RAPORTEJA

PEKKA RUOTSALAINEN

Suositukset terveydenhuollon asiakastietojen tietoturvalliselle sähköiselle arkistoinnille

Usean toimintayksikön yhteinen käyttäjän ja käyttöoikeuksien hallinta – periaatteet ja suositukset

STAKES

Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus

postimyynti: Stakes / Asiakaspalvelut PL 220, 00531 Helsinki
puhelin: (09) 3967 2190, (09) 3967 2308 (automaatti)
faksi: (09) 3967 2450 • Internet: www.stakes.fi

Taitto: Ursula Cornér

ISBN 951-33-1687-4 (paperimoniste)
ISSN 1236-0740
ISBN 951-33-1688-2 (verkkokirja)
ISSN 1795-8210

Stakesin monistamo
Helsinki 2006

Tiivistelmä

Pekka Ruotsalainen: Suositukset terveydenhuollon asiakastietojen tietoturvalliselle sähköiselle arkistoinnille/Usean toimintayksikön yhteinen käyttäjän ja käyttöoikeuksien hallinta - periaatteet ja suositukset. Stakes Raportteja 4/2006, 76 sivua. Hinta 17 euroa. ISBN 951-33-1687-4.

Terveydenhuollon toimintayksiköissä on parhaillaan käynnissä sähköisten potilaskertomusten ja potilaskertomusjärjestelmien laajamittainen käyttöönotto. Kansallisella tasolla on asetettu tavoitteeksi varmistaa näiden sähköisten dokumenttien saatavuus 24h/7d talletuspaikasta riippumatta koko niille säädetyn säilytysajan. Nämä tavoitteet edellyttävät, että kaikki toimintayksiköt toteuttavat digitaalisessa muodossa olevien asiakastietojen sähköisen arkistoinnin lainmukaisesti ja tietoturvallisesti.

Sähköinen arkistointi tulee ymmärtää laajempana kokonaisuutena kuin vain yhden toimintayksikön tietojen tallentamisena. Sähköinen arkisto voi ottaa vastaan, tallettaa ja jakaa usean eri toimintayksikön tietoja. Se voidaan toteuttaa paikallisena, alueellisena tai valtakunnallisena. Tällaisen arkiston tulee pystyä käsittelemään ja luovuttamaan tietoturvallisesti eri rekisterinpitäjien, eri käyttötarkoituksiin kerättyjä ja eri suojaustasoja vaativia tietoja.

Tämä raportti suosittelee, että terveydenhuollon asiakastietojen sähköisen arkistoinnin toimintaperiaatteeksi ratkaisua, jossa arkistoidut asiakastiedot (esim. potilasasiakirjat) säilytetään arkistossa rakenteisina dataobjekteina siten, että arkisto takaa niiden muuttumattomuuden ja samalla arkisto kykenee vastaanottamaan ja hallinnoimaan terveydenhuollon toimintayksikön tai muun toimijan lähettämiä asiakastietojen päivityksiä. Arkiston tulee kyetä jakamaan aktiivisesti arkistoituja asiakastietoja dataobjekteina. Tällaista arkistoa voidaan kutsua aktiivisia dokumentteja arkistoivaksi passiiviseksi arkistoksi.

Kansallisesti on parhaillaan käynnissä useita toisiinsa sovitettavia projekteja jotka joko määrittävät tai ottavat osaltaan kantaa terveydenhuollon asiakastietojen sähköiseen talletukseen. Sosiaali- ja terveysministeriössä on valmisteilla laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Samaten potilasasiakirja-asetusta ollaan uudistamassa. Kansallisen terveyshankkeen raportissa ”Ehdotus sähköisten potilaskertomusten viranomaismäärityksiksi” ja siitä saaduissa lausunnoissa on sekä otettu kantaa sähköiseen arkistointiin että tehty lukuisia kehittämisehdotuksia. Sähköisen potilaskertomushankeen ARKKI-ryhmän loppuraportissa on tehty ehdotus keskitetyn valtakunnallisen sähköisen potilaskertomusarkiston toiminnallisiksi vaatimuksiksi.

Edellä kuvattujen raporttien ja ehdotusten harmonisointityö samoin kuin lainsäädännön uudistamistyö on vielä kesken. Siksi tämä raportti keskittyy määrittämään terveydenhuollon asiakastietojen sähköisen arkistoinnin yleiset vaatimukset riippumatta arkistoinnin teknisestä tai organisatorisesta toteutustavasta. Tämä ohje ei myöskään ota kantaa arkistoinnin arkkitehtuurisiin malleihin,

fyysisiin toteutustapoihin ja tekniikoihin, joilla esitetyt vaatimukset toteutetaan. Raportin suositukset on pyritty laatimaan siten, että ne mahdollisimman hyvin noudattaisivat kansainvälisiä standardeja.

Tässä dokumentissa käytetään arkisto termin asemasta käsitettä arkistointi. Tällä halutaan korostaa sitä, että varsinainen sähköinen arkisto on aina osa laajempaa toiminnallista ja tietoteknistä kokonaisuutta.

Tämä dokumentti on osa kansallisen terveyshankeen sähköisen potilaskertomuksen käyttöönottoprojektia ja se on tuotettu Sosiaali- ja terveysministeriön ja Stakesin yhteisrahoituksella.

Sisällys

Suositukset terveydenhuollon asiakastietojen tietoturvalliselle sähköiselle arkistoinnille

Tiivistelmä

1. Rajaukset 7

2. Johdanto 8

2.1 Lainsäädännöstä johtuvia vaatimuksia 8
2.2 Sähköisen arkistoinnin ominaisuuksia 10

3 Sähköinen arkisto ja potilastieto- järjestelmät 12

3.1 Arkisto ja arkistointi 12
3.2 Tiedon sähköisen arkistoinnin ja varmuus- kopioinnin suhde 13
3.3 Arkistoivan tietojärjestelmän elementit 13
3.4 Arkistoivan tietojärjestelmän tyypit 15
3.5 Sähköisen potilastietojärjestelmän ja eArkiston yhteistoiminta 15

4 eArkiston toimintaympäristö 17

5 eArkiston tehtävät ja vastuut 18

5.1 Terveydenhuollon sähköisen arkiston perustehtävät 19
5.2 Terveydenhuollon tietoja arkistoivan organisaation vastuut 21

6 Tietoturvallisuus ja tietosuoja 23

7 Suositukset tietoturvalliselle sähköiselle arkistoinnille 24

7.1 Etukäteissuunnittelu 25
7.2 Arkistointipolitiikka 25
7.3 Infrastruktuuri 26
7.4 Tietoturvapolitiikka 26
7.4.1 Tiedon saatavuuden ja käytettävyyden turvaaminen 27
7.4.2 Tiedon muuttumattomuuden turvaaminen 28
7.4.3 Tiedon luottamuksellisuuden turvaaminen 29
7.5 Tietosuojapolitiikka 31
7.5.1 Suostumusten hallinta 32
7.6 Arkistoinnin tietomalli ja metatiedot 32
7.6.1 Tiedon luokittelu ja merkitseminen 33
7.7 Tiedon luovutuksen hallinta 34
7.8 Tiedon löytämisen palvelut 34
7.9 Arkistoitujen tietojen käyttö omassa toiminnassa 34
7.10 Toimintayksiköiden erillään pitäminen 34
7.11 Henkilötietolain mukainen tarkastuspyyntö 34
7.12 Lokitietojen tarkistaminen 35
7.13 Aikaleimapalvelut 35

8 Käsitteet ja termit 36

9 Tausta-aineisto 41

LIITTEET

Liite 1 POKA ryhmän ehdotus terveydenhuollon kansalliseksi tietojärjestelmä-arkkitehtuuriksi 43
Liite 2 Terveydenhuollon sähköisen arkistoinnin toteuttamisen yhteydessä huomioon otettavaa lainsäädäntöä 44
Liite 3 Aktiivinen arkisto 46
Liite 4 Sähköisen arkistoinnin tietomalli (OAIS-malli) 47
Liite 5 Arkistotyypit 48
Liite 6 Tiedon elinkaaren hallinta pitkäaikaisessa sähköisessä arkistoinnissa .. 49

Usean toimintayksikön yhteinen käyttäjän ja käyttöoikeuksien hallinta - periaatteet ja suositukset 50

Tiivistelmä 52

1 Johdanto 53

1.1 Yliorganisatoriset hoito- ja palvelumallit 54

2 Käyttöoikeuksien hallinnan malleja 57

2.1 Salasanojen ja käyttöoikeuksien antaminen toimintayksikön ulkopuolisille 57
2.2 Käyttöoikeuksien delegointimalli (Delegation Model) 58
2.3 Valvontamalli (Control Model) 59
2.4 Dokumenttimalli (Document Model) 59
2.5 Politiikkamalli (Policy Model) 60
2.6 Roolimalli (Role Model) 60
2.7 Tiedon etäisyysmalli (Information Distance Model) 61
2.8 Käyttöoikeuksien ja käytön hallinnan malli (Privilege Management and Access Control – PMAC- Model) 61
2.9 Mallien yhdisteleminen 62

3 Käyttäjän ja käyttöoikeuksien hallinnalle asetettavia vaatimuksia 63

4 Usean toimintayksikön yhteisen käyttäjän ja käyttöoikeuksien hallinnan toteuttamis- tapoja 64

4.1 Jaettuun LDAP- hakemistoon perustuva malli 64
4.2 PMI-malli (Privilege Management Infrastructure Model) 65
4.3 Identiteetin hallintamenetelmä (Identity Manage- ment Method, IM) 67
4.4 PKI- ja PMI-järjestelmät terveydenhuollon toiminta- yksiköiden välisessä tiedonvaihdossa 69

5 Suositus usean toimintayksikön yhteiseksi käyttäjien ja käyttöoikeuksien hallinnan kansalliseksi ratkaisuksi 70

6 Käsitteet 72

7 Viitteet ja lähteet 75

1. Rajaukset

Terveydenhuollon sähköisen arkistoinnin toteutukseen ja arkistoinnille asetettaviin vaatimuksiin vaikuttavat mm. vielä valmisteluvaiheessa oleva sosiaali- ja terveydenhuollon sähköisen asioinnin laki, potilasasiakirja-asetuksen uudistamistyö ja kansallisen terveydenhuollon tietojärjestelmä-arkkitehtuurin täydentyminen. Näistä syistä tämän raportti keskittyy määrittämään terveydenhuollon asiakastietojen tietoturvallisen sähköisen arkistoinnin yleiset vaatimukset riippumatta arkistoinnin toteutustavasta. Tämä ohje ei myöskään pyri ottamaan kantaa valittavaan arkistomalliin, sähköisen arkiston tietotekniseen toteutustapaan eikä niihin tietoturva- ja tietosuojatekniikoihin, joilla tässä dokumentissa esitetyt vaatimukset toteutetaan.

Tässä dokumentissa on esitetty vaatimukset ja suositukset terveydenhuollon tietojen lainmukaiselle ja tietoturvalliselle sähköiselle arkistoinnille. Esitetyt suositukset koskevat asiakastietojen sähköistä arkistointia riippumatta siitä, tapahtuuko se osana tosiaikaisen potilastietojärjestelmän toimintoja, erillisessä hajautetussa tai keskitetyssä arkistossa.

Tämä dokumentti ei määrittele:

- kansallista tietojärjestelmäarkkitehtuuria, joka on määritelty Sosiaali- ja terveysministeriön (STM) POKA-ryhmän raportissa Terveydenhuollon valtakunnallisen tietojärjestelmäarkkitehtuurin periaatteet. Alueellisista ratkaisuista kansalliseen kokonaisuuteen (STM: Selvityksiä 2006:8), liite 1.
- kansallista sähköisen arkistoinnin tietojärjestelmäarkkitehtuuria
- sähköisen arkiston ja potilastietojärjestelmän yhteistoiminnallista tietomallia
- arkistoinnin tietoteknistä toteutusta
- keskistetyn kansallisen arkiston ja potilastietojärjestelmien yhteistoiminnallisuutta
- arkistoitujen tietojen hakemistoja ja hakupalvelua
- arkiston käyttötapoja ja - prosesseja. Näiden osalta viitataan STM:n ARKKI-ryhmän loppuraporttiin (Eronen, H. et. al. Kansallinen sähköinen potilastietojen arkistopalvelu, Toiminnallinen määrittely, STM:n työryhmämuistioita 2005:21)

2. Johdanto

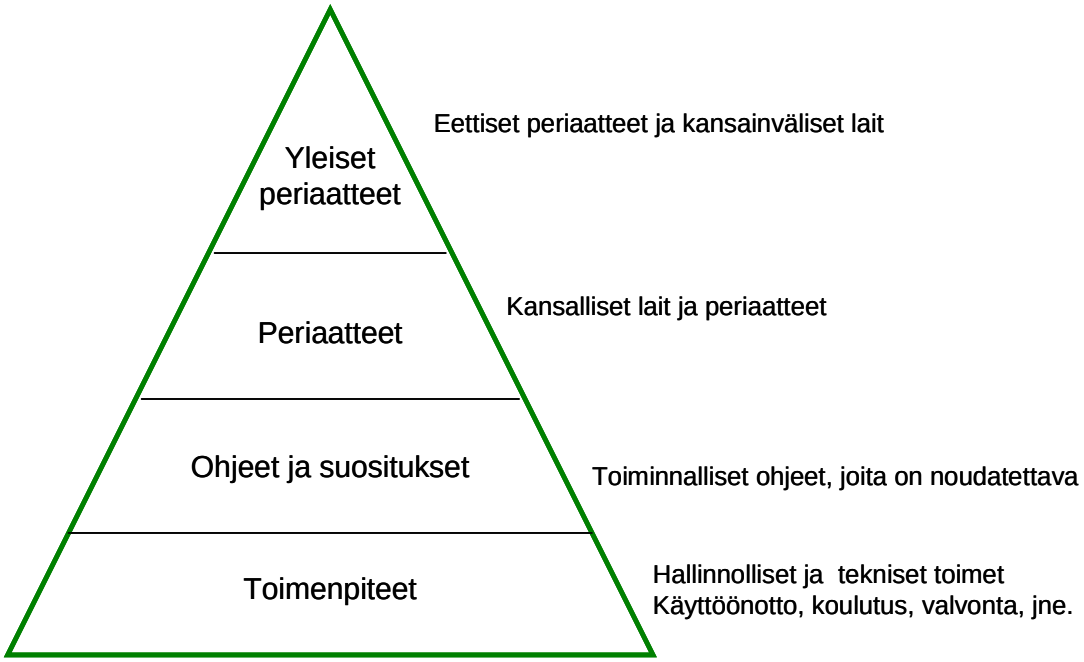
Terveydenhuollon asiakastietoa käsittelevät tietojärjestelmät kuten sähköinen potilaskertomusjärjestelmä ja sähköinen arkisto on toteutettava siten, että tietojen käsittely tapahtuu kansallisten lakien, asetusten ja STM:n antamien ohjeiden mukaisesti. Liitteessä 2 on esitetty tiivistelmä keskeisistä terveydenhuollon tietojenkäsittelyä ja tietojen arkistointia ohjaavista laeista ja asetuksista. Lainmukaisuuden lisäksi tulee asiakastietojen käsittelyn täyttää myös terveysalan eettiset vaatimukset. Arkistointi on osa asiakastietojen tietojenkäsittelyn kokonaisuutta ja se tulee toteuttaa lainmukaisesti ja tietoturvallisesti sekä perinteisessä paperidokumentti- että digitaalisessa ympäristössä.

2.1 Lainsäädännöstä johtuvia vaatimuksia

Perustuslaista, yleisestä lainsäädännöstä ja terveydenhuollon erityislainsäädännöstä voidaan johtaa mm. seuraavat vaatimukset potilasasiakirjojen käsittelylle ja arkistoinnille.

- Perustuslaki määrää yksityisyyden suojan perusoikeudeksi.
- Perustuslaki takaa luottamuksellisen viestinnän suojan.
- Perusoikeuksista johdetaan myös, että potilaalla on katsottu pääsääntöisesti olevan oikeus päättää asiakastietonsa luovuttamisesta antamalla suostumus.
- Asiakkaalla on oikeus rajata tietojen luovutusta.
- Terveydenhuollon varmennetussa asioinnissa asiakas ja ammattihenkilö tulee tunnistaa ja tarvittaessa todentaa.
- Sähköisessä asioinnissa terveydenhuollon organisaatio tulee tunnistaa ja tarvittaessa varmistaa.
- Sähköisten potilasasiakirjojen käyttöä on voitava seurata.
- Potilasasiakirjoja ei saa ilman suostumusta tai muuta laista johtuvaa perustetta luovuttaa sivulliselle.
- Vain tarpeellisia tietoja tulee käyttää ja luovuttaa.
- Rekisteritietoja saa ilman potilaan suostumusta tai laista johtuvaa perustetta käyttää vain niihin käyttötarkoituksiin joita varten ne on kerätty.
- Tiedon luovutuksen saajalla tulee olla hoitosuhde tai muu asiallinen yhteys asiakkaaseen tai laista johtuva muu peruste tiedon saamiselle.
- Terveystiedot eivät saa joutua sivullisten käsiin ja organisaatiolla tulee olla selkeä periaatteet siitä kuka on sivullinen.
- Erikseen määritellyt potilasasiakirjat (esimerkiksi potilasasiakirja-asetus) tulee allekirjoittaa joko omakätisesti tai sähköisellä (varmennetulla) allekirjoituksella.
- Tiedon alkuperä tulee voida tunnistaa.
- Tietojen käyttöä ja luovutusta tulee seurata.
- Tietojen luovutus, säilytys, ylläpito ja käyttö tulee olla suunnitelmallista.
- Tulee varmistaa, etteivät tiedot voi muuttua käsittelyn, säilytyksen tai siirron aikana.

Kuvassa 1 on esitetty asiakastiedon lainmukaisen ja luottamuksellisen käsittelyn kehikko.

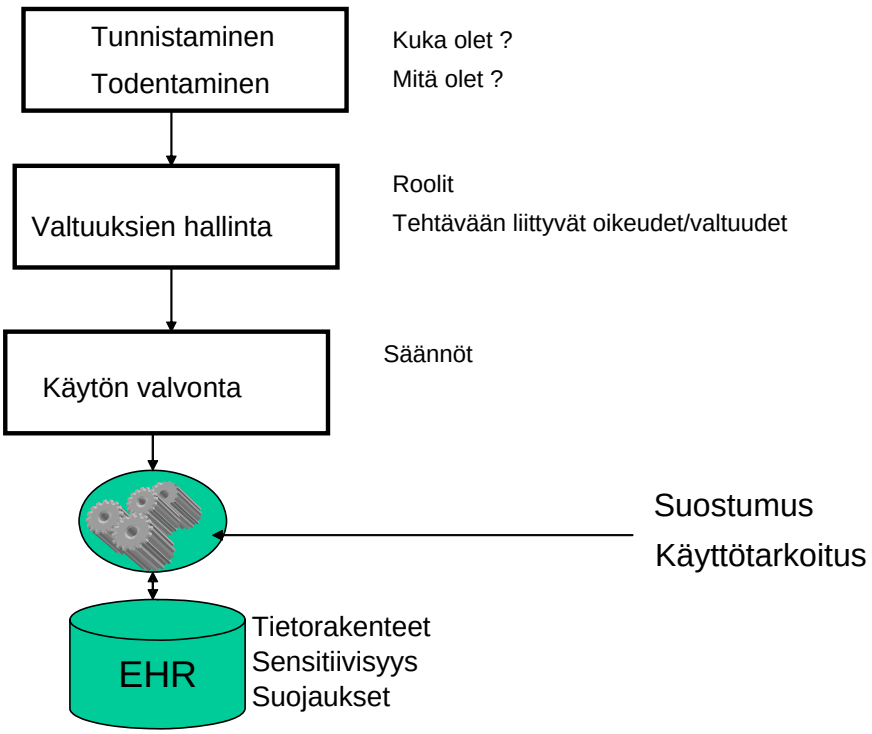


Kuva 1 Asiakastiedon lainmukaisen ja luottamuksellisen käsittelyn kehikko

Edellä kuvatuista vaatimuksista voidaan johtaa se, että asiakastietoja käsittelevällä ja tallettavalla sähköisellä arkistolla tulee olla tietojärjestelmäpalvelut, jotka kykenevät:

- tunnistamaan ja todentamaan tiedon tallettajat, käyttäjät ja ne joille tietoja luovutetaan
- hallinnoimaan käyttöoikeuksia. Tällainen käyttöoikeuksien hallintajärjestelmä kykenee antamaan käyttäjille heidän työtehtäviinsä ja rooleihinsa liittyvät valtuudet tietojen käyttämiseen
- hallinnoimaan tietojen käyttämistä ja luovuttamista (ts. käytön ja luovutusten hallintajärjestelmä)
- hallinnoimaan suostumuksia (ts. suostumusten hallinnan järjestelmä)
- hallinnoimaan tietojen luovutusta perustuen niiden käyttötarkoitukseen (ts. sääntöpohjainen käytön ja luovutuksen hallintajärjestelmä)

Kuvassa 2 on esitetty sähköisen asiakastietojärjestelmän käyttäjänhallinnan, käyttöoikeuksien ja käytön valvonnan periaatekaavio.



Kuva 2 Käyttäjien ja käyttöoikeuksien hallinta sähköisissä tietojärjestelmissä

2.2 Sähköisen arkistoinnin ominaisuuksia

Terveydenhuollon sähköinen arkisto ottaa vastaan asiakastietoa digitaalisessa muodossa, tallettaa sitä muuttumattomana säädetyn ajan ja mahdollistaa arkistoidun tiedon käytön siihen oikeutetuille ja tunnistetuille henkilöille, prosesseille ja tietojärjestelmille. Siirtymisellä perinteisistä paperi- ja kuva-arkistoista digitalisoitujen asiakastietojen sähköiseen arkistointiin tavoitellaan mm. arkistointikustannusten säästöjä, kykyä tehdä tieto saatavaksi ajasta ja paikasta riippumatta "24h/7d periaatteella". Lisäksi halutaan tukea työnkulkuja ja mahdollistaa uudenlaisia toimintamalleja ja prosesseja.

Asiakastietojen arkistoiminen digitaalisessa muodossa tuo mukanaan myös uudenlaisia haasteita:

- digitaalinen tieto voi korruptoitua helposti
- digitaalista tietoa voidaan jakaa ja kopioida jälkiä jättämättä
- digitaalisesti talletettua tietoa voidaan käyttää helposti asiattomasti tietoverkon kautta jopa yli valtakunnan rajojen

- digitaalisten dokumenttien elinaika on lyhyempi kuin paperidokumenttien ja tiedon saatavuuden varmistaminen pitkäaikaisessa talletuksessa on vaativa tehtävä. Käytännössä tämä edellyttää mm. tiedon rakennekonversioita
- tiedon hakeminen ja löytyminen on riippuvainen käytettävissä olevasta ohjelmaversiosta
- vihamielisten ohjelmien, virusten ja troijalaiset aiheuttamien uhkien torjunta on vaativa tehtävä
- tiedon ja arkistotapahtumien kiistämättömyyden todentaminen koko säilytysajan on tietoteknisesti vaativa tehtävä

On myös huomattava, että *terveydenhuollon sähköisessä toimintaympäristössä sähköinen arkisto ei esiinny yksin.* Se on kiinteässä vuorovaikutuksessa sähköisiin potilastietojärjestelmiin. Sähköinen arkisto ja sen palveluja käyttävät potilastieto-järjestelmät muodostavat toiminnallisen kokonaisuuden.

Terveydenhuollon asiakastietojen säilytysajat on Suomessa kiinnitetty STM:n asetuksella. Aika on pisimmillään 10 vuotta potilaan kuoleman jälkeen, mikä merkitsee sitä, että arkiston on varauduttava jopa 100 vuotta ylittävään tietojen säilytysaikaan. Digitaalisessa tietojenkäsittelyssä ja sähköisessä arkistoinnissa näin pitkä säilytysaika tuo mukanaan useita hankalasti ratkaistavia ongelmia, kuten miten taataan tiedon kiistämättömyys, muuttumattomuus ja käytettävyys. Käytännössä terveydenhuollon sähköinen arkisto joutuu varautumaan mm. tietojen rakennekonversioihin ja siihen, että tiedot tulee tallettaa ohjelmisto-, tietotekniikka ja säilytysmediariippumattomasti.

3 Sähköinen arkisto ja potilastieto-järjestelmät

3.1 Arkisto ja arkistointi

Arkisto voidaan määritellä organisaatioksi, joka tallettaa tietoa (esim. potilaskertomuksia) ja mahdollistaa tiedon käytön ja jakamisen tunnistetuille asiakkaille koko tiedolle määritellyn/määrätyn säilytysajan.

Sähköinen arkisto (eArkisto) on puolestaan organisaatio, jonka tehtävänä on tallettaa tietoa digitaalisessa muodossa säädetyn ajan ja mahdollistaa tiedon käyttö tunnistetuille ja oikeutetuille henkilöille ja prosesseille. Terveydenhuollon sähköiseltä arkistolta edellytetään, että talletettu tieto on saatavissa muuttumattomana ja kiistämättömänä koko tiedon säilytysajan. Terveydenhuollon sähköisen arkiston tulee olla turvallinen ja täyttää yksityisyyden suojan vaatimukset.

Sähköisen arkiston yhteydessä käytetään myös termejä passiivinen eArkisto ja aktiivinen eArkisto**.** Passiivinen eArkisto tallettaa tiedon, siihen liittyvät kuvailutiedot (esim. metatiedot ja politiikkatiedot) kiinteinä yksikköinä (tietoobjekteina). Tiedon tuottaja rakeistaa tiedon ennen sen lähettämistä arkistoitavaksi. Kun lähetetty tieto on arkistoitu, ei sitä voida muuttaa tai hävittää tiedon säilytysaikana. Passiivinen arkisto ei voi jakaa tietoa rakeistusta pienempinä osina. Tietoa siis haetaan ja luovutetaan samoina tietoyksikköinä (objekteina) kuin se on talletettu. Passiivisella arkistolla on oma itsenäinen käyttöoikeuksien hallintajärjestelmänsä.

Terveydenhuollossa on tyypillistä, että arkistoitu asiakasdokumentti palautetaan uuden hoitotapahtuman vuoksi toimintayksikköön ja siihen liitetään uutta tietoa. Tämä päivitetty dokumentti lähetään hoitoepisodin päätyttyä uudelleen arkistoitavaksi. Päivitetty dokumentti voidaan yhdistää arkistossa olevaan aikaisempaan dokumenttiin ja luoda uusi alkuperäisdokumentti. Lopuksi tämän uuden kokonaisuuden muuttumattomuus varmistetaan arkiston tekemällä allekirjoituksella (ns. nested signature principle). Vaihtoehtoinen menetelmä on linkittää päivitetty dokumentti sen aikaisempiin versioihin ja varmistaa uusimman version muuttumattomuus sähköisellä allekirjoituksella (ns. cascaded signature principle). Riippumatta siitä kumpaa menetelmää käytetään, voidaan tällaista arkistoa kutsua passiiviseksi arkistoksi joka jakaa aktiivisia dokumentteja.

Tässä raportissa suositellaan sähköisen arkiston ensisijaiseksi toteutustavaksi passiivista arkistoa joka kykenee jakamaan aktiivisia dokumentteja ja joka käyttää talletettavien dokumenttien päivityksen edellä kuvattua versiointimenetelmää.

Käsitteellä aktiivinen arkisto ei ole vakiintunutta merkitystä. Aktiivinen eArkistolla tarkoitetaan tavallisesti tietojärjestelmää joka mahdollistaa arkistoidun tiedon minkä tahansa yksittäisen tiedon päivittämisen ja hakemisen (random update and random access), liite 3. Tästä seuraa, että aktiivisen arkiston ja sähköisen potilaskertomusjärjestelmän välinen ero on lähes olematon.

Arkistointi ei ole pelkästään paperien, mikrofilmien tai bittien säilyttämistä. Arkistointi on kokonaisuus joka muodostuu:

- tiedon säilyttämisen ja käytön periaatteista ja menetelmistä (politiikasta)
- informaation hallinnoinnista
- tiedon migraation periaatteista (politiikasta)
- tiedon kuvaamisen periaatteista ja menetelmistä (politiikasta)
- tietoturvapolitiikasta
- tietosuojapolitiikasta
- tallennusteknologiasta

Sähköinen arkistointi nähdään monesti laajempana kokonaisuutena kuin vain yhden toimintayksikön tietojen tallentamisena. Arkisto voi ottaa vastaan, tallettaa ja jakaa usean eri toimintayksikön tietoja. Se voi olla alueellinen tai valtakunnallinen. Tällaisen arkiston tulee pystyä käsittelemään eri rekisterinpitäjien, eri käyttötarkoituksiin tuotettuja ja eri suojaustasoja vaativia tietoja lainmukaisesti ja tietoturvallisesti.

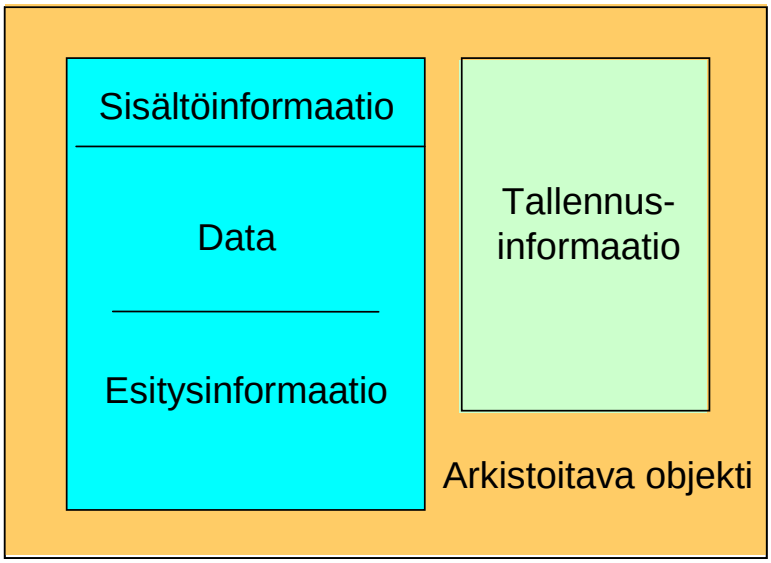
3.2 Tiedon sähköisen arkistoinnin ja varmuuskopioinnin suhde

Varmuuskopioinnilla (back-up) tarkoitetaan eArkiston sisällä tapahtuvaa tiedon digitaalista migraatiota (esim. tiedon uudelleenpakkaus tai replikointi). Sen tarkoitus on mahdollistaa tiedon palautus alkuperäiseen tilaan minkä tahansa katastrofin jälkeen (esim. kovalevyvaurio).

Potilastietojärjestelmissä tietojen varmuuskopionti ei ole vaihtoehtoinen ratkaisu eArkistolle. mutta se on yksi sekä sähköisen potilastietojärjestelmän että eArkiston toiminnoista.

3.3 Arkistoivan tietojärjestelmän elementit

Arkistoivan tietojärjestelmän vastuulla on tehdä tieto käytettäväksi oikeassa ja ymmärrettävässä muodossa koko säilytysajan. Jotta tieto voisi olla sekä ymmärrettävää käyttäjälle että tehty saavutettavaksi myös silloin kun kyseessä on pitkät säilytysajat (terveydenhuollossa tyypillisesti 20 - 100+ vuotta), on arkistoivan tietojärjestelmän talletettava varsinaisen datan lisäksi myös muuta tietoa. Sähköinen arkisto on arkistoiva tietojärjestelmä ja sen on talletettava varsinaisen datan lisäksi tiedon esitystapatietoa, kuvailutiedot, erilaiset politiikkatiedot ja sisältötiedot (kuva 3).

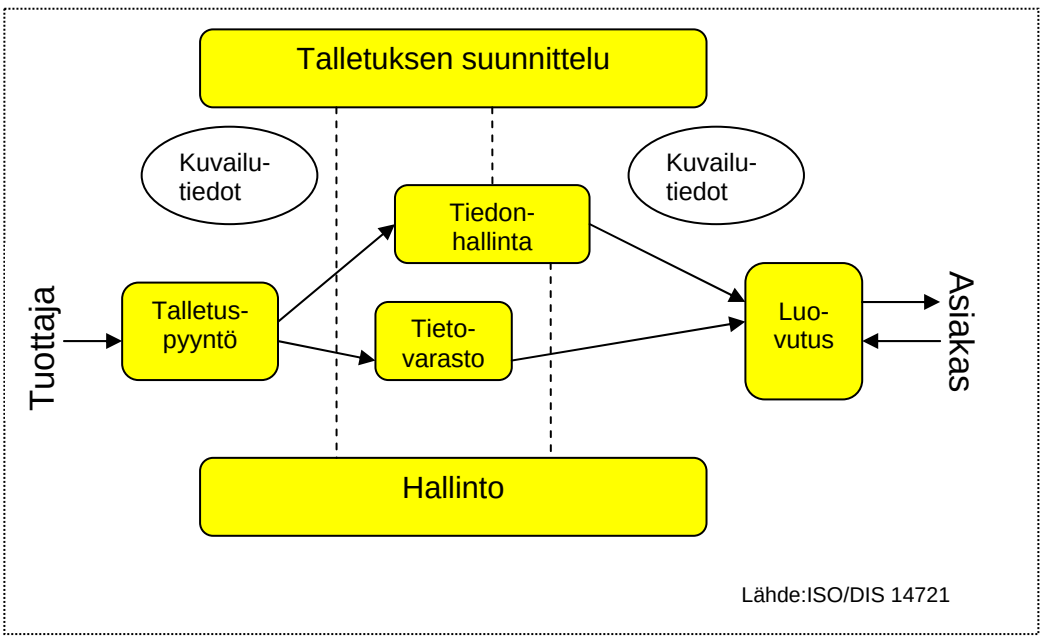


Kuva 3 Arkistoitava data ja sen kuvailutiedot

Arkistoivan tietojärjestelmän on talletettava tiedon kuvailutietojen lisäksi myös talletuksen organisoinnin edellyttämät kuvailutiedot. Tämä toteuttaminen edellyttää kokonaisvaltaista tietoarkkitehtuuria. Liitteessä 4 on esitetty kansainvälisen OAIS-järjestön suositteleman tietoarkkitehtuurin periaatemalli.

Sähköisen arkiston toiminnalliset peruselementit on esitetty kuvassa 4 perustuen ISO/DIS 1471 standardin määrittelyihin. Näitä peruselementtejä ovat mm.

- Tekninen tietovarasto (esim. kovalevyjärjestelmä tai magneettinauha)
- Hallinnolliset tietojärjestelmäpalvelut (hallinto)
- Talletuksen suunnittelu
- Arkiston tiedonhallinta (data management)

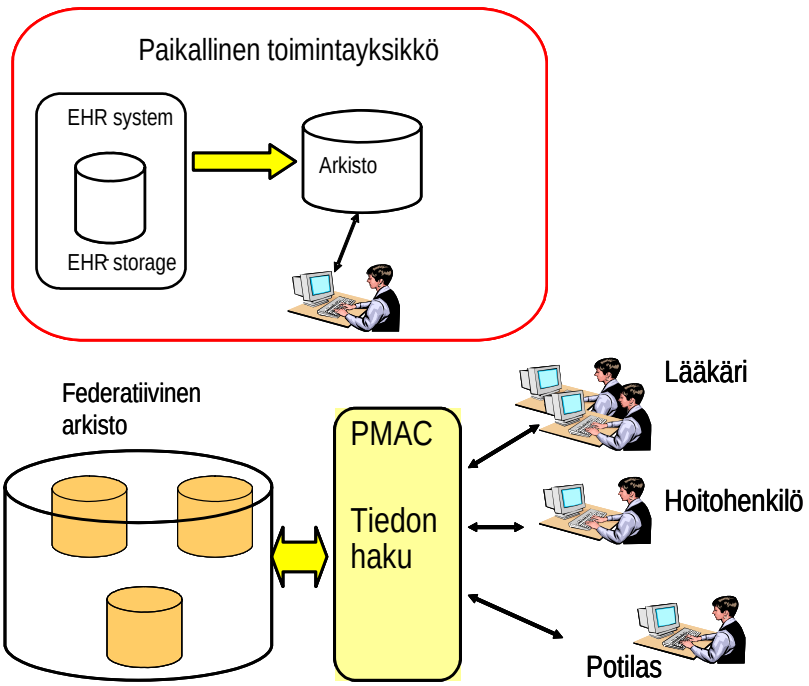


Kuva 4 eArkiston toiminnalliset osat

3.4 Arkistoivan tietojärjestelmän tyypit

Arkistoivat tietojärjestelmät voidaan jakaa useaan eri tyyppiin (liite 5). Näitä ovat:

- *Riippumaton* arkisto, joka on suljettu järjestelmä joka palvelee ennalta määrättyjä käyttäjiä.
- *Co-operatiivinen* arkisto, jolloin eri arkistoilla on yhteinen tiedon vastaanotto- ja jakelumekanismi mutta ei yhteistä tiedon hakujärjestelmää.
- Federatiivinen arkisto on usean eri organisaation (esim. terveydenhuollon toimintayksikön) yhteinen ratkaisu. *Federatiivisella* arkistoilla on yhteisiä toiminta-alueita kuten esimerkiksi tiedon haku yhteisten hakumekanismien avulla (esim. yhteiset tietohakemistot) tai yhteinen käyttöoikeuksien hallinnan järjestelmä.



Kuva 5 Riippumaton ja federatiivinen arkisto

Yllä olevassa kuvassa 5 on kuvattu riippumatonta ja federatiivista arkistojärjestelmää terveydenhuollon näkökulmasta.

3.5 Sähköisen potilastietojärjestelmän ja eArkiston yhteistoiminta

Sähköinen potilastietojärjestelmä (EHR-järjestelmä) ja eArkisto voidaan kombinoida usealla eri tavalla. Sähköinen arkistointi voi olla yksi toisaikaiseen potilastietojärjestelmään integroiduista toiminnoista, jolloin sähköinen potilastietojärjestelmä toimii myös arkistoivana tietojärjestelmänä. Tällaisella toteutuksella on yksi yhteinen käyttäjien tunnistus- ja käyttöoikeuksien hallintajärjestelmä sekä

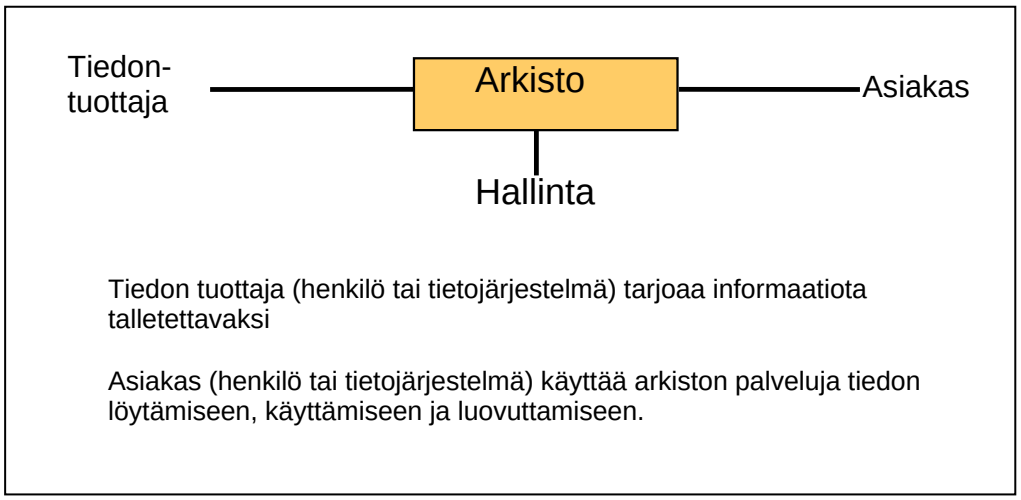
keskitetty tietoturvapolitiikka. On tärkeä huomata, että tällaisellakin ratkaisulla tulee olla arkistopolitiikka ja että arkistoivalla potilastietojärjestelmällä on vastuu tietojen talletuksesta koko tiedoille säädetyn säilytysajan.

Erillinen arkisto ja EHR-järjestelmä voivat myös muodostaa co-operatiivisen tietojärjestelmäkokonaisuuden. Tällaisessa toteutuksessa EHR-järjestelmä lähettää tiedot tyypillisesti sanomamuodossa eArkistoon ja pyytää tietoja arkistosta kyselysanomia käyttäen. Nämä sanomat voivat olla esimerkiksi Dicom tai HL7 sanomia.

Federatiivisen arkiston ja EHR-järjestelmän kokonaisuus on tavallisesti alueellinen tai valtakunnallinen. Tässä ratkaisussa arkisto ja toimintayksiköiden EHR-järjestelmät voivat käyttää yhteistä käyttöoikeuksien ja käytön hallintajärjestelmää ja niillä voi olla myös yhteinen tiedon hakupalvelu. Nämä palvelut voidaan toteuttaa myös yhteisen luotetun osapuolen tuottamina.

4 eArkiston toimintaympäristö

Kuva 6 esittää yksinkertaistettuna arkiston toimintaympäristöä perustuen ISO/DIS 1471 määrittelyihin.



Kuva 6 Arkiston toimintaympäristö

Kuvan 6 malli sovellettuna terveydenhuoltoon tarkoittaa, että arkiston *tiedon tuottaja* voi olla mm.

- Terveydenhuollon toimintayksikön potilaskertomusjärjestelmä
- Erillinen laboratorion- tai kuvantamisen tietojärjestelmä
- Potilas tai kansalainen henkilökohtaisen tietokoneensa välityksellä
- Lääkäri e-reseptejä tuottavan tietojärjestelmän välityksellä
- Automaattinen mittalaite, joka on kytketty potilaaseen tai jota potilas käyttää esimerkiksi kotona

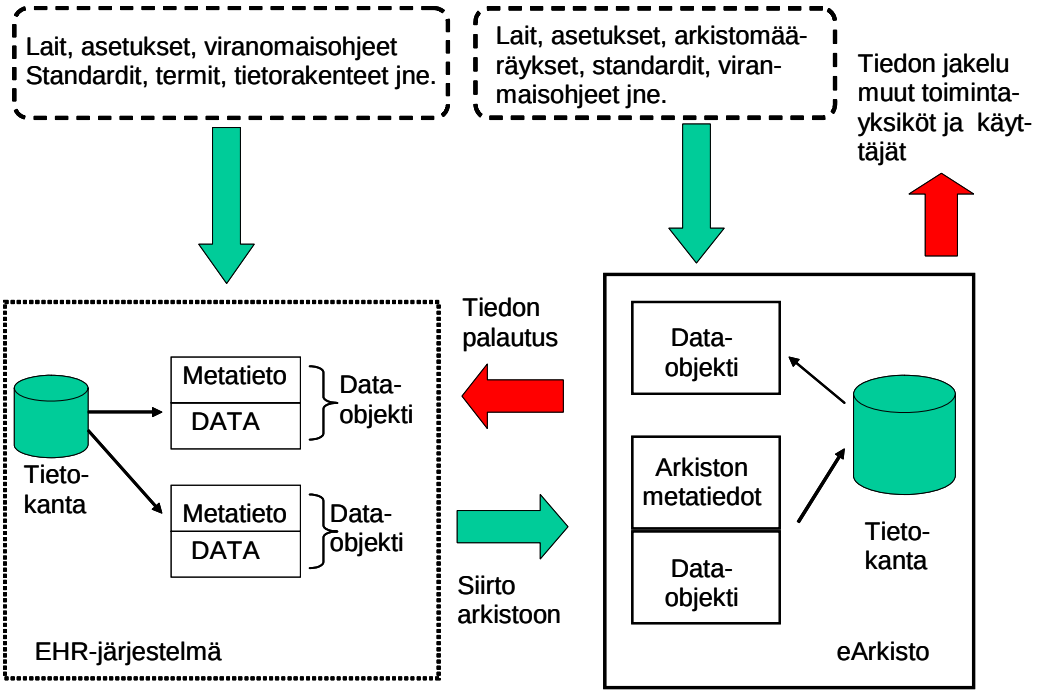
Arkiston asiakas on tietojärjestelmä tai henkilö jotka käyttävät arkistoa halutun tiedon löytämiseen ja käyttämiseen. Terveydenhuollossa arkiston asiakkaita ovat mm.

- Terveydenhuollon toimintayksikön potilaskertomusjärjestelmä
- Terveydenhuollon ammattihenkilöt
- Viranomaiset, joilla on laista johtuva oikeus tietojen saantiin
- Organisaatiot, joilla on potilaan suostumuksella oikeus tiedon saantiin
- Tutkijat ja opetustehtäviä hoitavat
- Potilas/kansalainen

5 eArkiston tehtävät ja vastuut

Sähköinen arkisto toimii läheisessä vuorovaikutuksessa potilastietojärjestelmien kanssa. Potilaskertomusjärjestelmä muodostaa raakatiedoista (ts. datasta) dataobjektin liittämällä dataan tarpeelliset kuvailutiedot (metatiedot). Metatieto on tarpeen mm. tiedon hakemisessa, käsittelyssä, suojaamisessa ja luovutuksessa. Potilaskertomusjärjestelmän tule varustaa digitaaliseen talletukseen lähetettävät dokumentit metatiedolla. Metatietoa varten on käytettävissä kansainvälisiä standardeja (mm. Dublin Core ja HL7/CDA header).

Dataobjekti siirretään tarvittaessa arkistoon, jotka liittää siihen arkistoinnin edellyttämät kuvailutiedot (kuva 7). Arkisto joko palauttaa dataobjektit pyydettäessä rekisterinpitäjälle tai luovuttaa dataobjekteja muille rekisterinpitäjille tai käyttäjille.



Kuva 7 eArkiston ja sähköisen potilastietojärjestelmän työnjako

Jotta arkisto kykenisi takaamaan tiedon saatavuuden riippumatta säilytysajasta ja tietotekniikan muutoksista, tulee arkistoitavalla tiedolla olla toimiva tietomalli. Tietomallissa määritellään mm.

- Yhtenäiset käsitteet
- Tiedon looginen rakenne, tietoalkiot (niiden nimet)
- Tiedon fyysinen rakenne, tietotyypit (esim. XML DTD), nimet ja formaatit
- Tietoa kuvaava metadata, sen sisältö, ymmärrettävyys, käytettävyys ja ylläpidettävyys

- Ohjaava metadata (mm. tietosuojan ja tietoturvan edellyttämät tiedot, tieto rekisterinpitäjästä ja säilytysaika)

Liitteessä 4 on kuvattu ISO/OASIS standardin mukaisen tietomallin rakenne

5.1 Terveydenhuollon sähköisen arkiston perustehtävät

Seuraavassa on käsitelty terveydenhuollon sähköisen arkiston perustehtävät arkistossa tapahtuvan tiedon vastaanoton, käsittelyn, tallentamisen ja jakamisen näkökulmista. ARKKI-ryhmän porteissa on tarkasteltu arkistoa käyttäjien ja arkistonmuodostuksen näkökulmasta ja esitetty arkistolle yksityiskohtaiset toiminnalliset määrittelyt.

1. Tiedon tallennuspyynnön vastaanotto ja käsittely

    - Tiedon toimittajan tunnistaminen ja todentaminen
    - Talletuspyynnön hyväksyttävyyden tarkistaminen
    - Lokimerkintöjen tekeminen

2. Datan/dokumentin vastaanotto

    - Turvallisen tietoyhteyden synnyttäminen
    - Tiedon lähettäjän (talletuspyynnön tekijän) tunnistaminen ja todentaminen
    - Tiedon vastaanotto arkiston hyväksymässä esitysmuodossa
    - Tiedon (esim. dokumentin) integriteetin tarkistaminen
    - Tarkistukset, joilla varmistetaan ettei arkistoitava tieto sisällä viruksia tai muita haitallisia koodeja
    - Lokimerkintöjen tekeminen
    - Kuittauksen lähettäminen talletuspyynnön tekijälle

3. Talletuksen suunnittelu

    - Tiedon muuntaminen arkiston käyttämään talletusformaattiin (jos tarpeen)
    - Arkistoinnin edellyttämän metakuvauksen muodostaminen talletettavalle tiedolle
    - Tunnistekoodin antaminen (esim.OID-koodi) dokumentille (jos tarpeen)
    - Dokumentissa tai dataobjektissa esiintyvien ja hakupalvelun tarvitsemien tietotyyppien merkkaaminen talletettavaan dataan. Tämä voi tapahtua esimerkiksi käyttämällä ns. XML- tagitystä ja DTD-luokitusta (data type definition). Tällainen merkkaaminen tulee tehdä, jos se on arkiston toiminnan kannalta tarpeellinen ja/tai jos tätä toimenpidettä ei ole tehty sähköisessä potilastietojärjestelmässä ennen tiedon lähettämistä arkistoitavaksi.
    - Tiedon linkittäminen saman henkilön muihin arkistossa sijaitseviin tietoihin yksikäsitteisellä tavalla (esim. dokumentin aikaisempiin versioihin tai toisten toimintayksiköiden tuottamiin dokumentteihin)
    - Tiedon hakuun tarvittavien osoitteiden ja indeksi-tiedostojen luominen ja päivittäminen

- Tiedon integriteetin varmistaminen (esim. e-allekirjoituksella)
- Tiedon salaaminen (jos tarpeen)

4. Tiedon tallettaminen ja talletuksen hallinta

   - Tiedon tekninen talletus
   - Varmuuskopiointi tietoturvapolitiikan määrittämällä frekvensillä
   - Säilytysajan hallinta (mm. päätökset rakennekonversioista ja tiedon hävittämisestä)
   - Katastrofitilanteiden hallinta ja tiedon palautus katastrofin jälkeen

5. Tiedon saatavuuden varmistaminen

   - Tiedon muuttumattomuuden ja kiistämättömyyden hallinta
   - Tiedon ja ohjelmistojen migraation hallinta
   - Indeksitaulujen, viitteiden ja avainsanojen ylläpito
   - Tiedon luovutusformaattien ja niiden versioiden (esim. luovutussanomien) hallinta
   - Erilaisten päätelaitteiden tukeminen

6. Tiedon käyttö tai luovutuspyynnön käsittely

   - Asiakkaan tunnistaminen ja todentaminen
   - Asiakkaan tietoturvapolitiikan tarkistaminen
   - Asiakkaan käyttöoikeuksien tarkistaminen ja käyttöoikeuksien luovuttaminen asiakkaalle (jos tämä ominaisuus on käytössä)
   - Tiedon luovutuksen edellytysten olemassaolon tarkistaminen (mm. laillisuus, suostumus, asiayhteys, käyttötarkoitus, erityissuojaukset, poikkeustilanteet jne.)
   - Suostumuksen hallinta
   - Lokimerkintöjen tekeminen

7. Tiedon haku käyttöä tai luovutusta varten

   - Tiedon hakeminen teknisestä varastosta (esim. arkiston tietokannasta)
   - Tiedon rakennemuunnosten tekeminen (jos tarpeen)
   - Luovutukseen liittyvien asiakirjamerkintöjen tekeminen
   - Tiedon integriteetin varmistaminen (esim. e-allekirjoituksella)

8. Tiedon toimitus asiakkaalle

   - Turvallisen tiedonvälityskanavan valitseminen
   - Tiedon salaaminen (jos tarpeen)
   - Tiedon tekninen lähetys
   - Asiakkaan lähettämän vastaanottokuittauksen käsittely
   - Poikkeustilanteiden hallinta (esim. tietoyhteys katkeaa kesken lähetyksen)
   - Lokimerkintöjen tekeminen

9. Erityiset hallinnolliset toimet

   - Tiedon osittaistoimitusten hallinta (esim. kun arkistoidusta dokumentista luovutetaan vain osa ja tämän osan alkuperä ja muuttumattomuus tulee varmentaa)
   - Henkilötietolain mukaisten tarkistuspyyntöjen käsittely
   - Potilaan informointi ja suostumuksen hankinta tiedon luovuttamiseen liittyvissä tilanteissa, joissa tiedon pyytäjän tietoturvapolitiikka ei täytä EU:n tai kansallisia tietoturva- tai tietosuojavaatimuksia.
   - Arkistotapahtumien kiistämättömyyden hallinta (esim. aikaleimojen ja evidence-recordien avulla

5.2 Terveydenhuollon tietoja arkistoivan organisaation vastuut

Terveydenhuollon asiakastietoja arkistoinnin vastuu on nykylainsäädännön perusteella terveydenhuollon toimintayksiköllä. Tämä pätee myös siihen tilanteeseen, jossa toimintayksikkö hankkii arkistointipalvelut toimintasopimuksella ulkopuoliselta toimijalta (tai esimerkiksi valtakunnalliselta arkistolta).

Terveydenhuollon asiakastietoja arkistoivan organisaation yleiset vastuut ovat:

1. Arkiston tehtävä on tehdä talletettu tieto käytettäväksi muuttumattomassa ja ymmärrettävässä muodossa koko tiedolle säädetyn talletusajan. STM:n asetus ja ohjekirja potilasasiakirjoihin tehtävistä merkinnöistä ja niiden säilytyksestä määrittelee terveystietojen säilytysajat. Suomen kansallisarkisto ohjeistaa pysyväisarkistoinnin vaatimukset. Arkiston tulee kyetä säilyttämään pysyvästi talletettavat tiedot ja varmistamaan niiden saatavuus.

2. Arkiston tulee varmistaa, että talletettuja tietoja käytetään lain ja eettisten periaatteiden mukaisesti ja etteivät ne joudu sivullisten käsiin.

3. Arkiston on kyettävä varmistamaan talletetun tiedon saatavuus, muuttumattomuus, luottamuksellisuus ja jäljitettävyys. Digitaalisessa muodossa talletetavan tiedon elinkaaren aikana tarvitaan sekä media- että rakennekonversioita (liite 6). Myös tiedon hakemiseen ja katseluun/käyttämiseen tarvittavat ohjelmistot voivat muuttua. Arkiston migraatiosuunnitelmalla ja se toteutuksella varmistetaan tiedon saatavuus. Digitaalisen tiedon muuttumattomuuden ja kiistämättömyyden varmistaminen edellyttää nykyteknologialla sähköisiä notariaattitoimintoja ja notariaatin varmistamia tapahtumatiedostoja (evidence record), aikaleimoja ja sähköisiä allekirjoituksia.

4. Arkistoivan järjestelmän on kyettävä säilyttämään alkuperäisdokumentti muuttumattomana siten että sen alkuperäisyys on kiistaton.

5. Arkiston on kyettävä hallinnoimaan talletetun dokumentin kuvailutietoja silloin, kun niihin on tarve tehdä korjauksia tai päivityksiä. Arkiston on samaten kyettävä hallitsemaan tilanne, jossa on tarve lisätä talletettuun dokumenttiin tietoja. Tämä voidaan toteuttaa mm. luomalla päivitetystä dokumentista uusi versio joka on linkitetty dokumentin aikaisempiin versioi-

hin. Tällöin arkiston tulee kyetä säilyttämään kaikki dokumentin eri versiot loogisena kokonaisuutena ja päivittämään dokumentin versioiden kuvailutietoja tarvittavilla tapahtumatiedoilla.

6. Arkisto on vastuussa siitä, että tiedon luovuttamisen edellytykset ovat voimassa ennen tietojen luovuttamista.

7. Terveydenhuollon toimintayksikkö on Suomessa potilastietojen rekisterinpitäjä. Mikäli arkistoon on talletettu usean eri toimintayksikön potilastietoja, tulee arkiston kyetä hallinnoimaan ja luovuttamaan tietoja rekisterinpitäjäkohtaisesti.

8. Arkistoitavien tietojen oikeudellinen merkitys saattaa muuttua säilytyksen aikana. Arkiston tulee kyetä ylläpitämään tietoa dataobjektien/dokumenttien kulloistakin oikeudellisesta merkityksestä. Tämän tieto tulee merkitä säilytettävän tiedon kuvailutietoihin.

9. Arkiston tulee kyetä hävittämään luotettavasti arkistoidut tiedot kun niiden säilytysaika on päättynyt.

6 Tietoturvallisuus ja tietosuoja

Tietoturvallisuudella tarkoitetaan asiantilaa, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä. Suomen lainsäädäntö lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti (Valtionvarainministeriö). Tietoturvallisuus on kiinteä osa jokaisen sosiaali- ja terveydenhuollon toimijan ja organisaation toimintaa ja se koskee koko henkilöstöä. Suomessa ei ole yhtenäistä tietoturvallisuuslainsäädäntöä ja tietoturvallisuuden järjestämistä koskevia säädöksiä sisältyy useisiin lakeihin (vrt. liite 2).

Tietosuojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käytöltä ja käsittelemiseltä. Tietosuojatoimien tavoitteena on tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen. Tietosuoja on yksilön suojaa.

Henkilötietojen käsittelyyn ja luottamuksellisen viestinnän suojaan liittyviä säännöksiä on lukuisissa eri laissa. EU:n tietosuojadirektiivi muodostaa puitelainsäädännön. Oikeudesta käsitellä arkaluontoisia ja salassa pidettäviä tietoja on säädetty henkilötietolaissa ja viranomaisten osalta julkisuuslaissa. Henkilötietolain lisäksi sosiaali- ja terveydenhuollon tietojen käsittelyä ohjataan erityislailla ja asetuksilla kuten potilaslailla ja potilasasiakirja-asetuksella (T. Mikola, H. Sorvari ja P. Ruotsalainen, Turvallinen kommunikaatioalusta, Suositukset sähköisen suostumuksen periaatteiksi, OSVE 3/2004, Marja Pajukoski, Sähköinen asiointi sosiaali- ja terveydenhuollossa. Lainsäädännön rajat ja mahdollisuudet, Stakes Raportteja 283-2004).

Arkistoinnin näkökulmasta:

- Potilasasiakirjojen arkistoinnin on täytettävä samanaikaisesti sekä tietoturva- että tietosuojavaatimukset.
- Potilasasiakirjojen arkistoinnin tietoturvan toteuttaminen merkitsee, että tietojen saatavuus, luottamuksellisuus ja muuttumattomuus on turvattu kaikissa tiedon käsittelyvaiheissa. Lisäksi tietojen käyttöä tulee voida seurata.

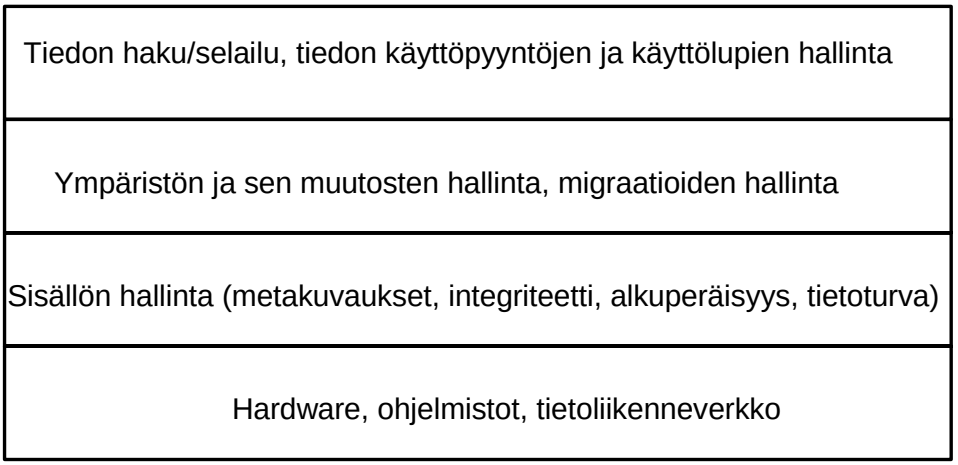
7 Suositukset tietoturvalliselle sähköiselle arkistoinnille

Peruslähtökohta sähköiselle arkistoinnille on, että sen tulee tapahtua eettisten periaatteiden, lakien, asetusten ja kansallisten normien edellyttämällä tavalla. Näiden lisäksi arkistoinnin tulee noudattaa hyvän toiminnan ohjeita ja noudattaa hyväksyttyjä standardeja (kuva 8).

Kuva 8 Arkistoinnin säätelyn ja ohjeistuksen kehikko

Tämä raportti pyrkii johtamaan voimassa olevasta lainsäädännöstä, STM:n tuottamasta ohjeistuksesta ja kansainvälisistä standardeista tekniikkariippumattomat vaatimusmäärittelyt asiakastietojen sähköiselle arkistoinnille.

Tarkastelemalla eArkistoa sisältä päin voidaan se jakaa kuvan 9 mukaisiin kerroksiin. Kaikkien näiden kerrosten toteuttaminen edellyttää teknisluonteista ohjeistusta, jotta voidaan taata arkiston ja asiakkaiden tietojärjestelmien yhteistoiminnallisuus.



Kuva 9 Sähköisen arkiston toiminnalliset kerrokset

7.1 Etukäteissuunnittelu

Perusvaatimus on se, että asiakastietojen arkistointi on suunniteltava etukäteen siten, että voidaan taata tietojen saatavuus, tietojen käsittelyn tietoturvallisuus ja yksityisyyden suoja. Etukäteissuunnittelussa eri toimintojen ja prosessien riskit tulee arvioida ja tuottaa tarvittavaa tietoa tietoturva- ja tietosuoja politiikoiden laatimiseen. Riskien arvioimisen ja tietoturvapolitiikan laatimisen jälkeen valitaan tavoitteeksi määritellyn tietoturvan ja tietosuojan kokonaistason toteuttavat toimet, palvelut ja tekniikat. Riskien arvioinnissa voidaan käyttää apuna esimerkiksi ISO/IEC 13335 standardia.

7.2 Arkistointipolitiikka

Lähtökohtana on, että terveydenhuollon tietoja arkistoivalla organisaatiolla (ts. eArkistolla tai asiakastietoja arkistoivalla tietojärjestelmällä) tullee olla kirjallinen arkistointipolitiikka. Tämä politiikka on niiden periaatteiden ja sääntöjen joukko, joka käsittää mm. seuraavat määrittelyt:

- mitkä ovat noudatettavat lait, asetukset ja normit?
- mitä standardeja noudatetaan?
- mikä on arkiston (liike)toimintamalli?
- ketkä ovat arkiston asiakkaita?
- mitä tietoja arkisto ottaa vastaan, luovuttaa tai palauttaa rekisterinpitäjälle sen omaan käyttöön?
- miten tietoja säilytetään (säilytyspolitiikka)?
- miten tiedot löydetään arkistosta?
- miten hallitaan tietojen konversiot ja migraatiot?
- poikkeuksellisten olojen toimintojen suunnitelma (ns. arkiston emergency mode)
- mitkä ovat arkiston vastuut?
- millaisia sopimuksia on olemassa?
- miten arkiston toimintaa valvotaan ja auditoidaan?
- miten ja millä menetelmillä arkisto toipua käyttöhäiriöistä?

Liitteessä 6 on kuvattutyypillisen potilaskertomuksen elinkaarta. Terveydenhuollon asiakastietojen pitkästä säilytysajasta johtuu, että säilytyksen aikana joudutaan toteuttamaan useita säilytysmedian ja säilytys/jakeluohjelmiston vaihdoksia. Tämän vuoksi arkistoivalla tietojärjestelmällä tulee olla sekä tiedon että ohjelmistojen migraatiosuunnitelmat, jonka avulla voidaan taata sekä tiedon muuttumattomuus että käytettävyys koko säilytysajan.

7.3 Infrastruktuuri

Kaikilla terveystietoja arkistoivalla toimintayksiköillä tulee olla hallinnollinen, tekninen ja fyysinen infrastruktuuri, jotta se voi varmistaa tiedon muuttumattomuuden, tietojen luottamuksellisuuden ja käytettävyyden sekä yksityisyyden suojan toteutumisen koko tietojen säilytysajan. Tämä infrastruktuuri käsittää mm.

- käyttäjien ja käyttöoikeuksien hallinnan
- käyttäjien luotettavan tunnistamisen ja todentamisen
- sähköisen allekirjoituksen
- tietojen salauksen
- poikkeustilanteiden hallinnan

7.4 Tietoturvapolitiikka

Kaikilla terveydenhuollon tietoja arkistoivalla toimintayksiköillä tulee olla kirjallinen tietoturvapolitiikka. Tietoturvapolitiikka merkitsee mm. sitä, että eArkiston tulee säilyttää asiakastieto siten, että tiedon luottamuksellisuus, saatavuus ja muuttumattomuus on turvattu koko tietojen säilytysajan. Tietoturvapolitiikan tulee perustua *riskien tunnistamiseen ja hallintaan*. Arkistoivalla organisaatiolla tulee olla riskien hallinnan järjestelmä ja mekanismit.

Tietoa arkistoivan organisaation tulee määritellä riskien hyväksyttävä taso. Tässä raportissa suositellaan, että riskien arviointi perustuu ISO/IEC 13335 standardiin. Tietoturvapolitiikan laatimisessa suositellaan noudatettavaksi ISO/IEC 17799, ISO WD 27799 standardeja ja Stakesin raportin 5/2005 esittämiä suosituksia.

Sähköisen arkiston tieturvapolitiikassa tulee määritellä mm.:

- Hallinnolliset, fyysiset ja tekniset menetelmät ja rakenteet joilla varmistetaan tiedon muuttumattomuus, luottamuksellisuus ja käytettävyys
- Miten käyttöoikeuksia hallitaan roolipohjaisesti
- Käyttäjien tunnistus ja todentamisjärjestelmät
- Vaatimukset turvallisille tietoliikenneyhteyksille
- Tietoturvarikkomusten sanktiot
- Tietotuvallisuuden auditointipolitiikka
- Vastuut tietoturvallisuuden näkökulmasta
- Arkistotoiminnan jatkuvuuden toteuttamisen edellyttämät toimet
- Osatietojen ja keskeneräisten tietojen luovutuksen periaatteet
- Tietoturvallisuuteen liittyvät toimeksiantosopimukset
- Miten talletetut tiedot on luokiteltu niiden sensitiivisyyden ja vaadittavan tietoturvan suhteen

7.4.1 Tiedon saatavuuden ja käytettävyyden turvaaminen

Arkiston vastuulla on turvata tiedon saatavuus ja käytettävyys (ymmärrettävyys) koko tiedolle määrätyn säilytysajan. Tätä varten tulee eArkiston:

1. Kyetä tallettamaan varsinaisen informaatiota**.** Tämä merkitsee sitä, että arkiston tulee kyetä tallettamaan varsinaisen raakadatan lisäksi tiedon esittämisen ja sisällön kuvailutiedot ja tietoon liittyvät politiikkatiedot. Lisäksi arkiston tulee kyetä liittämään talletettavaan arkiston "tietopakettiin" (tieto-objektiin) tiedon talletuksen hallintaan liittyvät tiedot yhtenä informaatioyksikkönä (kts. kuva 3 ja kuva 7)**.**

   Seuraava esimerkki selventää tätä vaatimusta. Potilaskertomuksen tiedot (raakadata) esitetään tavallisesti kirjaimilla. Sisällön ymmärtäminen edellyttää tietoa ja kykyä käyttää merkkeihin liittyvää kieltä. Tarvitaan siis tiedon esitysinformaatiota. Lisäksi, jos esimerkiksi kyseessä on potilaan laboratoriotulokset tulee meidän tietää mistä analyysimenetelmästä on kysymys ja mitkä ovat menetelmään liittyvät viitearvot. Tarvitaan siis tiedon sisältöinformaatiota.

2. Arkistolla tule olla menetelmä haluttujen tietojen yksikäsitteiseksi löytämiseksi. Tämä edellyttää tiedon yksikäsitteistä nimeämistä, indeksi- ja linkkihakemistoja, tietoa kuvaavia metatietoja ja terminologisia hakupalveluja.

3. Arkiston tulee kyetä ylläpitämään ajantasaisesti hakupalvelun ja tiedon tallettamisen edellyttämiä linkki-, indeksi- ja hakutietoja ja varmistamaan niiden yksikäsitteisyys.

4. Arkiston tulee kyetä ylläpitämään talletettujen asiakastietojen ja objekteihin liittyvät metakuvaukset. Jos eri toimintayksiköiden tuottamat potilaskertomukset talletetaan arkistossa (teknisesti) yhteen potilaskohtaiseen kansioon, tulee tälle kansiolle luoda oma metatiedosto. Arkiston tulee kyetä huolehtimaan tämän kansion ajantasaisuudesta ja kiistämättömyydestä.

5. Arkistolla tulee olla menetelmä palauttaa talletettu informaatio sen alkuperäiseen tilaan häiriötilanteiden jälkeen.

6. Arkistolla tulee olla menetelmä mahdollistaa tiedon luovutus silloinkin kun potilaan suostumusta ei voida saada, jos siihen on lainmukainen peruste (esim. potilaan hengen pelastaminen).

7. Arkiston tulee kyetä identifioimaan yksikäsitteisesti talletetut tiedot ja dokumentit ja nimeämään talletettava tietokokonaisuus ja tiedon eri komponentit yksikäsitteisesti vähintään kansallisella tasolla.

   Arkistoitava asiakastieto voi muodostua erilaista komponenteista (esim. teksti, multimedia, still- kuvat ja äänitallenteet). Näillä tiedolla voi olla myös hienorakenne (granulariteetti). Arkistolle tulee määrittää pienin tieto-objekti joita se tallettaa. Kaikki samaan dokumenttiin kuuluvat komponentit tulee nimetä yksikäsitteisesti siten, että niiden keskinäiset suhteet ovat yksikäsitteiset (vrt. Opas Sähköisen potilaskertomuksen rakenteesta, STM/Kansallinen terveys-

hanke versio 1.19). Suositeltava käytäntö on tehdä nimeäminen ISO 9834-3UID standardin mukaisesti.

Asiakirjan/objektin tunnuksen tulee pysyä muuttumattomana koko tiedon säilytysajan. Jos dokumenttia modifioidaan säilytyksen aikana, tulee dokumentin versionumeroa ja metakuvausta päivittää. Syntyneet versiot ja versiohistoria säilytetään kuten varsinainen dokumentti.

7.4.2 Tiedon muuttumattomuuden turvaaminen

Asiakastietoja arkistoivan tietojärjestelmän tulee taata tiedon muuttumattomuus koko säilytysajan. Tämän toteuttamiseksi arkiston tulee huolehtia seuraavista toimista:

1. Arkistolla tulee olla menetelmä säilyttää alkuperäisdokumentti koko säilytysajan.

2. Arkistolla tulee olla riittävät menetelmät havaita ja valvoa kaikkia talletetun tiedon modifikaatioita säilytysaikana.

3. Arkiston tulee varmistaa, ettei tieto, dokumentti tai sen osa voi tuhoutua tai muuttua säilytysaikana tai tietoa siirrettäessä.

4. Arkistolla tulee olla turvattu audit-lokijärjestelmä, joka sisältää tiedon kaikista tiedon luovutuksista ja käytöistä.

5. Arkiston tulee kyetä allekirjoittamaan sähköisesti dokumentteja ja purkamaan sähköisesti salattuja tiedostoja.

6. Arkiston tulee ylläpitää ja hallita itse generoimiaan ja käyttämiään salaus- ja allekirjoitusavaimia koko tiedon säilytysajan.

7. Arkiston tulee varmistaa sekä objektien sisältämän datan että niiden kuvailutietotojen muuttumattomuus.

8. Arkiston tulee varmentaa, etteivät sen käyttämät allekirjoitus- ja salausavaimet missään olosuhteissa joudu sivullisten käsiin.

9. Arkiston luovuttamat sähköiset dokumentit tulee olla allekirjoitettu joko henkilökohtaisesti tai luovuttavan organisaation tekemällä teknisellä palvelinallekirjoituksella.

10. Arkiston tulee hallita tiedon muuttumattomuus säilytysaikana tapahtuvien rakennekonversioiden yhteydessä koko tiedon säilytysajan.

11. Arkistolla tulee olla kyky allekirjoittaa dokumentit sillä rakeisuustasolla, jonka kansallinen lainsäädäntö tai muu normisto edellyttää. Arkisto voi käyttää sähköisen allekirjoituksen toteuttamiseen myös ulkopuolista ns. luotettua allekirjoituspalvelua (eli notariaattipalvelua).

12. Allekirjoitukseen tulee sisältyä luotettava aikaleima.

Sähköisten dokumenttien muuttumattomuus varmistetaan tavallisesti sähköisellä allekirjoituksella. Normaalisti potilaan hoidosta vastaava terveydenhuollon ammattihenkilö allekirjoittaa dokumentit henkilökohtaisesti. Allekirjoitetusta dokumentista tulee ilmetä myös allekirjoittajan tehtävä organisaatiossa (dynaaminen rooli) ja ammatillinen status (staattinen rooli) (kts. (STM:n asetus potilasasiakirjoihin tehtävistä merkinnöistä).

Saumattoman palveluketjun kokeilulain mukaan tiedon muuttumattomuus voidaan varmentaa myös toimintayksikön/organisaation tekemällä sähköisellä allekirjoituksella. Arkistoon sovellettuna tämä tarkoittaa sitä, että allekirjoituksen voi toteuttaa arkiston tietojärjestelmä. Tällaista ”palvelinallekirjoitusta” voidaan käyttää mm. seuraaviin tarkoituksiin:

- Varmistamaan kuvailutiedoston (metatiedoston) aitous ja muuttumattomuus
- Varmistamaan rakennekonversioiden jälkeen tiedon muuttumattomuus
- Varmentamaan tiedon toimituksen tai osatoimituksen aitous ja muuttumattomuus
- Varmistamaan potilaskansioon sisältyvien eri osadokumenttien muodostaman kokonaisuuden aitous ja eheys.

Sähköisen arkistoinnin yhteydessä ongelmalliseksi muodostuu sähköisten allekirjoitusten ja aikaleimojen voimassaolon lyhytikäisyys. Tyypillinen sähköisen allekirjoituksen voimassaoloaika on nykyisellään 5-10 vuotta. Tämän vuoksi sähköinen arkisto joutuu suorittamaan asiakastietojen kymmenien vuosien säilytysajan aikana jo allekirjoitettujen dokumenttien uudelleen allekirjoituksen ja aikaleimojen uudistamisen. Tämä voidaan toteuttaa ns. notariaattitoiminnalla, jonka voi toteuttaa arkisto itse tai vastaavat palvelut voidaan hankkia luotetulta ulkoiselta sähköiseltä notariaatilta.

7.4.3 Tiedon luottamuksellisuuden turvaaminen

Asiakastietoja arkistoivan tietojärjestelmän tulee turvata tiedon luottamuksellisuus koko tiedon säilytysajan ja myös silloin kun tietoa luovutetaan teknisellä käyttöyhteydellä. Tätä varten:

1. Arkistolla on velvollisuus varmistua siitä, että tarvittavat edellytykset tiedon luovuttamiselle ovat olemassa ennen kuin tietoa luovutetaan.

2. Arkiston tulee varmistaa, ettei tietoa luovuteta tunnistamattomille tai sivullisille henkilöille, prosesseille tai tietojärjestelmille. Arkiston tulee estää kaikki sellainen tiedon käyttö johon asiakkaalla ei ole valtuuksia.

3. Arkistolla tulee olla tiedon käytön hallintajärjestelmä. Terveydenhuollon toimintayksikkö voi rekisterinpitäjänä käyttää arkistoon tallettamiaan oman toimintayksikön tietoja ilman potilaan suostumusta. Tietoa saavat käyttää kuitenkin vain ne henkilöt jotka osallistuvat hoitoon ja sen järjestämiseen tai joilla on joko työtehtäviensä perusteella tai laista johtuvien muiden perusteiden johdosta on oikeus käyttää tietoja.(Suomessa näistä henkilöistä päättää hoitoa antava toimintayksikkö).

4. Arkistolla tulee olla tiedon luovutuksen hallintajärjestelmä. Tämän järjestelmän tulee kyetä toteuttamaan seuraavat tiedon luovuttamisen ja käytön yleiset periaatteet:

   - luovuttamisen edellytys on suostumus, muu asiayhteys tai laista johtuva muu peruste.
   - luovutetun tiedon käyttämiseen tulee olla hyväksyttävä syy.
   - luovutuksen pyytäjä ja hänen roolinsa tulee voida tunnistaa luotettavasti.

   Tietoja pyytävä rekisterinpitäjä on vastuussa siitä, että edellä kuvatut tiedon luovutuksen edellytykset ovat olemassa. Tämä edellyttää tiedon pyytäjien ja arkiston välisen keskinäisen luottamuksen olemassaoloa.

   Arkisto voi varmistua luovutuksen edellytysten olemassaolosta ns. luovutusvarmenteen, suostumusdokumentin ja tunnistamispalveluiden avulla (kts. tarkemmin Opas sähköisen potilaskertomuksen rakenteesta, STM/Kansallinen terveyshanke versio 1.19).

5. Arkistolla tulee olla palvelut, joilla voidaan varmistua (tunnistaa ja tarvittaessa todentaa) tiedon lähettäjästä ja havaita valheelliset tiedon lähettäjät ja vastaanottajat. Tunnistamiseen ja todentamiseen voidaan käyttää mm. terveydenhuollon PKI-järjestelmän palveluja.

6. Arkistolla tulee olla tapahtumien kirjaamis- ja seurantajärjestelmä. Arkiston tulee seurata ja valvoa kaikkea tiedon käyttöä (niin luovutusta kuin sisäistä käyttöä) järjestelmällisesti ja säännöllisesti.

7. Arkistolla tulee olla tiedon käytön valvontajärjestelmä ja sen tulee kyetä hallitsemaan tiedon käyttöoikeuksia yhdistettynä käyttäjien rooleihin (ns. role based access control system).

   Tiedon käyttöoikeuksien ja tiedon käytön hallinnan toteuttamiseen suositellaan käytettäväksi ISO TC215 standardia Health Informatics - PMAC – Privilege Management and Access Control.

   Mikäli arkisto tallettaa usean eri toimintayksikön asiakastietoja (esim. potilasasiakirjoja), suositellaan käytettäväksi raportissa " Kansallinen terveysprojekti - Usean toimintayksikön yhteinen käyttäjän- ja käyttöoikeuksien hallinta - Suositukset ja periaatteet " esitettyä toteutusmallia.

8. Arkiston tulee kyetä hallitsemaan tiedon toimittajien ja asiakkaiden tietoturvapolitiikoiden yhteensovittamista (ns. security policy bridging). Mikäli tiedon vastaanottajan tietoturvataso ei ole Suomen ja EU:n lakien mukainen, ei tietoa tule luovuttaa ilman potilaan informoitua suostumusta.

9. Arkiston tulee ylläpitää ja päivittää tiedon luovuttamisen lokia (audit-log). Loki tulee säilyttää siten, että sen muuttumattomuus, aitous ja kiistämättömyys voidaan varmistaa lokille määrätyn säilytysajan.

10. Arkiston tulee tarjota kansalaisille mahdollisuus tarkistaa häntä koskevien tietojen luovutusloki siten kun lainsäädännössä tarkemmin määritetään. Tarkistus tulee voida tehdä myös sähköisesti.

11. Arkiston tulee kyetä tarvittaessa salaamaan talletetut dokumentit sekä tiedon talletuksen että luovutuksen aikana.

    Salaamisen tarpeellisuus arkistoinnin aikana määritellään nykyisen potilasasiakirja-asetuksen päivitystyön yhteydessä STM:n toimesta.

12. Arkiston tulee kyetä muodostamaan talletetuista henkilötiedoista anonymisoituja kokonaisuuksia mm. tutkimuksen ja tilastoinnin tarpeisiin.

13. Arkistolla tulee olla menetelmät havaita ja torjua vihamieliset koodit kuten virukset, madot ja troijalaiset ja erilaiset vihamieliset hyökkäykset.

14. Arkiston tulee kyetä ilmoittamaan talletettujen tietojen rekisterinpitäjälle arkiston tekemistä tietojen luovutuksista.

15. Silloin kun, arkistoitu asiakirja hävitetään arkiston toimesta säilytysajan päätyttyä, tulee arkiston kyetä hävittämään kaikki komponentit (osadokumentit/objektit) ja versiot.

16. Sähköisen pitkäaikaisarkistoinnin yhteydessä ongelmaksi muodostuu sähköisten allekirjoitusten ja aikaleimojen uudistaminen, samoin kuin tehtyjen rakennekonversioiden kiistämättömyyden (non-repudiation) varmistaminen. Tämä voidaan toteuttaa mm. muodostamalla päivitystapahtumista ns. evidence-record, jonka sähköinen notaari varmistaa aikaleimalla. Arkiston tulee kyetä ylläpitämään tällaista tapahtumarekisteriä siten, että tapahtumaketjua (evidence-chain) voidaan katkottomasti seurata.

7.5 Tietosuojapolitiikka

Henkilötietolaki korostaa tietojärjestelmien ja henkilötiedon käsittelyn etukäteissuunnittelua. Tietojenkäsittelytoiminnat tulee kartoittaa etukäteen, suunnitella ja toteuttaa lainmukaisesti. Henkilötietolain periaatteista voidaan johtaa mm. seuraavat tietojenkäsittelyn vaatimukset (T. Itälä ja P. Ruotsalainen, Tietoturvallinen kommunikaatioalusta, Luovutusten ja luovutuslokin hallinnan suositukset, OSVE 6/2004):

- etukäteissuunnittelun vaatimus
- huolellisuus ja virheettömyys-, eheys ja luotettavuusvaatimus
- tiedon käyttötarkoitussidonnaisuus
- tiedon tarpeellisuusvaatimus. Arkiston näkökulmasta tämä tarkoittaa, että asiakkaan tule esittää hyväksyttävä syy ja käyttötarkoitus tietojen luovutukseen.
- yhteysvaatimus (tiedon käytön edellytys on hoitosuhde tai muu laista johtuva peruste)
- asiakkaan informointivelvoite

- tietojen suojaamisvelvoite (tietoa ei saa luovuttaa sivulliselle henkilölle tai informaatioprosessille)
- asiakkaan tarkastusoikeus tietoihin
- virheellisen tiedon korjaamisoikeus

Sähköisellä arkistolla tulee olla kirjallinen tietosuojapolitiikka, jossa on kuvattu miten edellä esitetyt tietosuojan toteuttamiseen liittyvät vaatimukset toteutetaan.

Muita tietosuojan toteutuksen hyvän käytännön vaatimuksia ovat:

1. Tietojen luovuttaminen edellyttää, että tietojen vastaanottajan tietosuojapolitiikan on vähintään saman tasoinen kuin tietojen luovuttajan politiikka, ellei potilaan antamasta suostumuksesta tai lainsäädännöstä muuta johdu.

2. Arkiston tulee tarkistaa tietojen luovutusta pyytävän toimintayksikön ja organisaation tietosuojapolitiikka. Tämä voi tapahtua myös luotetun kolmannelta osapuolelta hankittuna palveluna.

3. Koska tiedolla voi olla sen elinaikana useita eri käyttötarkoituksia, tulee tiedon kuvailutietoihin sisällyttää tieto sen käyttötarkoituksista. Arkiston tulee hallita tiedon/dokumentin luovuttamista perustuen tiedolle määriteltyihin ja kuvailutiedoista ilmeneviin tiedon käyttötarkoituksiin.

4. Arkiston tulee kyetä tarvittaessa estämään tiedon luovuttaminen muihin kuin sen kuvailutiedoissa merkittyihin käyttötarkoituksiin.

5. Potilaalla/kansalaisella tulee olla mahdollisuus muuttaa tiedon käyttötarkoitusta.

7.5.1 Suostumusten hallinta

Asiakastietoja arkistoivan organisaation on kyettävä hallinnoimaan ja käsittelemään potilaan antamia tiedon luovutuksen liittyviä suostumuksia. Jos tiedon luovuttaminen edellyttää suostumusta, tulee arkiston varmistaa, että vain niitä tietoja luovutetaan, joita suostumus koskee. Tämän toteuttamiseksi arkistolla tulee olla suostumuksen hallinnan tietojärjestelmä.

Mikäli kansallinen lainsäädäntö niin edellyttää/mahdollistaa, voi potilas/kansalainen kieltää tiedon luovuttamiseen (ns. käänteinen suostumus) tiettyyn käyttötarkoitukseen, tietylle toimintayksikölle, henkilölle tai prosessille.

Suostumusta tiedon luovuttamiseen ja sähköistä suostumusta on käsitelty tarkemmin raportissa OSVE 3/2004 ja oppaassa sähköisen potilaskertomuksen rakenteesta (STM. kansallinen terveyshanke, versio 1.20).

7.6 Arkistoinnin tietomalli ja metatiedot

Asiakastietojen sähköisen arkistoinnin toteuttaminen edellyttää kokonaisvaltaista tietomallia joka kattaa sekä asiakaskertomuksen tuottamisen että arkistoinnin.

Liitteessä 4 on esitetty OASIS standardin mukainen tietomalli. Tietoon ja tietoalkioihin liittyvät metatiedot tuottaa tavallisesti rekisterinpitäjän asiakastieto-järjestelmä (luku 5) Tämän lisäksi arkisto tuottaa arkistoinnin edellyttämät metatiedot.

Arkistoivan järjestelmän tulee kyetä varustamaan talletettavat dokumentit arkistoinnin edellyttämillä metatiedoilla.

Arkisto tallettaa tavallisesti tiedot kiinteinä yksikköinä (vrt. USA:n HIPAA vaatimukset) joita kutsutaan objekteiksi (objects, containers). Riippuen objektien koosta voidaan puhua tiedon eri tasoisesta rakeisuudesta (granulariteetista). Pienin rakeistettu tieto-elementti (objekti) on pienin tietojoukko, joka voidaan arkistosta hakea ja luovuttaa.

Asiakastietoja arkistoivalla organisaation on kyettävä säilyttämään tietoja rakeisessa muodossa. Arkiston tulee kyetä liittämään metatiedot kuhunkin objektiin. Objektin ja metatietojen muodostaman kokonaisuuden muuttumatto-muus tulee varmistaa sähköisellä allekirjoituksella.

Arkisto voi tallettaa potilaan eri toimintayksiköiden tuottamat dokumentit yhteiseen kansioon (patient folder, personal lifelong health record). Tällainen kansio tulee varustaa metatiedolla, jonka avulla voidaan ylläpitää kansion eheys.

7.6.1 Tiedon luokittelu ja merkitseminen

Arkistoitaviin objekteihin tulee voida liittää ominaisuuksia. Asiakastietoja tuottavan organisaation on kyettävä luokittelemaan talletettavat tiedot (objektit) ainakin seuraavien ominaisuuksien suhteen tiedon pienimmällä rakeisuuden tasolla:

- Tietotyyppi
- Tiedon tuottaja (esim. toimintayksikkö, mittalaite, palvelujen tuottaja tai asiakas)
- Tietoturvapolitiikka
- Käyttötarkoitus
- Tuottamisympäristö (context)
- Tietosuoja
- Luottamuksellisuus
- Yksityisyyden suoja
- Erityissuojaustarve
- Positiiviset ja negatiiviset käyttörajoitukset
- Säilytysaika

Erityissuojaus voi olla tarpeen esimerkiksi henkilön geneettisen tiedon ja elintapoihin, sosiaalisiin suhteisiin tai työssäkäyntiin liittyvien tietojen kohdalla.

Asiakastietoja arkistoivalla organisaation on tarvittaessa kyettävä liittämään objekteihin tiedon säilytyksen tai luovutuksen kannalta tarpeellisia luokitustietoja.

7.7 Tiedon luovutuksen hallinta

Asiakirjatietoa arkistoivalla organisaatiolla on oltava luovutuksen hallinnan järjestelmä joka mahdollistaa tiedon luovutuksen hallinnan ja seurannan tiedon luokitteluun ja käyttötarkoitukseen perustuen tiedolle määritellyllä pienimmällä rakeisuuden tasolla.

7.8 Tiedon löytämisen palvelut

Sähköisellä arkistolla on oltava tiedon hakupalvelut (retrieval services, browsing services), joiden avulla varmistetaan arkistoidun tiedon löytäminen ja hakeminen. Edelleen arkistolla tulee olla käytettävissään tarpeelliset hakemistot ja muut tekniset palvelut, jotka mahdollistavan tiedon monipuolisen hakemisen.

7.9 Arkistoitujen tietojen käyttö omassa toiminnassa

Terveydenhuollon toimintayksikön työntekijöillä ja prosesseilla on oikeus käyttää sähköiseen arkistoon lähettämiään oman toimintayksikkönsä tietoja perustuen ko. toimintayksikössä voimassa oleviin käyttöoikeuksiin.

7.10 Toimintayksiköiden erillään pitäminen

Asiakastietoja arkistoiva organisaatio voi tallettaa samaan tekniseen arkistoon/arkistoivaan tietojärjestelmään usean eri terveydenhuollon toimintayksikön tuottamia ja hallinnoimia asiakastietoja.

Toimintayksiköiden arkistoon lähettämät tiedot tulee merkitä (”tagittää”) siten, että kukin toimintayksikkö voidaan tunnistaa yksikäsitteisesti. Arkiston tulee mahdollistaa se, että kaikkien toimintayksiköiden tietoja voidaan käsitellä omina kokonaisuuksina siten, että ne toiminnallisesti muodostavat kunkin rekisterinpitäjän oman arkistokokonaisuuden.

7.11 Henkilötietolain mukainen tarkastuspyyntö

Potilas/kansalainen voi osoittaa tarkistuspyynnön arkistoivalle organisaatiolle ja sen tulee kyetä toteuttamaan pyyntö lainsäädännön ja STM:n määräysten mukaisesti.

Tarkistuspyyntöön liittyvät tiedot tulee säilyttää omassa osarekisterissä, jota saavat käyttää vain siihen erikseen oikeutetut käyttäjät.

Tarkistuspyyntötiedot tulee suojata siten, etteivät ne ole ilman perusteltua syytä toimintayksikön tai hoitoon osallistuvien ammattihenkilöiden käytettävissä.

Arkistolla tulee olla tarvittavat tekniset valmiudet mahdollistaa tarkistuspyynnön toteuttaminen ns. teknisen yhteyden avulla.

7.12 Lokitietojen tarkistaminen

Kansalaisella/potilaalla on oikeus tarkistaa hänen tietojensa luovutusta koskevat merkinnät arkiston ylläpitämästä lokista siten kuin lainsäädännössä erikseen säädetään.

Tarkistaminen voidaan tehdä myös sähköisesti teknisen yhteyden avulla, jolloin asiakas tulee tunnistaa ja todentaa luotettavasti esimerkiksi sähköisellä kansalaiskortilla tai vastaavan tasoisella muulla todentamispalvelulla.

7.13 Aikaleimapalvelut

Arkistolla on oltava aikaleimapalvelu, joka avulla voidaan luotettavasti todeta tiedon arkistointi- ja luovutusaika ja varmistaa arkistotapahtumien kiistämättömyys koko tiedon säilytysajan.

8 Käsitteet ja termit

Käsitteiden ja termien määrittelyssä on käytetty hyväksi seuraavia lähteitä:

- - ISO TC 215/WG4 - Glossary of Security Terms
- - ISO TC 215/WG4 - Background Paper- Health Information Security Standards Framework and Glossary of terms.
- - ISO/DTS 17090
- - ISO/DDTS 22600
- - ISO/IEC 17799
- - VAHTI 4/2003
- - Stakes raportteja 5/2005

aikaleima (time stamp)
tapahtumatietoon tai viestiin liitetty tieto luomis-, lähetys-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista. Aikaleimalla voidaan varmistaa tapahtumien ajankohdan kiistämättömyys

arkisto
Arkisto voidaan määritellä organisaatioksi, joka tallettaa tietoa (esim. potilaskertomuksia) ja mahdollistaa tiedon käytön ja jakamisen tunnistetuille asiakkaille koko tiedolle määritellyn/määrätyn säilytysajan.

- *Sähköinen arkisto (eArkisto)* on organisaatio, jonka tehtävänä on tallettaa tietoa digitaalisessa muodossa säädetyn ajan ja mahdollistaa tiedon käytön tiedon käyttö tunnistetuille (oikeutetuille) henkilöille ja prosesseille.
- *Passiivinen eArkisto* tallettaa tiedon, siihen liittyvät metatiedot ja politiikkatiedot kiinteässä muodossa (kts. HIPAA-määrittelyt).
- *Pysyvä arkisto* on passiivisen arkiston erityisluokka. Se tallettaa tietoa pysyvästi.
- *Notariaattiarkisto* on luotetun osapuolen varmistama arkisto

asiakas
terveydenhuollon toimintayksikkö, muu organisaatio tai potilas tai prosessi, joka käyttää arkistoon tai EHR-järjestelmään tallennettua tietoa.

asiakastieto
Potilasasiakirjat ja muu hoitoon liittyvä tieto

attribuuttivarmentaja (Attribute Authority)
taho joka myöntää attribuuttivarmenteen.

attribuuttivarmenne
tietorakenne, jonka attribuuttivarmentaja on sähköisesti allekirjoittanut, joka liittää yhteen attribuuttien arvot ja niiden haltijan identifioinnin.

digitaalinen aineisto (digital material)
Kokonaisuus, joka muodostuu digitaalisessa muodossa olevasta tekstistä, muusta datasta ja dokumenteista

dokumentti (Document)
Mikä tahansa asiakirja (tai tiedosto), joka voi sisältää kirjoitusta, merkkejä, kuvia, symboleja, ääniä ja joilla on merkitys niitä tulkitseville henkilöille.

hakemistopalvelu (directory service)
kokoelma ohjelmia, laitteistoja, prosesseja menetelmiä (policies) ja hallinnollisia toimia, joita käytetään hakemistoon talletetun tiedon järjestämiseen ja jakamiseen käyttäjille

Hakemistopalvelun ominaisuuksista on luotu standardit X.500 ja LDAP (kevytversio, *lightweight directory access protocol*), joissa määritellään esimerkiksi hakemistojen ja niissä sijaitsevien objektien ja tietojen rakenteet ja ominaisuudet, tietojen hakumenetelmät ja hakuprotokollat.

henkilövarmenne (personal certificate, identity certificate)
varmenne, jota käytetään henkilön henkilöllisyyden vahvistamiseksi

identiteetti
joukko ominaisuuksia, jotka kuvaavat käyttäjää ja joiden avulla käyttäjä voidaan tunnistaa

käyttäjien hallinta (user management)
palvelu, jolla ylläpidetään käyttäjien ominaisuuksia ja tietoa siitä minkä tyyppinen käyttäjä voi käyttää palvelua.

käyttäjäidentiteetti
palveluntarjoajan tiedossa olevat käyttäjän henkilöllisyyttä yksilöivät ja kuvaavat tiedot.

käytön hallinta (access control)
toimet, joilla varmistetaan, että tietoa käsittelevien prosessien resursseja voivat käyttää vain ne henkilöt, prosessit tai järjestelmät, joilla on siihen valtuus.

käyttöoikeus (access right)
käyttäjälle annettava tiettyyn tietoon, ohjelmistoon tai järjestelmään annettava oikeus

Käyttöoikeuksia ovat esimerkiksi lukuoikeus, kirjoitusoikeus, muutosoikeus, tuhoamisoikeus ja hallintaoikeus eli muiden käyttäjien oikeuksien määrittely.

käyttövaltuus (user right, authorization, privilege)
tietojärjestelmän käyttäjälle myönnetyt yksilöidyt oikeudet nimettyjen tietojen, järjestelmien, ohjelmistojen tai niiden osien käyttöön

luottamuksellisuus (confidentiality)
tietoon liittyvä ominaisuus joka kertoo, että tieto ei ole paljastunut tai käytössä ulkopuoliselle henkilölle, prosessille tai järjestelmälle.

palvelinvarmenne (server certificate)
tietojärjestelmän palvelimelle myönnetty varmenne, jonka avulla käyttäjä voi varmistua siitä, että asioi oikean palvelimen kanssa.

PMAC (privilege management and access control)
käyttöoikeuksien hallinnointi ja tiedon käytön hallinta

politiikka (policy)
toimintatapa, menettelyperiaate.

Periaatteiden ja sääntöjen joukko, joka kattaa kohteena (piirissä) olevien osapuolten vuorovaikutukset. Sähköisen arkiston hallinnoijan määrittelemät säännöt, jotka määrittävät keillä käyttäjillä on valtuutus käyttää ja mitä aineistoa

potilaskertomusjärjestelmä (EHR-system)
potilaskertomusjärjestelmä mahdollistaa potilaskertomusten luomisen ja sillä on tarpeelliset mekanismit tiedon hakua, säilytysta ja käyttämistä varten.

pääsynhallinta (access control)
toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille. Pääsynhallinnassa tietojärjestelmien, tietoverkkojen ja tietojen käyttäjät tunnistetaan ja todennetaan sovitulla tavalla.

rooli (role)
pätevyyksien ja/tai tehtävien joukko jotka liittyvät johonkin tehtävään.

roolivarmenne (role certificate)
varmenne, joka vahvistaa sekä henkilön henkilöllisyyden että oikeuden toimia jossakin roolissa kuten työtehtävässä.

STM
Sosiaali- ja terveysministeriö

sähköinen potilaskertomus (EHR)
EHR on tietovarasto johon on talletettu hoidon kohteena olevan henkilön asiakastietoa tietoturvallisesti tietokoneella käsittelyyn sopivassa muodossa siten, että tietoa voidaan käyttää ja siirtää autorisoiduille käyttäjille ja prosesseille.

tiedon tuottaja (producer)
Terveydenhuollon toimintayksikkö, muu organisaatio tai potilas tai prosessi joka lähettää tietoa tallennettavaksi.

tietosuoja (privacy protection, data protection)
Tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen. Henkilötietojen suojaaminen valtuudettomalta ja henkilöä vahingoittavalta käytöltä. Tietosuojaon yksilön suojaa ihmisten yksityiselämän ja yksityisyyden suoja ja näitä turvaavat oikeudet esimerkiksi henkilö- tai asiakastietoja käsiteltäessä. Tietosuoja-termi on nimenomaan juridinen, ja sen toteuttamisesta ja vaatimuksista on säädetty useassa eri laissa.

tietoturva, tietoturvallisuus (information security)
tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu.

Asiantila, jossa tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää riskiä.

tietosuojapolitiikka (privacy policy, privacy protection policy, data protection policy)
tietosuojasäädökset ja niiden toimeenpanoa koskevat päätökset

Jos organisaatio käsittelee yksityishenkilöiden henkilötietoja, se laatii asiakirjan *tietosuojapolitiikka* tai *henkilötietojen käyttö*, jossa kuvataan henkilöön liittyvien henkilötietojen tai muiden luottamuksellisten tietojen käytön periaatteet ja käytäntö organisaatiossa. Asiakirja voidaan jakaa myös niille, joiden henkilötietoja organisaatio käsittelee, jolloin voidaan edesauttaa luotettavan kuvan syntymistä organisaation toiminnasta.

tietoturvapolitiikka (security policy, information security policy, data security policy)
organisaation tasolla johdon hyväksymä näkemys ja julkaistu kannanotto tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta

Tietoturvapolitiikka annetaan tyypillisesti esimerkiksi asiakkaiden, yhteistyökumppaneiden tai toimittajien luettavaksi. Se on osoitus organisaation tahdosta ja kyvystä käsitellä tietoja turvallisesti ja luotettavasti. Tietoturvapolitiikka ei yksilöi periaatteita eikä käytäntöä niin tarkasti, että dokumentin jaolla organisaation ulkopuolelle olisi vaikutusta tietoturvallisuuteen.

todennus (authentication, verification)
tietojärjestelmän käyttäjän (kuten henkilö, laite tai ohjelmisto) tai viestinnän toisen osapuolen aitouden ja oikeellisuuden varmistaminen halutulla luottamustasolla.

tunnistus (identification)
menettely, jolla yksilöidään joku tai joki esimerkiksi tietojärjestelmän käyttäjä.

uhka (threat)
(esimerkiksi) organisaatioon, tietoihin tai tietojärjestelmään tietyltä taholta kohdistuvan vahingon tai häiriön mahdollisuus

vahva tunnistus (strong authentication)
käyttäjän tunnistus ja todennus, joka käyttää ainakin kahta kolmesta todennustavasta: jotakin, mitä käyttäjä on jotakin, mitä käyttäjä tietää tai jotakin, mikä käyttäjällä on hallussaan.

varmenne (certificate)
aitoustodistus, sähköinen todistus, jolla vahvistetaan, että todistuksen haltija on tietty henkilö, organisaatio tai järjestelmä. Varmenne on yleensä ulkopuolinen luotettu tahon (varmentaja) myöntämä. Varmenne voi sisältää muun muassa käyttäjän julkisen avaimen, henkilötiedot, varmenteen voimassaolopäiväyksen ja varmentajan sähköisen allekirjoituksen. Kun varmenne on varmentajan sähköisesti allekirjoittama, sen aitous on varmistettavissa.

Varmenne voidaan myöntää esimerkiksi henkilölle, laitteelle tai sovellukselle. Varmenteiden ominaisuuksia on määrittelty mm. ITU:n standardissa X.509.

Laitteistolle tai ohjelmistolle myönnettyä varmennetta kutsutaan tapauskohtaisesti laitevarmenteeksi, palvelinvarmenteeksi tai ohjelmistovarmenteeksi. Koska tällainen varmenne identifioi tyypillisesti sen organisaation, jonka palveluita kyseisellä laitteistolla ja ohjelmistolla tuotetaan, käytetään tässä yhteydessä joskus myös termiä organisaatiovarmenne.

varmentaja (certificate authority)
taho joka myöntää varmenteen.

Väestörekisterikeskus (VRK) toimii varmentajana, joka myöntää kansalaisille sähköistä asiointia varten sähköisiä henkilöllisyystodistuksia, kansalaisvarmenteita.

varmenteiden hallinnointi (Certificate management)
varmenteisiin ja niiden käsittelyyn liittyvät menetelmät ja prosessit kuten varmenteen generointi, varmenteen jakaminen, varmenteiden tallettaminen ja peruuttaminen.

varmenteen jakaminen (Certificate distribution)
menetelmä varmenteiden jakamiseksi.

X.509
ITU-T standardi X.509

9 Tausta-aineisto

Tämän ohjeen teossa on käytetty seuraavia dokumentteja:

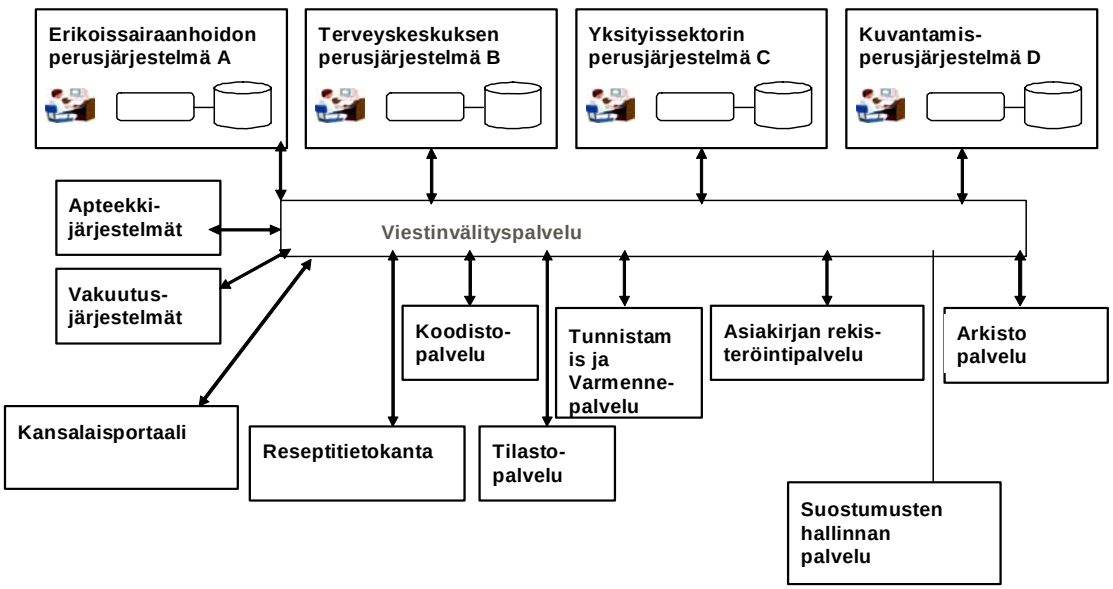
- ARKKI- sähköisen arkiston toiminnallinen määrittely -projektin loppuraportti, 15.12.2005.
- Australian Standard for Records Management – AS ISO 15489.
- Ensio A ja P. Ruotsalainen , Tietoturvallinen kommunikaatioalusta, Tehtävä 7 Sähköisen arkistoinnin hyvät periaatteet, Suostukset (Julkaisematon sisäinen OSKEn raportti).
- Ensio A ja Ruotsalainen P, Tietoturvallinen kommunikaatioalusta: Suositus kansallisesti noudatettaviksi standardeiksi, OSVE 7/2004.
- Ensio A ja Ruotsalainen P, Tietoturvallinen kommunikaatioalusta: Suositus kansallisesti noudatettaviksi standardeiksi, OSVE 7/2004.
- HIPAA dokumentaatio, www.hipaadvisory.com.
- ISO/PDTS 22600, Health Informstics -Privilege Management and Access Control, parts 1-3.
- ISO/DIS 1471 Reference Model for open Archival Information Systems (OAIS).
- ISO 15489 Information and Documentation – Records management
- ISO/TCc215 WD ”Health Informatics – Secure Archiving of Electronic Health Records”, 2004-8-09.
- ISO/IEC 17799:2005, Information technology – Code of practice for information security management.
- ISO DTS 27799 Health Informatics -Security Management in Health using ISO/IEC17799.
- Itälä T ja Ruotsalainen P, Tietoturvallinen kommunikaatioalusta: Luovutusten ja luovutuslokin hallinnan suositukset, OSVE 6/2004.
- Kansallinen sähköinen potilastietojen arkistopalvelu- Toiminnallinen vaatimusmäärittely, STM:n työryhmämuistio 2005:21.
- Metadata Reference Guide, About the Metadata Encodong and Transmission (METS), http://libraries.mit.edu.
- Mikola T, Sorvari H ja Ruotsalainen P:Tietoturvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi, OSVE 3/2004.
- Opas sähköisen potilaskertomuksen rakenteesta, STM, Kansallinen terveyshanke, versio 1.19.
- Peterson H., Long-Term storage of electronic healthcare information in XML-format, The Park project, 01.01.2000.
- Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen, Opas terveydenhuollon henkilöstölle, STM:n oppaita 2001:3.
- Ruotsalainen P, Attachment 8, Interreg PACS. Final Report, University of Helsinki 2003.
- Ruotsalainen P and Manning B, Security Requirement for Digital Archiving of Personal Health Information, outline for ISO TC215 WG4, September 2005.

- Ruotsalainen P, A cross-platform model for secure Electronic Health Record communication, International Journal of Medical Informatics (2004) 73.
- Ruotsalainen P, Security requirements in EHR systems and Archives, Stud Health Technol Inform 2004;203;453-8.
- Ruotsalainen P, HER security: present requirements and future challenges, PHHE 2006.
- Ruusalepp R, Riskarkivet, Digital Preservation in Archives: An Overview of Current Research and Practices, Eesti ÄriARHIIV, February 2005.
- Recih L and Sawyer D, Reference Model for an Open Archival Information Systems (OAIS): Overview and Current Status, Digital Curation Workshop, London, 2001.
- Sosiaali- ja terveysministeriön asetus 99/2001.
- Tammisalo T, Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt, Stakes Raportteja 5/2005.
- Terveydendenhuollon valtakunnallsien tietojärjestelmäarkkitehtuurin periaatteet, Alueellisista ratkaisuista kansalliseen kokonaisuuteen, STM:n selvityksiä 2006:8.
- Trusted Digital Repositories: Attributes and responsibilities, An RLG-OCLC report, Mountain View, CA, May 2002.
- Valtionarkisto, SÄHKE-hanke, Toiminnallinen määrittelyt.
- Valtionarkisto, SÄHKE-hanke, Toiminnallinen mallintaminen.
- Valtionarkisto, SÄHKE-hanke, Abstrakti mallintaminen.
- Valtionarkisto, SÄHKE-hanke, Metatiedot.
- Valtionarkisto, SÄHKE-hanke, Tekninen mallintaminen.
- Victorian Electronic Records Strategy : Prototype Archival Design, Ernst & Young, 11 June, 1998.

Liite 1

POKA ryhmän ehdotus terveydenhuollon kansalliseksi tietojärjestelmäarkkitehtuuriksi

Valtakunnallinen arkkitehtuuri



Liite 2

Terveydenhuollon sähköisen arkistoinnin toteuttamisen yhteydessä huomioon otettavaa lainsäädäntöä

- **EU:n Directive 95** on the protection of individuals with regard to the processing of personal data and on the free movement of such data

YLEISET LAIT

- Suomen perustuslaki (731/1999); 10 pykälä
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Arkistolaki (831/1994)
- Henkilötietolaki (523/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Viestintämarkkinalaki (393/2003)
- Rikoslaki 38 luku ja 34 luvun 9a pykälä
- Laki eräiden suojausten purkujärjestelmien kieltämisestä (1117/2001)
- Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki Kainuun maakuntakokeilusta 343/2003 ja laki Kainuun hallintokokeilusta annetun lain muuttamisesta.

TERVEYDENHUOLLON ERITYISLAINSÄÄDÄNTÖ

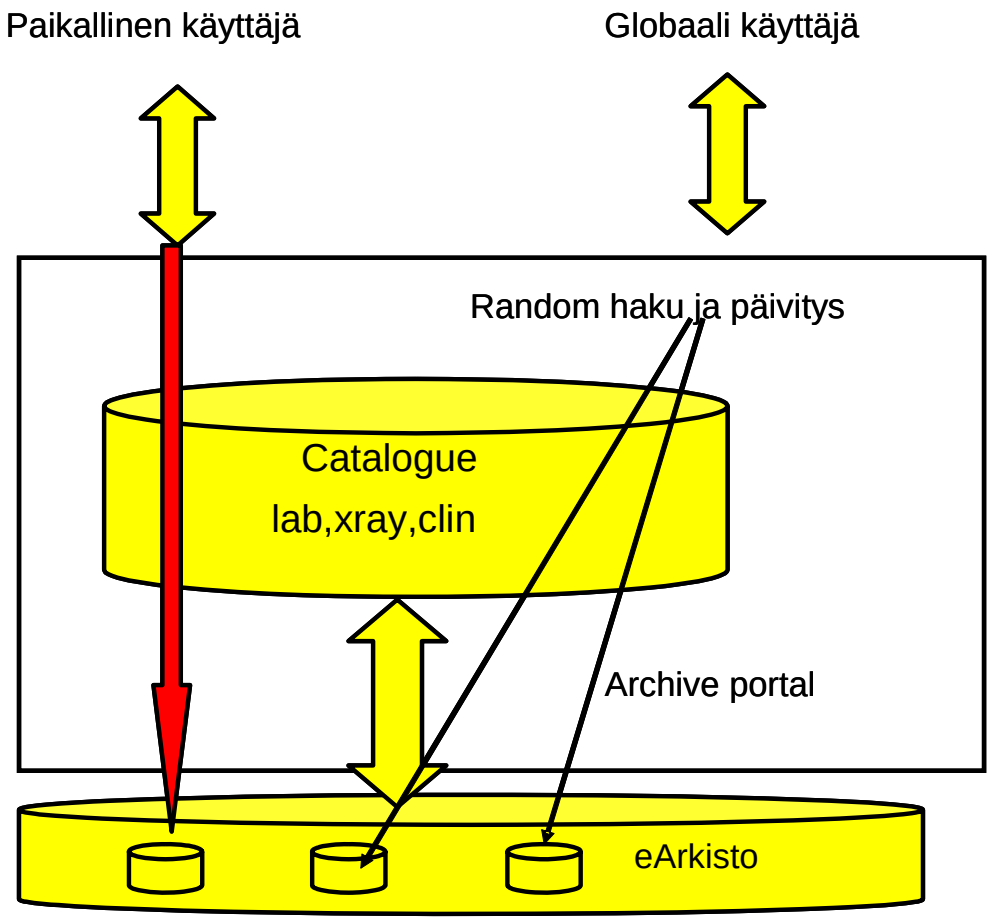
- Erikoissairaanhoitolaki ja siihen tehdyt muutokset 1.8.2000 (652-653/200) ja (856/2004)
- Laki potilaan asemasta ja oikeuksista (1992/785) ja siihen tehdyt muutokset 857/2004
- Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaalikortin kokeilusta 811/2000 ja siihen myöhemmin tehdyistä päivityksistä.
- Valtioneuvoston asetus hoitoon pääsyn toteuttamisesta ja yhteistyöstä 1019/2004
- STM:n asetus potilasasiakirjojen laatimisesta ja niiden ja muiden hoitoon liittyvän materiaalin säilyttämisestä (99/2001)
- Asetus sähköisen lääkemääräyksen kokeilusta (771/2003)
- Valmisteilla oleva laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä.

MUU LAINSÄÄDÄNTÖ

- Arkistolaki 831/1994
- Arkistotoimen vaatimukset automaattisessa tietojenkäsittelyssä. Annettu Helsingissä 26 päivänä maaliskuuta 1987. Valtionarkiston yleinen ohje n:o 14. Helsinki 1987. 13 s. ISBN 951-47-0502-5. ISSN 0357-6191.
- Arkistolaitoksen suositus arkistonmuodostussuunnitelman laadinnan, käytön ja ylläpidon periaatteiksi.

Liite 3

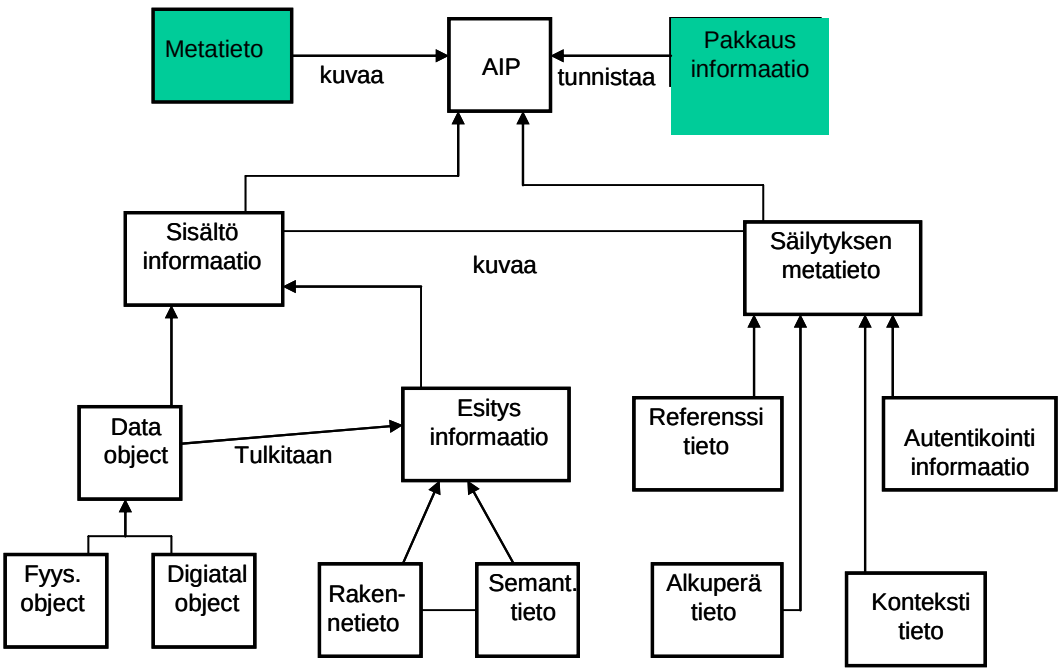
Aktiivinen arkisto



Liite 4

Sähköisen arkistoinnin tietomalli (OAIS-malli)

OAIS Tietomalli



Liite 5

Arkistotyypit

Arkistokategoriat

Independent	Ei hallinnollista tai teknistä vuorovaikutusta toisten arkistojen kanssa
Cooperating	Yhteiset proseduurit ja tiedon lähetys- ja jakelustandardit mutta EI yhteisiä hakumekanismeja
Federated	Arkistoilla on myös yhteinen hakumekanismi
Shared resources	Arkistolla on sopimus toisten arkistojen yhteisten palvelujen käytöstä

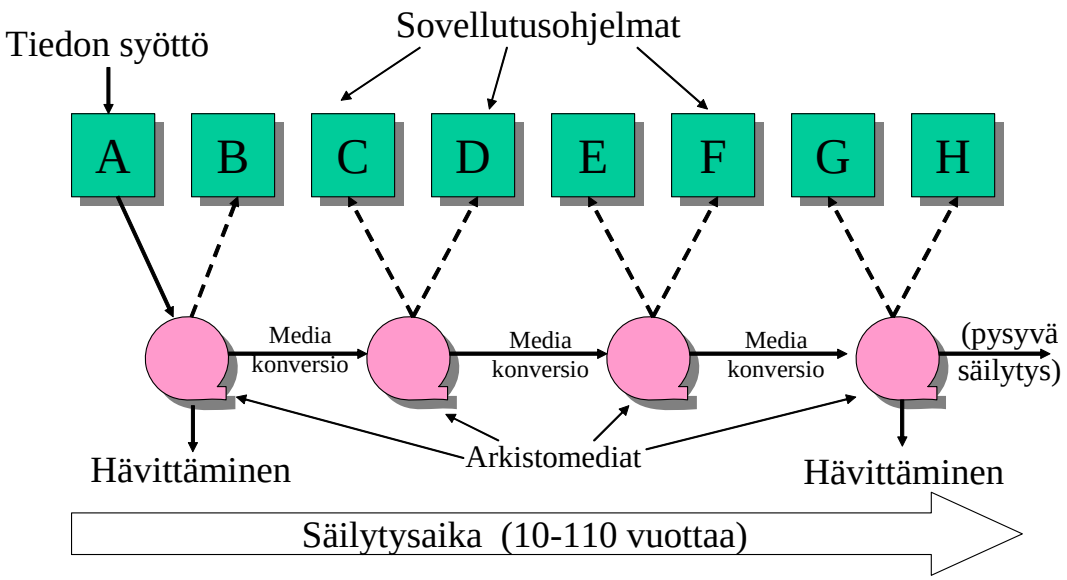
Lähde: ISO

Liite 6

Tiedon elinkaaren hallinta pitkäaikaisessa sähköisessä arkistoinnissa

Tiedon elinkaari voi olla pitempi kuin 100 vuotta. Tänä aikana sekä säilytysohjelmistot ja lukuohjelmistot että säilytysmediat muuttuvat. Tiedon saatavuuden varmistamiseksi tarvitaan sekä tiedon rakenne että säilytysmedian konversioita.

Tiedon elinkaari arkistoinnissa



Usean toimintayksikön yhteinen käyttäjän ja käyttöoikeuksien hallinta - periaatteet ja suositukset

Tiivistelmä

Kansallisissa terveydenhuollon strategioissa on vuodesta 1998 lähtien korostettu sekä potilaan hoidon ja palvelun yliorganisatorisen järjestämisen että näiden palvelujen tarvitseman tietojärjestelmätuen välttämättömyyttä. Saumattoman palveluketjun, monen organisaation yhteisen palvelukokonaisuuden ja organisaatiorajat ylittävän tiimityön tietotekniikkatuki tarkoittaa muun muassa sitä, että potilastietojärjestelmissä oleva tieto tulee olla 24h/7d käytettävissä riippumatta siitä kenen rekisterinpitäjän tietojärjestelmässä tieto on talletettuna. Tätä tavoitetta on pyritty realisoimaan kehittämällä aluetietojärjestelmiä ja joissain tapauksissa myös antamalla oman tietojärjestelmän käyttöoikeuksia toisen toimintayksikön ammattihenkilöille. Aluetietojärjestelmien kehittyminen on synnyttänyt myös kaupallisia ratkaisuja, joissa useat eri toimintayksiköt käyttävät samaa toimittajakohtaista tietojärjestelmäpalvelua**.**

Toimintayksikkökohtaisissa tietojärjestelmissä (ns. perinnejärjestelmissä) loppukäyttäjät tunnistetaan ja heidän käyttöoikeuksiaan hallitaan toimintayksikön sisäisellä tietojärjestelmällä. Niissä tilanteissa, joissa halutaan sallia toimintayksikön henkilökuntaan kuulumattoman käyttäjän olevan tietojärjestelmän loppukäyttäjä, joudutaan etsimään uusia toimintamalleja ja tekniikoita, joiden avulla voidaan hallinnoida tällaisten ulkopuolisten käyttäjien tunnistamista, käyttöoikeuksia ja tietojen käyttöä. Lähtökohtana on, että tiedon käyttö tai luovutus on kaikkien käyttäjien kohdalla lainmukaista ja, että tiedon käyttöä ja luovutusta kyetään seuraamaan ja valvomaan.

Tämä muistio tarkastelee vaihtoehtoisia malleja ja tekniikoita, joiden avulla voidaan toteuttaa usean eri toimintayksikön käyttäjien ja käyttöoikeuksien hallinta keskitetysti, tietoturvallisesti ja kansainvälisiin standardeihin perustuen. Tämä muistio suosittelee kansalliseksi ratkaisuksi mallia, joka perustuu PMI-, PKI ja LDAP-hakemistopalvelujen yhdistämiseen toiminnalliseksi kokonaisuudeksi. Tämä periaate soveltuisi myös käytettäväksi kansallisen keskitetyn digitaalisen arkiston yhteydessä. Edelleen raportti suosittelee, että tunnistaminen ja käyttöoikeuksien hallinta pidetään toistaan erillä.

Raportissa suositellun ratkaisumallin pohjalta olisi tarpeellista käynnistää yksityiskohtainen toiminnallinen ja tekninen suunnittelutyö, jonka yhteydessä tulisi laatia sekä migraationsuunnitelma siitä, miten toimintayksikkökohtaisista käyttäjän ja käyttöoikeuksien hallinnan ratkaisuista siirrytään suositellun arkkitehtuurin mukaiseen toteutukseen.

Tämä dokumentti on lähetetty lausunnolle Suomen HL7-yhdistyksen teknisen komitean jäsenille ja hankepäällikkö Maritta Korhoselle. Erityiset kiitokset saaduista palautteista haluan lausua toimitusjohtaja Antero Ensiolle ja hankepäällikkö Maritta Korhoselle.

Tämä raportti on osa kansallisen terveyshankkeen sähköisen potilaskertomuksen käyttöönotto -projektia ja se on tuotettu osana STM:n ja Stakesin yhteisrahoitteista kehittämishanketta.

Pekka Ruotsalainen
Tutkimusprofessori

1 Johdanto

Terveydenhuollon potilasasiakirjojen käyttö toimintayksikön omassa toiminnassa samoin kuin tietojen luovutus tulee tapahtua lainmukaisesti, tietoturvallisesti ja potilaan yksityisyyttä kunnioittaen. Terveydenhuollon asiakastietojen käyttöön ja luovutukseen liittyvää lainsäädäntöä on kuvattu yksityiskohtaisemmin seuraavissa terveyshankkeen ja Stakesin raporteissa:

- Ruotsalainen P, Suositukset terveydenhuollon asiakastojen tietoturvalliselle sähköiselle arkistoinnille (painossa)
- Itälä T ja Ruotsalainen P, Tietoturvallinen kommunikaatioalusta: Luovutusten ja luovutuslokin hallinnan suositukset, OSVE 6/2004.
- Mikola T, Sorvari H ja Ruotsalainen P. Tietoturvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi, OSVE 3/2004.
- Marja Pajukoski, Sähköinen asiointi sosiaali- ja terveydenhuollossa, lainsäädännön rajat ja mahdollisuudet (Stakes raportteja 282/ 2004).

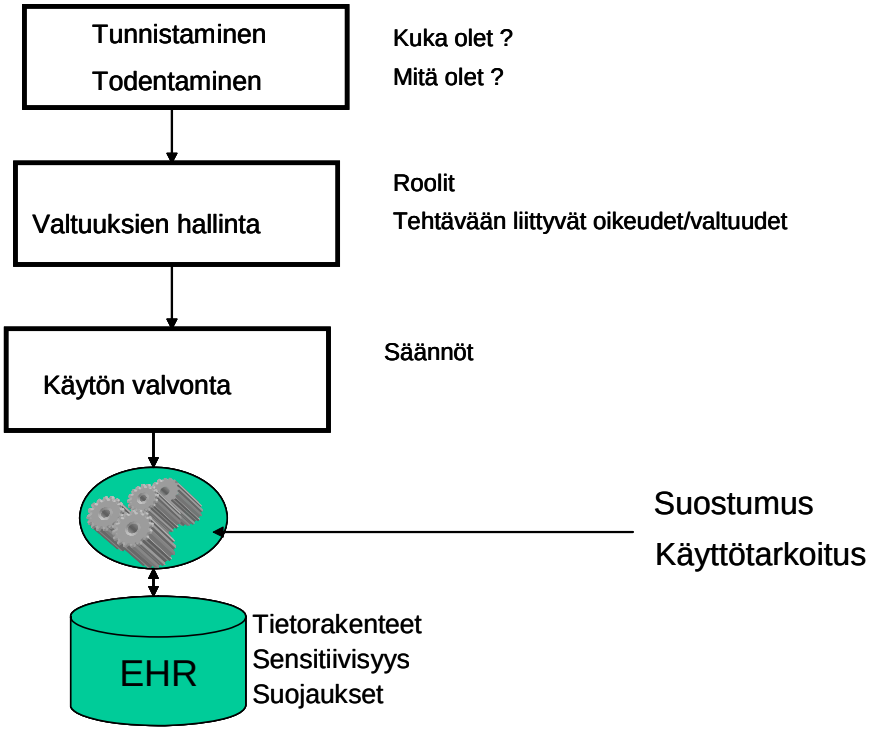
Voimassa olevasta lainsäädännöstä ja muusta säätelystä voidaan johtaa potilasasiakirjatiedon ja muun terveyteen liittyvän henkilötiedon sähköiselle käsittelylle seuraavat yleiset vaatimukset:

- Tietojen käyttö, talletus, ylläpito ja luovutus tulee olla suunnitelmallista.
- Tiedot eivät saa joutua ilman suostumusta tai laista johtuvaa muuta perustetta sivullisten käsiin.
- Terveydenhuollon ammattihenkilö tulee voida tunnistaa ja todentaa sähköisessä asioinnissa.
- Potilas/asiakas tulee voida tunnistaa ja todentaa sähköisessä asioinnissa.
- Toimintayksiköt, palvelimet ja muut entiteetit tulee voida tunnistaa ja varmentaa.
- Vain hoidon kannalta tarpeellisia tietoja saa käsitellä.
- STM:n norminannolla erikseen määritellyissä potilasasiakirjoissa tulee olla omakätinen tai sähköinen allekirjoitus.
- Tietojen käsittelyn edellytys on hoitosuhde, asiayhteys tai muu laista johtuva peruste.
- Jollei laista muuta johdu, ei henkilötietoja saa käyttää muuhun käyttötarkoitukseen kuin mihin ne on kerätty.
- Potilaalla on oikeus määrätä (lain säätämissä rajoissa) omien terveystietojen käytöstä ja luovutuksesta
- Rekisterinpitäjän tulee voida seurata tietojen käyttöä ja luovutusta

Edellä esitetyt vaatimukset johtavat siihen, että terveydenhuollon tietoja käsittelevällä tietojärjestelmällä tulee olla käytössä järjestelmät, jotka tuottavat seuraavat palvelut:

- käyttäjien hallinnan ja tunnistamisen palvelut
- käyttöoikeuksien hallinnan tietojärjestelmäpalvelut
- tietojen käytön hallinnan tietojärjestelmäpalvelut (access control services)

Lisäksi on tarpeen toteuttaa erillinen tietojen käytön, seurannan ja valvonnan tietojärjestelmäjärjestelmäpalvelu.



Kuva 1 Käyttäjän hallinnan ja käyttöoikeuksien periaatemalli

Terveydenhuollon toimintayksikkö on Suomessa potilastietojen rekisterinpitäjä. Toimintayksikkökohtaiset tietojärjestelmät on suunniteltu tukemaan ensisijaisesti toimintayksikön sisäisiä prosesseja. Tästä johtuu, että perinnejärjestelmää käyttävä toimintayksikkö:

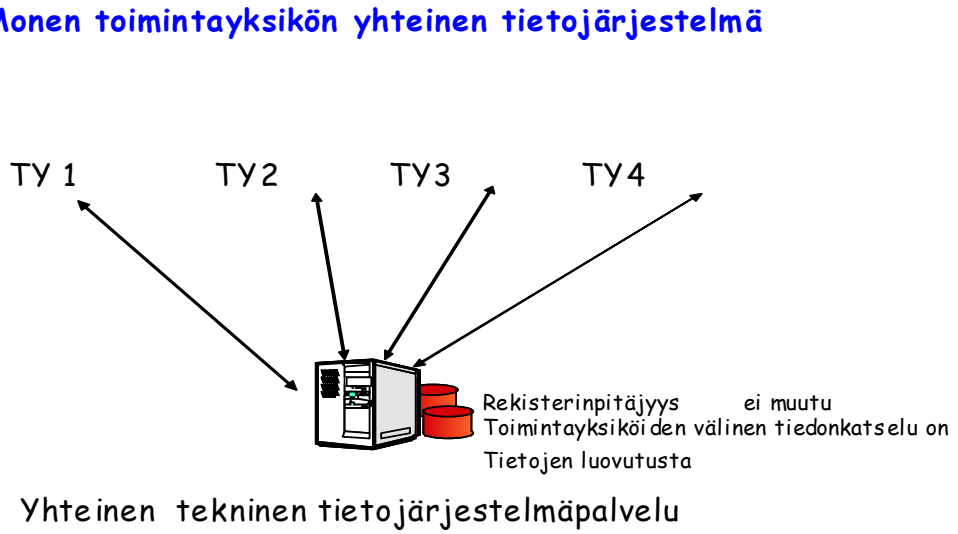
- valitsee ja tunnistaa tietojärjestelmänsä käyttäjät
- päättää käyttäjien työtehtävistä ja määrittää käyttäjille niiden mukaiset roolit
- antaa käyttäjille käyttöoikeudet heidän rooliensa mukaisiin sovellutuksiin sekä työtehtävien edellyttämiin tietoihin

Tietosuojan näkökulmasta toimintayksikkö muodostaa tietoturva-alueen (ns. security domain), jolla tulee olla yhtenäinen tietoturvapolitiikka.

1.1 Yliorganisatoriset hoito- ja palvelumallit

Kansallisissa terveydenhuollon strategioissa on vuodesta 1998 lähtien korostettu potilaan hoidon ja palvelujen yliorganisatorista palvelun järjestämistä ja näiden palvelujen tarvitseman tietojärjestelmätuen tarpeellisuutta. Tämä tarkoittaa mm. sitä, että tarpeellinen potilastietojärjestelmissä oleva tieto tulee olla 24h/7d terveydenhuollon ammattihenkilöiden ja prosessien käytettävissä riippumatta siitä kenen rekisterinpitäjän tietojärjestelmässä tieto on talletettuna. Tätä tavoitetta on pyritty realisoimaan mm. kehittämällä aluetietojärjestelmiä ja joissain tapauksissa antamalla toimintayksikön oman tietojärjestelmän käyttöoikeuksia toisen toimintayksikön ammattihenkilöille.

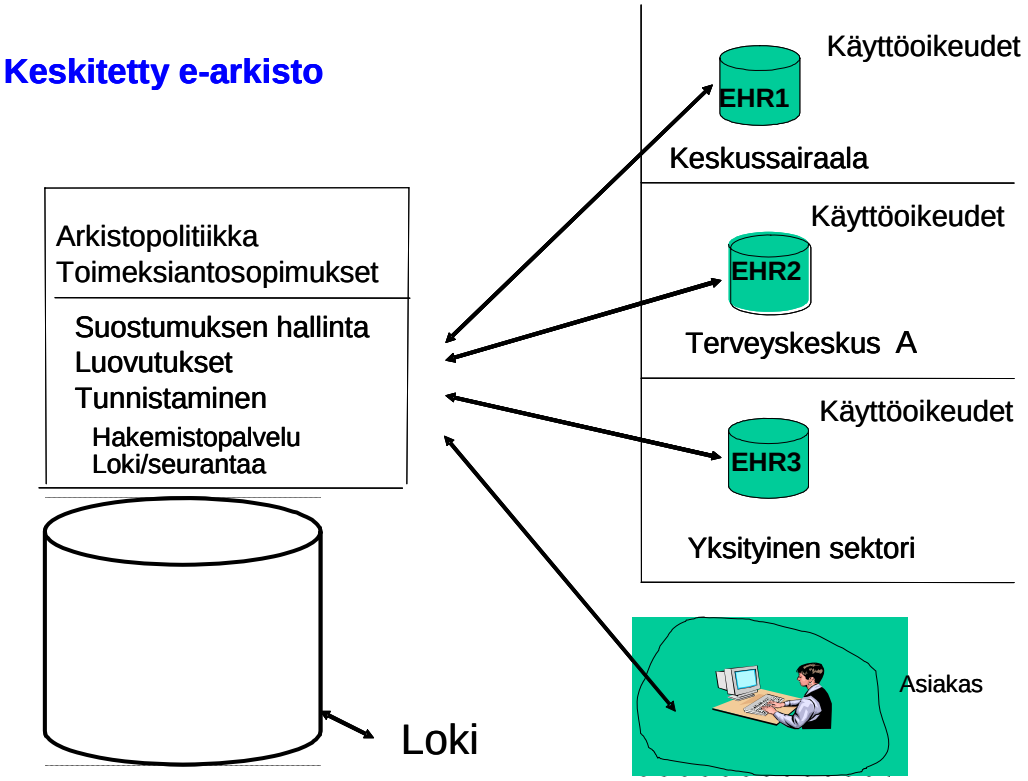
Aluetietojärjestelmien kehittyminen on synnyttänyt myös teknisiä ratkaisuja, joissa useat eri toimintayksiköt käyttävät yhteistä toimittajakohtaista tietojärjestelmäpalvelua (mm. Alue-Effica ja Kunta-Esko). Kuva 2 esittää periaatetasolla tällaista ratkaisua.



Kuva 2 Usean toimintayksikön yhteisesti käyttämä tietojärjestelmä

STM:n asettaman POKA-ryhmän ehdottamassa valtakunnallisessa terveydenhuollon tietojärjestelmäarkkitehtuurissa on esitetty toteutettavaksi kaikille toimintayksiköille yhteinen keskitetty sähköinen potilaskertomusarkisto. Kuvassa 3 on esitetty tällaisen arkiston periaatemalli.

Sekä keskitetyn arkiston että usean toimintayksikön yhteiskäyttöisen tietojärjestelmän tietojen käytön ja luovutuksen hallinta voidaan toteuttaa usealla eri tavalla. Tiedon käyttö ja luovutus voi tapahtua esimerkiksi sanomamuotoista kommunikaatiota käyttäen siten, että toisen toimintayksikön tietojärjestelmän käyttäjä ei kirjaudu tietoja luovuttavan järjestelmän käyttäjäksi. Tiedon käyttö ja luovutus voidaan toteuttaa myös siten, että tietojärjestelmillä on yhteinen käyttäjien ja käyttöoikeuksien hallintajärjestelmä ja eri toimintayksiköiden käyttäjät pääsevät käyttämään loppukäyttäjinä toistensa tietoja. Jälkimmäisessä vaihtoehdossa toisen toimintayksikön käyttäjällä on aidosti myös tietoja luovuttavan järjestelmän käyttäjän status.



Kuva 3 Usean toimintayksikön yhteisen eArkiston periaatemalli

2 Käyttöoikeuksien hallinnan malleja

Käyttöoikeuksien hallinta perustuu tavallisesti johonkin seuraavista periaatteista:

- yhteiseen politiikkaan (common policy)
- yhteiseen ympäristöön (common environment)
- yhteiseen teknologiaan (common technology)

Käyttöoikeuksien hallintaa varten on kehitetty useita eri periaatteita (malleja). Seuraavassa käsitellään yksityiskohtaisemmin näistä keskeisimpiä.

2.1 Salasanojen ja käyttöoikeuksien antaminen toimintayksikön ulkopuolisille

Kyseessä on menetelmä, jossa toimintayksikkö antaa oman tietojärjestelmänsä salasanoja ja käyttöoikeuksia toisten toimintayksiköiden työntekijöiden käyttöön. Tällä mallilla ei tarkoiteta tilannetta, jossa usealla toimintayksiköllä on yhteinen käyttäjien ja käyttöoikeuksien hallinnan palvelu, joka jakaa salasanoja ja käyttöoikeuksia kunkin toimintayksikön henkilökunnalle niiden omiin tietojärjestelmiin.

Salasanojen jakamista käytetään jossain määrin mm. Pohjois-Pohjanman sairaanhoitopiirin alueella, antamalla valituille terveyskeskuksen ammattihenkilöille käyttöoikeudet ja salasanat keskussairaalan potilastietojärjestelmään (suullinen tieto, K. Säkkinen). KAAPO-projektissa on käytössä "yhteisesti sovitut käyttöoikeudet oman ja toisen organisaation kertomukseen" (K. Hassinen).

Tietosuojan ja tietoturvan näkökulmasta muun kuin oman toimintayksikön työntekijän suorittama tietojen katseleminen teknisellä yhteydellä merkitsee tietojen luovuttamista toiselle toimintayksikölle. Salasanojen ja käyttöoikeuksien luovuttaminen toimintayksikön ulkopuolisille henkilöille tai prosesseille nostaakin esille useita tietoturvan ja -suojan hallintaan liittyviä ongelmia. Näitä ovat mm.

- miten on varmistettu, että tietoja vastaanottavan ja luovuttavan toimintayksikön tietoturvapolitiikat ovat samantasoisia?
- miten tietojen luovuttaja kykenee varmistumaan potilaan suostumuksen tai laista johtuvan muun perusteen olemassaolosta ennen tietojen luovuttamista?
- miten tietojen luovuttaja varmistuu asiayhteyden (esimerkiksi hoitosuhteen) olemassaolosta?
- miten tietojen luovutus voidaan rajata vain siihen asiakkaaseen, jonka tietojen luovutukseen on olemassa asianmukaiset perusteet?
- miten varmistetaan, että vain tarpeellisia tietoja luovutetaan?
- miten voidaan olla selvillä tietojen mahdollisesta jatkokäytöstä tietoja vastaanottavassa organisaatiossa ja miten käyttöä voidaan valvoa?
- miten valvotaan, että toimintayksikön ulkopuoliselle annettuja salasanoja ja käyttäjätunnuksia käytetään vain niistä toimintayksiköstä ja työpisteitä, jossa tapahtuvaan käyttöön ne on tarkoitettu?

Vaikka osa edellä esitetyistä ongelmista voidaan ratkaista toimintayksiköiden välisillä sopimuksilla ja tietojärjestelmien sertifioinnilla, on tietojen luovuttajan hyvin vaikea varmistua ilman perusteellista seurantajärjestelyä siitä, että vaadittava asiayhteys ja suostumus ovat olemassa ja että vain se henkilö, jolle käyttäjätunnus ja salasana ovat luovutettu, voi käyttää teknistä yhteyttä ja katsella tietoja.

Koska tietoja luovuttavalla toimintayksiköllä on aina vastuu siitä, että tietojen luovutuksen edellytykset ovat olemassa, ei edellä kuvatun kaltainen salasanojen ja käyttäjätunnusten antaminen toimintayksikön henkilökunnan ulkopuolisille käyttäjille ole tietosuojan ja tietoturvan näkökulmasta suositeltava menetelmä.

2.2 Käyttöoikeuksien delegointimalli (Delegation Model)

Tällä mallilla tarkoitetaan menetelmää, jossa toimintayksikön määrittelemiä käyttöoikeuksia delegoidaan sähköisesti edelleen uusille organisaatioille/käyttäjille. On myös mahdollista, että käyttöoikeuksien vastaanottaja delegoi saamiaan käyttöoikeuksia seuraaville organisaatioille, mikä johtaa käyttöoikeuksien delegoinnin ketjuttamiseen.

Tässä mallissa jokainen uusi käyttöoikeuksien saaja toimii käyttöoikeuksien omistajan puolesta. Mallissa tarvitaan seuraavat toimijat:

- - käyttöoikeuksien haltija
- - käyttöoikeuksien tarkistaja
- - valtuuksien antaja
- - luotettu kolmas osapuoli (ns. attribute authority, AA), joka toimii oikeuksien lähteenä.

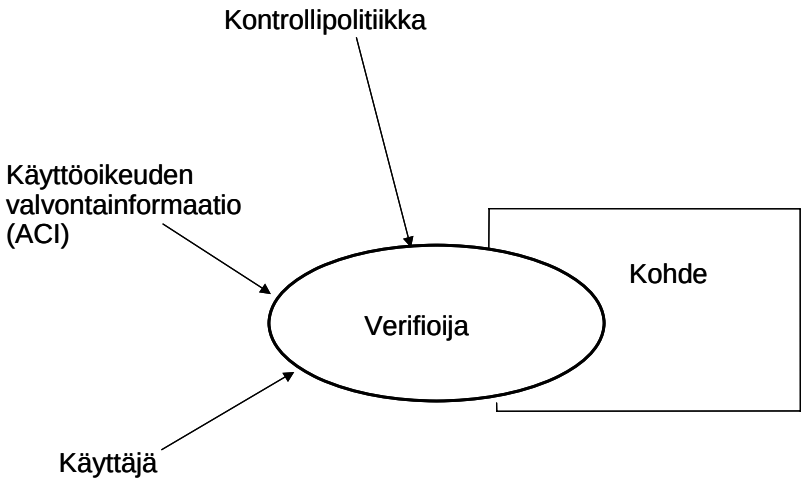
Yleisesti käytetty käyttöoikeuksien jakamisen malli perustuu roolipohjaiseen käytön hallintaan (ns. RBAC). American Society for Testing and Materials organisaation standardiluonnoksessa ASTM E31.20 todetaan rooleista seuraavaa:

"Health information systems such as EHR should at minimum have a patient policy, an enterprise policy, policies defined by laws and regulations, one policy per Structural Role and one policy per Functional Role."

Käyttöoikeuksien delegointi usealle peräkkäiselle toimijalle voi johtaa varmenneketjujen syntymiseen. Tällaisessa ketjussa uusi toimija luottaa edellisten muodostaman luottamusketjuun.

2.3 Valvontamalli (Control Model)

Mallin lähtökohtana on luoda mekanismi, jonka avulla kohteessa (kuva 4) olevien sensitiivisten tietojen (objektien) käyttöä voidaan valvoa. Tässä mallissa käyttäjä saa käyttöoikeusattribuuttinsa toimintayksiköltä.



Kuva 4 Käyttöoikeuksien valvontamalli (ASTM E31.21)

Käyttöoikeuksien pyytäjän oikeudet on tavallisesti sijoitettu ns. attribuuttivarmenteeseen, joka voi sijaita joko varmentajalla tai erillisessä hakemistossa. Kohde vastaanottaa käytön valvontatiedot, jotka voivat sijaita esim. paikallisessa tietokannassa. Verifioija, voi olla joko kohteen omistama tai ulkopuolinen riippumaton organisaatio, hallitsee tiedon käyttöä valvontapolitiikan ja muiden käytön edellytysten perustella. Tätä varten se vertaa käyttäjän oikeuksia kohteen politiikkaa ja kohteessa sijaitsevan tiedon (objektien) sensitiivisyysinformaatiota vastaan. Tiedon käyttö on mahdollista vain sillä edellytyksellä, että käyttäjän oikeudet ylittävät sekä kohteen tietosuojapolitiikan vaatimukset että tiedon sensitiivisyysvaatimukset.

Valvontamallissa käyttäjän tunnistaminen ja todentaminen voi tapahtua esimerkiksi PKI-järjestelmän avulla.

2.4 Dokumenttimalli (Document Model)

Mallin lähtökohta on se, että prosessit, roolit, käyttöoikeudet jne. ensin dokumentoidaan ja sitten varmennetaan. Varmentaminen tapahtuu siten, että auditoinnin jälkeen kummatkin osapuolet allekirjoittavat samansisältöisen sähköisen käyttöoikeusdokumentin. Koska molempien osapuolten tulee olla varma siitä, että ne ovat allekirjoittaneet saman sisältöisen käyttöoikeusdokumentin tai sen päivityksen, saattaa menetelmä johtaa tarpeeseen hallita moninkertaisia sähköisiä allekirjoituksia.

2.5 Politiikkamalli (Policy Model)

Tietoturvapolitiikka on monimutkainen, lakiperustainen, eettinen, sosiaalinen, organisatorinen, psykologinen, toiminnallinen ja tekninen keino synnyttää luottamus tietojärjestelmissä. Tietoturvapolitiikka kuvaa mm. lakiympäristön, säännöt ja säädökset, toiminnallisen ympäristön, tavoitteet ja periaatteet. Se voi olla joko formaalia politiikkaa ja/tai perustua malliohjeiden (templates) käyttöön. Yhteistoiminnallisuuden saavuttamiseksi politiikka tulee formuloida ja koodata siten, että se voidaan tulkita eri tilanteissa oikein tietojärjestelmän toimesta. Tietoturvapolitiikka edellyttää, että sen käyttäjillä on yhteinen syntaksi, semantiikka ja sanasto, jotka ilmaistaan politiikkadokumenteissa tai politiikkasopimuksissa (esimerkiksi käyttäen OASIS ja XACML- standardeja). Tietoturvapolitiikka tulee olla yksikäsitteisesti identifioitu ja nimetty.

Tietoturvapolitiikan on syytä olla muotoiltu siten, että sen tulkinta on yksikäsitteinen ja käytännöllinen. Politiikan elementtejä ovat mm.

- käyttöoikeuksien periaatteet
- osapuolten velvollisuudet
- delegoinnin periaatteet
- tietojen luovuttamisesta tai käytön mahdollistamisesta pidättäytyminen
- käyttäjien roolit
- käyttäjille asetetut rajoitteet
- sopimukset
- tietoturvan teknisen toteutuksen periaatteet

2.6 Roolimalli (Role Model)

Roolipohjaisen käyttäjien ja käyttöoikeuksien hallinnan periaate on se, että käyttäjille on annettu heidän tarvitsemansa roolit. Kuhunkin tehtävään ja rooleihin liitetään lupia (esimerkiksi lupa käyttää resursseja, ohjelmia tai dataa). Ennen kuin käyttäjä saa luvan käyttää tiettyä resurssia, tarkistetaan hänen roolinsa organisaation käytönhallinnan politiikkaa (toimintaperiaatteita) vastaan.

Roolit liittyvät sekä henkilön ammatilliseen statukseen että työtehtäviin. Terveydenhuollon Informatiikan standardisoinnin tekninen komitea ISO TC 215 on määritellyt kaksi rooliluokkaa:

- rakenteellinen rooli (structural role)
- toiminnallinen rooli (functional role)

Roolien hallintaan ja välittämiseen voidaan käyttää roolivarmenteita ja ns. rooliattribuutteja.

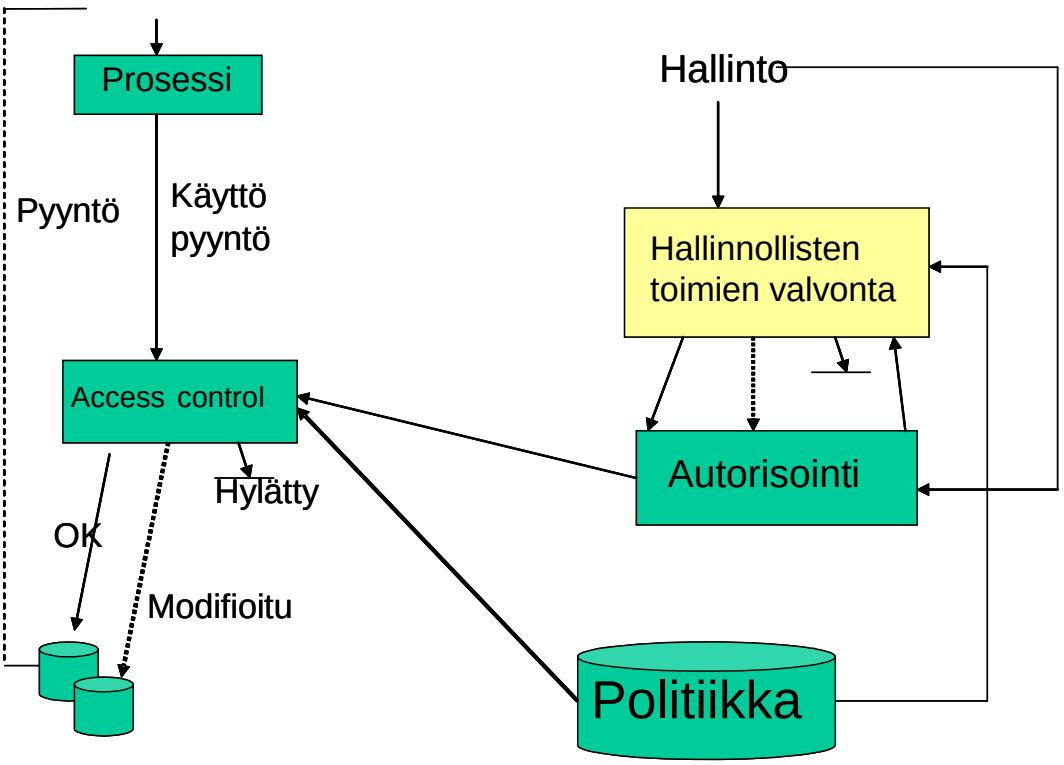
2.7 Tiedon etäisyysmalli (Information Distance Model)

Tämä malli koostuu kolmesta toimijasta:

- tiedon lähde (ns. data originator), joka on tavallisesti potilas
- tiedon tuottaja/tulkitsija, joka on tavallisesti lääkäri tai muu ammattihenkilö
- tiedon hallinnoija

2.8 Käyttöoikeuksien ja käytön hallinnan malli (Privilege Management and Access Control – PMAC- Model)

Käyttöoikeuksien hallinnan mallin eli PMAC-mallin periaate on esitetty kuvassa 5.



Kuva 5 Käyttöoikeuksien ja käytön hallinnan ja käytön valvonnan periaate malli (lähde Castrano et al. 1995)

Jos PMAC-mallia käytetään usean organisaation käyttöoikeuksien hallintaan, tarvitaan hakemisto, joka sisältää kaikki ne henkilöt, joille on annettu rooleja. Lisäksi tarvitaan säännöt, jotka koskevat koskien politiikan hyväksymiä henkilöitä.

2.9 Mallien yhdisteleminen

Edellä kuvattuja malleja yhdistelemällä tai niiden yhteiskäytöllä kyetään toteuttamaan haluttuun käyttötarkoitukseen soveltuva käyttäjien ja käyttöoikeuksien hallinnan arkkitehtuuri.

3 Käyttäjän ja käyttöoikeuksien hallinnalle asetettavia vaatimuksia

Käyttöoikeuksien hallinnan toteuttaminen asianmukaisesti edellyttää, että on olemassa politiikka johon pohjautuen käyttäjät ja entiteetit tunnistetaan ja todennetaan. Tämän lisäksi tulee tuntea kohteena olevaan tiedon käyttöön liittyvät säännöt ja hallita käyttäjään liittyvät käyttöoikeussäännöt.

Roolipohjainen käyttöoikeuksien hallinta puolestaan edellyttää, että ammattihenkilöiden toiminnallisia rooleja voidaan hallinnoida dynaamisesti. Käytännössä tämän funktionaalisen roolin voi identifioida vain se toimintayksikkö, johon terveydenhuollon ammattihenkilö on työsuhteessa.

4 Usean toimintayksikön yhteisen käyttäjän ja käyttöoikeuksien hallinnan toteuttamistapoja

Seuraavassa kuvataan yksityiskohtaisemmin kolmea erilaista usean toimintayksikön yhteisen käyttäjän ja käyttöoikeuksien hallinnan toteuttamiseen soveltuvaa menetelmää.

1. Yhteiseen/jaettuu LDAP-hakemiston käyttöön perustuva ratkaisu
2. PMI-arkkitehtuuriin perustuva ratkaisu
3. Identiteetin hallinnan järjestelmän käyttöön perustuva ratkaisu

4.1 Jaettuun LDAP- hakemistoon perustuva malli

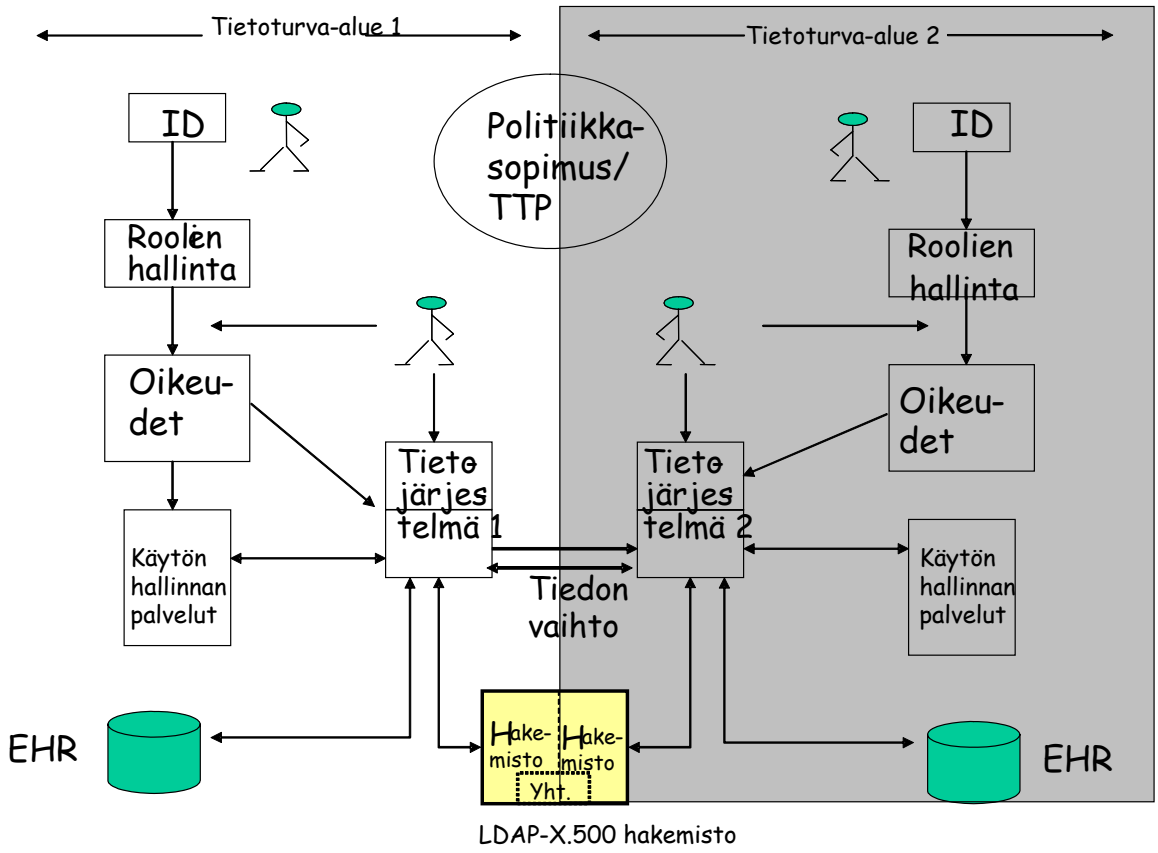
Usean eri toimintayksikön käyttöoikeuksia on mahdollista hallinnoida yhteisen/jaetun käyttäjähakemiston avulla. Tämä yhteinen tiedonlähde voi sisältää tietoa käyttöoikeuksista, niiden poistamisesta, rooleista ja muuta yksityiskohtaista käytön hallinnan ohjaustietoa. Hakemiston avulla voidaan myös toteuttaa ns. SSO toiminta (Single Sign On). Tällainen hakemisto kykenee tarvittaessa toimimaan yhdessä PKI-järjestelmän kanssa.

Kuva 6 esittää jaettuun LDAP-hakemistoon perustuvan mallin periaatteen. Toimintayksiköillä tulee olla samantasoinen tietoturvapolitiikka ja sen lisäksi niillä on joko kokonaan yhteinen tai osaksi jaettu LDAP-hakemisto, jonka avulla käyttöoikeuksia voidaan hallita ja välittää käyttöoikeustietoa hakemiston piirissä oleville.

ITU-T X.500 standardi määrittelee em. LDAP-hakemiston rakenteen ja runsaasti sen arkkitehtuuriin, protokolliin ja hallintaan liittyviä asioita. Hakemiston käyttäminen terveydenhuollon komplisoidussa toimintaympäristössä edellyttää standardissa olevien laajennusmahdollisuuksien käyttöönottoa. Nämä puolestaan mahdollistavat mm. terveydenhuoltospesifisten tunnisteiden ja roolipohjaisen informaation hyödyntämisen.

Yksi terveydenhuollon erityispiirteistä on se, että sama ammattihenkilö voi toimia usean eri organisaation puolesta siten, että hänellä on kussakin organisaatiossa erilaiset työtehtävät. Terveydenhuollon ammattihenkilöllä voi olla samassakin organisaatiossa useita eri rooleja. Vastaavasti terveydenhuollon asiakkaat voivat olla samanaikaisesti usean eri organisaation potilaina. Terveydenhuollon ammattihenkilöt voivat myös olla asiakkaita, ja siksi heidän asiakasidentiteettinsä ja ammatti-identiteettinsä tulee voida pitää erillä toisistaan. ISO TC215 standardiluonnos (ISO/CD Health informatics- Directory services for Security, Communications, and Identification of Professionals and Patients) on ottanut nämä piirteet huomioon. Tämän standardiluonnoksen laatimien laajennusten avulla terveydenhuollon tunnisteet ja roolit sekä varmenneorganisaatiota, rekisteröintiorganisaatiota ja attribuuttisertifikaatteja hallinnoivaa organisaatiota kuvaavat tiedot voidaan julkaista laajennetussa LDAP-hakemistossa.

Edellä mainitun ISO standardiehdotuksen avulla voidaan ITU-T X.500 hakemistoa käyttää terveydenhuollossa useiden organisaatioiden käyttöoikeuksien hallinnan toteuttamiseen.



Kuva 6 Käyttöoikeuksien hallinta LDAP-hakemiston avulla

4.2 PMI-malli (Privilege Management Infrastructure Model)

PMI-arkkitehtuurin lähtökohtana on se, että pelkkä identitetti ole riittävä käyttöoikeuksien määrittelemiseksi. ITU-T X.509 suosituksessa määriteltiin julkisen avaimen infrastruktuurin pääelementit (ts. PKI-arkkitehtuuri). ISO TC 215 komitean vuonna 2005 tuottamassa kolmiosaisessa standardissa (ISO 17090) on kuvattu X.509 standardiin perustuen terveydenhuollon tarpeisiin soveltuvan PKI-arkkitehtuurin vaatimukset.

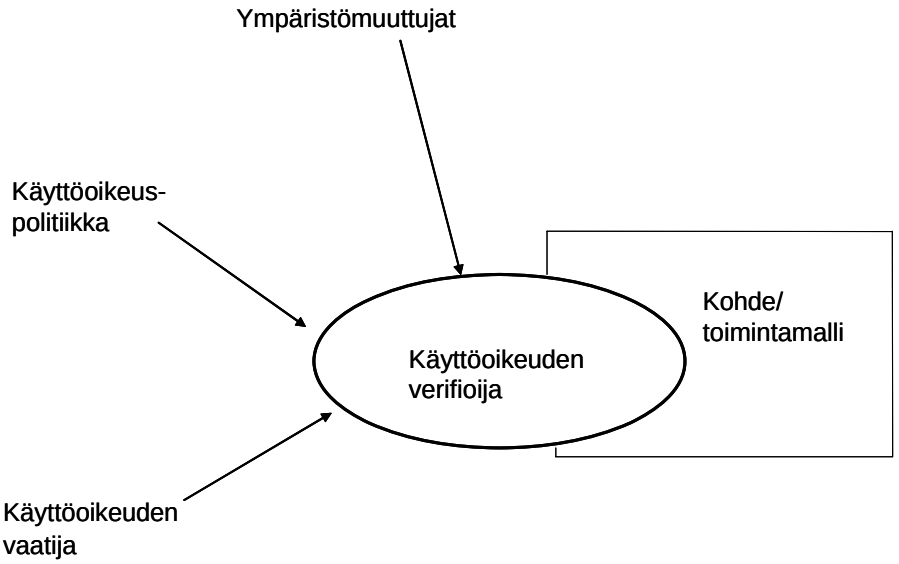
Edellä mainitun ITU-T X.509 standardin uudistettu versio vuodelta 2000 määritteli sekä ns. attribuuttivarmenteet että PMI-arkkitehtuurin perusteet. Tiivistetysti voidaan sanoa, että PMI arkkitehtuuri hallinnoi käyttöoikeuksia ja tarjoaa yhdessä PKI-palvelujen kanssa kattavat käyttöoikeuksien hallintapalvelut.

Sekä PKI-arkkitehtuurin että PMI-arkkitehtuurin peruskonseptit ovat samanlaiset, mutta PKI-arkkitehtuurin keskittyessä todentamiseen on PMI-arkkitehtuurin kohteena käyttöoikeudet. Taulukossa 1 on vertailu kummankin arkkitehtuurin keskeisiä ominaisuuksia.

Taulukko 1 PKI- ja PMI infrastruktuurien ominaisuuksia (lähde ITU-T)

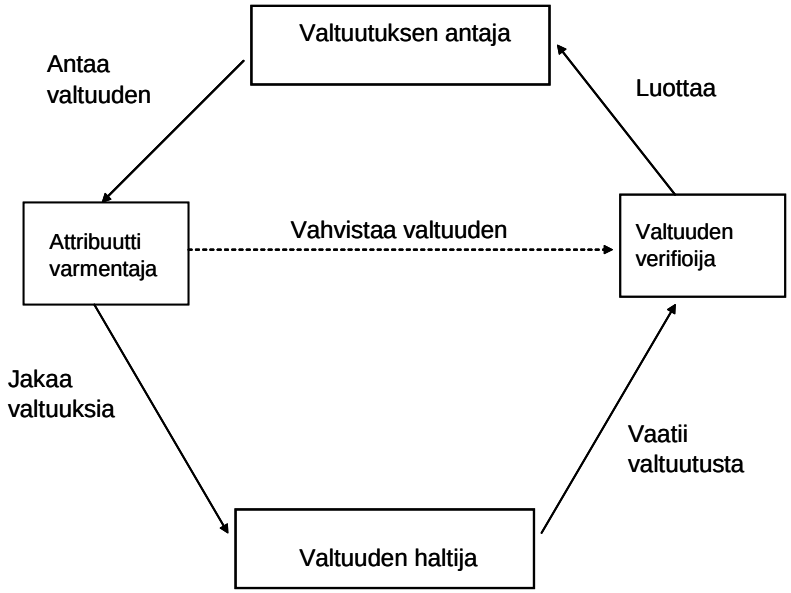
PMI	**PKI**
Valtuuksien lähde (SoA)	Juurivarmentaja (ns. Trust Anchor)
Attribuutti varmentaja (AA)	Varmentaja (CA)
Attribuutti varmenne	PKI- varmenne
Attribuuttivarmenteen kumoamislista	PKI-varmenteen kumoamislista
PMI revokatiolistan ylläpitäjä	PKI revokatiolistan ylläpitäjä

PMI-arkkitehtuuri käyttää luvussa 2.3 kuvattua valvonta-mallia. PMI-arkkitehtuuri koostuu kuvassa 7 esitetyistä viidestä komponentista. Käyttöoikeuksien liittämisellä käyttäjään varmistetaan, että hän noudattaa valtuuksien lähteen määrittelemää tietoturvapolitiikkaa.



Kuva 7 ITU-T X.509 standardin mukaiset PMI-arkkitehtuurin komponentit

PMI-arkkitehtuurin yhteydessä käytetyt käyttöoikeuksien hallinnan menetelmät perustuvat useimmiten rooli-pohjaiseen käytön hallintaan. PMI-arkkitehtuurin yhteydessä voidaan toteuttaa myös käyttöoikeuksien delegointi kuvassa 8 esitetyn periaatteen mukaisesti.



Kuva 8 ITU-T X.509 suosituksen mukainen käyttöoikeuksien delegointimalli

4.3 Identiteetin hallintamenetelmä (Identity Management Method, IM)

Identiteetin hallinnan järjestelmä voidaan määritellä seuraavasti:

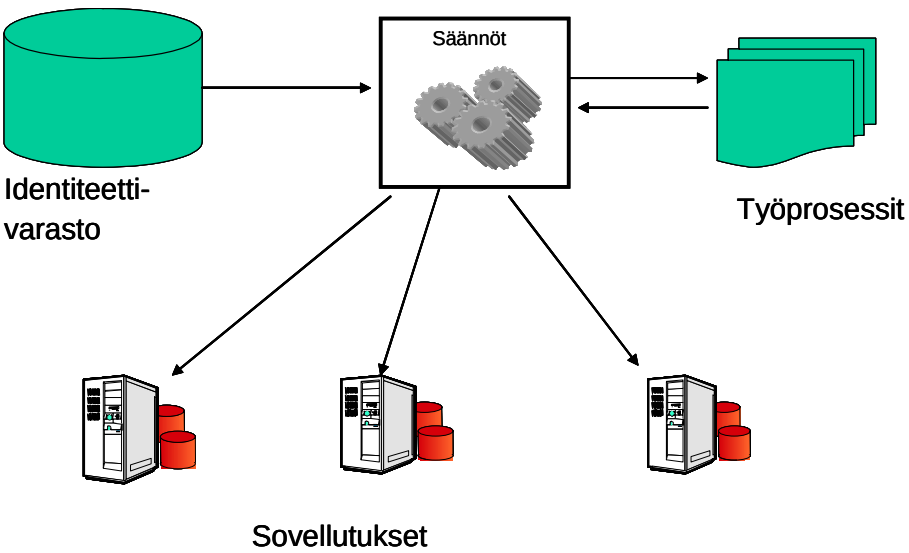
Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. The driver licensing system is a simple example of identity management: drivers are identified by their license numbers and user specifications (such as "can not drive after dark") are linked to the identifying number.

In an IT network, identity management software is used to automate administrative tasks, such as resetting user passwords. Enabling users to reset their own passwords can save significant money and resources, since a large percentage of help desk calls are password-related. Password synchronization (p-synch) enables a user to access resources across systems with a single password; a more advanced version called single signon enables synchronization across applications as well as systems

IM-menetelmän keskeinen palvelu on identiteetin siirtäminen, mutta myös käyttäjien todentaminen ja valtuuksien antaminen voidaan liittää mukaan tarjottaviin palveluihin. Menetelmällä pyritään siis hallinnoimaan samalla kertaa sekä sitä, kenelle tiedon käyttö on sallittua että sitä kuka on antanut luvan tiedon käyttöön.

Tällä hetkellä tarjolla olevat kaupalliset IM-toteutukset perustuvat tavallisesti ns. identiteettikeskuksen käyttöön. Identiteettikeskus kontrolloi organisaation tietojärjestelmän identiteettejä, oli kyseessä käyttäjän oma henkilökunta, käyttäjä toisesta organisaatiosta tai asiakas (esim. potilas). Kuvassa 9 on esitetty identiteettikeskukseen perustuvan IM-palvelun periaate.

IM-järjestelmällä voidaan myös tukea rooli- ja sääntöpohjaista ohjelmien käynnistämistä, tuottaa audit-lokeja ja hallita dynaamisesti salasanoja.



Kuva 9 Yhteiseen identiteettivarastoon perustuva identiteetin hallinnan periaatemalli

Identiteetin hallinnan järjestelmät tukevat tyypillisesti seuraavia toimintoja:

- Rooleihin kytkettyjä käyttöoikeuksien hallintaa siten, että yhteen rooliin voi liittyä useita erilaisia käyttöoikeuksia
- Roolihierarkiaa
- Tilapäisten roolien hallintaa
- Salasanojen hallintaa ja niiden jakamista

IM:n kaupallisissa toteutuksissa identiteettivarasto muodostaa tavallisesti ns. metahakemiston. Käytön hallinnan politiikat (ts. säännöt) ovat organisaatioiden määrittelemiä. IM-järjestelmässä käyttöoikeudet voidaan julkaista myös LDAP-hakemiston kautta. LDAP:in käyttö onkin vakiintunut standardiratkaisuksi käyttöoikeuksien hallintaan. Vaihtoehtoinen toteutustapa käyttöoikeuksien hallintaan on käyttää ns. Virtual Directory palvelua. Tällöin identiteetin jakamispyyntö voi tulla joko LDAP-hakemistosta tai esimerkiksi Web-palvelusta.

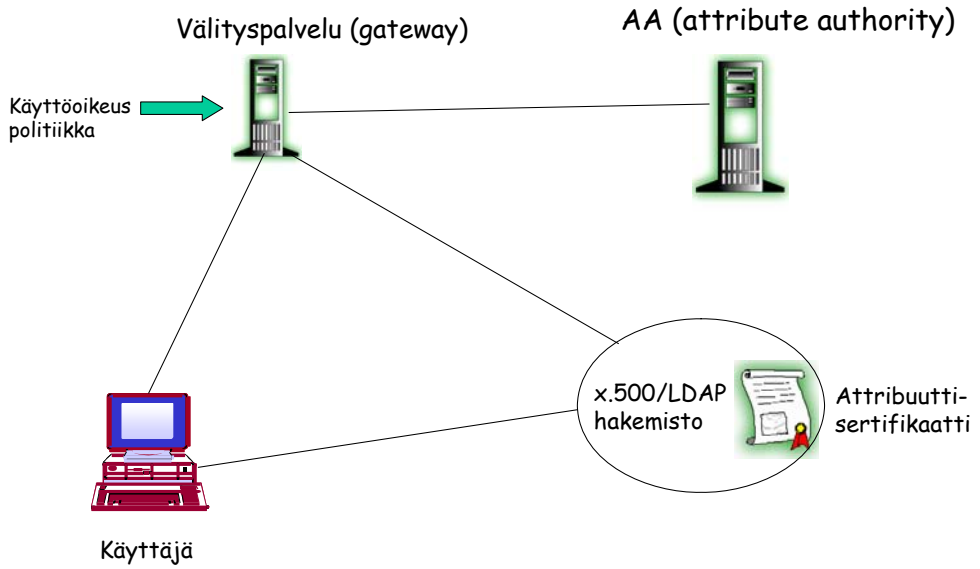
Markkinoilla on myös identiteetin hallinnan toteutuksia, jotka perustuvat erityisen federaatio- palvelimen (Federation Server) käyttöön. Kaupallisissa sovellutuksissa

yleisimmin käytetty identiteetin federaatiotekniikka perustuu mm. SAML tai ID-WSF standardeihin. Tarjolla on myös IM toteutuksia, jotka mahdollistavat Web-yhteyden kautta tapahtuvan Single Sign-On toiminnan.

4.4 PKI- ja PMI-järjestelmät terveydenhuollon toiminta-yksiköiden välisessä tiedonvaihdossa

PKI-järjestelmän tehtävä usean toimintayksikön välisessä tiedonvaihdossa on muodostaa osaltaan organisaatioiden välinen luottamus. PKI-järjestelmän avulla voidaan toteuttaa yliorganisationaalinen käyttäjien vahva tunnistus hyödyntäen kansainvälisiä standardeja.

PMI (Privilege Management Infrastructure) on konseptiltaan samanlainen kuin PKI-järjestelmä, mutta se on tarkoitettu antamaan PKI-järjestelmän palveluiden lisäksi tarvittavat käyttöoikeuspalvelut. PMI-mekanismi mahdollistaa sen, että käyttäjille voidaan antaa käyttöoikeuksia sekä monen toimijan että monen sovellutuksen verkoissa. Käyttöoikeuksien antaminen edellyttää etukäteen laadittua tietoturvapolitiikkaa. PMI-arkkitehtuuri yhdistää tietoturvapolitiikkaan sidotun käyttöoikeuden käyttäjään ns. attribuutti-sertifikaatilla. ITU-T X. 509 suosituksen mukaisesti PMI-arkkitehtuuri muodostuu kuvassa 10 olevista komponenteista.



PMI-järjestelmän komponentit (ITU-T)

Kuva 10 PMI-järjestelmän komponentit (lähde ITU- T X.509, Public Key and attribute certificate frameworks standard)

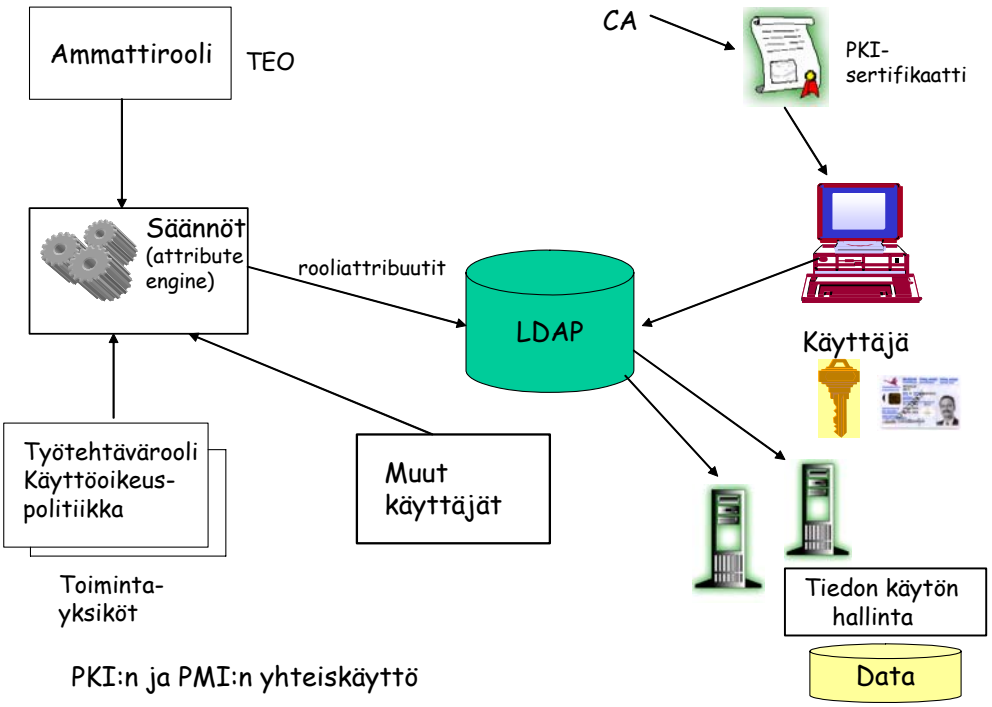
5 Suositus usean toimintayksikön yhteiseksi käyttäjien ja käyttöoikeuksien hallinnan kansalliseksi ratkaisuksi

Kuva 11 esittää kokonaisarkkitehtuuria, jossa usean toimintayksikön käyttäjien ja käyttöoikeuksien hallinta on toteutettu perustuen PKI- ja PMI-arkkitehtuurien yhteiskäyttöön ja yhteiseen LDAP-hakemistoon. Toteutuksessa käyttöoikeudet talletetaan sähköisesti allekirjoitettuun attribuuttivarmenteisiin, jotka julkaistaan käyttöoikeusvaraston (LDAP-enabled service) kautta.

Kuvan 11 arkkitehtuurille vaihtoehtoinen ratkaisu olisi käyttää identiteetin hallintajärjestelmää käyttöoikeuksien julkaisemiseen. Kaupalliset IM-tuotteet ovat kuitenkin vasta alkaneet kehittyä kahden toimijan välisistä toteutuksista kohti federatiivisia toteutuksia. Tämän hetkiset kaupalliset IM-tuotteet ovat lisäksi tarkoitettu etupäässä käyttäjätunnusten ja salasanojen jakeluun toimijoiden välillä. Terveydenhuollon e-palveluiden tarvitseman dynaamiseen identiteettien federaatioon kykeneviä IM toteutuksia ei ole tällä hetkellä tarjolla.

Kuvan11 arkkitehtuurin etuja ovat:

- ratkaisu on modulaarinen
- arkkitehtuuri muodostaa luontevan jatkumon käyttöönottovaiheessa olevalle terveydenhuollon PKI-arkkitehtuurille
- arkkitehtuuri perustuu valmiisiin kansainvälisiin standardeihin
- arkkitehtuurin komponentit ovat kaupallisesti saatavissa
- ratkaisussa käyttäjien tunnistaminen ja käyttäjänhallinta ovat erotettu toisistaan
- arkkitehtuurissa säilytetään paikallinen kontrolli siihen, kuinka informaation käyttöä hallitaan tiedon sensitiivisyyden perusteella.



Kuva 11 Ehdotus monen toimintayksikön yhteiseksi käyttäjien ja käyttöoikeuksien hallinnan arkkitehtuuriksi

Edellisen perusteella tämä raportti suosittelee kuvan 11 mukaista arkkitehtuuria käytettäväksi terveydenhuollossa käyttöoikeuksien ja käyttäjien hallinnan menetelmänä silloin, kun kyseessä on usean ei toimintayksikön välinen tiedonvaihto.

6 Käsitteet

Käsitteiden ja termien määrittelyssä on käytetty hyväksi seuraavia lähteitä:

- ISO TC 215/WG4 - Glossary of Security Terms
- ISO TC 215/WG4 - Background Paper- Health Information Security Standards Framework and Glossary of terms.
- ISO/DTS 17090
- ISO/DDTS 22600
- ISO/IEC 17799
- VAHTI 4/2003
- Stakes raportteja 5/2005

aikaleima (time stamp)
tapahtumatietoon tai viestiin liitetty tieto luomis-, lähetys-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista. Aikaleimalla saadaan aikaan tapahtuman ajankohdan kiistämättömyys

attribuuttivarmentaja (Attribute Authority)
taho joka myöntää attribuuttivarmenteen.

attribuutti varmenne
tietorakenne, jonka attribuuttivarmentaja on sähköisesti allekirjoittanut ja, joka liittää yhteen attribuuttien arvot ja niiden haltijan identifioinnin

hakemistopalvelu (directory service)
kokoelma ohjelmia, laitteistoja, prosesseja menetelmiä (policies) ja hallinnollisia toimia, joita käytetään hakemistoon talletetun tiedon järjestämiseen ja jakamiseen käyttäjille

Hakemistopalvelun ominaisuuksista on luotu standardit X.500 ja ns. kevytversio LDAP (*lightweight directory access protocol*), joissa määritellään esimerkiksi hakemistojen ja niissä sijaitsevien objektien ja tietojen rakenteet ja ominaisuudet, tietojen hakumenetelmät ja hakuprotokollat.

henkilövarmenne (personal certificate, identity certificate)
varmenne, jota käytetään henkilön henkilöllisyyden vahvistamiseksi

identiteetti
joukko ominaisuuksia, jotka kuvaavat käyttäjää ja joiden avulla käyttäjä voidaan tunnistaa

luottamuksellisuus (confidentiality)
tietoon liittyvä ominaisuus joka kertoo, että tieto ei ole paljastunut tai käytössä ulkopuoliselle henkilölle, prosessille tai järjestelmälle.

käyttäjien hallinta (user management)
palvelu, jolla ylläpidetään käyttäjien ominaisuuksia ja tietoa siitä minkä tyyppinen käyttäjä voi käyttää palvelua. Käyttäjien hallinnan palveluihin kuuluu myös käyttäjien lisääminen ja poistaminen.

käyttäjäidentiteetti
palveluntarjoajan tiedossa olevat käyttäjän henkilöllisyyttä yksilöivät ja kuvaavat tiedot

käytön hallinta (access control)
toimet, joilla varmistetaan, että tietoa käsittelevien prosessien resursseja voivat käyttää vain ne henkilöt, prosessit tai järjestelmät, joilla on siihen valtuus.

käyttöoikeus (access right)
käyttäjälle annettava tiettyyn tietoon, ohjelmistoon tai järjestelmään annettava oikeus

Käyttöoikeuksia ovat esimerkiksi lukuoikeus, kirjoitusoikeus, muutosoikeus, tuhoamisoikeus ja hallintaoikeus eli muiden käyttäjien oikeuksien määrittely.

käyttövaltuus (user right, authorization, privilege)
tietojärjestelmän käyttäjälle myönnetyt yksilöidyt oikeudet nimettyjen tietojen, järjestelmien, ohjelmistojen tai niiden osien käyttöön

palvelinvarmenne (server certificate)
tietojärjestelmän palvelimelle myönnetty varmenne, jonka avulla käyttäjä voi varmistua siitä, että asioi oikean palvelimen kanssa.

pääsynhallinta (access control)
toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille. Pääsynhallinnassa tietojärjestelmien, tietoverkkojen ja tietojen käyttäjät tunnistetaan ja todennetaan sovitulla tavalla.

rooli (role)
pätevyyksien ja/tai tehtävien joukko, jotka liittyvät johonkin tehtävään

roolivarmenne (role certificate)
varmenne, joka vahvistaa sekä henkilön henkilöllisyyden että oikeuden toimia jossakin roolissa kuten työtehtävässä.

TEO
terveydenhuollon oikeusturvakeskus

todennus (authentication, verification)
tietojärjestelmän käyttäjän (henkilö, laite tai ohjelmisto) tai viestinnän toisen osapuolen aitouden ja oikeellisuuden varmistaminen halutulla luottamustasolla

tunnistus (identification)
menettely, jolla yksilöidään joku tai jokin (esimerkiksi tietojärjestelmän käyttäjä)

vahva tunnistus (strong authentication)
käyttäjän tunnistus ja todennus, joka käyttää ainakin kahta kolmesta todennustavasta: jotakin, mitä käyttäjä on jotakin, mitä käyttäjä tietää tai jotakin, mikä käyttäjällä on hallussaan.

varmenne (certificate)
aitoustodistus, sähköinen todistus, jolla vahvistetaan, että todistuksen haltija on tietty henkilö, organisaatio tai järjestelmä. Varmenne on yleensä ulkopuolinen luotettu tahon (varmentaja) myöntämä. Varmenne voi sisältää muun muassa käyttäjän julkisen avaimen, henkilötiedot, varmenteen voimassaolopäiväyksen ja varmentajan sähköisen allekirjoituksen. Kun varmenne on varmentajan sähköisesti allekirjoittama, sen aitous on varmistettavissa.

Varmenne voidaan myöntää esimerkiksi henkilölle, laitteelle tai sovellukselle. Varmenteiden ominaisuuksista on määritelty ITU-T X.509 standardissa.
Laitteistolle tai ohjelmistolle myönnettyä varmennetta kutsutaan tapauskohtaisesti laitevarmenteeksi, palvelinvarmenteeksi tai ohjelmistovarmenteeksi. Koska tällainen varmenne identifioi tyypillisesti sen organisaation, jonka palveluita kyseisellä laitteistolla ja ohjelmistolla tuotetaan, käytetään tässä yhteydessä joskus myös termiä organisaatiovarmenne.

varmentaja (certificate authority)
taho, joka myöntää varmenteen

Väestörekisterikeskus (VRK) toimii varmentajana, joka myöntää kansalaisille sähköistä asiointia varten sähköisiä henkilöllisyystodistuksia ja kansalaisvarmenteita.

varmenteiden hallinnointi (Certificate management)
varmenteisiin ja niiden käsittelyyn liittyvät menetelmät ja prosessit kuten varmenteen generointi, varmenteen jakaminen, varmenteiden tallettaminen ja peruuttaminen.

varmenteen jakaminen (Certificate distribution)
menetelmä varmenteiden jakamiseksi.

X.509
ITU-T X.509 standardi

7 Viitteet ja lähteet

Standardit

Health Informatics – Directory Services for Security, Communications, and Identification of Professionals and Patients, ISO/CD 125.4, ISO TC 215/WG4, 22-06-2004.

Health Informatics - privilege management and access control – Part1 and Part 2, ISO`/PDTS 22600-1 and ISO/PDTS 22600-2, 30-01-2005.

Health Informatics -PMAC – Privilege Management and Access Control, ISO 17090 parts 1-3.

ITU-T Standards for Directory Services andAuthentication

X.500 Overview of concepts, model and services

X.509 Public Key and attribute certificate frameworks

Liberty Alliance project, www-projectliberty.org

OASIS SAML Committee, www.oasis-open.org/committees

Privilege Management Infrastructure American Society for Testing and materials (ASTM) organisaation standardiluonnos ASTM E31.20, Working Draft 0.9h, April 18, 2005.

Role Based Access Control (RBAC) Healthcare Permission Catalog, HL7 Security Technical Committee, 13 July 2005.ASTM E31.20.

Muut viitteet

Blobel, B, Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems, Studies in Health Technology and Informatics 89, IOS Press 2002.

Ensio A, Ruotsalainen P, Tietoturvallinen kommunikaatioalusta: suositus kansallisesti noudatettaviksi standardeiksi.

Gardier, J, Identity Management – Introduction, Value & Evolution, ISSE 2005 Securing Electronic Business Processes, Vieweg 2005.

Hassinen, K., Case Kymenlaakso, Terveydenhuollon tietojärjestelmät 15-16.2.2006, management Events.

Itälä T , Ruotsalainen P, Tietoturvallinen kommunikaatioalusta: Luovutusten ja luovutuslokin hallinnan suositukset, OSVE 6/2004.

ITU-T Security in Telecommunications and Information Technology, An Overview of issues, October 2004.

Maxware Product Information, Maxware Virtul Directory, Maxware Identity Center, Maxware Federation Server, August 2005.

Mikola T, Sorvari H ja Ruotsalainen P. Tietoturvallinen kommunikaatioalusta: Suositukset sähköisen suostumuksen periaatteiksi, OSVE 3/2004.

Pajukoski M., Sähköinen asiointi sosiaali- ja terveydenhuollossa, lainsäädännön rajat ja mahdollisuudet (Stakes raportteja 282/ 2004).

Ruotsalainen P. Ehdotus Sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri, OSVE 4/2002.

Valtionhallinnon kehittämisosasto, VAHTI, Identiteetti- ja käyttövaltuushallinnon periaatteet ja hyvät käytännöt, Ohje 25.10.2005, Valtiovarainministeriö.