnat, alueet ja palveluntuottajat priorisoivat omat tietojärjestelmä- ja infrastruktuurihankkeensa. Valtakunnallinen ohjaus on ensisijaisesti informaatio-ohjausta. Tyypillistä on, että eri alueet ja palveluntuottajat etenevät sosiaali- ja terveydenhuollon sähköisen asioinnin käyttöönotossa eri tahtiin. Tämä eriaikaisuus uhkaa synnyttää valtakunnallisesti yhteen sopimattomia alueellisia ja paikallisia ratkaisuja.

Stakesin tietoteknologian osaamiskeskuksen "sosiaali- ja terveydenhuollon sähköisen tietoverkkopalvelun ja asioinnin kansallinen yhteistoiminnallinen arkkitehtuuri" -hanke käynnistettiin synnyttämään malli kansallisesta sosiaali- ja terveydenhuollon yhteistoiminnallisesta tietoturvallisesta sähköisen asioinnin arkkitehtuurista.

Kuva 1.1 esittää hankkeen kokonaisuutta ja sen osaprojekteja. Osahankkeet valottavat lisää terveydenhoitoalan sähköisen asioinnin kenttää. Koska potilaan suostumukseen, käyttönäkökulman pohdintaan ja arkistointiin on kiinnitetty huomiota muissa osaprojekteissa, niihin ei tässä raportissa paneuduta (kuva 1.1).



Kuva 1.1 Käynnissä olevat hankkeet, katkoviivalla erotettu alue kuvaa tämän dokumentin osuutta

1.2 Tavoitteet

Tämän osaprojektin tavoitteeksi asetettiin synnyttää puitemalli PKI-ratkaisulle, jossa käyttäjät tunnistetaan tietojärjestelmien käyttäjiksi toimikorttien avulla ja jolla lainsäädännön edellyttämät potilastietojen suojaustarpeet tiedonsiirrossa tyydytetään sekä mahdollistetaan dokumenttien digitaalinen allekirjoitus ja kiistämättömyys. Tavoitteena oli:

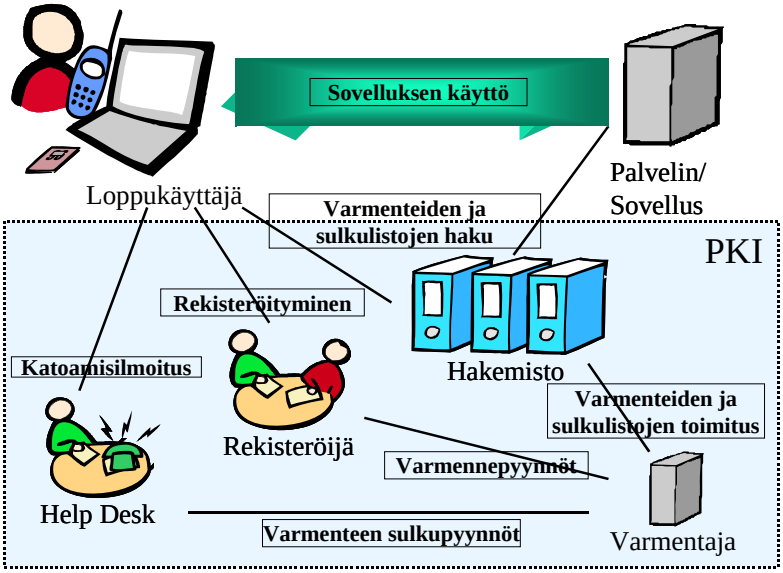
- kuvata "oppikirjamaisesti" PKI-järjestelmää,
- luoda malleja kansalliselle sosiaali- ja terveysalan PKI-arkkitehtuurille,
- hahmotella työnjako PKI-ratkaisun kansallisen ja alueellisen tason tehtäville,
- kuvata perusvaatimukset varmennepolitiikalle,

Koska todentamismenetelmien käyttö edellyttää tietoturvapoliittisia linjauksia siitä, kuka tai ketkä ovat palveluntuottajan kannalta varmentajiksi hyväksyttäviä luotettuja kolmansia osapuolia, valotetaan varmennepolitiikkaa tässä vain varmentamisen yleisten suuntaviivojen osalta.

2. JULKISEN AVAIMEN JÄRJESTELMÄ PKI

2.1 Yleistä PKI:stä

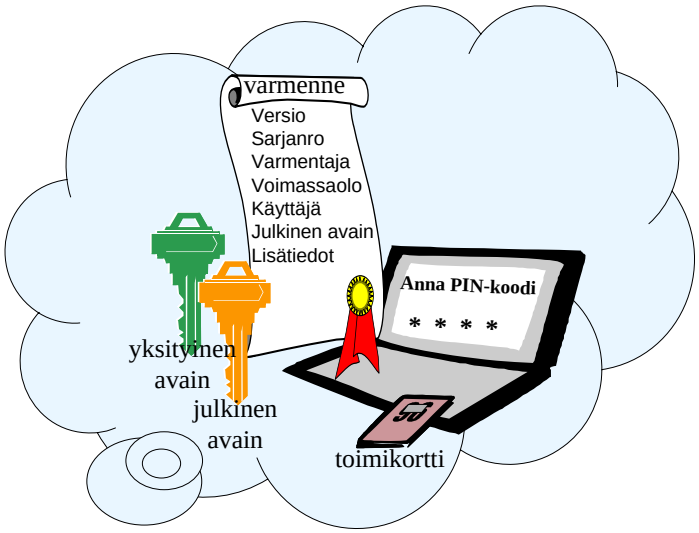
PKI, (Public Key Infrastructure), *julkisen avaimen järjestelmä on yhdistelmä teknologisia ratkaisuja, menettelyjä ja hallinnollisia toimia, joilla mahdollistetaan arkaluonteisen tiedon vaihto turvattomassa ympäristössä.* Se muodostaa alustan (platform), jonka päälle sähköisen asioinnin palveluita ja sovelluksia voidaan rakentaa. Sähköisellä asioinnilla puolestaan ymmärretään yleisesti minkä tahansa palvelun käyttöä tai asioiden hoitamista verkossa eli sähköisiä tietoliikenneyhteyksiä hyödyntäen. Yksittäinen palvelu tai sovellus, esimerkiksi sähköposti, ei yksin ole julkisen avaimen järjestelmä.



Kuva 2.1 PKI-arkkitehtuuri.

Laajasti tarkastellen PKI-arkkitehtuurin elementtejä ovat ensinnäkin pelisäännöt, joihin luottamus osapuolten välillä perustuu, ja käytännöt, kuinka sovelluksia/palveluita hyväksikäytetään. Lisäksi tarvitaan varmenteen myöntämiseen vaadittavat työkalut; hakemisto, johon varmenteet myönnetään ja ylläpidetään, järjestelmä, josta on rajapinta integroitavaan asiointipalveluun ja joka voi tarkistaa asioivien osapuolten varmenteet sekä loppukäyttäjälle työkalut, joilla liittyä palveluun.

PKI on suppeasti ajateltuna tekninen arkkitehtuuri, joka luo ja myöntää varmenteita sekä varastoi ne hakemistoon. PKI-palvelu tai -sovellus on järjestelmä, joka hyväksikäyttää rakennettua infrastruktuuria ja sen luomia varmenteita. PKI-kokonaisratkaisu on järjestelmä, jossa loppukäyttäjä ja palveluntarjoaja kommunikoivat ja asioivat sähköisessä verkossa keskenään, käyttävät hakemistoa varmentamaan ja todentamaan osapuolten aitous ja/tai takaamaan asioinnin luottamuksellisuus osapuolten välillä.



Kuva 2.2 Työkaluja, jotka toteuttavat PKI:n takaaman luotettavuuden

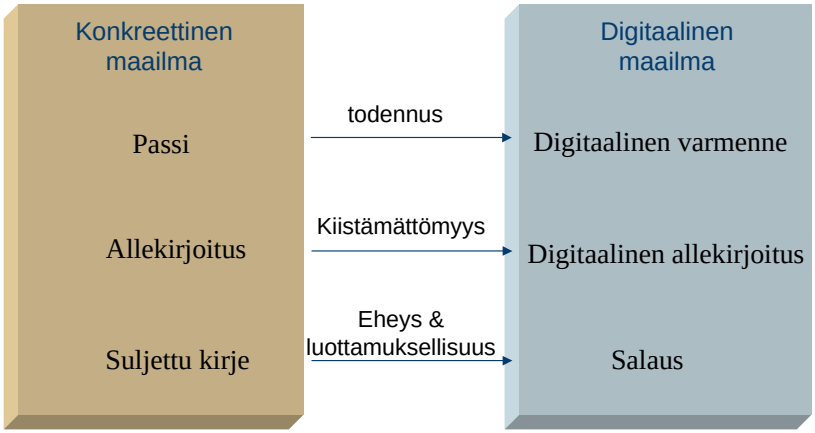
PKI-järjestelmien yksi elementti on digitaaliset "avaimet". PKI-järjestelmissä on käytössä ns. epäsymmetristen avainten järjestelmä. Epäsymmetriset avaimet tarkoittavat, että käytössä on kaksi erilaista avainta: **yksityinen avain** ja **julkinen avain**. Ne yhdessä muodostavat avainparin, jotka liittyvät toisiinsa matemaattisen kaavan kautta. Käytetty kaava on sellainen, että yksityisellä avaimella salattu tieto voidaan tulkita vain ja ainoastaan julkisella avaimella ja päinvastoin. Osapuolten hallussa olevia yksityisiä avaimia tulee säilyttää turvallisessa paikassa, niin että ulkopuolisilla ei ole mahdollisuutta päästä käsiksi niihin. Yleisesti turvallisimpana avainten säilytyspaikkana pidetään omaa erillistä laitteistomoduulia, kuten **toimikorttia.**

Julkinen avain on talletettu **varmenteeseen**. Varmenne on puolestaan on varastoitu **hakemistoon**. Varmenne itse on allekirjoitus julkiselle avaimelle ja siihen liittyvälle tunnistetiedolle. **Varmentaja (CA, Cerification Authority)** antaa tämän allekirjoituksen. Tunnistetieto on sen henkilön tai toimijan yksilöivää tietoa, kenen hallussa on yksityinen avain. Varmenne sitoo siis julkisen avaimen ja identiteetin yhteen. Varmenneviranomaisen on oltava kaikille osapuolille luotettava taho, sellainen johon osapuolet uskovat – siksi sitä usein kutsutaan luotetuksi kolmanneksi luotetuksi osapuoleksi.

Jotta varmenteet tulevat luoduiksi hyväksyttyjen pelisääntöjen mukaisesti, niitä ohjaa **varmennepolitiikka (CP, Certificate Policy)**. Myös **varmennekäytännötä (CPS, Certification Practice Statement) on** sovittava, ennen kuin palveluita voidaan liittää varmenneympäristöön.

2.2 PKI:n tarjoamat hyödyt

PKI:tä käytetään tietoturvapalveluna, koska se on osoittautunut tehokkaaksi menetelmäksi ylläpitää luottamus ja kiistämättömyys sähköisessä asioinnissa.



Kuva 2.3 PKI- järjestelmän palvelujen avulla voidaan luoda nykyisen ei sähköisen maailman korkeimmatkin vaatimukset täyttävä luottamuksen taso

PKI-infrastruktuuri tarjoaa seuraavat neljä luotettavaa ja tehokasta turvallista palvelua:

1. Vahva tunnistaminen. Todennetaan varmasti asioiva osapuoli (esim. henkilö, laite tai ohjelmisto)

2. Tiedon eheys. Osoitetaan, että osapuolten välisessä viestissä mitään ei ole muutettu.

3. Luottamuksellisuus. Taataan, että kukaan muu kuin vastaanottaja ei voi saada selville viestin sisältöä.

4. Kiistämättömyys / Digitaalinen allekirjoitus. Varmennetaan, että lähetetty viesti on lähettäjän lähettämä ja muuttumaton.

2.3 PKI-arkkitehtuurin osa-alueet

Suppeasti määriteltynä PKI-infrastruktuurissa mukana olevat osapuolet ovat varmentaja, rekisteröijä ja hakemisto. Niiden avulla luodaan varmenneympäristö, jota palvelut ja sovellukset voivat käyttää hyväkseen luodessaan palveluita loppukäyttäjille. Laajemmin määriteltynä loppukäyttäjän toimikortti, kortin valmistaja valmistusprosesseineen, loppukäyttäjäohjelmisto, kortinlukija, sovelluspalvelimen varmentaja ja salakirjoitusohjelmistot ovat osa kokonaisuutta.

2.3.1 Varmenne

Julkista avainta käytettäessä on ehdottoman tärkeää tietää, kenelle avain kuuluu. Tämä validiteetin tarkistus voidaan tehdä luottaen kolmanteen osapuoleen (Trusted Third Party, TTP), joka vakuuttaa tarkistaneensa, kenelle avain kuuluu.

Tämä ”vakuutus” toteutetaan sähköisellä allekirjoituksella, jossa varmentaja allekirjoittaa digitaalisen dokumentin eli varmenteen omalla yksityisellä avaimellaan, joka sitoo toisiinsa julkisen

avaimen sekä avaimen haltijan, sovelluksen tai palvelun. Julkista avainta käyttävä osapuoli (relying party) voi nyt halutessaan tarkistaa varmenteen käyttäen varmentajan julkista avainta.

Yhdellä loppukäyttäjällä voi olla useita varmenteita ja yhdellä yksityisellä avaimella voi olla useita käyttötarkoituksia. Edelleen yhtä käyttötarkoitusta varten voi olla useita varmenteita.

2.3.2 Sulkulista

Sulkulistalla julkaistaan vanhentuneet, perutut ja kuoletetut tai määräaikaisesti käytöstä poistetut varmenteet. Sulkulistapalvelu on osa rekisteröijän tehtävistä. Rekisterin pitäjän on kyettävä rajaamaan sulkulistapalvelusta vastaavien henkilöiden käyttöoikeudet vain varmenteen perumiseen. Varmennepolitiikassa voidaan määritellä, kuinka korkea palvelutaso tarjotaan – eli kuinka luotettava ja turvallinen varmenne on. Sulkulistan julkaisutiheys ja sulkulistapalvelun tavoitettavuus määritellään laadittavissa varmennepolitiikassa tai varmennekäytäntölausumassa.

Sulkulista julkaistaan varmenteiden tavoin julkisessa hakemistossa. Sulkulistan palvelujen on oltava katkotonta ja ympärivuorokautista. Nämä vaatimukset asettavat käytetyille hakemistoratkaisuille, CA-järjestelmälle sekä verkkoratkaisulle ankarat vaatimukset luotettavuuden, käytettävyyden ja hallinnoinnin suhteen.

2.3.3 Toimikortti

Tässä yhteydessä toimikortilla tarkoitetaan kontaktillista ISO-7816 standardien mukaista toimikorttia. Se ei sisällä pelkästään muistia tiedon (kuten varmenteen) talletusta varten, vaan kortti kykenee prosessorin ja käyttöjärjestelmä avulla mm. tekemään digitaalisen allekirjoituksen vaatimia toimenpiteitä. Toimikortin keskeisiä ominaisuuksia ovat sen turvallisuus (mm. yksityisiä avaimia ei kyetä lukemaan kortilta) ja helppokäyttöinen käyttäjille tuttu käyttöliittymä.

Kortin hallinnointitavan perusteella kortit voidaan jakaa yleisiin viranomaisten jakamiin sähköisiin asiointikortteihin, kuten HST-kortti ja Kelan sosiaaliturvakortti, tai organisaatiokortteihin, joiden ulkoasun ja sisällön työnantaja määrittelee ja joka annetaan työntekijälle hänen työtehtäviensä suorittamista varten.

2.3.4 Kortin valmistaja

Kortin valmistaja vastaa kortin fyysisestä tuottamisesta, sovellustietojen alustamisesta kortille sekä henkilön yksilöintitietojen painamisesta kortin pinnalle ja/tai tallettamisesta kortin sisälle. Nämä yksilöintitehtävät voidaan toteuttaa myös rekisteröijän toimesta, jolloin kortin valmistajan rooli on pieni.

Tavallisesti myös avainten (mm. allekirjoitus ja salausavaimet) sekä PIN- ja PUK-koodien generointi kuuluu kortin valmistajan vastuulle. Kortin valmistaja voi huolehtia salausavaimen tallettamisesta kortille jakelijaorganisaation puolesta ns. riippumattomana osapuolena. Allekirjoitusavaimen talletus kortille tule olla kertaluontoinen tapahtuma.

Visuaalisessa personoinnissa kortille tulostetaan kortinhaltijan kuva, nimi, kortin sarjanumero sekä mahdolliset muut tarvittavat tiedot. Visuaalisen personoinnin tarkoitus on sitoa kortti tiiviisti käyttäjän identiteettiin. On myös odotettavissa, että kuvallisesta kortista huolehditaan tarkemmin kuin jos kortti olisi vain valkea muovipala ilman näkyvää sidosta haltijaansa. Kortin loogisessa personoinnissa kortilla oleva julkinen avain liitetään rekisteröinnissä saatuihin käyttäjätietoihin ja näin muodostettu varmennepyyntö lähetetään varmentajalle. Palautteena saatu varmenne talletetaan usein myös kortille.

2.3.5 Rekisteröijä (RA)

Rekisteröijän (Registration Authority) tehtävänä on kerätä tarvittavat käyttäjätiedot ja varmistua käyttäjän henkilöllisyydestä tunnistamalla käyttäjä esimerkiksi virallisesta henkilödokumentista. Rekisteröijä voi myös tehdä varmenteen peruutuspyyntöjä tai tuottaa toimikortteja.

Vaikka nämä tehtävät ovat erillään varmenteen myöntämisprosessista, voi rekisteröinti olla osa varmentajan toimintaa. Hajauttamalla toimintoja ja vastuita usealle organisaatiolle, saadaan kokonaisuudesta vaikeasti petettävä.

Sovitun ohjeistuksen mukaan (varmennepolitiikan ja –käytännön perusteella) rekisteröidään käyttäjä. Alimmalla turvatasolla varmistetaan esimerkiksi, ettei samaa nimen ja sähköpostiosoitteen yhdistelmää ole useita varmennepalvelun tarjoajan rekisterissä. Korkeammalla turvatasolla varmistetaan lisäksi käyttäjän tiedot jostain luotettavasta rekisteristä. Ylimmällä turvatasolla tarkistetaan tiedot luotettavasta rekisteristä ja lisäksi tunnistetaan käyttäjä henkilökohtaisesti ja todennetaan hänen henkilöllisyytensä asiakirjoista.

2.3.6 Varmentaja (Certification Authority, CA)

Varmentajan keskeisenä tehtävänä on varmistaa, että käyttäjä, jolle varmenne myönnetään, on tunnistettu sovitulla tavalla ja taata, että käyttäjä on ainutkertainen (kyseisessä kontekstissa). Varmentaja huolehtii myönnettyjen varmenteiden hallinnasta sekä varmistaa, että yksityisten ja julkisten avainten käsittely on ollut turvallista niiden luomisen ja käyttäjälle toimittamisen välisenä ajanjaksona.

Varmentajan tarjoamia peruspalveluita ovat:

- avainten generointi,
- käyttäjän rekisteröinti,
- julkisen avaimen varmentaminen,
- julkisten avainten ja varmenteiden julkaiseminen
- varmenteiden sulkulistojen päivitys ja julkaiseminen.

Julkisen avaimen varmentaminen tapahtuu siten, että varmentaja (CA) allekirjoittaa omalla salaisella avaimellaan tietokokonaisuuden, joka sisältää halutun määrän tietoa käyttäjästä (esimerkiksi nimen, sähköpostiosoitteen tms. tunnistetiedon) sekä käyttäjän julkisen avaimen. Näin muodostuva varmenne julkaistaan varmentajan varmennehakemistossa. Hakemiston yhteydessä ylläpidetään myös sulkulistaa, jolle merkitään käytöstä poistetut eli mitätöidyt varmenteet.

Varmentajan lisäpalveluita voivat laajemmin ja yksityiskohtaisemmin olla mm.:

- aikaleimapalvelu
- elektronisten dokumenttien notariaattipalvelut
- kiistojen selvittäminen
- käytöstä poistettujen avainten arkistointi
- pääsynvalvontaa tukevat palvelut
- salakirjoitusohjelmistojen levittäminen
- avainten palautuspalvelut (key recovery)

2.3.7 Hakemistot

Hakemisto on paikka tallettaa ja hakea tietoa. Hakemistossa säilytetään tyypillisesti tietoja, joita haetaan ja luetaan paljon, mutta päivitetään suhteellisen vähän. PKI-järjestelmä on tästä hyvä esimerkki: varmenne myönnetään kerran ja julkisen avaimen sisältämä tieto talletetaan hakemistoon kerran, mutta sitä käytetään sen jälkeen jopa vuosia.

PKI-järjestelmässä hakemisto on järjestetty hierarkiseen puurakenteeseen perustuen. Hierarkia voi perustua mm. maahan, organisaatioon tai henkilöön.

Varmennehakemisto

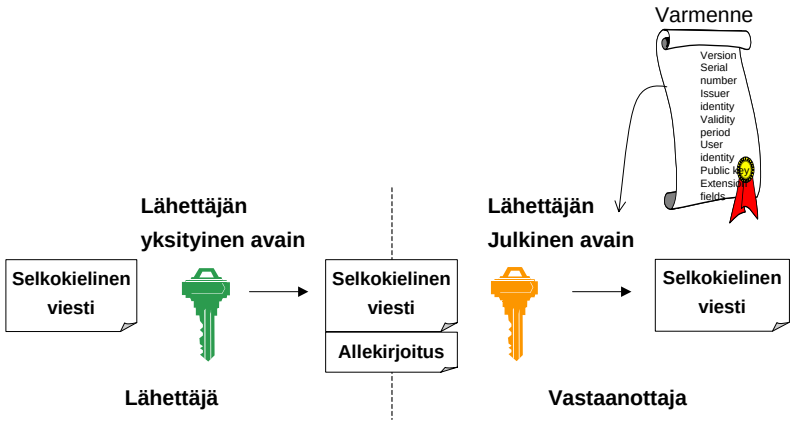
Varmentaja käyttää varmennehakemistoa varmenteiden ja sulkulistan julkaisuun. Hakemiston käyttörajapintana on yleensä ns. LDAP-pinta. Mikäli hakemiston tietoja jaetaan edelleen toisiin hakemistoihin, on suositeltavaa, että hakemisto tukee X.500-hallintaprotokollia.

2.4 PKI:tä hyödyntäviä sovelluksia ja palveluita

Julkisen avaimen järjestelmää hyödyntäviä palveluita on suuri joukko. Niitä ovat mm.:

- PKI-pohjainen sähköposti
- PKI-pohjainen tunnistautuminen verkossa
- sähköinen allekirjoitus
- aikaleimapalvelu
- elektronisten dokumenttien notariaattipalvelut
- pääsynvalvontaa tukevat palvelut.

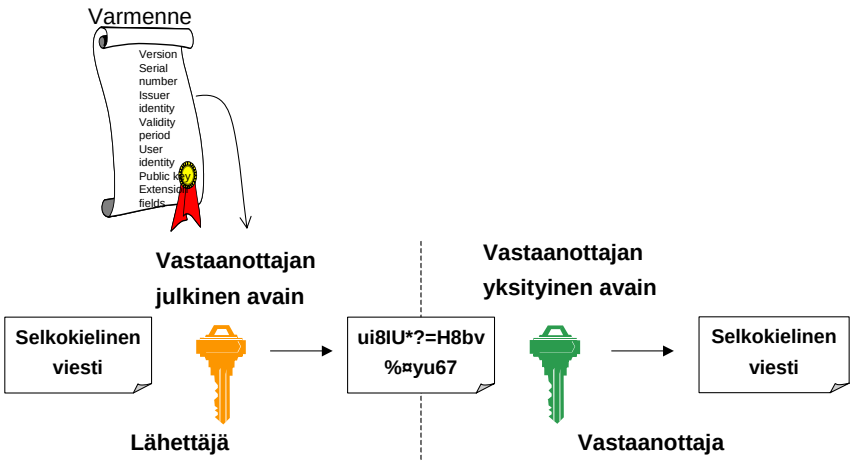
2.5 Yksityisen ja julkisen avaimen käyttö PKI-järjestelmässä, esimerkkejä



Kuva 2.4 Esimerkki allekirjoituksesta PKI-avaimilla

Esimerkki 1 Allekirjoitus ja alkuperäisyys

- Viestistä lasketaan tiiviste, jonka viestin lähettäjä allekirjoittaa omalla yksityisellä avaimellaan.
- Allekirjoitus liitetään lähetettävään viestiin ja sanoma lähetetään.
- Vastaanottaja laskee myös samalla periaatteella vastaanottamastaan viestistä tiivisteen, tarkistaa allekirjoituksen lähettäjän julkisella avaimella (jonka hän saa hakemistossa olevasta varmenteesta) ja lopuksi vertaa lähettäjän allekirjoittaman tiivisteen arvoa itse laskemaansa.
- Jos tiivisteet ovat saman, viesti on alkuperäinen.



Kuva 2.5 Esimerkki salauksesta PKI-avaimilla

Esimerkki 2 Viestin salaaminen:

- Lähettäjä salaa viestin vastaanottajan julkisella avaimella.
- Vain vastaanottaja pystyy avaamaan viestin omalla yksityisellä avaimellaan.

Käytännössä tehokkuussyistä pitkien dokumenttien salaukseen käytetään usein ns. symmetrisiä avaimia. Käytetty symmetrinen avain voidaan edelleen salata PKI-järjestelmän avaimella ennen kuin se viestitetään vastaanottajalle.

Usein viestit sekä allekirjoitetaan että salataan. Salaukseen liittyväksi ongelmaksi voi muodostua se, että jos vastaanottaja rikkoo tai hävittää esimerkiksi. älykorttinsa, jossa yksityinen avain on talletettuna, ei kukaan voi enää avata viestiä - ellei salaukseen käytettävistä avaimista pidetä varmuuskopioita.

3. SÄÄDÖKSET JA STANDARDIT

3.1 Lainsäädäntötilanne

Useat lait, asetukset sekä määräykset ja ohjeet sisältävät etenkin viranomaisia koskevia tietoturvallisuusvelvoitteita, jotka on otettava lähtökohdiksi myös PKI-järjestelmien tietoturvallisuudelle. Suomi on jo OECD:n jäsenmaana sitoutunut noudattamaan OECD:n hyväksymiä tiedonsiirron salauspolitiikan yleisohjeita (OECD:n neuvoston suositus tiedonsiirron salauspolitiikan yleisohjeiksi, 27. maaliskuuta 1997). Siinä todetaan mm.: ”lainsäädännöllä luodaan turvallisiin käyttäjän tunnistamiseen tarvittaviin varmennepalveluihin sekä salauspalvelujen tarjoamiseen sovellettavat toimilupa- tai muut valtuutusjärjestelmät, joiden tulee olla yksinkertaisia ja vapaaehtoisia. Käyttäjille tiedotetaan tiedon salauksessa käytettävän salaisen avaimen katoamiseen liittyvistä vaaroista ja heitä kannustetaan turvallisten avaintenhallintajärjestelmien ja muiden varmennepalvelujen käyttöön. Salauksessa käytettävien yksityisten avainten tallettamista viranomaiskäyttöä varten ei säädetä pakolliseksi. Sähköisen allekirjoituksen tuottamiseen tarvittavista yksityisistä avaimista ei säilytetä kopioita.”

Esimerkkejä tietoturvallisuusvelvoitteita sisältävistä säädöksistä ovat:

- Laki sähköisestä asioinnista hallinnosta (1318/1999)
- Hallituksen esitys eduskunnalle laiksi sähköisistä allekirjoituksista ja siihen liittyvästä lainsäädännöstä 26.10.2001
- Henkilötietolaki (523/1999)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Arkistolaki (831/1994)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta (811/2000 – ”Lex Makropilotti”)

Suomen lainsäädäntö hyväksyy sinänsä digitaalisen allekirjoituksen, koska se ei ota kantaa siihen, millä tekniikalla allekirjoitus on tehty. EU-direktiivi sähköisistä allekirjoituksista kuitenkin velvoittaa Euroopan unionin jäsenmaat ottamaan kansallisissa laeissa eksplisiittisesti kantaa sähköiseen allekirjoitukseen, mistä syystä Suomen hallitus on tehnyt lakiesityksen, jolla täytetään direktiivin muodolliset vaatimukset.

Lisäksi on olemassa lukuisia muita viranomaisia koskevia tietoturvallisuusvelvoitteita sisältäviä säädöksiä, kuten esimerkiksi arkistolaki (831/1994), asetus valtionhallinnon tietohallinnosta (155/1988 ja muutos 1401/1992), asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999), laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999), sekä lain nojalla annettu asetus (723/1999), valtion virkamieslaki (750/1994), valtioneuvoston ohjesääntö (1522/1995), valtioneuvoston periaatepäätös valtion tietohallinnon kehittämisestä (2.3.2000), valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (11.11.1999), väestötietolain muutos (527/1999) jne.

3.2 Standardointitilanne

PKI-alueen standardointi kattaa laajan alueen alkaen laiteteknisistä standardeista PKI-sovellusstandardeihin ja -suosituksiin sekä viranomaismääräyksiin ja suosituksiin ja lainsäädäntöön asti. Yleisesti voidaan todeta, että PKI-tekniikan käyttöönottoa suunnittelevan organisaation näkökulmasta olennaisia ovat viranomaisten lait ja asetukset sekä erilaiset yleiset tai toimialakohtaiset sovellusstandardit.

ICTSB (The Information and Communications Technologies Standards Board) on kolmen eurooppalaisen standardointiorganisaation CEN, CENELEC ja ETSI muodostama elin, jonka teh-

tävänä on koordinoida ajankohtaisiksi ja tärkeiksi katsottuja standardointihankkeita. Konkreettisia, sähköisiä allekirjoituksia koskevaan direktiiviin liittyviä, standardointitarpeita selvittämään perustettiin projekti EESSI (European Electronic Signature Standardization Initiative). Ensimmäisenä työnään EESSIn kokoama asiantuntijaryhmä laati raportin, jossa toisaalta analysoidaan ja kommentoidaan direktiivin (tuolloin vielä valmisteilla olleen luonnoksen) sisältöä ja toisaalta esitetään konkreettisia suosituksia jatkotyön organisoinnista. Tämän jälkeen EESSI on keskittynyt määrittelemään tuotteiden ja järjestelmien yhteentoimivuuteen liittyviä suosituksia.

Laatuvarmenteiden luomiseksi EU:ssa on laadittu direktiivi sähköisistä allekirjoituksista. Sen ohella tärkeimmät laatuvarmenteen pohjana olevat kansainväliset standardit ja suositukset ovat standardit toimikortille (ISO/IEC-7816-X) ja sen sisällölle (PKCS#15), varmenteesta ja sulkulistasta (RFC 2459) ja laatuvarmenteesta (IETF_PKIX QC).

Matkapuhelimiin perustuva viestinnän WAP Forum on pitkällä langattoman PKI:n standardisointityössä. Keskeisimpiä näistä ovat:

- Wireless Application Protocol – Wireless Transport Layer Security Specification (WTLS)
- Wireless Application Protocol – Public Key Infrastructure (WPKI)
- Wireless Application Protocol – Identity Module Specification (WAP WIM)
- Wireless Application Protocol – WML Script Crypto API

3.3 EU-direktiivi sähköisistä allekirjoituksista

EU on direktiivissään joulukuulta 1999 asettanut puitteet jäsenmaidensa kansallisille lainsäädännöille sähköisen allekirjoituksen luomisesta. Tavoite on tukea tavaroiden ja palveluiden vapaata liikkuvuutta EU:n sisämarkkinoilla ja yhtenäistää sähköisen allekirjoituksen pelisäännöt ja lainmukaiseksi ja oikeustoimikelpoiseksi tunnustaminen. Lisäksi esitetyn lainsäädännön tavoitteena on edistää kuluttajien ja muiden käyttäjien luottamusta sähköiseen asiointiin ja verkkoliiketoimintaan. Direktiivi pitää lisäksi hyväksyttää kansalliseen lainsäädäntöön, jotta se saa lainvoiman. Sen ei kuitenkaan pidä asettaa sähköisen liiketoiminnan kehittymiselle tarpeettomia esteitä.

Direktiivi määrittelee sähköisen allekirjoituksen ja laatuvarmenteen vaatimukset, muu jää edelleen vapaaksi elinkeinoksi. Varmentamista voidaan harjoittaa liiketoimintana, ja varmentajan on tehtävä ilmoitus: tärkeitä asioita ovat varmentaja, voimassaolo-, ja käyttörajoitukset sekä, miten varmistetaan turvallisuus ja millainen henkilökunta vaaditaan hoitamaan tehtävää.

Sähköinen allekirjoitus viranomaistoiminnassa on direktiivillä tavoitellaan sähköisessä asioinnissa henkilöllisyyden vahvaa tunnistamista ja viestien muuttumattomuutta.

Sähköiset allekirjoitukset perustuvat salauskirjoitustekniikkaan eli kryptografiaan. Kaikissa salakirjoitusmenetelmissä keskenään asioivilla osapuolilla on yleensä ainakin yksi salainen avain, jonka avulla tietoja koodataan ja tulkitaan ja jonka perusteella osapuolet voivat vakuuttua toistensa identiteetistä. Jos avaimet ovat molempien osapuolten hallussa, kyseessä on symmetrinen järjestelmä. Jos ne ovat vain toisen osapuolen tiedossa, kyseessä on asymmetrinen järjestelmä, kuten PKI.

Direktiivissä otetaan kantaa allekirjoitukseen, siinä käytettyihin varmenteisiin, allekirjoituksen tarkistamiseen, varmenteiden tuottamiseen ja käyttöön liittyvien palvelujen valvontaan ja mahdollisiin lupakäytäntöihin. Varmenteiden tuottamiseen ja käyttöön liittyvien palvelujen tuottajien - varmentajien - suhteen direktiivi ottaa liberaalin asenteen. Se kieltää palvelujen tuottamisen asettamisen luvanvaraiseksi, mutta sen sijaan korostaa palvelujen ja tuotteiden vapaaehtoista sertifiointia ja sitä kautta toteutuvaa valvontaa.

Kannattaa selvyyden vuoksi huomioida, että EU-direktiivissä puhutaan sähköisestä allekirjoituksesta, jonka yksi muoto digitaalinen allekirjoitus on. Digitaalinen allekirjoitus vastaa "kehittynyttä sähköistä allekirjoitusta", jolla on edelleen erityisen jalostunut alaluokka "laatuallekirjoi-

tus", jollaisen aikaansaaminen edellyttää laatuvarmenteiden ja turvalliseksi varmennettujen tuottamisvälineiden käyttöä.

3.4 Terveydenhuollon näkökulma

Sosiaali- ja terveydenhuollon toimialalla käsitellään lähes aina tietoja, jotka ovat joko henkilön yksityisyyden tai jonkin muun syyn vuoksi luottamuksellisia ja salassa pidettäviä. Potilasasiakirjahallinnossa, kun dokumentit viedään sähköiseen muotoon, tarvitaan sähköisiä allekirjoituksia; sanomien ja aineistojen suojaamisessa on käytettävä salaamista ja turvallisia tiedonvälitysmenetelmiä (esim. turvallinen sähköposti). Asiakirjojen on oltava kiistämättömiä, ja tämän takaavat sähköinen allekirjoitus ja esimerkiksi varmennetut aikaleimat. PKI-tekniikalla voidaan nykyisin toteuttaa tarvittava toiminnallisuus.

Terveydenhuollon sähköisen asioinnin osalta PKI-arkkitehtuuria määriteltäessä tulee huomioida ISO:n tekniset vaatimusmäärittelyt ISO/TC 215 N188 ”Health Informatics – Public Key Infrastructure; Part 1: Framework and Overview”; N189 ”Part 2: Certificate Profile”; N190 ”Part 3: Policy Management of Certificate Authority”.

Jos terveydenhuollon toimintayksikkö toimii varmentajana, on sen laatuvarmenteita luodakseen noudatettava EU:n direktiivissä osoittamia vaatimuksia. Varmentajan on tehtävä ilmoitus toiminnastaan Viestintävirastolle. Jotta toimintayksikön varmenteet voidaan hyväksyä laatuvarmenteiksi, on ne auditoitava. Viestintävirasto tulee ylläpitämään listaa tarkastuslaitoksista. Se myös ylläpitää hyväksyttyjen varmentajien listaa.

4. SÄHKÖISET TUNNISTUSTEKNIIKAT

Tietoverkossa asioitaessa on mahdollista eri menetelmin tunnistaa toinen osapuoli. Se voidaan tehdä ns. heikkojen tai vahvojen tunnistusmenetelmien avulla, riippuen osapuolien haluamasta turvatasosta ja luotettavuudesta. Järjestelmän vahvuuden tai heikkouden määrittelevät osapuolet kulloistenkin turvatarpeensa mukaisesti. Yleisesti voidaan sanoa, että kryptografisesti vahvat järjestelmät ovat vahvoja tunnistusmenetelmiä.

4.1 Yleistä tunnistamisesta ja todentamisesta

Termejä tunnistaminen ja todentaminen käytetään yleisesti jokseenkin vapaasti ristiin, mutta lienee helpompaa mieltää niiden ero, jos ajatellaan, että:

- Käyttäjä **tunnistetaan**, käyttäjätunnuksen, pankkitilin numeron tai vaikka henkilötunnuksen avulla.
- Käyttäjä **todennetaan** tunnistetietoon liittyvän salasanan, kertakäyttösalasanan tai PKI:n mukaisen avainparin avulla.

Tunnistamisessa yksilöidään identiteetti, todentamisessa vakuuttaudutaan identiteetin oikeellisuudesta. Tällaisena vakuutuksena pidetään jotain tunnistusasiakirjaa (esimerkiksi passi). Kun asioidaan kasvokkain, voidaan tunnistaa henkilö ja todentaa se hänen esittämästään tunnistusasiakirjasta. Todentaminen on luotettava, jos voidaan luottaa todentamisen välineen myöntäjään, silloin voidaan uskoa tunnistusasiakirjan autenttisuuteen.

Kun siirrytään sähköiseen asiointiin, on mahdollista edelleen tunnistaa ja todentaa käyttäjä – tai hänen tunnuksensa – mutta tällöin sähköisesti.

Osapuolen (käyttäjän, palvelun tai palvelimen) vahva todentaminen on kaikkiin PKI-sovelluksiin liittyvä perustoiminto. Vahvassa todentamisessa käytettävä tekniikka on myös sähköisten allekirjoitusten keskeinen perusta.

Tunnistaminen/todentaminen voi tapahtua monella tietojärjestelmän eri tasolla siten, että se voi avata pääsyn joko verkkoon, palvelimeen, palveluun tai sovellukseen/tietoon. Käyttäjän tunnistaminen edellyttää käyttäjän rekisteröitymistä palveluun tai olemassa olevaa asiakassuhdetta muihin palveluntarjoajan palveluihin. Käyttäjä voidaan hyväksyä tunnetuksi myös jonkun kolmannen osapuolen tunnisteen perusteella.

Tunnistaminen itsessään perustuu käyttäjäidentiteettiin. Se voidaan ilmoittaa esim. käyttäjätunnuksen muodossa tai saadaan selville muulla tavalla (esim. käyttäjän päätelaitteelle tallennetun kuitin (engl. *Cookie)* avulla).

Yksisuuntaisuus tunnistamisessa tarkoittaa sitä, että sähköisen asioinnin osapuolet voivat tunnistautua toisilleen yksisuuntaisesti, jolloin vain toisen identiteetistä tarvitaan varmuus. Kaksisuuntaisuus tarkoittaa sitä, että molemmat osapuolet tunnistautuvat toisilleen ja varmistavat, todentavat toinen toisensa.

Luotettava todentaminen perustuu siihen, että yhteyden kummassakin päässä käytetään tunnettujen varmentajien myöntämiä varmenteita, joiden allekirjoittaja ja sulkulistat tarkistetaan ja joiden salaiset avaimet ainakin käyttäjän osalta ovat toimikortilla. Todentamisessa voidaan käyttää standarditekniikoita, joita ovat mm. IPSec, SSL ja haastevaste-menetelmät.

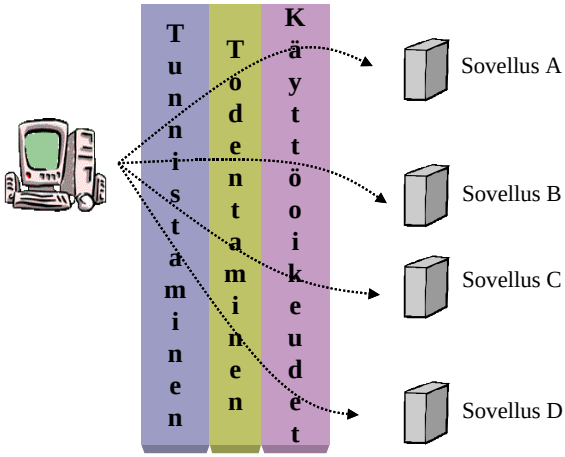
Tunnistettu käyttäjäidentiteetti todennetaan käyttäen jotain todentamismenetelmää. Sellaisia ovat mm. kiinteä salasana, vaihtuva salasana, kertakäyttöinen salasana, haastelukulaskin (ns. SecurID-laskuri), PKI-varmenne, biometrinen todentaminen, televerkon kautta tehtävä tunnistus, luotetun kolmannen osapuolen varmennus.

Organisaation jäsenenä yksilö voidaan tunnistaa ja/tai todentaa henkilötunnistamisen sijasta - tai sen lisäksi - organisaation tai roolin perusteella. Organisaatiokäyttäjien ja heidän roolinsa toden-

tamisen menetelmät eivät vielä ole samalla tavalla vakiintuneet kuin yksityishenkilöiden todentamisessa.

Silloin kun todentamisessa tarvitaan erilaisia apulaitteita, ”laiterekvisiittaa”, sekä ulkoista varmentajaa, paranee yleisesti ottaen todentamisen luotettavuus mutta samalla järjestelmät mutkistuvat ja kustannukset nousevat.

Tunnistamista ja todentamista hyväksikäytetään määriteltäessä käyttöoikeuksia eri sovelluksiin ja järjestelmiin. Pääsynvalvonnan tukena tarvitaan käyttäjähakemisto tai –tietokanta, jonka on sisällettävä tiedot palvelujen käyttöön oikeutetuista käyttäjistä.



Kuva 4.1 Asioitaessa verkossa käyttäjä tarvittaessa tunnistetaan, todennetaan ja hän saa pääsynvalvonnassa identiteetilleen ja roolilleen määritellyt käyttöoikeudet.

Pääsynvalvonnassa käytetään menettelyinä tunnistamista, todentamista ja käyttäjäoikeuksia. Kun tieto on luottamuksellista tai sitä halutaan jakaa vain valikoidulle käyttäjäryhmälle, silloin otetaan käyttöön pääsynvalvontaa. Pääsynvalvontaa ei tarvita, jos tarjolla on anonyymipalveluita, ts. sellaisia palveluita, joiden sisältämistä tiedoista ei voida tunnistaa tai yksilöidä henkilöä.

4.2 Tunnistautuminen ja todentamisen menetelmiä

Tässä kuvataan lyhyesti sähköisen asioinnin menetelmiä tunnistautua tai tunnistautua ja todentautua verkossa. Näitä kahta sekä pääsynvalvontaa tarvitaan, kun halutaan rajoittaa pääsyä sähköisessä verkossa olevaan tietoon. Menetelmän valinta riippuu siitä, millainen turvataso järjestelmään halutaan. Lisäksi tulevat kustannuskysymykset ja käyttäjänäkökulma. Jos ei ole aivan pakko, monimutkaisia ja hankalia järjestelmiä ei haluta käyttää.

Todentaakseen henkilöllisyytensä ja oikeutensa käyttäjän on todistettava identiteettinsä käyttäen jotain luotettavaa ja varmaa todentamisen menetelmää voidakseen vakuuttaa, että hän on se kuka väittää olevansa. Usein käytetään kolmatta osapuolta, joka takaa tunnistustiedon oikeellisuuden. Lisäksi tavallista on käyttää haaste-vaste-menettelyä. Tunnistava osapuoli lähettää tunnistettavalle haasteen, johon tämän on osattava reagoida ja vastata oikealla yhdessä sovitulla tavalla. Tunnistava osapuoli tarkistaa tämän vastauksen.

Aina kun tallennetaan todentamisen välineenä käytettyä tietoa, se on tallennettava turvallisesti ja varmasti. Esimerkiksi salasanalistoja joudutaan usein tallentamaan palvelimille. Tällöin on huolehdittava, että ne eivät joudu ulkopuolisten käsiin. Turvallisuutta voidaan lisätä yhdistämällä useita tunnistusmenetelmiä.

4.2.1 Yleisiä menetelmiä

Salasana/käyttäjätunnus

Käyttäjätunnuksen ja salasanan käyttö on muodostunut sähköisen verkon perusmenetelmäksi. Käyttäjällä on yksilöllinen käyttäjätunnus. Salasanaa käytetään todentamiseen; sen tarkoitus on ilmaista, että sen ilmoittaja on oikea haltija. Suurin ongelma tällaisessa järjestelmässä on, että tunnistetiedot kulkevat verkossa selväkielisinä.

Turvallisuuden kannalta pulmallista on myös salasanan salaisuus ja pysyminen salaisena. Tietoliikennettä voidaan salakuunnella, ja urkittuja tietoja voidaan toistaa ja kopioida. Järjestelmiä on mahdollista vahvistaa erilaisin keinoin. Salasanan pakollinen vähimmäispituus tekee siitä vaikeammin arvattavan tai purettavan. Järjestelmä voi vaatia käyttäjää vaihtamaan salasanaa tietyn aikajakson tai käyttökertojen välein.

Kertakäyttöiset salasanat

Turvallisuutta voidaan lisätä käyttämällä jokaisella tunnistautumiskerralla uutta salasanaa. Tällaisten listojen ylläpito on tehtävä huolellisesti, jotta synkronisaatio käyttäjän ja järjestelmän välillä säilyy. Listat ovat usein hankalia käyttää, eivätkä ne poista varastamisen tai väärinkäytön mahdollisuutta.

Aikaperusteiset salasanat

Salasanan muodostuminen voidaan asettaa aikaperusteesta riippuvaiseksi. Tällöin salasana vaihtuu esimerkiksi kerran minuutissa. Salasanan muodostamista varten tarvitaan kaava, jossa on ajasta riippuva muuttuja. Selkeimmin tällaista edustaa haastelukulaskin, joka on myös laitepohjainen todentamisen väline (esim. SecurID).

Laitepohjainen tunnistautuminen

Tämä menetelmä perustuu laitteeseen, joka on vain tunnistettavan hallussa ja joka pitää esittää, kun halutaan tunnistautua tai todentautua. Laitteiden käyttö on sopivaa erityisesti paikallisissa järjestelmissä, koska käyttäjää ei voi siirtää etäjärjestelmään tunnistettavaksi. Suurin tietoturvariski on se, että laitetta lainataan tai se varastetaan.

Tunnistautuminen televerkon pohjalta

Puhelinyhteyden kautta voidaan soittaja tunnistaa mm. televerkon tunnisteen, soittajan A-numerotiedon perusteelle. Yksi mahdollisuus on pyytää sovellusta lähettämään tunnistautumispyyntö käyttäjälle rekisteröityyn matkapuhelimeen.

Biometrinen tunnistus

Biometrinen tunnistus perustuu ihmiskehon jonkin yksilöllisen osan rakenteeseen tai erityispiirteisiin. Tällaisella ruumiinosan muodon tai ominaisuuden mittaamisella voidaan erittäin vahvasti tunnistaa yksilön henkilöllisyys. Biometriaa käytetään tunnistamisessa ja todentamisessa molemmissa, yhdessä tai erikseen. Parhaiten se sopii paikalliseen tunnistamiseen.

Sormenjälkitunnistukseen perustuvat tekniikat ovat pitkälle kehittyneitä, mutta vielä standardoimattomia, joten se soveltuvat toistaiseksi vain rajattuihin kohteisiin. Sormenpään ihosta muodostetaan kuva ja tätä käytetään tunnistetietona. Muut biometriset tunnistusmenetelmät ja niiden avulla toteutettavat vastaavat tietoturvallisuusinfrastruktuurit ovat vasta kehitteillä. Näitä ovat mm. silmänpohjan tunnistus, äänen tunnistus tai hahmon tunnistus. Silmänpohjatunnistuksessa luodaan henkilön silmäpohjasta kuva, jota verrataan alkuperäiseen tunnistetietoon; äänen tunnistuksessa puhe muutetaan digitaaliseen muotoon tunnistusanalyysiä varten.

Biometristen tunnistusjärjestelmien käyttö tulee pitkään rajoittumaan vain erityistarkoituksiin, mahdollisesti esimerkiksi täydentämään toimikorttipohjaista todennusta. Turvallisuusriski järjestelmissä on olemassa, jos alkuperäinen tunnistustieto on tallennettu keskitettyyn tietokantaan. Tiedon säilyttäminen ja sisällyttäminen toimikortin sisälle poistaa tämän tietosuojaongelman. Lisäksi ns. FAR (false acceptance ratio) eli tunnistamisen tarkkuus yksilöintitiedosta asettaa omat rajoitteensa. Liian tiukoilla kriteereillä yksilön normaali vaihtelu esimerkiksi äänen värissä tai puheen nopeudessa estäisi järjestelmän käytön - ja liian laaja vaihteluväli mahdollistaisi pääsyn asiattomille osapuolille.

Jaettu salaisuus

Kaikki sähköiset allekirjoitukset perustuvat kryptografiaan eli salakirjoitustekniikkaan. Kryptografiset järjestelmät sisältävät jonkinlaisen haaste-vaste-menettelyn. Jaettua salaisuutta (molemmilla osapuolilla on tiedossaan käytetty salausavain) käytettäessä, toinen osapuoli lähettää haasteen, johon toinen vastaa käyttämällä sovittua krypto-funktiota. Vastaus lähetetään takaisin. Toinen laskee samasta informaatiosta saman funktion. Jos tulos on sama, voidaan luottaa vastapuolen tunnistamiseen.

Jaetun salaisuuden käytössä pulmana on salaisuus, salaisen avaimen jako osapuolten kesken. Jokaiselle kommunikaatio-osapuolelle tulee välittää oma jaettu salaisuus. Allekirjoitus ei ole yksiselitteinen, koska usea osapuoli tuntee saman avaimen eikä todentamista voida tehdä jaettuun salaisuuteen perustuen.

4.2.2 PKI-pohjaisista menetelmistä

PKI-järjestelmä toteuttaa tällä hetkellä muita ratkaisuja luotettavammin ja standardirajapinnoin sähköiselle asioinnille asetetut turvallisuusvaatimukset erityisesti kun kyseessä on hajautetut tietojärjestelmät. Toisaalta PKI-järjestelmien käyttöä on kritisoitu niiden monimutkaisuudesta ja raskaudesta.

Käytössä olevat PKI-menetelmät ja avaimet on valittu niin, että niillä koodattujen tietojen murtaminen ei ole käytännössä mahdollista. PKI-pohjaisissa todennuskäytännöissä molemmat osapuolet voivat todentaa toinen toisensa ilman että osapuolten välillä lähetetään salaisuuksia, esimerkiksi salasanaa. Nämä ominaisuuden tekevät PKI:stä vahvan tunnistamismenetelmän.

Lisäksi järjestelmää voidaan käyttää moniin muihin turvapalveluihin, kuten viestien varsinaiseen salaukseen tai allekirjoittamiseen.

PKI ja matkapuhelimet

Lähtökohtana käyttäjien luotettavassa todentamisessa voidaan Suomessa pitää toimikorttipohjaista todentamista. EU-lainsäädäntö allekirjoituksista edellyttää luotettavaa allekirjoituksen luontivälinettä tehtäessä laatuallekirjoituksia. Muovikorttipohjaisen toimikortin rinnalle nousee tunnistusvälineenä GSM-puhelin, jonka SIM-korttia voidaan käyttää yksityisten avainten ja varmenteiden säilytyspaikkana. Matkapuhelimessa voi (laiteriippuvaisesti) olla SIM-kortin rinnalla toinen toimikortti, johon avaimet ja varmenteet sijoitetaan. Varmenteiden jakelu voidaan hoitaa tällöin tietoverkon kautta.

Tätä nykyä langattoman toimintaympäristön ongelma on rajoittunut siirtokapasiteetti. Tästä syystä langattoman PKI-ympäristön rakentamisessa on pyritty ratkaisuihin, joilla siirrettävien tietojen määrää pyritään supistamaan pienimpään mahdolliseen. Varmenteista muodostetaan minimoituja versioita mobiilikäyttöön – tai ylläpidetään vain tietoa siitä missä alkuperäistä varmennetta säilytetään.

PKI ja biometria

PIN-koodin antamista pidetään toisinaan turvattomana toimenpiteenä tunnistamisprosessissa. Siksi on etsitty ratkaisuja, joissa esimerkiksi biometriset järjestelmät korvaisivat PIN-koodin. Markkinoilla on jo tuotteita, joissa käytetään sormenjälkeä PKI-ympäristössä PIN-koodin korvaajana. Tekniikan uutuuden vuoksi myös kustannukset ovat normaaleja toimikortti ja -lukijaratkaisuja suuremmat. Ratkaisua pidetään todella luotettavana silloin, kun biometrinen tunnistaminen voidaan suorittaa suoraan toimikortilla. Järjestelmässä tunnistuslaite tunnistaa yksilöllisen ominaisuuden ja vertaa sitä esimerkiksi toimikortilla olevaan tunnistustietoon.

4.3 Sähköinen tunnistautuminen terveydenhuollossa

Terveydenhuollossa edelleen pääosa asioinnista tapahtuu potilaan ja ammattilaisen henkilökohtaisen tapaamisen yhteydessä, ja tunnistaminen/tunnistautuminen on ollut ongelmatonta. Ammattilaisten välisessä konsultaatiossa käytetään nykyään puhelimen ja faksin lisäksi entistä enemmän tietoliikenneverkon palveluja, kuten sähköpostia. Osa kommunikaatiosta tapahtuu

sähköisesti organisaatioiden tai niiden alayksiköiden kesken tai siten, että ammattilainen asioi toisen organisaation kanssa (esimerkiksi yksityislääkäri lähettää elektronisen lähetteen sairaalan klinikalle tai vastaanotolle). Tulevaisuudessa on odotettavissa, että sekä potilaan ja lääkärin että potilaan ja palveluntuottajan välinen sähköinen asiointi lisääntyy. Uusimpana yhteydenpitomuotona on nähtävissä lääkärin ja tietämysohjelman välinen kommunikaatio.

Silloin kun terveydenhuollon sähköiseen asiointiin sisältyy salassa pidettävien asiakas/potilastietojen siirtoa tai käyttöä, on perusvaatimuksena, että kyetään tunnistamaan luotettavasti palveluntuottajat, niiden alaorganisaatiot, ammattilaiset, asiakkaat/potilaat, tietojärjestelmien palvelimet ja tarvittaessa käytettävät ohjelmistot.

Monissa maissa käytetty henkilöiden vahvan tunnistamisen menetelmä on toimikorttipohjainen todentaminen. Toimikortin asemesta voidaan käyttää myös ulkoasultaan muunlaisia tunnisteen kantajia ns. ”hard tokens". Kansalaisen/potilaan sähköinen tunnistaminen perustuu monesti toimikorttipohjaiseen kansalaiskorttiin, sairasvakuutuskorttiin tai sosiaaliturvakortiin. Ammattilainen tunnistetaan tyypillisesti ammattijärjestön tai työnantajan jakamalla toimikortilla (esimerkki lääkärikortti). Heikompi tunnistamisen menetelmä perustuu mm. organisaation sisäisiin bittisertifikaatteihin. Palvelimia varten on kehitteillä erityisiä palvelinsertifikaatteja ja vastaavasti organisaatioita varten organisaatiosertifikaatteja.

Terveydenhuollossa on roolipohjaisella tunnistautumisella suuri merkitys. Samankin organisaation sisällä saattaa esimerkiksi lääkärillä olla yhden päivän aikana useita dynaamisesti muuttuvia rooleja. Lisäksi voi hänellä olla käytössään sekä julkisen sektorin että yksityisen sektorin roolit saamanaikaisesti. Terveydenhuollossa tulee tunnistautumisen tapahtua lähtökohtaisesti roolipohjaisena.

Terveydenhuollon sähköinen tunnistautuminen on perusteltua rakentaa olemassa olevaa ja toimivaksi havaittua infrastruktuuria hyödyntäväksi. Lähtökohtana ammattilaisten tunnistamiselle voidaan pitää toimikorttipohjaista todentamista.

Terveydenhuollossa käsiteltävä informaatio on useimmiten salassa pidettävää, ja informaation laatineen ammattilaisen allekirjoitus tarvitaan. Varmenneympäristö on ainoa oikea tapa vakuuttua allekirjoittajasta ja allekirjoitetun tiedon muuttumattomuudesta. Varmenteiden luottamusketjun perusteella voidaan löytää luotettava kolmas osapuoli, jonka todistukseen henkilön identiteetistä ja sen oikeellisuudesta voidaan luottaa.

5. VARMENTEET JA VARMENTAMINEN

5.1 Varmenne

Julkista avainta käytettäessä on ehdottoman tärkeää tietää, kenelle avain kuuluu. Tämä voidaan tarkistaa varmenteesta, jossa julkinen avain ja avaimen haltijan tiedot on yhdistetty ja taattu kolmannen luotettavan osapuolen allekirjoituksella. Onko varmenne luotettava, riippuu siitä, voivatko osapuolet luottaa sen varmentajaan. Jos varmentaja on todettu ja osoitettu luotettavaksi varmennepolitiikan ja -käytäntöjen kautta, voivat osapuolet luottaa toisiinsa, jos luotettu kolmas osapuoli on molemmille yhteinen ja vastaa molempien luottamuksellisuudesta.

Sähköisen allekirjoituksen ja varmenteiden suhteen nykyiset säädökset ja standardit jättävät yhä auki monia asioita. Tällaisia ovat esimerkiksi useamman henkilön allekirjoitus sekä roolivarmenteet ja attribuuttivarmenteet**.**

Viimeksi mainittu asia eli rooli- ja attribuuttivarmenteiden ja niiden käyttöön liittyvien säädöksien ja standardien puutteellisuus on seikka, joka omalta osaltaan saattaa hidastaa varmennepohjaisten tunnistusjärjestelmien käyttöönottoa. Rooli- ja attribuuttivarmenteet mahdollistaisivat yksinkertaisempien ja käyttötavoiltaan monipuolisempien järjestelmien rakentamisen kuin nykyiset yksilökohtaiset varmenteet. Näiden perusideana on varmentaa jokin varmenteen käyttäjään liittyvä attribuutti eli ominaisuus tai rooli. Näin rooli- ja attribuuttivarmenteiden avulla palvelujen käyttäjiä voitaisiin käsitellä ryhminä eikä yksilöinä, mikä joissain tilanteissa – mutta ei tietenkään aina – olisi kätevää. Roolivarmenteet voidaan toteuttaa joko attribuuttivarmenteina tai tavalliseen yksilövarmanteeseen liitettävänä sekundäärivarmenteena. Kun sähköisessä asioinnissa tulee eteen tilanne, jossa asioita on hoidettava täysin anonyymisti – siis ilman että käyttäjää tunnistetaan, silloin voidaan käyttää attribuuttivarmenteita, jotka eivät sisällä henkilötietoja.

Valmistelevaa työtä tällä alueella on tehty, sillä varmenne-perusstandardin X.509 uusimmat versiot sisältävät laajennuksia, jotka mahdollistavat rooli- ja attribuuttivarmenteiden tuottamisen. Myös standardien soveltamiseen liittyvää perustyötä tekevä IETF:n PKIX-ryhmä on luonnostelemassa X.509-profiileja rooli- ja attribuuttivarmenteiden toteuttamiselle.

5.2 Laatuvarmenne

EU-direktiivi sähköisistä allekirjoituksista edellyttää, että jäsenvaltion hyväksyttävät lainsäädäntöönsä direktiivin mukaisen lain sähköisistä allekirjoituksista. Siinä asetetaan laatuvarmenteelle vaatimukset, jotka sen on täytettävä ollakseen hyväksytty laatuvarmenne. Direktiivi pitää lisäksi hyväksyttää kansalliseen lainsäädäntöön, jotta se saa lainvoiman.

Laatuvarmenteiden tarjoaja on vastuussa myöntämistään varmenteista. Viestintävirasto on kansallinen toimija, joka valvoo laatuvarmenteiden tarjontaa. Se voi nimetä tarkastuslaitoksia, joiden tehtävä on selvittää ja arvioida varmenteita myöntävän tahon luotettavuus.

EU:n direktiivin asettamien ohjeiden mukaan laatuvarmenteessa on oltava:

- tieto siitä että varmenne on myönnetty laatuvarmenteena
- laatuvarmenteen myöntäjä ja maa, missä se on julkaistu, tulee identifioida
- allekirjoittajan nimi tai salanimi sekä tieto siitä, että käytössä on salanimi
- mahdollisuus lisätä allekirjoittajaan kuuluva erityismääre
- todentamiseen tarvittava tieto (PKI: julkinen avain), joka vastaa vain ja ainoastaan allekirjoittajan hallussa olevaa tietoa (PKI: yksityinen avain)
- voimassaoloaika, alkamis- ja päättymisajankohta

- varmenteen yksilöivä tieto, tunnuskoodi
- varmenteen myöntäjän kehittynyt sähköinen allekirjoitus
- mahdolliset käyttörajoitukset
- mahdolliset arvomääräiset rajoitukset, mihin varmennetta voi käyttää.

Mm. sähköposti-osoitteen ilmaiseminen varmenteen sisällä on valinnainen optio eikä välttämätön, jotta varmennetta voidaan pitää laatuvarmenteena.

Direktiivi asettaa vaatimuksia myös laatuvarmenteen varmentajalle, allekirjoituksen luomismenetelmälle että todentamiselle.

Varmentajaa koskevat seuraavat vaatimukset:

- varmentajan on osoitettava tarjotun varmennepalvelun luotettavuus
- taattava nopea sekä luotettava hakemisto- ja viivytyksetön revokointipalvelu
- varmentajan on kyettävä osoittamaan tarkasti varmenteen myöntämis- ja revokointiajankohta
- todentaa kansallisen lainsäädännön mukaisesti erityismääreineen sen henkilön henkilöllisyys, jolle varmennetta myönnetään
- pidettävä palveluksessa sellaista henkilökuntaa, jolla on palvelun edellyttämä asianmukainen ja riittävä asiantuntemus – tämä koskee erityisesti johtotehtävissä toimivia.
- sovellettava hallinnollisia ja liikkeenjohdollisia menettelytapoja, jotka ovat riittävät ja vastaavat tunnustettuja standardeja
- käytettävä luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutoksilta ja jotka takaavat tekniikan ja kryptografisten prosessien turvallisuuden
- tehtävä toimenpiteitä varmenteiden väärentämistä vastaan. Silloin kun varmennepalvelun tarjoaja luo allekirjoituksen luomiseen käytettävät tiedot (PKI: yksityinen avain), on avaimien luomisprosessin luottamuksellisuus taattava
- ylläpidettävä riittäviä taloudellisia resursseja operoida sopusoinnussa direktiivin asettamien vaatimusten kanssa, erityisesti kantaa vahinkovastuun riski esimerkiksi hankkimalla asianmukainen vakuutus
- arkistoitava mahdollisesti sähköisesti kaikki asiaankuuluva laatuvarmenteeseen liittyvä tieto tarkoituksenmukaiseksi ajaksi, jotta sitä voidaan tarvittaessa käyttää todisteena oikeudellisissa menettelyissä
- oltava tallentamatta tai kopioimatta allekirjoituksen luomiseen käytettävät tiedot henkilöltä, jolle varmennepalvelun tarjoaja tuottaa avainten hallintaa liittyviä palveluja
- ennen sopimussuhteen aloittamista kirjallisesti selvitettävä varmenteen käyttöön liittyvät ehdot ja edellytykset mm. käyttörajoituksineen ja valitusmenettelyineen
- käyttää luotettavia järjestelmiä tallentaa varmenteita todennettavassa muodossa.

Allekirjoituksen luomismenetelmän tulee täyttää mm. seuraavat vaatimukset:

- yksityistä avainta vastaavia (allekirjoituksen luomiseen käytettäviä) tietoja voi käyttää vain kerran ja niiden luottamuksellisuus on varmistettavissa
- yksityisen avaimen tietoja ei voi johtaa mistään ja tiedot ovat suojattu väärentämistä vastaan
- turvalliset allekirjoituksen luomismenetelmät eivät saa muuttaa allekirjoitettavia tietoja eivätkä estää niiden esittämistä allekirjoittajalle ennen allekirjoitusprosessia.

Turvallista allekirjoitusta todennettaessa on varmistettava mm.:

- allekirjoituksen todentamiseen käytetyt tiedot vastaavat todentajalle esitettyjä tietoja
- allekirjoitus on luotettavasti todennettu ja tämä todentamisen tulos asianmukaisesti esitetty
- todentaja voi tarvittaessa luotettavasti todeta allekirjoitettujen tietojen sisällön.
- varmenteen aitous ja oikeellisuus allekirjoituksen todentamishetkellä voidaan luotettavasti todentaa
- todentamisen tulos ja allekirjoittajan henkilöllisyys on asianmukaisesti esitetty
- salanimen käyttö on selkeästi osoitettu
- kaikki turvallisuuteen liittyvät muutokset ovat havaittavissa.

5.3 Varmentaminen

Varmentaja varmentaa omalla allekirjoituksellaan tiedot, jotka se on saanut varmennepyynnössä. Varmenteella varmentaja siis takaa, että varmenteessa esitetyt varmenteen haltijan yksilöintitiedot ja julkinen avain kuuluvat samalle avaimenhaltijalle.

Organisaation sisäisessä käytössä luottaminen varmentajan toimintaan on suoraviivaista. Kuitenkin organisaatiot joutuvat päättämään, hyväksyäkö vai hylätä varmenteita sellaisilta varmentajilta, jotka eivät ole heidän hallinnassaan. Tässä päätöksentekoprosessissa varmennepolitiikan rooli on merkittävä.

Teknisenä ratkaisuna tähän ongelmaan voi olla eksplisiittinen luottaminen useampaan varmentajaan tai varmentajien väliset suorat ristiinvarmennukset tai hierarkkiset luottamussuhteet.

5.3.1 Ristiinvarmentaminen

Ristiinvarmentaminen tarkoittaa tilannetta, jossa kaksi varmentajaa jakavat keskenään luotettavasti toinen toisensa avainten informaatiota ja myöntävät toisilleen varmenteen. Kun tästä on päästy yhteisymmärrykseen, voi varmentaja taata toisen varmentajan allekirjoittaman varmenteen oikeellisuuden. Ristiinvarmentamisessa on tärkeää, että varmentajat hyväksyvät toistensa varmennepolitiikat ja että ne ovat molemmille riittävät. Ristiinvarmentaminen on mahdollista tehdä molemminpuolisesti tai niin, että toinen myöntää varmenteen toiselle mutta ei toisinpäin.

Kahdenkeskisen ristiinvarmennuksen ollessa kyseessä varmentajien välillä varmentajat vaihtavat todentamisavaimiaan. Näitä avaimia käytetään tarkistamaan varmenteissa olevia toisen varmentajan allekirjoituksia.

Käytännössä tämä tarkoittaa esimerkiksi sitä, että rekisteröityessään varmennetta vaativaan palveluun käyttäjä todennetaan toisen varmentajan aiemmin myöntämän varmenteen perusteella.

5.3.2 Luottosuhteet

Sellaisissa tilanteissa joissa varmenteita luodaan useisiin käyttötarkoituksiin, perustuu usein uuden varmenteen luonti jo olemassa olevalle varmenteelle. Luottamus siis siirtyy luottamusketjua pitkin. Varmenteesta taas on aina ilmettävä, mistä sen luottamus tulee (ts. varmentaja-tieto). Todennettaessa varmennetta todennetaan luottamusketjussa olevia varmenteita yksi kerrallaan, kunnes päästään varmentajaan, johon luotetaan.

On useita malleja rakentaa varmentamisen luottamussuhteet. Luottamus voidaan rakentaa hierarkkisesti, käyttäen ristiinvarmennusta tai näiden yhdistelmää..

Hierarkkisen luottamusmallin lähtökohta on juurivarmenne. Juurivarmennetta seuraava varmenne perustuu tähän varmenteeseen, sitä seuraava tähän juurivarmenteeseen luottavaan varmenteeseen jne. Tällaisen hierarkia-luottamuspolun purkaminen on suoraviivaista, ja kaikki varmennetut omaavat saman juurivarmentajan. Harvoin kuitenkaan kaupallisesti osapuolet pääsevät so-

pimukseen tällaisesta mallista – ja olisi todella katastrofaalista koko luottamusketjulle, jos juurivarmenteen tai sitä hierarkkisesti lähellä olevan varmenteen salainen avain paljastuisi.

Ristiinvarmentamalla synnytetään luottamussuhteiden verkosto, jonka etuja on mm. joustavuus. Ristiinvarmennuksessa kukin osapuoli valitsee sen tai ne organisaatiot, jotka yhdistetään eli ristiinvarmennetaan muiden luottamusorganisaatioiden kesken. Tärkeintä on luottamus lähinnä olevaan varmentajaan eli omaan varmentajaan, suhteet muihin varmentajiin luodaan oman varmentajan kautta . Varmennepolun löytäminen ja verkoston luottamussuhteiden ylläpitäminen on ristiinvarmennnuksessa hallinnollisesti työläämpää kuin hierarkkisessa järjestelmässä.

Käytännöllisintä on rakentaa luottamusketju – mikäli sellaista tarvitaan ja se sopii sovellusympäristöön ja varmennepolitiikkaan – pohjautuen sekä ristiinvarmentamisen että hierarkkisen luottamuksen malleihin; silloin voidaan mm. minimoida avaimen paljastumisen riski.

6. VARMENNEPOLITIIKKA

Varmenteiden luomista varten – ja jotta ne täyttäisivät lainsäädännön asettamat määräykset – on luotava varmennepolitiikka ja dokumentoitava se. Varmennepolitiikkan luomisessa on siis kysymys siitä, että luodaan yhteiset periaatteet ja sopimukset siitä, mikä on yhteinen luottamusmalli.

Varmennepolitiikkaa tarvitaan, koska sen avulla varmentaja perustelee, miksi sen myöntämät varmenteet ovat luotettavia ja sen generoimat julkiset avaimet aitoja ja ehyitä.

Varmenneorganisaation toiminnallisuus kuvataan varmentajan (CA) varmennepolitiikassa, jonka tehtävänä on osoittaa sen luotettavuus.

Varmennepolitiikassa kuvataan tyypillisesti:

- Osapuolten vastuut ja velvollisuudet selkeästi ja tyhjentävästi
- CA:n, RA:n ja varmennehakemiston toiminta ja niihin liittyvät prosessit
- Varmennejärjestelmän ylläpito ja hallinnointi.

Laatuvarmenteiden luojan varmennepolitiikka tulee auditoida viestintäviraston ohjeiden mukaisesti. Viestintävirastosta saa varmennepolitiikan luomiseksi ohjeet, jotka noudattelevat EEMAn (The European Forum for Electronic Business) ohjesuosituksia.

6.1 Yleistä

Varmennepolitiikka luodaan sekä varmentajalle että kaikille varmenteille (kuten henkilövarmenne, roolivarmenne ja laitevarmenne). Euroopan Unionin alueella on noudatettava EU:n sähköisen allekirjoituksen direktiivin asettamia vaatimuksia laatuvarmenteille.

Varmennepolitiikan laatii varmentaja eli se taho, joka myöntää varmenteita. Varmennepolitiikka vastaa kysymyksiin, mitä varmenteella voidaan tehdä, mitä valtuuksia, oikeuksia ja velvollisuuksia se sisältää. Vähimmäisvaatimuksena tulee varmennepolitiikkaan kirjata ainakin organisaatiotiedot varmentajasta, vastuunjako osapuolten välillä (kaikki osapuolet tulee kirjata, myös rekisteröijät), osapuolten velvollisuudet, varmentamiseen liittyvät turvatoimet, varmenteen sekä sulkulistan sekä varmenteen tallennusvälineen (esim. toimikortin) kuvaukset ja tiedot siitä, kuinka varmennepolitiikkaa hallinnoidaan.

Varmennekäytäntö kertoo, miten varmenteet luodaan, myönnetään ja miten niiden aitous ja turvallisuus taataan. Vähimmillään sen tulee kuvata varmenneorganisaatio ja varmenneympäristö, velvollisuudet ja vastuut, varmennetoiminnan loppumisen toimintatavat ja varmennekäytäntölausuman hallinnointi. Tämä dokumentti ei pääsääntöisesti ole julkinen.

6.2 Varmennepolitiikka dokumentti

Seuraavassa kuvattu esimerkki varmennepolitiikka-dokumentissa tarkennettavista tiedoista:

- **Varmennusorganisaatio**. Selvitetään varmennepolitiikan yksilöintitiedot. Kuvataan varmenteeseen liittyvät toiminnot ja toimijat, joita varmennepolitiikka koskee. Näitä ovat esimerkiksi varmentaja, rekisteröijä, toimikortin haltija, toimikortin käyttö, toimikortin valmistaja, sulkulistat ja palvelu, jolla niitä ylläpidetään, hakemistot ja palvelu, jolla niitä ylläpidetään, sekä varmennepolitiikan sovellusalue ja sen ylläpitäjän tiedot.
- **Vastuut ja velvollisuudet**. Kuvaus kaikkien varmennetta käsittelevien toimijoiden tehtävistä: mitä rekisteröijän, varmennepalvelun tarjoajan ja kortinvalmistajan tulee tehdä; mitä velvollisuuksia on varmenteen käyttäjällä, haltijalla; miten tai miksi varmenteeseen voi luottaa; mikä on varmentajan vastuu; kuinka varmenteet mitätöidään. Lisäksi on kuvattava toimenpiteet tilanteessa, jos varmennustoiminta lopetetaan.

- **Turvatoimet ja varmentaminen**. On kirjattava ne edellytykset, joita varmentaminen vaatii henkilöstön, fyysisen turvatoimen ja tietoteknisten turvavaatimusten osalta. Silloin on otettava huomioon kaikki eri varmentamisprosessin osissa olevat toimijat, kuten rekisteröijä, varmennepalvelu itse sekä toimikortin valmistaja – ja sulkulistapalvelun käsittely. Myös rekisteröitävän varmenteenhakijan tunnistamiseen liittyvät vaatimukset on syytä huomioida samoin kuin toimenpiteet yksityisen avaimen suojaamiseksi.
- **Kuvaukset toimikortista, varmenteesta ja sulkulistasta**. Nämä kirjataan siten, että kuvataan esim. varmenteen ja sulkulistan profiilit. Toimintatavat varmenteen ja kortin uusimiseksi, mitätöimiseksi, luomiseksi jne. on myös esitettävä.
- **Varmennepolitiikka-asiakirjan ylläpito.** On syytä kuvata, kuka hallinnoi asiakirjaa, ylläpitää siihen tehtäviä muutoksia ja vastaa muutoksien tiedottamisesta; mitä tehdä ongelma- tai katastrofitilanteessa.

6.3 Varmennepolitiikka terveydenhuollossa

Terveydenhuollolle tulee laatia kansallinen varmennepolitiikkaluvaus ja mahdollisille alueellisille PKI-toteutuksille alueellinen varmennepolitikka. Terveydenhuollon varmennepolitiikkaa laadittaessa on perusteltua noudattaa sitä varten laadittuja kansainvälisiä standardeja kuten ISO TC 215 N189 Part 3: Policy Management of Certificate Authority.

Luotetuksi kolmanneksi osapuoleksi valittu varmentaja tekee jokaiselle varmennetyypille varmennepolitiikkakuvauksen. Mikäli rakennetaan useiden alueellisten varmentajien verkosto, on yhteensopivuuden ja laatuvarmentamisen vuoksi suositeltavaa luoda kansalliset ohjeet ja pelisäännöt, mikä on sallittua, mikä pakollista ja mikä kiellettyä varmentamisessa. Päätös on tehtävä mm. siitä, tallennetaanko yksityinen avain toimikortille vai onko tiedostomuodossa oleva varmenne (ns. ”softavarmenne”, joka on varmenne tiedostona käyttäjän laitteen muistissa) yhtä pätevä.

7. TERVEYDENHUOLLON VAATIMUKSET PKI-ARKKITEHTUURILLE

7.1 Terveydenhuoltosektorin toiminnalliset vaatimukset

Vuonna 1996 julkaistun sosiaali- ja terveysministeriön tietoteknologian hyödyntämisstrategian eräs tavoite on ollut saumattomien palveluketjujen kehittäminen. Saumattomilla palveluketjuilla tarkoitetaan niitä terveydenhuollon palveluprosesseja, joiden perusteella potilas saa palvelua organisaatiorajoista riippumatta. Organisaatiorajoja voivat olla esimerkiksi julkinen/yksityinen terveydenhoito, perusterveydenhuolto/erikoissairaanhoito tai vaikkapa yksittäisen organisaation eri toimintayksiköiden välinen raja. Organisaatiorajojen muodostumiseen vaikuttavat muun muassa potilastietolaki ja henkilötietolaki.

Nykyisin käytössä olevat asiakas- ja potilasjärjestelmät on rakennettu tukemaan ensisijaisesti organisaatiokeskeistä toimintatapaa, ja siksi ne tukevat heikosti palveluketjumallia. Organisaatioiden välinen yhteistoiminta kuitenkin edellyttää potilastietojen lisääntyvää ”tietokoneistumista” samoin kuin vaatimus potilaan aktiivisesta osallistumisesta ja vaikuttamisesta itseensä kohdistuvaan hoitoon.

Potilastietojen yksityisyyden suojan lähtökohtana on, että henkilöllä on määräämisoikeus omiin tietoihinsa. Henkilötietolain perusteella salassa pidettäviä potilastietoja ei voida luovuttaa tai siirtää ulkopuolisille ilman asianmukaista lupaa ja jokaisen luovutuksen tai siirron osalta tulee olla laillinen oikeus luovuttaa tietoja.

Palveluketjujen osalta tämä vaatimus korostuu, sillä arkaluonteisten potilastietojen käyttö tai siirto eri terveydenhuollon palvelutarjoajien välillä lisääntyy, jotta potilaan nopea ja joustava palvelu voidaan tarvittaessa järjestää. Siirrettäessä tietoa organisaatiorajojen yli tulee potilaalta pääsääntöisesti pyytää tähän suostumus. Poikkeustilanteissa ammattilainen voi päästä potilaan tietoihin käsiksi ilman potilaan suostumusta silloin, kun potilaan kiireellinen hoito sitä välttämättä edellyttää ja ammattilaisella on roolinsa mukaan oikeus (asiallinen yhteys) tietojen saantiin.

Vaatimus nopeaan ja joustavaan palveluun edellyttää uusien välineiden ja tietoverkkopalvelujen mahdollistaman ajasta ja paikasta riippumattoman potilastietojen käsittelyn. Kasvavan tiedonsiirron lisäksi olemassa oleviin tietovarastoihin kohdistuu uusia uhkia, jolloin perinteisen asioinnin muuttuminen ”e-asioinniksi” edellyttää tietoturvatason nostoa fyysisen turvallisuuden vähetessä esimerkiksi järjestelmän käyttäjien tunnistamis- ja todentamistilanteissa.

Organisaatiokohtaisen tietoturvan toteuttaminen ei yksin riitä, vaan lisäksi tarvitaan organisaatiorajat ylittävä tietoturvapolitiikka, infrastruktuuri ja kaikki ammattiryhmät kattava tietoturvakoulutus (”Sosiaali- ja terveydenhuollon tietoteknologian hyödyntäminen. Osa I. Saumaton hoito- ja palveluketju. Asiakaskortti.”, STM työryhmämuistio 1998:8) jotta potilastiedot voidaan suojata jokaisen tiedon käsittelyn vaiheessa eri palveluntarjoajilla.

Lisäksi terveydenhuollon erityispiirteenä ovat ammattilaisten lukuisat lyhyet ja rinnakkaiset työsuhteet sekä hyvin dynaamisesti vaihtuvat roolit. Lääkäri voi yhdenkin päivän kuluessa työskennellä esimerkiksi tutkijan roolissa tutkimuslaitoksessa, toimia virassaan erikoissairaanhoidon yksikössä sekä pitää vastaanottoa yksityisellä lääkäriasemalla. Toisaalta erikoissairaanhoidossa lääkärin tehtävät (ja käyttöoikeudet) voivat vaihtua osastolääkäristä päivystäjäksi työvuoron aikana. Hyvin nopeasti muuttuvat roolit yhdistettynä potilastietojen tiukkoihin tietosuojavaatimuksiin asettavat erityisiä teknisiä ja toiminnallisia vaatimuksia käyttäjän tunnistamiseen ja todentamiseen sekä erityisesti hänen käyttöoikeuksiensa hallintaan.

Terveydenhuollon PKI-järjestelmälle asettamia vaatimuksista tarkastellaan seuraavassa käyttötapausesimerkkien kautta. Kussakin esimerkissä listataan ne varmenteita tarvitsevat toimijat, jotka osallistuvat kulloinkin potilastietojen käsittelyyn. Esimerkkien käyttötapausten ja toimijaluokittelun ei ole tarkoitus olla kattava ja yhtenäinen kuvaus terveydenhuoltosektorin toiminnasta, vaan tarjota ainoastaan puitteet PKI-tarpeiden analysoimiseksi.

7.1.1 Toimijat

Toimijoilla tarkoitetaan tässä niitä käyttäjärooleja (*actor*), joiden toiminta terveydenhuollon palveluissa ja prosesseissa vaikuttaa PKI-arkkitehtuurin vaatimuksiin. Toimijoiksi kuvataan myös sovellukset ja laitteet, jotka itsenäisesti toimivat PKI:n osapuolina.

Tämän jaottelun lisäksi terveydenhuollon PKI- ja sovellusarkkitehtuurissa esiintyy myös muita toimijoita, jotka ovat varmenteidenhaltijoita, kuten esimerkiksi varmentajat, rekisteröijät tai aikaleimapalvelu. Näiden arkkitehtuurin sisäisten toimijoiden hallinta hoidetaan erillään varsinaisten hyödyntäjien hallinnoinnista.

Terveydenhuollon laillistettuja ammattihenkilöitä ovat lääkärit ja hoitajat, jotka Terveydenhuollon oikeusturvakeskus on laillistanut. Terveydenhuollon oikeusturvakeskus ylläpitää rekisteriä terveydenhuollon ammattihenkilöistä. Muita ammattihenkilöryhmiä ovat luvan saaneet ammattihenkilöt sekä nimikesuojatut ammattihenkilöt. Vastedes tässä dokumentissa termillä ammattilaiset viitataan nimenomaan laillistettuihin ammattihenkilöihin.

Muita terveydenhuollon työntekijöitä ovat ne terveydenhuoltoyksikön palveluksessa olevat henkilöt, joita ei ole laillistettu terveydenhuoltotehtäviin. Esimerkkejä heistä ovat sairaalafyysikot, sihteerit tai ATK-suunnittelijat.

Sovelluksilla tarkoitetaan niitä ohjelmistoprosesseja, jotka voivat toimia yksityisen avaimen käyttäjänä ilman ihmisen jatkuvaa apua. Sovellus on voitu myös sulauttaa kiinteäksi osaksi laitetta. Esimerkkinä sovelluksista ovat Web-palvelinsovellukset tai sanomanvälitysohjelmistot.

Potilas on henkilö, joka saa terveydenhoitopalveluja muilta tässä mainituilta toimijoilta.

Palveluntuottaja on luvanvarainen terveydenhoitopalveluja tarjoava organisaatio, kuten sairaala, sairaanhoitopiiri, yksityinen lääkärikeskus tai (työ)terveysasema. Organisaatio voi esimerkiksi koostua useista itsenäisistä henkilötietolain tarkoittamista rekisterinpitäjistä.

Tukiorganisaatiolla tarkoitetaan organisaatioita, jotka tarjoavat terveydenhuoltoyksikölle palveluja tai tavaroita. Tukiorganisaatioita ovat mm. lääkealan yritykset, ATK-palvelutoimittajat tai terveydenhuollon laite- ja tarviketoimittajat.

Tukiorganisaation työntekijät ovat niitä tukiorganisaation palveluksessa olevia henkilöitä, joilla on mahdollisuus työtehtäviensä kautta saada käsiinsä potilastietoja tai jotka muuten ovat yhteydessä terveydenhuoltoyksikön järjestelmiin.

7.1.2 Käyttötapaukset

Seuraavassa on kuvattu kuusi käyttötapausesimerkkiä, jotka selventävät PKI-järjestelmälle asetettavia vaatimuksia sekä kansallisesta että paikallisesta näkökulmasta. Muita mahdollisia käyttötapauksia voisivat olla esimerkiksi potilaskertomusjärjestelmien käyttö, sähköiset laskujen käsittelyjärjestelmät tai kuvantamistietojen etäsiirrot.

Aluetietojärjestelmän käyttö

Aluetietojärjestelmällä tarkoitetaan integraatiokerrosta (ns. *middleware*) eli tietojärjestelmää joka mahdollistaa laajahkolla maantieteellisellä alueella hajautetusti sijaitsevien eri rekisterinpitäjien potilastietojärjestelmiin arkistoitujen potilastietojen katselun ja käytön yhtenä kokonaisuutena hoitoa annettaessa ja suunniteltaessa.

Terveyskeskuslääkärin vastaanoton yhteydessä lääkäri saa potilaalta suostumuksen tarkastella potilaan aikaisemmin erikoissairaanhoidossa ja työterveydenhuollossa tehtyjä kyseiseen vaivaan liittyviä tutkimuksia. Lääkäri tunnistautuu aluetietojärjestelmään roolinsa mukaisesti ja kirjaa järjestelmään potilaan antaman suostumuksen (mahdollisine rajoituksineen), joiden perusteella hän saa käyttöönsä aluetietojärjestelmän avulla haluamansa tiedot aiemmista hoidoista ja tutkimuksista. Näin lääkäri voi kokonaisvaltaisesti ja potilaan omaa muistikuvaa luotettavammin muodostaa käsityksensä potilaan terveydentilasta ja ongelmasta.

Paikallisen potilastietojärjestelmän etäkäyttö

Palveluntuottajan omaan henkilöstöön kuuluva ammattilainen ottaa yhteyden palveluntuottajan palveluihin sisäverkon ulkopuolelta. Mikäli palvelut sijaitsevat sisäverkossa käyttäjä tulee todentaa keskitetyssä etäkäytön sisäänkirjautumispalvelussa, jonka jälkeen hänen oikeutensa järjestelmien käyttöön toimivat samoin kuin normaalisti hänen työpisteessään olevasta työasemasta.

Mikäli palvelut on erityisesti suunniteltu ulkoista käyttöä (ekstranet, internet) varten ja sijoitettu sisäverkon ulkopuolelle, voidaan käyttäjän todentaminen tehdä palvelukohtaisesti tai keskitetysti. Jos yhteys luodaan julkisen internetin yli ja lisäksi käsiteltävät potilastiedot ovat luottamuksellisia, on yhteys suojattava vahvasti työaseman ja etäkäyttöpalvelimen välillä.

Etäkäyttäjä voi olla mikä tahansa edellä luetelluista toimijoista ja hänellä on rooleistaan ja henkilöllisyydestään riippuen erilaisia käyttöoikeuksia palveluihin ja palveluiden toimintoihin.

Kotihoito-ohjeiden pyyntö

Potilas ottaa yhteyden kotoaan palveluntuottajan web-palveluun, todentautuu palveluun ja täyttää lomakkeeseen kysymyksensä, allekirjoittaa sen ja lähettää lomakkeen palvelulle. Kysymystä lukiessaan palveluntuottajan päivystävä lääkäri voi varmistua potilaan henkilöllisyydestä ja hakea häntä koskevat potilastiedot, vastata annettuun kysymykseen sekä allekirjoittaa vastauksensa. Kysymys ja siihen liittyvä vastaus voidaan salata tarvittaessa.

Potilaan antama sähköinen suostumus

Vastaanotolla potilas kertoo lääkärille olleensa hoidossa saman sairauden johdosta aikaisemmin toisella palveluntuottajalla. Koska toimintayksiköiden välinen potilastiedon siirto edellyttää voimassa olevien määräysten mukaisesti potilaan kirjallista suostumusta toteutetaan se osana aluetietojärjestelmän palveluita. Sisäänkirjautuneena viitetietojärjestelmään lääkäri pyytää potilasta allekirjoittamaan sähköisesti suostumuksen potilaan henkilökohtaisella toimikortilla. Allekirjoitetussa suostumuksessa kyseiselle lääkärille annetaan lupa katsoa tietyltä ajanjaksolta kyseiseen sairauteen liittyvät viitteet ja niiden osoittamien dokumenttien sisällön. Potilaan suostumus arkistoidaan viitetietojärjestelmän yhteyteen, jotta myöhemmin lokitiedoista voidaan tarvittaessa tarkistaa lääkärin oikeudet kyseisten dokumenttien katseluun.

Elektroninen lääkemääräys

Lääkärissä käynnin päätteeksi lääkäri määrää potilaalle lääkkeitä elektronisella reseptillä. Lääkäri allekirjoittaa sähköisesti reseptin ja lähettää sen suojatusti keskitettyyn reseptijakelujärjestelmään. Potilaan mentyä apteekkiin, apteekkihenkilöstö hakee reseptin, tarkistaa allekirjoituksen ja valmistelee lääkkeen potilaalle. Järjestelmään voi kuulua esimerkiksi automaattinen lääkemäärien tai lääkärin lääkemääräämisoikeuksien tarkistus.

Epäselvissä tapauksissa (määrättyä lääkettä tai rinnakkaisvalmistetta ei ole saatavissa) lääkärin henkilöllisyys voidaan vaivatta todentaa ja häneen voidaan ottaa yhteyttä korvaavan lääkkeen löytämiseksi.

Potilas- ja asiakaskertomusten arkistointi

Arkistointi itsessään on paljon enemmän kuin paperin, mikrofilmin tai bittien säilyttämistä. Se on kokonaisuus, joka käsittää tiedon säilyttämisen ja luovuttamisen politiikan, tietoturvapolitiikan, tiedon hallinnan, versioiden ja konversioiden hallinnan, arkiston hallinnoinnin, tiedon kuvaamisen menetelmät ja tallennustekniikan.

Sosiaali- ja terveysministeriön ohjeiden mukaisesti palveluntuottajien on säilytettävä potilasasiakirjat alkuperäisenä ja muuttumattomana erikseen nimetyn talletusajan (Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen, Sosiaali- ja terveysministeriö, Oppaita 2001:3). Ministeriön ohjeistus on periaatteellinen eikä käsittele erikseen sähköistä potilasdokumentaatiota. Onkin lähdettävä siitä, että potilasasiakirjojen sähköisessä tallentamisessa on noudatettava samoja periaatteita kuin mitä perinteiselle paperikertomukselle on asetettu mainitussa ministeriön ohjeistuksessa. Edelleen on huomattava, että säilytyksen määrä-

ykset ja periaatteet koskevat sekä toteutuksia, joissa on käytössä erillinen arkisto, että tietojärjestelmiä, joissa potilastiedot on talletettu operatiiviseen tietokantaan (ns. On-line arkisto).

Tyypillistä terveydenhuollon potilasasiakirjojen säilyttämiselle on niiden pitkä tallennusaika, joka voi Suomessa vaihdella 10-110 vuoden välillä. Potilasta hoitavan ammattilaisen pitää myös allekirjoittaa asiakirjat, mikä edellyttää sähköisen allekirjoittamisen käyttämistä. Allekirjoittamisen yhteydessä tulee ilmetä allekirjoittaneen ammattilaisen rooli.

Potilasasiakirjojen sähköisen säilyttämisen ja arkistoinnin perusvaatimuksia ovat

- Käyttäjien vahva tunnistaminen (*identification/authenfication*) — Muotoiltu
- Tietojen muuttumattomuus (*integrity*) — Muotoiltu
- Tietoturva (*security, access control*) — Muotoiltu
- Saatavuus (*accessibility and availability*) — Muotoiltu
- Vastuullisuus ja luotettavuus (*accountability*) — Muotoiltu

Muotoiltu
Muotoiltu
Muotoiltu
Muotoiltu

Keskeisiin periaatteisiin kuuluu se, että arkistosta voi potilastietoja luovuttaa tai antaa käyttää vain erikseen määrättyjen edellytysten vallitessa (ns. *conditions to access*). Kaikesta tietojen käytöstä ja luovuttamisesta tulee jäädä arkistoon jälki. — Muotoiltu

Koska Suomessa potilastiedot allekirjoittaa hoitava lääkäri, muodostuu hoitojaksokohtaisesti sähköiseen arkistoon yhtä potilasta kohti useita erikseen allekirjoitettuja osadokumentteja. Näiden muodostaman kokonaisuuden tulee olla ehjä ja kiistämätön koko säilytysajan. Tämä voidaan toteuttaa esimerkiksi arkiston laatimalla potilaskertomuksen metakuvauksella ja arkiston tekemällä kaikki osadokumentit käsittävällä organisaatio-allekirjoituksella (vrt. ISO/TC 215/WG4/N99, 1st WD, P. Ruotsalainen, Aug. 2002). Toiminnallisesti arkistoallekirjoitus merkitsee sitä, että arkisto sulkee potilaan osadokumentit digitaaliseen kirjekuoreen.

Potilaskertomuksen tietojen muuttumattomuus varmistetaan lääkärin tekemällä sähköisellä allekirjoituksella. Tämä voidaan tehdä lääkärin omalla sähköisellä henkilökohtaisella allekirjoitusavaimella (esim. HST-kortin ja kansalaisvarmenteen avulla tai sosiaaliturvakortilla) tai erillisellä ammattiin liittyvällä allekirjoitusavaimella (ammattilaiskortti ja ammattivarmenne). Tarvittaessa voidaan allekirjoitukseen liittää ns. rooliatribuutti.

Tietojen muuttumattomuuden kannalta ongelmallinen tilanne syntyy, kun arkisto luovuttaa vain osan kokonaisuutena sähköisesti allekirjoitetusta potilaskertomuksesta. Tällöin alkuperäisen lääkärin tekemän allekirjoituksen takaama tiedon integriteetti murtuu luovutetun osan osalta. Mahdollinen ratkaisu tähän ongelmaan on se, että arkisto allekirjoittaa omalla arkistoallekirjoituksellaan luovutettavan osan ja siten takaa sen aitouden ja muuttumattomuuden.

Edellä esitetyn perustella on ilmeistä, että sähköinen asiakas- ja potilasarkiston tulee olla osa terveydenhuollon PKI-järjestelmää. Stakesin asettama *sähköisen arkistoinnin hyvän käytännön* työryhmä laatii yksityiskohtaiset suositukset hyvistä menettelytavoista. Nämä suositukset julkaistaan omana osaraporttinaan (kuva 1.1 s. 6).

7.2 Muut vaatimukset

Keskeinen vaatimus terveydenhuollon PKI-arkkitehtuurille on yleisten standardien ja yhteisesti hyväksyttyjä periaatteita noudattaminen koko maassa. Vain siten voidaan taata järjestelmien ongelmaton yhteentoimivuus nyt ja tulevaisuudessa.

Tämän raportin loppupuolen luvuissa arkkitehtuurivarmentajamalleja verrattaessa kiinnitetään huomiota arkkitehtuurin toimivuuteen mm. seuraavissa keskeisissä tilanteissa:

- Koska terveydenhuollon kansallista PKI-arkkitehtuuria tullaan toteuttamaan vähitellen usean vuoden kuluessa, on uuden palvelutuottajan lisäämisen oltava helppoa (laajennettavuus).

- Varmennepolun selvittämisen ja validoinnin tulee olla helppoa, jotta valmisohjelmistot voivat tukea arkkitehtuuria ilman muutoksia (helppokäyttöisyys).
- Jotta terveydenhuollolle voitaisiin laatia yhtenäinen turvakäytäntö ja eri toimijat voisivat olla varmoja toimintansa turvallisuudesta myös organisaatiorajat ylittävissä toiminnoissa, on varmentajien välisten luottosuhteiden määrään ja laatuun kiinnitettävä huomiota (selkeys).
- Katastrofitilanteista (kuten varmentajan avaimen paljastuessa) toipumisen tulee olla suunnitelmallista ja vahinkojen tulee rajautua mahdollisimman pienelle alueelle (kestävyys).
- Nykyisten toimintojen ja prosessien on oltava siirrettävissä PKI-arkkitehtuuriin ilman radikaaleja muutoksia (evoluutionomaisuus).
- Toteutusmallin tulee tukea niin paikallisia tarpeita (käyttäjä- ja käyttöoikeushallinta) kuin lainsäädännöstä aiheutuvia vaatimuksia (laatuvarmenteet ja –allekirjoitukset sekä allekirjoitusvälineet). Mallin on sovittava myös erikokoisille ja -tyyppisille organisaatioille sekä yksityisille toimijoille (joustavuus).

8. TERVEYDENHUOLLON PKI-ARKKITEHTUURI

Kuten luvussa 7 kuvattiin, PKI-infrastruktuuri koostuu kolmesta peruskomponentista, varmentajasta, rekisteröijästä sekä hakemistosta, joita PKI:n käyttäjät eli varmenteen haltijat ja varmennetta hyödyntävät osapuolet (*relying party*) käyttävät.

Muotoiltu

PKI-arkkitehtuurilla puolestaan tarkoitetaan infrastruktuurin komponenttien ja toimintojen välisiä suhteita sekä tehtävien jakoa paikallisiin tai keskitettyihin toimintoihin. Tämän työn kannalta PKI-arkkitehtuurin käsitettä on laajennettu koskemaan myös käyttöoikeuksien hallintaa ja niiden talletusta, toimikorttien hallintaa sekä muita tarpeellisia lisäpalveluja, joita tarvitaan pääsääntöisesti PKI:n hyödyntäjien toiminnoissa.

Muotoiltu

Jatkossa kuvataan kolme arkkitehtuurin vaihtoehtoa, joiden varaan tekninen arkkitehtuuri voidaan toteuttaa. Vaihtoehdoista kaksi kuvaavat ääriratkaisuja toiminnallisuuden keskityksen (kansalliset toiminnot) ja hajautuksen (paikalliset tai alueelliset toiminnot) suhteen sekä kolmantena vaihtoehtona osin hajautetuista ja osin keskitetyistä toiminnoista koostuva ratkaisu. Paikallisuudella/alueellisuudella tarkoitetaan tässä hallinnollisesti itsenäisiä palveluntuottajia, kuten esimerkiksi yksityiset lääkäriasemat tai sairaanhoitopiirit.

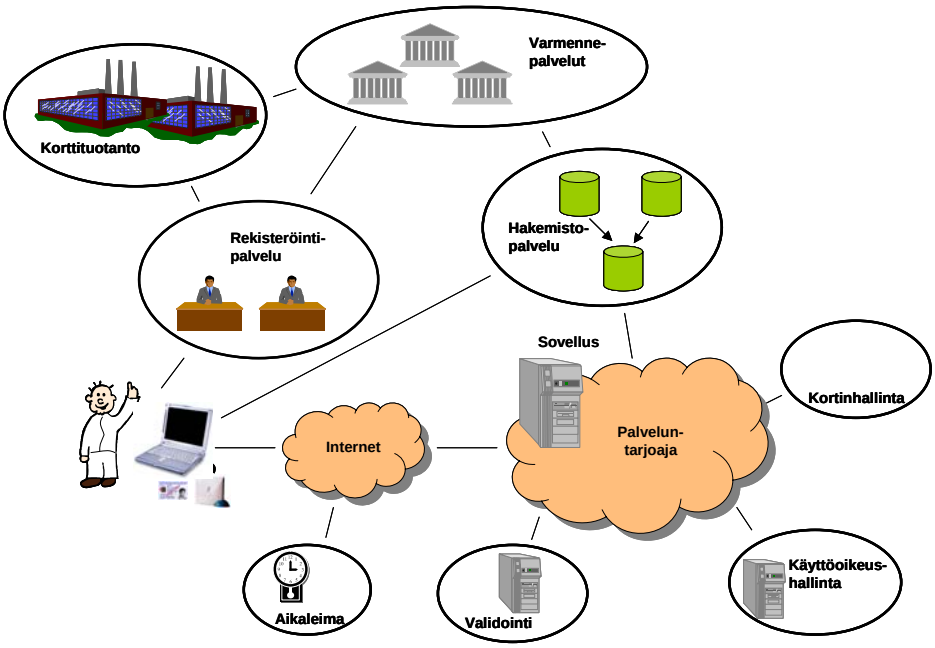
Näiden ääriratkaisujen ja kuvatun ”keskitien” välistä eroa voidaan kaventaa säätelemällä toimintokohtaisesti keskityksen/hajautuksen määrää, jolloin saadaan lukuisia eri variaatioita. Tähän valittujen kolmen vaihtoehdon tarkoitus onkin esitellä mahdollisuudet sekä niiden keskeiset vahvuudet ja heikkoudet.

Arkkitehtuuriehdotuksesta on pyritty laatimaan yhteensopiva ISOn alustavien terveydenhuollon PKI-määritysten (ISO/DTS 17090) kanssa.

8.1 Arkkitehtuurivaihtoehtojen yhteiset osiot

Koska osa PKI-toiminnoista kannattaa toteuttaa aina samalla tavalla riippumatta arkkitehtuurivaihtoehdon rakenteesta, on nämä eri arkkitehtuurivaihtoehdoille yhteiset määritykset kuvattu tässä luvussa (luku 8.1). Yhteiset määritykset voivat siis olla joko paikallisia tai kansallisia keskitettyjä toimintoja. Vaihtoehtoisia arkkitehtuureja kuvaavissa luvuissa (8.2.1, 8.2.2, 8.2.3) keskitytään kuvaamaan kuhunkin vaihtoehtoon liittyviä erityiskysymyksiä. Kuvaukset ovat toiminnallisia, eikä teknisiä toteutusratkaisuja ole syvällisesti pohdittu näiden mallien yhteydessä.

Alla (Kuva 8.1) on kuvattu laajennetun PKI-arkkitehtuurin toiminnalliset osakokonaisuudet sekä näiden väliset loogiset suhteet. Esitettäessä eri toteutusvaihtoehtoja otetaan näiden toimintojen sijaintiin kantaa.



Kuva 8.1 Laajennetun PKI-arkkitehtuurin osakomponentit.

8.1.1 Varmennepalvelut

CA-hierarkia

Arkkitehtuurivaihtoehtojen yleinen luottamusmalli perustuu oletusarvoisesti luotettujen varmentajien listaan. Listassa terveydenhuollon varmentajien lisäksi on luotettava mm. joukkoon yleisiä henkilövarmenteita myöntäviin varmentajiin, jotka toimivat potilaiden henkilövarmentajina.

Niissä arkkitehtuurivaihtoehdoissa, joissa on juurivarmentaja, on mahdollista tehdä ristiinvarmennus juurivarmentajan ja muiden luotettujen varmentajien välillä.

Varmenne

Alla olevassa taulukossa (taulukko 8.2) on lueteltu terveydenhuollossa tarvittavat keskeiset varmennetyypit. Henkilö- ja palveluvarmenteiden lisäksi tullaan tarvitsemaan teknisiä varmentajien välisiä varmenteita (itsensä tai toisen varmentajan allekirjoittama CA-varmenne tai ristiinvarmenne) sekä myöhemmin attribuuttivarmenteita varmenteiden haltijoiden lisätietojen käsittelyyn.

Tekniset varmenteet		
	Juuri-CA	
	Ala-CA	
	Ristiinvarmenne	
Henkilövarmenteet		
	Terveydenhuollon laillistettu ammattilainen	
	Muu terveydenhuollon työntekijä	
	Potilas	
	Tukiorganisaation työntekijä	
Palveluvarmenteet		
	Laite-/-sovellus-/-palvelu	
	Organisaatio	
Attribuuttivarmenteet		

Taulukko 8.2 Terveydenhuollossa käytettävät varmennetyypit

Henkilöllä voi olla useita rinnakkaisia varmenteita, jotka varmentavat julkisen avaimen, henkilöllisyyden sekä tarvittavia lisätietoja. Käytännössä henkilövarmenteen tietosisältö on syytä minimoida. Käyttäjiin liittyvät mahdolliset lisäattribuutit (lisämääreet) kannattaa yleensä hallita erikseen, sillä jokainen lisätieto lyhentää varmenteen elinikää ja lisää varmenteen perumisen todennäköisyyttä. Koska attribuuttivarmenteen käsite- ja toteutusstandardit eivät vielä ole riittävän stabiileja eikä ohjelmistotukea löydy, on perusteltua toteuttaa stabiilien roolitietojen käsittely joko osana henkilövarmennetta tai osana käyttöoikeushakemistoa. Terveydenhuollossa keskeisimmät henkilövarmenteeseen talletettavat roolitiedot ovat työsuhdetieto sekä laillistetun ammattilaisen status.

Kaikkien henkilövarmenteiden on syytä olla RFC-2459 -profiilin ja/tai laatuvarmennevaatimusten mukaisia X.509v3-varmenteita. Käyttäjäryhmät, jotka tarvitsevat sähköisiä laatuallekirjoituksia, voivat hankkia laatuvarmenteen lisäksi rinnakkaisia, organisaatiokohtaisia varmenteita, joiden sisältö noudattaa FINEID S4-2-määritystä tai muita tarvittavia (esimerkiksi sovelluskohtaisia) lisävarmenteita. Muille käyttäjäryhmille riittää laatuvarmenteen sijaan organisaatiokohtainen henkilövarmenne.

Sähköistä laatuallekirjoitusta on tarkoitus käyttää tilanteissa, joissa perinteisesti on vaadittu henkilökohtainen, käsin tehty allekirjoitus. Lainsäädännön ja osapuolten keskinäisillä sopimuksilla tai organisaation sisäisellä ohjeistuksella määritellään laatuallekirjoitusta edellyttävät tapahtumat tarkemmin. Esimerkkejä laatuallekirjoitusta vaativista toimenpiteistä voisivat olla potilaan antaman suostumuksen allekirjoitus, lääkärin kirjoittaman reseptin tai epikriisin allekirjoitus.

Varmenteen haltijan nimentä on tehtävä yksikäsitteisesti siten, ettei kahdella eri haltijalla ole samaa nimeä edes eri aikoina. Organisaation henkilöiden nimentään soveltuu esimerkiksi henki-

lönumero, edellyttäen että se on ainutkertainen. Henkilön yksikäsitteisen nimen perusteella on pystyttävä helposti yhdistämään varmenteesta saatava tieto sisäisiin käyttäjähakemistotietoihin. Laitteiden ja palveluiden yksilöintiin soveltuu esimerkiksi IP-osoite.

Koska terveydenhuollossa potilaan yksilöintitietona käytetään tyypillisesti henkilötunnusta, on potilaan varmenteen yksilöintitieto (kuten HST:n sähköinen asiointitunnus) voitava yhdistää henkilötunnukseen. Tämä yhdistäminen saadaan aikaan joko varmentajan tarjoaman lisäpalvelun (esimerkiksi Väestörekisterikeskuksen väestötietojärjestelmän palvelu) avulla tai rekisteröimällä potilaat ensimmäisen käyttökerran yhteydessä paikallisesti.

Henkilövarmenteet

Laillistetun ammatinharjoittajan varmenteen tulee olla laatuvarmenne ja siihen on talletettava esimerkiksi SV-numero ammattilaisstatuksen ilmaisemiseksi ja henkilön yksilöimiseksi. Ammattilaisten laatuvarmenteita myönnettäessä ammattilaisuusstatus tarkistetaan Terveydenhuollon Oikeusturvakeskuksen (TEO) ylläpitämästä rekisteristä. Laatuvarmenteen lisäksi ammattilaisella voi olla organisaatiokohtaisia lisävarmenteita, joiden avulla henkilö voidaan mm. yksilöidä ja tunnistaa työnantajansa edustajaksi.

Muiden terveydenhuollon työntekijöiden varmenteet voivat olla laatuvarmenteita tai organisaatiokohtaisia henkilövarmenteita. Varmenteen tyyppi riippuu mm. siitä, halutaanko varmennetta käyttää paikallisesti käyttöoikeuksien käsittelyyn vai pelkästään käyttäjän tunnistamiseen.

Potilaiden varmenteet ovat tyypillisesti peräisin terveydenhuoltosektorin ulkopuolelta, kuten Väestörekisterikeskukselta, pankeilta, Kansaneläkelaitokselta tai muilta suuria asiakasjoukkoja käsitteleviltä organisaatioilta. Näiden suhteen on laadittava yhteiset varmennepolitiikkavaatimukset, jotka ulkopuolisten varmentajien täytyy täyttää, jotta potilaan varmenne olisi hyväksyttävissä potilastietojen käsittelyssä. Laatuvarmenne on vaatimuksena silloin, kun potilaan antama suostumus allekirjoitetaan sähköisesti.

Tukiorganisaatioiden työntekijöiden varmenteet voivat olla ohjelmisto- tai toimikorttipohjaisia, ja paikallinen terveydenhuoltoyksikkö voi päättää, hyväksyykö se muiden myöntämiä varmenteita.

Laite/sovellus/palveluvarmenteella tarkoitetaan niitä varmenteita, joita käytetään esimerkiksi sovelluspalvelimen tai arkistopalvelun todentamiseen esimerkiksi SSL- tai IPSec-protokollilla.

Organisaatiovarmenne identifioi organisaation, ja sitä voidaan käyttää esimerkiksi sanomanvälityksessä tunnistautumiseen, tiedon salaukseen tai eheyden varmistamiseen, mikäli sovelluskohtaista varmennetta ei ole käytössä.

Varmennepolitiikka

Laatuvarmentajat noudattavat yleistä laatuvarmentamiseen tarkoitettua varmennepolitiikkaa, mutta terveydenhuollon varmentajahierarkian toteuttamiseksi on laadittava vähimmäisvaatimukset toiminnoille ja niiden turvallisuudelle (mukaan lukien rekisteröinti, kortinhallinta jne.), jotta ristiinkäytössä saavutetaan yhteinen turvataso.

Mikäli varmenteiden hyödyntämisessä tavoitellaan yhteistä turvatasoa terveydenhuoltosektorilla, on myös varmenteiden ja allekirjoitusten validoinnille laadittava yhteiset pelisäännöt minimivaatimuksineen.

8.1.2 Kortinhallinta

Toimikortti

Toimikorttia voidaan käyttää sekä potilaiden että ammattilaisten varmentamiseen. Kansainvälinen standardisointijärjestö ISO on määrittelee parhaillaan sekä potilaan toimikorttia (Patient Data Card, PDC) että terveydenhuollon ammattilaskorttia (Health Professional Card, HPC). Erillistä terveydenhuollon ammattilaiskorttia ei Suomessa ole tähän mennessä kuitenkaan suunniteltu. Satakunnan Makropilotti-hankkeessa on koekäytetty sähköistä Kela-korttia (ns. sosiaaliturvakorttia) sekä potilaiden, että ammattilaisten tunnistamisessa. Sosiaaliturvakortti käyttää tunnistamiseen liittyvissä toiminnoissa Väestörekisterikeskuksen varmennepalveluita. Tämä raportti ei

ota kantaa potilaan kortin ominaisuuksiin, joskin sähköisen kansalaiskortin (ns. HST-kortin) ja sosiaaliturvakortin ominaisuuksien yhdistäminen luultavasti edesauttaisi toimikorttien yleistymistä ja vähentäisi kokonaiskustannuksia. Potilaan asiakaskortin käyttöä ja hyväksymistä koskevat samat huomautukset kuin vastaavia varmenteita.

Hallituksen esityksessä laiksi sähköisestä allekirjoituksesta kehittyneen sähköisen allekirjoituksen tuottamiseksi edellytetään turvallisen allekirjoituksen luomisvälineen (ts. toimikortin) käyttöä. Mikäli tätä lakia voidaan soveltaa ja ryhdytään soveltamaan terveydenhuollossa, edellytetään toimikorttia niiltä terveydenhuollon toimijoilta, jotka omistavat laatuvarmenteita.

Suomessa laajalti hyväksytty periaate on se, että toimikorteille talletetaan mahdollisimman vähän tietoa ja kortin keskeisimmät käyttöalueet ovat käyttäjän todentaminen palveluun sekä kehittyneen sähköisen allekirjoituksen teko. Sähköinen allekirjoitus koskee erityisesti niitä käyttäjäryhmiä, joiden nykyiseenkin toimintaan kuuluu asiakirjojen allekirjoitus virkansa tai työtehtäviensä puolesta. Toimikorttia voidaan käyttää myös visuaalisen tunnistamisen välineenä tai sille voidaan tallettaa myös muita sähköisestä identiteetistä riippumattomia sovelluksia. Näin on laita mm. perinteisen muovisen Kela-kortin korvaavan sosiaaliturvakortin suhteen, Näihin lisäsovelluksiin ei tässä raportissa oteta kantaa.

Ammattilaisten ja potilaiden ohella voi olla perusteita varustaa myös muita käyttäjäryhmiä toimikortilla. Tällaisen kortin tarpeellisuus on paikallinen kysymys, joskin todennäköinen ratkaisu. Myös näiden korttien käytön tulee tapahtua varmennepolitiikan rajoissa.

Paikka- ja aikariippumattomuuden tukemiseksi kortille on voitava tallettaa henkilövarmenteen lisäksi myös joukko muita käyttäjän rooleihin sidottuja toissijaisia varmenteita. Näillä varmenteilla käyttäjä voi osoittaa sen roolin, jossa hän kyseisellä hetkellä toimii (esimerkiksi työsuhdetieto) tai mahdollisia sovelluskohtaisia tietoja (kuten ”Win2000 logon” -tiedot). Erityisesti tämä tarve nousee esille tilanteessa, jossa ammattilainen työskentelee usean eri terveydenhuoltoyksikön palveluksessa, joissa hyödynnetään tässä kuvattavaa PKI-teknologiaa ja joissa käytetään organisaatiokohtaisia varmenteita.

Organisaatiokohtaiset kortit ovat kortin myöntäneen organisaation omaisuutta. Työpaikan vaihtuessa työntekijän toimikortti vaihtuu, ja toisaalta hänellä on yhtä monta toimikorttia kuin on rinnakkaisia työsuhteita terveydenhuollossa. Usean organisaatiokortin (ja sitä kautta usean varmenteen) omistaminen aiheuttaa käytettävyysongelmia. Käyttäjän on mm. ymmärrettävä ja tiedettävä, mitä hänen varmenteistaan (tai korteistaan) kulloinkin tulee käyttää (vrt. prokura-oikeus perinteisissä allekirjoituksissa). Vastaavasti, kun lähetetään salattua tietoa, on lähettäjän kyettävä valitsemaan oikea salausvarmenne, joka perustuu esimerkiksi vastaanottajan rooliin tai työsuhdetietoon. Nämä toiminnot vaativat ohjelmistojen käyttöliittymiltä sellaisia ominaisuuksia, joita tätä nykyä ei välttämättä ole toteutettu yleisesti käytettävissä ohjelmistoissa.

Kortin vaihtuessa myös kortin haltijan yksityiset avaimet ja niitä vastaavat varmenteet vaihtuvat. Kortin vaihtuminen saattaa olla ongelma laillistettujen ammattilaisten allekirjoitusten arkistoinnin ja validoinnin osalta.

Toimikorttien tuottaminen voidaan toteuttaa paikallisesti kortin alustus- ja tulostuslaitteilla tai vaihtoehtoisesti ulkoistaa varsinaisille korttitoimittajille.

	Yleinen TH-kortti	Organisaatiokortti
Ammattilaiset	• Tarjoaa työsuhteista riippumattoman lainvoimaisen sähköisen allekirjoitusvälineen • Minimoi ammattilaisten korttimäärää • Tarvitaan joka tapauksessa yksityisille toimijoille ja niille organisaatioille, joilla ei ole omaa korttiratkaisua	• Useat mahdolliset rinnakkaiset työsuhteet saattaisivat johtaa useisiin organisaatiokortteihin käyttäjälle.
Muut toimijat	• Ei tarjoa luontevaa toimintamallia kortin myöntämiseen (ja hallinnointiin) muille toimijoille: muu oma henkilökunta, ulkopuoliset käyttäjät	• Useat mahdolliset rinnakkaiset työsuhteet saattaisivat johtaa useisiin organisaatiokortteihin käyttäjälle.
Yleiset näkökulmat	• Korttia ei voi käyttää visuaaliseen tunnistamiseen organisaation jäseneksi	• Tilapäiskorttien käsittely ratkaistava organisaation omalla ratkaisulla riippumatta TH-kortista • Uusien sovellusten lisääminen kortille helpompaa • Voi toimia visuaalisena tunnistimena

PKI-arkkitehtuurin näkökulmasta toimikortti on yksityisten avainten säilytysmedia, ja tässä raportissa ei oteta kantaa terveydenhuollon toimikorttien liikkeellelaskijoihin. Käytettävästä korttivaihtoehdosta riippumatta kortin teknisen ratkaisun tulisi mahdollisuuksien mukaan sallia myös lisävarmenteiden sijoittamisen kortille: vaikkapa terveydenhuollon ammattilaisen kortille (TH-kortille) sijoitettavat paikallisten organisaatioiden varmenteet ja organisaatiokortille talletettu laatuvarmenne.

Yllä olevaan taulukkoon on koottu eräitä korttipolitiikkaan vaikuttavia näkökohtia. Toimikortin jakelua ja hallinnointia on toisaalta tarkasteltava käyttäjien (ammattilainen/muut toimijat) ja toisaalta kortin myöntäjän (yleinen terveydenhuollon kortti/organisaatiokohtainen kortti) näkökulmasta. Erityistä terveydenhuollon ammattilaiskorttia ei tarvita siinä tapauksessa, että syntyy sähköisen allekirjoituslainsäädännön asettamat vaatimukset täyttävä kortti, jolle kyetään sijoittaa terveydenhuollon ammattilaisvarmenne.

Tilapäiskortit

Tilapäiskortteja tarvitaan muun muassa lyhytaikaisille sijaisille tai kun oma kortti on kadonnut, unohtunut kotiin tai vaurioituu äkillisesti. Tilapäiskorttien hallintaan on kiinnitettävä erityistä huomiota. Käytännössä paikallisissa työpisteissä (esim. osasto/klinikka) on oltava joukko personoimattomia kortteja, joista voidaan tuottaa korttinsa unohtaneille ja tilapäistyöntekijöille varten toimivia, lyhytaikaisia kortteja, joilla käyttäjä voi todentautua järjestelmiin, mutta joilla ei voi tehdä kehittyneitä sähköisiä allekirjoituksia.

8.1.3 Rekisteröintipalvelut

Rekisteripalvelun tärkein tehtävä on varmistaa, että oikea henkilö saa oikean varmenteen ja toimikortin. Toimikorttipohjaisia varmenteita luotaessa rekisteröijä (RA) tunnistaa käyttäjän, tarkistaa käyttäjätiedot ja välittää varmennehakemuksen korttitoimittajalle sekä luovuttaa valmiin kortin käyttäjälle. Ammattilaisten laatuvarmenteita myönnettäessä ammattilaisuusstatus tulee tarkistaa Terveydenhuollon Oikeusturvakeskuksen (TEO) ylläpitämästä rekisteristä.

Varmennehakemusten käsittely on paikallinen toiminto, jonka tarkka toiminta on määriteltävä varmennepolitiikassa, lukuun ottamatta laatuvarmenteita, joiden toimitusprosessin on noudatettava yleisiä säännöksiä. Laatuvarmenteita koskevan lainsäädännön soveltamisohjeiden tultua voimaan on erikseen selvitettävä laatuvarmenteen rekisteröintiprosessille asettamat vaatimukset sekä mahdollisuus toteuttaa ne terveydenhuollon palveluntuottajan toimesta.

Tukiorganisaatioiden työntekijöiden rekisteröinti, tunnistaminen ja varmenteen toimitusprosessi ovat paikallisia toimintoja, jotka palveluntuottaja voi itse määritellä.

Sulkulistapalvelut

Sulkulistapalvelu on osa rekisteröijän ja varmentajan yhteisiä tehtäviä, mutta sulkulistapalvelusta vastaavien henkilöiden käyttöoikeudet on pystyttävä rajaamaan vain varmenteen perumiseen. Varmenteen perumispyynnöt otetaan vastaan puhelimitse tai kirjallisesti ja perumistoiminnon on oltava käytössä 24 tuntia vuorokaudessa.

Sulkulista on varmentajakohtainen, ja se julkaistaan kyseisen varmentajan varmennehakemistossa, jonka osoite on talletettu varmenteisiin. Sulkulistojen hyödyntämisen helpottamiseksi on luotu järjestelmiä, jotka mm. keräävät sulkulistat yhteen paikkaan, josta käyttäjät voivat kysellä varmenteiden tilaa (ks. luku 8.1.5). Koska sulkulistan on oltava saatavilla keskeytymättömänä palveluna, täytyy hakemisto- ja CA-järjestelmän sekä verkkoratkaisujen täyttää korkean käytettävyyden palvelulle asetettavat vaatimukset luotettavuudesta, käytettävyydestä ja hallinnoinnista.

Sulkulistan julkaisutiheys ja sulkulistapalvelun tavoitettavuus määritellään osana varmennepolitiikkaa.

8.1.4 Hakemistopalvelut

Hakemistopalvelua käytetään mm. organisaation sisäisten käyttäjä- ja käyttöoikeustietojen sekä julkiseen käyttöön tarkoitettujen yhteys-, varmenne- ja sulkulistatietojen tallettamiseen ja jakeluun. Organisaation hakemistopalvelu koostuu paikallisista sisäisistä hakemistoista, yhteystietoja jakavasta julkisesta hakemistosta, mahdollisesta organisaatio- tai toimialakohtaisesta ”keskushakemistosta” sekä hakemistokokonaisuuden hallintaan tarkoitetuista metahakemistovälineistä.

On mahdollista, että osa paikallisista sovelluksista edellyttää varmenteiden paikallista talletusta sovelluskohtaisiin tietovarastoihin käyttöoikeuksien hallinnassa. Tällaisessa tapauksessa on tarvittavat varmenteet kopioitava muista hakemistoista paikallisiin hakemistoihin.

PKI-arkkitehtuurin näkökulmasta korostuu hakemistopalveluissa varmenne- ja sulkulistanäkökulma, jossa kullakin varmentajalla on oma hakemistonsa varmenteiden ja sulkulistojen julkaisemiseksi.

Yksi kansallisen tason tehtävistä on selvittää keskitetyn terveydenhuollon henkilöstön yhteystietohakemiston tarpeellisuus ja tarvittaessa määritellä kansallisen tason hakemistopalvelun sisältö, arkkitehtuuri ja sen toteutusratkaisut.

8.1.5 Lisäpalvelut

Lisäpalveluista aikaleima on luonteeltaan yleinen hyödyntäjistä riippumaton palvelu kun taas käyttäjä- ja käyttöoikeushallinta on kyseisen organisaation oma sisäinen toiminto. Validointipalvelun voi toteuttaa joko keskitettynä tai paikallisena palveluna, eikä sillä ole vaikutusta PKI-arkkitehtuurin muuhun rakenteeseen.

Aikaleima

Kaikki allekirjoitukset mitätöityvät ajan mittaan varmenteen peruutuksen, avaimen katoamisen, uuden teknologian, vanhenemisen tai muun syyn seurauksena. Aikaleimapalvelua käytetään takaamaan ”sopimusten” voimassaolo riippumatta varmenteiden perumisesta. Aikaleimaa voidaan käyttää tärkeiden tapahtumien, kuten allekirjoitettujen dokumenttien (lääkemääräys) tai järjestelmän lokitapahtumien (hoitotapahtuman ajankohta) varmistamiseen.

Aikaleiman on oltava varmennettu, jäljitettävissä ja jälkikäteen tarkistettavissa. Se sisältää yksikäsitteisesti ymmärrettävän ajankohdan ja alkuperäisen dokumentin tiivisteen allekirjoitettuna.

Koska aikaleiman standardointi on vielä kesken, eivät yleiset työasemaohjelmistot, kuten sähköposti tai www-selaimet tue sitä. Palvelinsovelluksiin sitä vastoin aikaleiman liittäminen on kohtuullisen helppoa.

Aikaleiman objektiivisuuden varmistamiseksi aikaleimapalvelu ja aika on syytä hankkia kolmannelta luotettavalta osapuolelta organisaation oman toteutuksen asemesta. Vastuuta hajauttamalla aikaleimaaja ei voi vaikuttaa käytettyyn kellonaikaan eikä aikaleiman pyytäjä itse aikaleimaan.

Varmenteen validointipalvelu

Koska varmenteen (ja allekirjoitusten yleensä) validointi ei ole helppo eikä kevyt tehtävä, on PKI:tä hyödyntävien organisaatioiden syytä harkita erityisten varmenteiden ja allekirjoitusten validointipalvelujen kehittämistä, joilla kyseisten näkökohtien lisäksi voidaan toteuttaa yhteistä tietoturvapolitiikkaa näiden toimintojen osalta. Validointipalvelun tulee myös tukea eritasoisia validointiprofiileja palvelemaan eri käyttötarkoituksia.

Validointipalvelu on varmentajaan verrattava luotettu palvelu, jonka tehtävä on tarkistaa haluttu tietoelementti pyydetyn profiilin mukaisesti ja vastata palvelun pyytäjälle, onnistuiko validointi vai ei. Teknisesti validointipalvelu sisältää allekirjoituksen, sulkulistan ja koko varmennepolun muodostamisen ja käsittelyn sekä halutun turvapolitiikan noudattamisen mainituissa tehtävissä. Validointipalvelujen toteuttamiseksi IETF on kehittänyt ja parhaillaan kehittää useita eri määrityksiä.

Käyttäjä- ja käyttöoikeushallinta

Ennen rooleja tukevien attribuuttivarmennemääritysten vakiintumista, on käyttäjän todentaminen sidottava henkilövarmenteeseen ja dynaamiset roolitiedot on syytä ainakin pääosin hallinnoida paikallisilla hakemistoratkaisuilla.

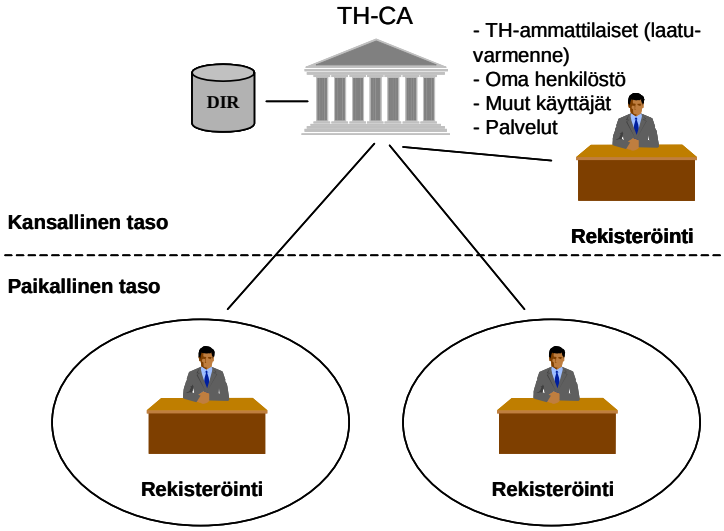
Varsinainen järjestelmäkohtainen käyttöoikeushallinta on täysin toiminto.

8.2 PKI-arkkitehtuurivaihtoehdot

PKI-arkkitehtuurin mahdolliset toteutusmallit sijoittuvat keskitetyn toteutuksen ja täydellisen hajautuksen väliin. Erilaisia teoreettisia vaihtoehtoja ja yhdistelmiä on suuri määrä. Tämän raportin tavoitteena on muotoilla suositusmalli sosiaali- ja terveydenhuollon PKI-arkkitehtuuriksi. Kolmea erilaista vaihtoehtoista ratkaisua tarkastellaan toimintojen hajautuksen suhteen. Näiden vaihtoehtojen analyysin pohjalta esitetään yhtä toteutusvaihtoehtoa jatkokehittelyn pohjaksi.

8.2.1 ”Keskitetty vaihtoehto”

Keskitetyssä arkkitehtuurivaihtoehdossa toteutetaan varmennepalvelut keskitetyllä kansallisella varmennus- ja hakemistopalvelulla. Varmenteet ja kortit myönnetään koko terveydenhuoltosektorille samojen pelisääntöjen perusteella ja keskitettyyn hakemistoon talletetaan käyttäjätietoja. Käyttäjien rekisteröinti ja toimikorttien jakelu toteutetaan paikallisina toimintoina.



Kuva 8.3 Keskitetty arkkitehtuurivaihtoehto.

Ratkaisun vahvuudet:

+ Yhteentoimivuus hyvä, koska vain yksi varmennepolitiikka.
+ Varmennepolun muodostaminen ja validointi yksinkertaista. Käyttäjän tarvitsee terveydenhuoltosektorin puitteissa luottaa vain yhteen varmentajaan.
+ Kokonaiskustannukset pienemmät kuin hajautetuissa malleissa.
+ Laatuallekirjoituksiin käytettyjen varmenteiden ja niitä vastaavien sulkulistojen arkistointi helposti järjestettävissä.

Ratkaisun heikkoudet:

– Keskitetty järjestelmä on jo alussa toteutettava riittävän massiivisena, jotta laajennettavuus on taattu käyttäjämäärän kasvaessa (ts. kustannusten etupainotteisuus).

- Yhden CA-järjestelmän ominaisuudet eivät välttämättä täytä kaikkien eri osapuolten erityisvaatimuksia etenkään tulevaisuudessa.
- Kustannustenhallinta ja -jako vaikeaa.
- Ei tue hyvin nykyistä suomalaista terveydenhuollon toimintamallia, jossa keskitetysti määritellään toiminnan vain yleiset suuntaviivat ja varsinaiset palveluntuottajat toteuttavat palvelunsa itsenäisesti yhteisen ohjeistuksen varassa.
- Paikallisten palveluntarjoajien toimintatapojen on oltava samat riippumatta toiminnan laajuudesta tai muista paikallisista olosuhteista.
- Arkkitehtuuri ei skaalaudu määritelmänsä mukaan useisiin varmentajiin. Mikäli ristiinvarmennuksia tehdään, menetetään osa vahvuuksista.
- Muutosten teko on hidasta ja niiden hallinta vaikeaa, koska vaikutukset ulottuvat moniin osapuoliin.
- Varmentajan yksityisen avaimen paljastuttua kaikki varmenteet ja kortit on uusittava.

8.2.1.1 Varmennepalvelut

CA-hierarkia

Keskitetyssä vaihtoehdossa terveydenhuollon toimialueelle perustetaan yksi keskitetty varmentajaorganisaatio, joka vastaa kaikkien terveydenhuoltosektorilla tarvittavien varmenteiden myöntämisestä. Laillistettujen ammattilaisten osalta varmentajan on täytettävä sähköisen allekirjoituslakiesityksen edellyttämät vaatimukset laatuvarmenteita myöntävälle varmentajalle.

Varmennepolitiikka

Koska kutakin varmennetyyppiä kohden terveydenhuollossa on vain yksi varmennepolitiikka ja yhdet tekniset määritykset, on yhteentoimivuuden aikaansaaminen helppoa. Toisaalta paikallisten tarpeiden toteuttaminen saattaa olla ylivoimaista osapuolten lukumäärän kasvaessa suureksi.

8.2.1.2 Kortinhallinta

Keskitetyn varmentajaorganisaation tulee tarjota palveluna korttituotanto- ja kortinjakelupalvelut laillistettujen ammattilaisten osalta yksityisille toimijoille sekä niille (pienille) organisaatioille, jotka eivät itse halua tai kykene toteuttamaan paikallisia toimintoja.

8.2.1.3 Rekisteröintipalvelut

Keskitetyn varmentajaorganisaation tulee toteuttaa rekisteröintipalvelut laillistettujen ammattilaisten osalta yksityisille toimijoille sekä niille (pienille) organisaatioille, jotka eivät itse halua tai kykene toteuttamaan paikallista rekisteröintiä.

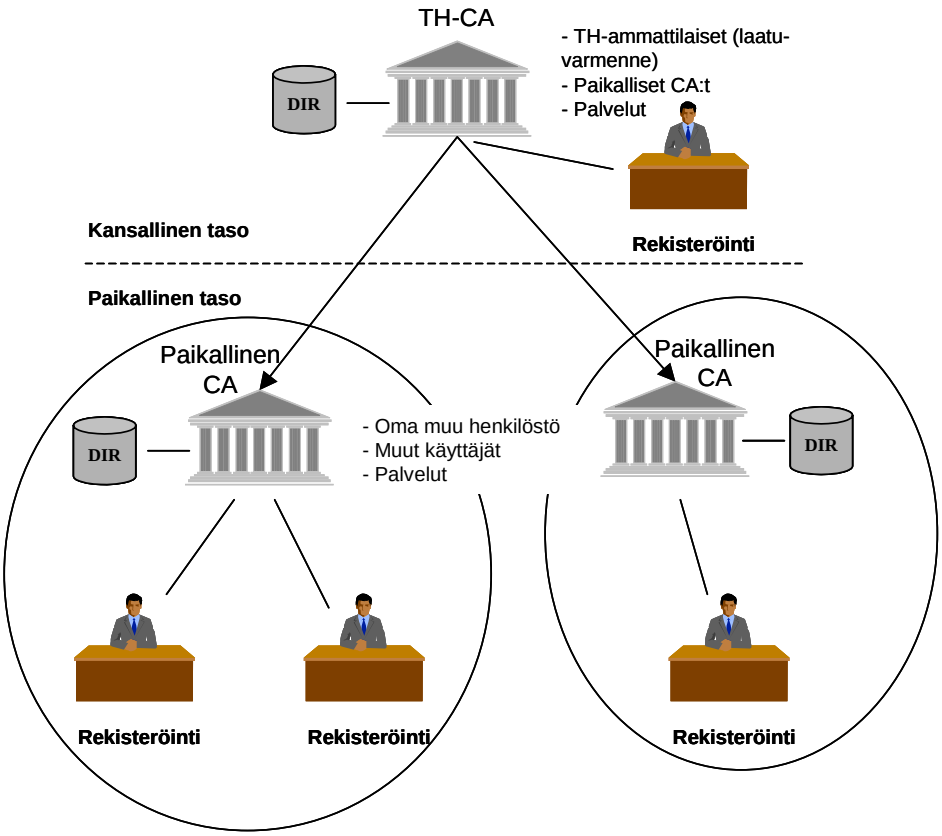
8.2.1.4 Hakemistopalvelut

Ei lisämäärityksiä.

8.2.2 ”Osittain keskitetty vaihtoehto”

Tässä arkkitehtuurivaihtoehdossa on toimintojen jaossa keskitettyihin ja paikallisiin pyritty noudattamaan pitkälle nykyisin käytössä olevaa työnjakoa terveydenhuollon henkilöiden työsuhteen ja ammatillisen statuksen määrittelyssä. Laillistettujen ammattilaisten henkilövarmenteet myönnetään keskitetysti, kun taas organisaatiokohtaisten varmenteiden myöntäminen tapahtuu paikallisella tasolla.

Keskitetyn juurivarmentajaorganisaation tulee tarjota palveluna varmenne- ja korttituotanto sekä rekisteröintipalvelut laillistettujen ammattilaisten osalta yksityisille toimijoille sekä niille (pienille) organisaatioille, jotka eivät itse halua tai kykene toteuttamaan paikallisia toimintoja.



Kuva 8.4 Osittain keskitetty arkkitehtuurivaihtoehto.

Arkkitehtuurin vahvuudet:

+ Varmennepolun muodostaminen ja validointi on helppoa. Käyttäjän tarvitsee terveydenhuoltosektorin puitteissa luottaa vain yhteen juurivarmentajaan.
+ Laatuallekirjoituksiin käytettyjen varmenteiden ja niitä vastaavien sulkulistojen arkistointi helposti järjestettävissä.
+ Jokainen palveluntuottaja voi lähteä liikkeelle suhteellisen itsenäisesti ja omalla tahdillaan omien palveluiden osalta.
+ Varmentajan yksityisen avaimen paljastuminen vaikuttaa ainoastaan kyseisen varmentajan myöntämiin varmenteisiin.
+ Uusien sisäisten palvelujen (esim. uusi sovelluskohtainen lisävarmenne) käyttöönotto on nopeaa. Yhteiskäyttöiset palvelut edellyttävät sopimista toisten osapuolten kanssa.
+ Kustannusten hallinta (mukaan lukien ulkoistamispäätökset) on suurelta osin organisaation omassa hallinnassa.

Arkkitehtuurin heikkoudet:

- Kokonaiskustannukset ovat suuremmat kuin keskitetyssä malleissa (ja pienemmät kuin hajautetussa).
- Yhteentoimivuuden aikaansaaminen edellyttää enemmän kontrollia kuin keskitetyssä vaihtoehdossa.

8.2.2.1 Varmennepalvelut

CA-hierarkia

Osittain keskitetyssä vaihtoehdossa terveydenhuollon toimialueelle ehdotetaan perustettavan yksi juurivarmentajaorganisaatio, joka vastaa laillistettujen ammattilaisten sekä paikallisten varmentajien varmentamisesta. Lisäksi juuri-CA voi tarjota mm. palvelu/palvelin-varmenteita terveydenhuoltosektorille. Laillistettujen ammattilaisten osalta varmentajan on täytettävä sähköisen allekirjoituslakiesityksen edellyttämät vaatimukset laatuvarmenteita myöntävälle varmentajalle.

Paikalliset organisaatiokohtaiset varmentajat puolestaan vastaavat henkilöstönsä varmentamisesta omaan henkilökuntaansa kuuluvaksi. Lisäksi paikalliset varmentajat myöntävät tarvittaessa varmenteita omille palveluilleen/palvelimilleen sekä sellaisille organisaatioon kuulumattomille henkilöille, joilla on tarve tunnistautua organisaation järjestelmiin. Organisaation myöntämiä varmenteita käytetään pääsääntöisesti käyttäjän todentamiseen ja käyttöoikeuksien määräytymiseen organisaation sisällä sekä sisäisiin allekirjoitustarpeisiin, joissa ei välttämättä edellytetä kehittynyttä sähköistä allekirjoitusta.

8.2.2.2 Kortinhallinta

Juurivarmentajaorganisaation tulee tarjota palveluna korttituotanto- ja kortin jakelupalvelut laillistettujen ammattilaisten osalta yksityisille toimijoille sekä niille (pienille) organisaatioille, jotka eivät itse halua tai kykene toteuttamaan paikallisia toimintoja.

8.2.2.3 Rekisteröintipalvelut

Juurivarmentajaorganisaation tulee toteuttaa rekisteröintipalvelut laillistettujen ammattilaisten osalta yksityisille toimijoille sekä niille (pienille) organisaatioille, jotka eivät itse halua tai kykene toteuttamaan paikallista rekisteröintiä.

8.2.2.4 Hakemistopalvelut

Kullakin varmentajalla on oma julkinen hakemistonsa varmenteiden ja sulkulistojen julkaisemiseksi.

Koska osa sovelluksista saattaa edellyttää varmenteiden paikallista talletusta sovelluskohtaisiin tietovarastoihin käyttöoikeuksien hallinnassa, on tarvittavat ammattilaisten varmenteet kopioitava keskitetystä hakemistosta paikallisiin hakemistoihin.

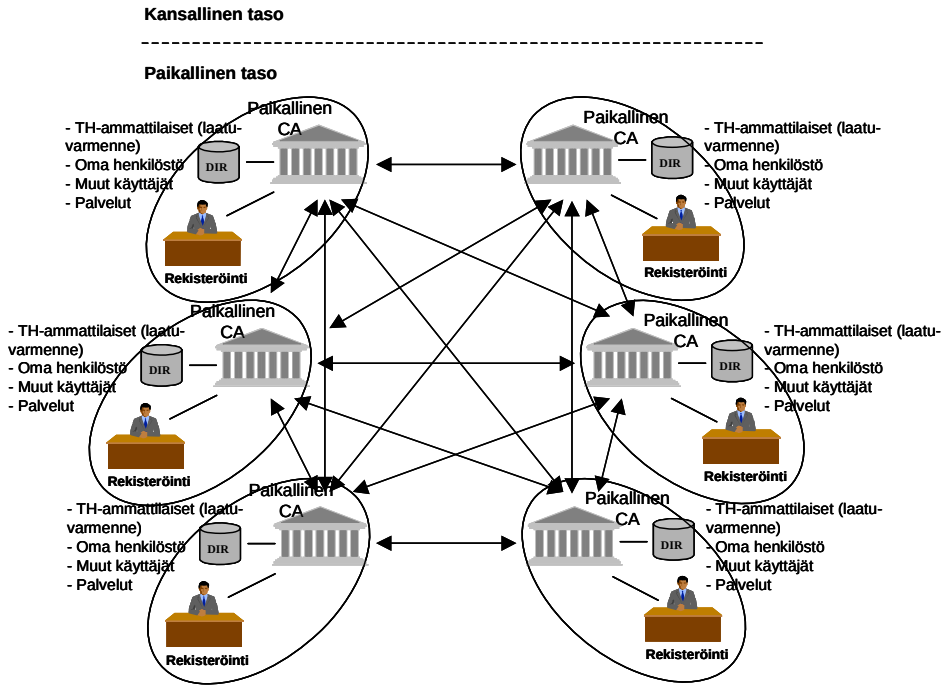
8.2.3 ”Hajautettu vaihtoehto”

Äärimmilleen hajautetussa arkkitehtuurivaihtoehdossa kaikki toiminnot hoidetaan paikallisesti. Jotta palveluiden ja varmenteiden ristiinkäyttö olisi mahdollista, on tässäkin vaihtoehdossa toimintojen täytettävä yhteisen varmennepolitiikkarungon minimivaatimukset.

Jotta laillistettujen ammattilaisten osalta yksityisille toimijoille sekä niille (pienille) organisaatioille, jotka eivät itse halua tai kykene toteuttamaan paikallisia toimintoja, voidaan tarjota varmenne-, korttituotanto-, rekisteröinti- sekä kortin jakelupalvelut, on löydettävä kaupallinen osapuoli tarjoamaan ym. palvelut.

Paikalliset varmentajat voivat ristiinvarmentaa toisensa ja näin helpottaa loppukäyttäjän työtä luotettavien varmentajien hyväksymisessä. Kunkin osapuolen tekemien ristiinvarmennusten lu-

kumäärä kasvaa neliöllisesti, jolloin 20 toimijan verkossa tulee tehdä lähes 400 ristiinvarmennusta.



Kuva 8.5 Hajautettu arkkitehtuurivaihtoehto.

Arkkitehtuurin vahvuudet:

+ Jokainen palveluntuottaja voi lähteä liikkeelle suhteellisen itsenäisesti ja omalla tahdillaan.
+ Varmentajan yksityisen avaimen paljastuminen vaikuttaa ainoastaan kyseisen varmentajan myöntämiin varmenteisiin. Muut varmentajat voivat perua ristiinvarmennukset.
+ Uusien sisäisten palvelujen (esim. uusi sovelluskohtainen lisävarmenne) käyttöönotto on nopeaa. Yhteiskäyttöiset palvelut edellyttävät sopimista toisten osapuolten kanssa.
+ Kustannusten hallinta (mukaan lukien ulkoistamispäätökset) on täysin organisaation hallinnassa.

Arkkitehtuurin heikkoudet:

– Jokaisen varmentajan tulee täyttää laatuvarmentajalle asetettavat tekniset ja toiminnalliset vaatimukset, jotka nostanevat järjestelmäkohtaiset kustannukset korkeiksi, jolloin kokonaiskustannukset nousevat korkeammiksi kuin keskitetymmissä malleissa.
– Varmentajien lukumäärän kasvaessa luottosuhteiden lukumäärä kasvaa hallitsemattomaksi. Nykyisin Suomessa on 20 sairaanhoitopiiriä ja suuri joukko yksityisiä palveluntuottajia.
– Varmennepolun muodostaminen ja validointi on hyvin vaikeaa (useat sovellukset eivät tue ristiinvarmennuksella aikaansaadun varmennepolun validointia).

- Hakemistojen välinen liikennöinti ja mahdollisesti siirrettävien tietojen ajantasaisuuden varmistaminen saattaa olla työlästä.
- Laatuallekirjoituksiin käytettyjen varmenteiden ja niitä vastaavien sulkulistojen arkistointi on kunkin varmentajan vastuulla, joten arkistokokonaisuuden hallinta on vaikeaa.

8.2.3.1 Varmennepalvelut

CA-hierarkia

Hajautetussa vaihtoehdossa kukin terveydenhuollon palveluntuottaja perustaa organisaatiokohtaisen varmentajan, joka vastaa omaan henkilökuntaan kuuluvien laillistettujen ammattilaisten ja muun henkilöstönsä varmentamisesta. Lisäksi paikalliset varmentajat myöntävät tarvittaessa varmenteita omille palveluilleen/palvelimilleen sekä sellaisille organisaatioon kuulumattomille henkilöille, joilla on tarve tunnistautua organisaation järjestelmiin. Laillistettujen ammattilaisten osalta varmentajan on täytettävä sähköisen allekirjoituslakiesityksen edellyttämät vaatimukset laatuvarmenteita myöntävälle varmentajalle.

Varmennepolitiikka

Kukin varmentaja ristiinvarmentaa toisensa tarjoten varmenteiden hyödyntäjille valmiit luottosuhteet. Tämä ristiinvarmennusverkko edellyttää varmentajilta yhteistä varmennepolitiikkaa erityisesti henkilövarmenteiden osalta. Paikalliseen käyttöön tarkoitetut varmenteet eivät ole yhteisten määritysten alaisia.

8.2.3.2 Kortinhallinta

Ei lisämäärityksiä.

8.2.3.3 Rekisteröintipalvelut

Ei lisämäärityksiä.

8.2.3.4 Hakemistopalvelut

Kullakin varmentajalla on oma julkinen hakemistonsa varmenteiden ja sulkulistojen julkaisemiseksi.

Koska osa sovelluksista saattaa edellyttää varmenteiden paikallista talletusta sovelluskohtaisiin tietovarastoihin käyttöoikeuksien hallinnassa, on tarvittavat varmenteet kopioitava (ja jaeltava) paikallisten hakemistojen välillä.

9. YHTEENVETO JA SUOSITUKSET

Sosiaali- ja terveydenhuolto on enenevässä määrin siirtymässä sähköiseen asiointiin ja palveluihin. Digitaalisen dokumentaation käyttöönoton myötä siirrytään myös tallentamaan potilas- ja asiakasdokumentaatiot digitaaliseen muotoon. Sähköinen asiointi tapahtuu sekä ammattilaisten että asiakkaan ja ammattilaisen kesken. Osa sähköisestä asioinnista on ammattilaisen ja tietokoneen välistä kommunikaatiota. Koska sosiaali- ja terveydenhuollon sähköisessä asioinnissa hyvin usein käsitellään asiakkaan/potilaan arkaluonteisia ja salassa pidettäviä tietoja, tulee asiointia tukevan tietojärjestelmän täyttää korkean luottamuksen ja tietoturvan vaatimukset.

Useiden sosiaali- ja terveydenhuollon asiakirjojen täytyy olla ammattilaisen allekirjoittamia. Karkeasti arvioiden nykyisin allekirjoitetaan pelkästään terveydenhuollossa vuosittain useita kymmeniä miljoonia asiakirjoja (mm. noin 1,2 miljoonaa hoitojaksokohtaista sairauskertomusta, 1,7 miljoonaa työterveyskertomusta sekä osa noin 31 miljoonasta perusterveydenhuollon käynnin dokumentaatiosta). Lisäksi allekirjoitetaan vuosittain lähes 37 miljoonaa reseptiä (joista 27 miljoonaa oikeuttaa Kela-korvaukseen). Määrä on sinällään suuri, mutta teknologia ei aseta esteitä niiden hoitamiseksi sähköisesti.

Suomalainen terveydenhuolto on eurooppalaisittainkin katsoen hyvin hajaantunutta. Sama koskee terveydenhuollon tietojärjestelmiä. Itsenäisiä kunta-, alue- tai piirikohtaisia tietojärjestelmiä on maassamme toista sataa käytössä. Moderni hoito ja palvelu edellyttää potilaan hoitamiseen tarvittavan tiedon saantia riippumatta siitä, missä se on teknisesti talletettuna. Kansallisen tason tavoitteena onkin näiden tietojärjestelmien yhteistoiminnallisuus ja kyky kommunikoida turvallisesti keskenään.

Tietoturvan ja tietosuojan samoin kuin potilaan antamien suostumusten ja tiedon luovuttamisen periaatteet eivät voi vaihdella alueiden ja kuntien välillä. Tarvitaan kansallisesti määritelty tietoturvapolitiikka ja siitä johdetut hyvän toiminnan säännöt, jotta voidaan taata potilaiden yhtenevä yksityisyyden suoja ja tietosuoja koko maassa.

***Tässä raportissa ehdotetaan PKI-arkkitehtuurin perustuvaa toteutusta sosiaali- ja terveydenhuollon sähköisen asioinnin tietoturvalliseksi alustaksi*. PKI-arkkitehtuuri mahdollistaa henkilöiden, toimintayksiköiden ja palvelinten luotettavan tunnistamisen, sähköisen allekirjoituksen, tukee digitaalista arkistointia ja mahdollistaa yhteisen tietoturvapolitiikan muodostamisen. Sen avulla voidaan myös hallita sähköisiä suostumuksia ja erilaisia rooleja. Edelleen PKI-järjestelmä mahdollistaa potilasasiakirjojen muuttumattomuuden ja kiistämättömyyden varmistamisen.**

9.1 Esitys sosiaali- ja terveydenhuollon kansalliseksi PKI-arkkitehtuurimalliksi

Kansalliseksi sosiaali- ja terveydenhuollon PKI-arkkitehtuuriksi esitetään kuvan 9.1 mukaista *kaksitasoista osittain hajautettua mallia.* Toteutus muodostuu yhdestä valtakunnan tason varmentajasta (valtakunnallinen CA) ja alueellista varmentajista (alueelliset CA't)..

Valtakunnallisen CA:n tehtävinä on

- Tietoturvapolitiikan muodostaminen ja ylläpito
- Alueellisten CA'den varmentaminen
- Ammattilaisten varmentaminen silloin, kun tarvitaan laatusertifikaattiin perustuvaa sähköistä allekirjoitusta (ts. allekirjoitetaan potilasasiakirjoja ja –dokumentteja sekä lääkemääräyksiä)
- Palveluntuottajien varmentaminen (julkiset ja yksityiset palveluntuottajat)
- Turvallisten arkistojen (sähköisten notariaattiarkistojen) varmentaminen
- Kansainväliset ristiinsertifioinnit

- Valtakunnallisten hakemisto- ja varmennepalvelujen tuottaminen
- Ammattilaisten, palveluntuottajien ja notariaattiarkistojen avainten pitkäaikaissäilytys

Paikallis- tai alueorganisaatioiden vastuulla on

- Vastata siitä, että alueellinen varmennepolitiikka vastaa kansallisia määrityksiä
- Hallita käyttöoikeuksia ja työsuhteita ja tuottaa niiden tarvitsemat tunnistamis- ja varmennepalvelut
- Tuottaa paikalliset ei laatusertifiointia edellyttävät allekirjoitus- ja varmennepalvelut henkilöille, järjestelmille ja ohjelmistoille
- Hallita dynaamisia rooleja ja tuottaa asiakirjoihin tieto kulloisestakin roolista tarvittaessa
- Ylläpitää alueellisia varmenne- ja hakemistopalveluja

Kansalaisen varmentaminen palvelujen käyttäjänä tai asiakkaana perustuu olemassa olevaan varmennejärjestelmään (esim. Väestörekisterikeskuksen HST- palvelut tai sosiaaliturvakortti). Mikäli pankit ryhtyvät tulevaisuudessa tarjoamaan pankkikorttiin kytkettyjä laatuvarmennepalveluja laajamittaisesti, on erikseen selvitettävä niiden tarjoamien varmenteiden mahdollinen soveltuvuus edellisten kanssa rinnakkaiseksi varmenteeksi.

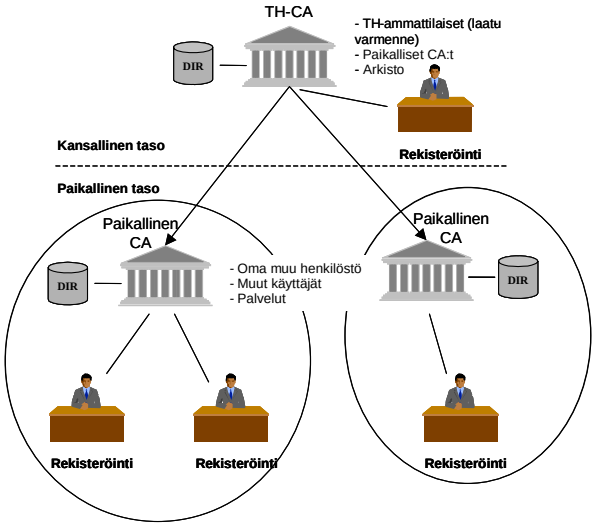
Tarvitaan kansalliset yhtenäiset ohjeet, joiden perusteella esimerkiksi laillistettujen ammattilaisten varmentaminen hoidetaan. **Tämän projektin johtoryhmä suosittaa, että laatuallekirjoitusten todentaminen suoritetaan aina luotettavasti keskitetystä hakemistosta ja sulkulistalta. Lisäksi organisaatiolle ja digitaalisille arkistoille (notariaattiarkistoille) tarvitaan laatuvarmenteen tasoinen valtakunnallinen varmennepalvelu**. Tämä kansallisesti yhtenäinen käytäntö ei estä aluetasoa laajentamasta varmenteiden käyttöä omissa ratkaisuissaan tai esimerkiksi käyttämästä bittivarmenteita omissa paikallisissa sovellutuksissaan.

Terveydenhuollon ammattilaisroolien julkaiseminen keskitettyyn julkiseen hakemistoon tai tietovarastoon on suotavaa, jotta kaikki osapuolet voisivat tarkistaa ammattilaisen juridiset oikeudet ammattilaisena. Julkaistavina tietoina suositellaan vähintään nimitietoa ja varmennetietoa.

Ryhmän näkemyksen mukaan niin kauan kuin attribuuttivarmenteiden standardisoituminen on kesken, voidaan palveluntuottajan alaorganisaatioiden tai ammattilaisten kulloisinkiin rooleihin liittyvät tiedot viedä paikallisesta tietojärjestelmästä allekirjoitettavan sähköisen dokumentin sisään ennen allekirjoitusta (ts. käyttää rooliin liittyvää bittivarmennetta tai ”softavarmennetta”).

Edelleen esitetään selvitettäväksi mahdollisuuksia korvata potilasasiakirjan laatuvarmenne määräajan kuluttua (esimerkiksi on kulunut 10 vuotta potilasdokumentin allekirjoituksesta) laatuvarmennetasoisella arkistovarmenteella.

Kansallisen CA'n olemassaolo takaa pienille organisaatioille ja yksityiselle sektorille yhtäläisen mahdollisuuden sovittaa toimintansa osaksi kokonaisterveydenhuollon palveluketjuja. Samalla se luo kansallisesti yhtenäisen toimintatapamallin yli alueellisten organisaatiorajojen.



Kuva 9.1 Esitys terveydenhuollon kansalliseksi arkkitehtuurimalliksi.

Esitetyn mallin tärkeimmät vahvuudet ovat:

- Tukee nykyistä suomalaista terveydenhuollon toimintamallia, jossa keskitetysti voidaan määritellä toiminnan suuntaviivat. Varsinaiset palveluntuottajat toteuttavat palvelunsa varsin itsenäisesti yhteisen ohjeistuksen varassa. Tällöin jokainen palveluntuottaja voi lähteä liikkeelle omalla tahdillaan omien palveluidensa osalta. Uusien sisäisten palvelujen (esim. uusi sovelluskohtainen lisävarmenne) käyttöönotto on nopeaa. Yhteiskäyttöiset palvelut edellyttävät sopimista toisten osapuolten kanssa.
- Kaikilla on mahdollisuus toteuttaa erityisvaatimuksensa ja järjestelmänsä haluamillaan välineillä.
- Varmennepolun muodostaminen ja validointi on helppoa. Käyttäjän tarvitsee terveydenhuoltosektorin puitteissa luottaa vain yhteen juurivarmentajaan.
- Laatuallekirjoituksiin käytettyjen varmenteiden ja niitä vastaavien sulkulistojen arkistointi helposti järjestettävissä.
- Malli tukee yksityisiä toimijoita ja niitä organisaatioita, jotka eivät itse halua tai kykene toteuttamaan tarvittavia toimintoja.
- Kustannusten hallinta (mukaan lukien. ulkoistamispäätökset) on suurelta osin organisaation omassa hallinnassa

Kuvassa 9.2 on hahmoteltu, miten ehdotetussa PKI-arkkitehtuurissa toiminnot jakautuisivat valtakunnallisen ja alueellisen tason kesken.

Kuva 9.2 PKI-toimintojen jako kansallisiin ja alueellisiin/paikallisiin tehtäviin

Varmentamiseen liittyvät perustehtävät on jokaisen varmenteita myöntävän organisaation itse hoidettava. Esitetyssä mallissa näiden ohelle jää paikallis- tai aluetasolla ratkaistavaksi työsuhteeseen ja järjestelmien käyttöoikeuksiin liittyen hallinnointi. Käyttäjien todentaminen on myös tällaisten organisaatioiden vastuulla, koska tiedon luovuttaja on vastuussa tietopyynnön tekijän ja tämän oikeuksien todentamisesta. Kansallinen varmennepolitiikka ja yhtenäiset kansalliset ohjeet aluetason organisaatioille täytyy tehdä keskitetysti. Ammattilaisroolia, oikeutta toimia lääkärinä, hallitaan jo nyt keskitetyssä rekisterissä (terveydenhuollon oikeusturvakeskuksen Terhikki-järjestelmä) eikä tämän toiminnon muuttamista nähdä tarpeelliseksi. Alueellinen rooli voi olla esimerkiksi sairaanhoitopiirillä. Paikallisen tason ratkaisuista voi vastata sairaala tai terveyskeskus, työterveyshuollon organisaatio tai yksityinen palvelujentuottaja. Yksityiset ja pienet terveydenhuoltoalan yksiköt voivat ostaa palveluita kansallisesti ohjatuilta palveluntarjoajilta.

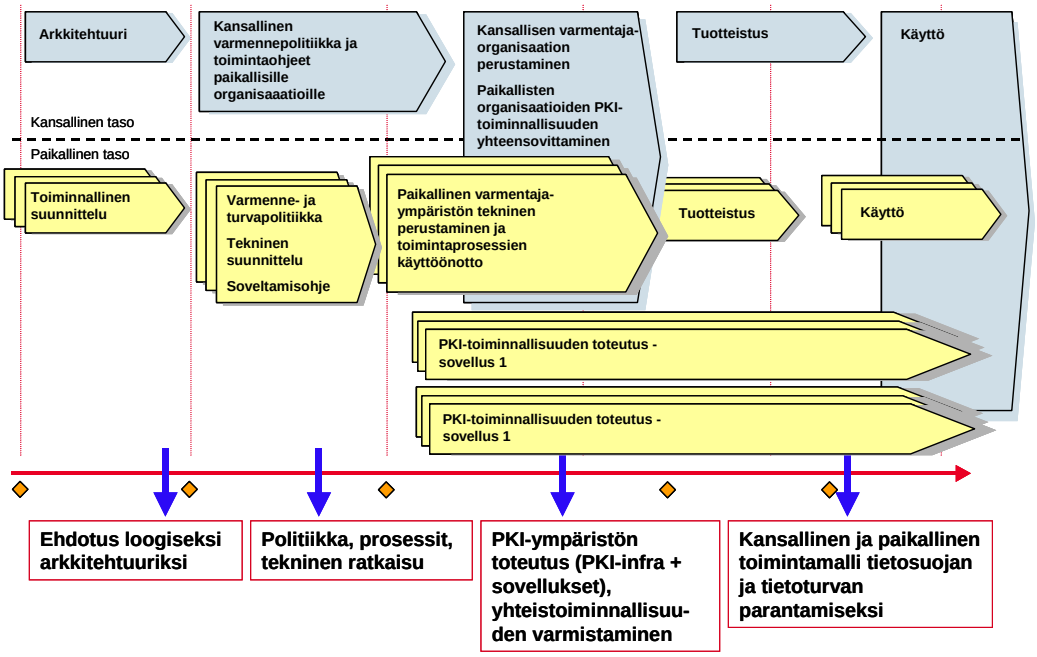
9.2 Ehdotuksia jatkotoimiksi

Tästä raportista annettujen kommenttien perusteella on jatkossa selvennettävä seuraavia seikkoja:

- Dedikoidut PKI-SIM kortit ovat yleistymässä ja niiden avulla tapahtuva "matkapuhelin tunnistus" on perusteltua integroida osaksi PKI-arkkitehtuuria.
- Roolivarmenteet voidaan katsoa myös henkilövarmenteiksi ja siten EU:n direktiivin mukaiseksi laatuvarmenteeksi (Väestörekisterikeskus). Roolivarmenteen, jota voidaan kutsua

myös "työvarmenteeksi", ei tarvitse olla sekundaarivarmenne. Väestörekisterikeskus tulee tuottamaan tulevaisuudessa mm. sisäasiainministeriön määrittelemiä "virkavarmenteita". Terveydenhuollossa voidaan erotella useamman tasoisia rooleja ja niihin liittyviä varmenteita. Ammatinharjoittajan laillistaminen luo hänelle pysyväluonteisen roolin. Toisaalta ammatinharjoittajalla voi olla yhdenkin päivän aikana useita paikallisia dynaamisesti muuttuvia rooleja. Tämä raportti ehdottaa työnjakoa, jossa kansalaisvarmenne liittyy henkilön yksityisyyteen ja ammattivarmenteita käytetään työtehtävissä. Ammattivarmenteet puolestaan jaetaan laatuvarmennetasoiseen roolivarmenteeseen, jota kansallinen CA hallinnoi, ja paikallisen CA'n hallinnoimaan sekundaariseen ja dynaamiseen roolivarmenteeseen. Jatkotyössä on tarkennettava eri roolivarmenteiden työnjakoa.

- On keskusteltava, mikä on valtakunnallisen CA:n allekirjoitusten suhde alueellisiin varmentajiin. On päätettävä, haluaako valtakunnallinen CA allekirjoittaa alueellisen CA:n varmenteen ja ottaa vastuulleen alueellisen CA:n olemassaolon oikeutuksen vai halutaanko sitä, että valtakunnallinen CA vastaa myös alueellisen varmentajan tuottamista varmenteista. Tätä raporttia kirjoitettaessa on ollut lähtökohtana ensin mainittu vaihtoehto.
- On synnytettävä mekanismi, jolla voidaan varmistaa se, että alueelliset CA't noudattavat valtakunnallista ja omaa varmennepolitiikkansa.
- Selvitetään onko tarvetta alueellisten CA'n omien varmenteidensa ristiinvarmennukseen.
- Varmenneketjujen (esim. alueellinen CA, Terveydenhuollon-CA ja VRK) toiminta revokointilistojen tarkastustilanteissa on kuvattava.
- Alueellisten ja valtakunnallisten varmennehakemistojen yhteiskäyttöä tulee kuvata yksityiskohtaisesti. Siinä yhteydessä tulee selvittää mahdollisuus kopioida varmennehakemistoja alueelliselle tasolle.



Kuva 9.3 PKI-arkkitehtuurin toteutuksen etenemissuunnitelma

9.3 Muut ehdotut jatkotoimet

1. Varsinainen PKI-järjestelmä voidaan rakentaa vasta varmennepolitiikan vaatimusten perusteella. Siksi on kansallisella tasolla *aloitettava varmennepolitiikan laatiminen sekä kansallisten pelisääntöjen ja ohjeiden laatiminen paikalliselle tasolle*. Mikäli varmenteiden hyödyntämisessä tavoitellaan yhteistä turvatasoa, on myös varmenteiden ja allekirjoitusten validoinnille laadittava yhteiset pelisäännöt ja vähimmäisvaatimukset. Lisäksi on määriteltävä, miten hallinnoidaan ja auditoidaan eri varmennepolitiikat, jotta kaikkien varmentajien luotettavuus ja laadun minimikriteerien noudattaminen voidaan varmistaa. Samalla on sovittava ristienvarmentamismenettelyn toteuttamisesta.
2. Stakesin tietoteknologian osaamiskeskuksen kokonaishankkeen (Sosiaali- ja terveydenhuollon sähköisten tietoverkkopalvelujen ja -asioinnin yhteistoiminnallinen arkkitehtuuri) muiden osaprojektien tulokset saattavat vaikuttaa tässä esitettyihin ratkaisuihin (esim. sähköinen allekirjoituslainsäädäntö ja sähköinen arkistointi). Nämä vaikutukset tulee huomioida kansallista varmennepolitiikkaa laadittaessa.
3. Edelleen on sovittava keskitettyjen toimintojen haltuunottajat ja vastuunjako niiden välillä. Tärkeää on myös määritellä taho, joka vastaa näiden toimintojen jatkosuunnittelusta ja toteutuksesta.
4. Kansallisen tason varmenneorganisaation perustaminen on järkevää toteuttaa samalla testaten eri organisaatioiden välistä PKI-yhteistoiminnallisuutta.

9.4 Lopuksi

Vaikka tässä esitetyn PKI-arkkitehtuurin rakentaminen aloitettaisiin jo vuonna 2002, kuluu kansallisen palvelun käyttöönottoon arviolta 2-3 vuotta. *Vuoden 2004 aikana tulisi kuitenkin olla käytössä terveydenhuollon varmennepalvelu ammattilaisten osalta*. Paikallisesti rajoitettuun käyttöön voidaan päästä huomattavan nopeasti, kun kansalliset pelisäännöt ja ohjeet ovat olemassa.

Paikallisella tasolla voidaan aloittaa määrittelemällä toimintasuunnitelmat, luomalla varmennepolitiikka ja toteuttamalla arkkitehtuurimalli. Kun rakennetaan kansallista mallia tukeva PKI-pohjainen ympäristö, on luontevaa sovittaa prosessit valtakunnallisten ohjeiden mukaisesti ja hioa yhteen yhdessä muiden järjestelmien kanssa.

Lyhenteitä

API	Application Programming Interface
CA	Certification Authority, Varmentaja
CEN	European Committee for Standardization
CENELEC	European Committee for Electotechnical Standardization
CP	Certificate Policy, Varmennepolitiikka
CPS	Certification Practice Statement, Varmennekäytäntö
DIR	Directory, Hakemisto
EEMA	European Forum for Electronic Business
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
FAR	False Acceptance Ratio
FINEID	Finnish Electronic Identification
HST	Henkilön sähköinen tunnistaminen
ICTSB	Information and Communications Technologies Standards Board
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
IP	Internet Protocol
IPSec	IP Security Protocol
LDAP	Lightweight Directory Access Protocol
OECD	Organization for Economic Co-Operation and Development
PIN	Personal Identification Number
PKCS	Public Key Crypto Standards (by RSA Labs)
PKI	Public Key Infrastructure, Julkisen avaimen järjestelmä
PKIX	PKI X.509
PUK	PIN Unblocking Key
QC	Qualified Certificate, Laatuvarmenne
RA	Registration Authority, Rekisteröijä
RFC	Request For Comments
RSA	Julkisen avaimen epäsymmetrinen algoritmi (Rivest-Shamir-Adelman)
SSL	Secure Sockets Layer
SV-numero	
TEO	Terveydenhuollon Oikeusturvakeskus
TH	Terveydenhuolto
TTP	Trusted Third Party, Luotettu kolmas osapuoli
VRK	Väestörekisterikeskus
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
WML	Wireless Mark-up Language
WTLS	Wireless Transport Layer Security
WPKI	Wireless PKI
X.500	X.500 hakemistopalvelu. ITUn ja ISOn määrittelemä hakemistostandardi
XML	Extensible Mark-up Language