KÄYTTÖOIKEUKSIEN HALLINNAN JA KÄYTTÄJÄN HALLINNAN MUUTOS TERVEYDENHUOLLOSSA

LAHDEN AMMATTIKORKEAKOULU
Liiketalouden laitos
Sähköinen liiketoiminta
Opinnäytetyö
31.10.2008
Eija Lyytikkä

Lahden ammattikorkeakoulu
Sähköinen liiketoiminta

EIJA LYYTIKKÄ: Käyttöoikeuksien hallinnan ja käyttäjän hallinnan muutos terveydenhuollossa

Sähköisen liiketoiminnan opinnäytetyö, 59 sivua
Syksy 2008

TIIVISTELMÄ

Tämä opinnäytetyö on osa laajemmasta esiselvitysraportista terveydenhuollon käyttöoikeuksien hallintaan ja käyttäjän hallintaan liittyvästä muutoksesta. Tämä opinnäytetyö käsittelee terveydenhuollon toimintaympäristön organisaatioissa menossa olevaa muutosta, joka tarkoittaa siirtymistä kohti kansallista sähköistä arkisto- ja välityspalveluratkaisua potilasasiakirjoille (KANTA). KANTAan terveydenhuollon organisaatioilla on liittymisvelvollisuus yhteisen sovitun aikataulun mukaisesti.

KANTAssa ovat mukana Kansaneläkelaitos (Kela), Terveydenhuollon oikeusturvakeskus (TEO), Stakes, apteekit ja terveydenhuollon organisaatiot. Kelan vastuulla on sähköinen potilasarkisto (eArkisto), sähköinen resepti (eResepti), ja kansalaisen katseluyhteys omiin tietoihinsa (eKatselu). Muiden vastuut ovat seuraavat: TEO:n vastuulla on varmennepalvelu, Stakesin vastuulla ovat luokitukset ja koodistot, apteekkien vastuulla apteekkijärjestelmät ja terveydenhuollon organisaatioiden vastuulla ovat mm. potilastietojärjestelmät, tietoliikenne, kortinlukijat, infrastruktuuri, tietosuojavastaavien nimeäminen, tietoturvapolitiikan laatiminen ja käyttäjänhallinnan ajantasalle saattaminen.

Käsittelen opinnäytetyössä käyttöoikeuksiin ja käyttäjän hallintaan liittyviä tekijöitä terveydenhuollon organisaation näkökulmasta, kuten tunnistautumisen ja todentamisen merkitystä käyttöoikeuksien hallinnassa sekä eri varmenteita. Toimintaympäristöä määrittävät luonnollisesti myös useat lait, asetukset, säännökset ja standardit, joita työssäni myös tarkastelen. Opinnäytetyön teoriaosassa käyn läpi eri teorioita/malleja käyttöoikeuksien hallinnassa, joiden soveltuvuutta käsittelen opinnäytetyön johtopäätöksissä. Työn tarkoituksena oli löytää malliratkaisuehdotuksia, joita voisi soveltaa käyttöoikeuksien hallinnassa ja käyttäjän hallinnassa terveydenhuollossa. Johtopäätöksissä esitän myös oman näkemykseni käyttöoikeuksien hallintaan sopivasta mallista tai niiden mahdollisesta yhdistämisestä terveydenhuollon toimintaympäristössä käyttöoikeuksien ja käyttäjän hallinnassa. Työn rajaamiseksi, olen käsitellyt aihetta rajatusti terveydenhuollon organisaation näkökulmasta tarkasteltuna, sillä KANTAan liittyvän muutoksen kokonaisvaltainen käsittely olisi ollut liian laaja kokonaisuus opinnäytetyöhön.

Avainsanat: terveydenhuolto, käyttöoikeudet, käyttäjän hallinta, sähköinen tunnistaminen, varmenne

Lahti University of Applied Sciences
Faculty of Business Studies

EIJA LYYTIKKÄ: Access rights and user control in the computer systems of health care

Bachelor's Thesis in eBusiness, 59 pages

Autumn 2008

ABSTRACT

This thesis is a part of a wider preliminary report on access rights and user control in the area of health care. The aim of this thesis was to examine the shift from local computer systems to national electronic patient files (the KANTA-consortium). All organisations of health care have to join this solution within a common schedule.

The participants of the KANTA-consortium are the Social Insurance Institution of Finland (KELA), the National Authority for Medicolegal Affairs (TEO), Stakes (National Research and Development Centre for Welfare and Health), pharmacies and other organisations of health care. KELA is responsible for the national electronic patient files, electronic prescriptions and the electronic patient file view. TEO is responsible for digital certificate services. Stakes' responsibility is the categorisation and codes. Pharmacies take care of their own computer systems, but other organisations of health care have the biggest responsibility for the patient systems, information networks, card readers, infrastructure, data protection persons, drawing up data security policy and for reforming user_control and access rights.

This thesis discusses authentication and identification and also different kinds of digital certificates, which are an important consideration in the matter of access rights and_user group control. There are quite a few laws, regulations and standards in health care and they were considered in this thesis as well. The theory part of this thesis introduces several different models of access rights and it also examines how these models suit the healthcare area. As a conclusion, a new user control solution is introduced, or a solution for combining several models of access rights or user control. In order to narrow down the topic, only some aspects of the consortium's access rights and user control shift were discussed in this thesis.

Key words: health, health care, access rights, user control, electronic identification, digital certificate services

SISÄLLYS

1 JOHDANTO

1.1 Työn tausta

Tämä opinnäytetyö on tehty osana laajempaa selvitysraporttia käyttöoikeuksien ja käyttäjän hallinnan meneillään olevasta muutoksesta terveydenhuollossa. Työn tavoitteena oli löytää malliratkaisuehdotuksia, joita voisi soveltaa käyttöoikeuksien hallinnassa ja käyttäjän hallinnassa terveydenhuollossa. Meneillään oleva muutos, Kansallinen sähköinen arkisto (KanTa), koostuu kolmesta osasta, reseptikeskuksesta (eResepti), potilastiedon arkistosta (eArkisto) ja kansalaisen katseluyhteydestä (eKatselu) sekä näihin palveluihin liittymiseksi tarvittavat viestinvälitysratkaisuista. Kansallinen terveysarkisto tule olemaan Suomen suurin tietojärjestelmä, johon terveydenhuollon organisaatioilla on liittymisvelvollisuus yhteisen sovitun aikataulun mukaisesti.

KANTAssa ovat mukana Kansaneläkelaitos (Kela), Terveydenhuollon oikeusturvakeskus (TEO), Stakes, apteekit ja terveydenhuollon organisaatiot. Kelan vastuulla on sähköinen potilasarkisto (eArkisto), sähköinen resepti (eResepti), ja kansalaisen katseluyhteys omiin tietoihinsa (eKatselu). Muiden vastuut ovat seuraavat: TEO:n vastuulla on varmennepalvelu, Stakesin vastuulla ovat luokitukset ja koodistot, apteekkien vastuulla apteekkijärjestelmät ja terveydenhuollon organisaatioiden vastuulla ovat mm. potilastietojärjestelmät, tietoliikenne, kortinlukijat, infrastruktuuri, tietosuojavastaavien nimeäminen, tietoturvapolitiikan laatiminen ja käyttäjänhallinnan ajantasalle saattaminen. (Ahlblad, 2008, 3).

Kansallisen KANTA-vaatimuksen lisäksi Euroopan unioni asetti jäsenmailleen vaatimuksen laatia kansallinen eTerveyden tiekartta vuoden 2006 loppuun mennessä. Vaatimus perustui Euroopan union eHealth Action Plan (COM 2004(356)) suunnitelmaan. Suomessa kansallinen strategiatyö alkoi jo 1990-luvun puolessa välissä ja eTerveystie-kartta on ollut selkeää jatkoa jo aiemmin tehtyyn kansalliseen kehitystyöhön. eTerveyden tiekartta kokoaa yhteen kymmenen viime vuoden

kansallisen kehittämistyön keskeiset linjaukset ja aikaansaannokset ja sen tarkoituksena on linjata tulevia haasteita erityisesti suhteessa Euroopan tason yhteistyöhön. (Iivari, Ruotsalainen, 2007, 3.)

Iivari ja Ruotsalainen (2007, 3) toteavat, että Suomen kansallisena tavoitteena on ollut taata tiedon saatavuuden varmistaminen hoitoon osallistuville ajasta ja paikasta riippumatta – saumattomalla palveluketjulla. Saumattomalla palveluketjulla tarkoitetaan usean organisaation yhteistä palvelukokonaisuutta ja organisaatiorajat ylittävää tiimityötä ja sen tarvitsemaa tietojärjestelmien 24h/7d -periaatetta. Tähän on pyritty asiakastietojen kattavalla digitalisoinnilla, sähköisten potilaskertomusjärjestelmien semanttisen ja teknisen yhteistoiminnallisuuden kehittämisellä koko kertomuksen sisällön osalta, kansallisen terveydenhuollon infrastruktuurin ja tietoverkkoratkaisujen kehittämisellä, tunnistamis- ja todentamisratkaisuilla ja sähköisellä allekirjoituksella sekä ylläpitämällä päätöksentekoa tukevaa tietoa verkossa.

Toisena keskeisenä kansallisena tavoitteena on kansalaisen ja potilaan osallistumisen mahdollistaminen ja kansalaisen tiedonsaannin lisääminen ja laadukkaan terveystiedon varmistaminen. Tähän pyritään kansalaisen terveystietoportaalin kehittämisellä, tarjoamalla kansalaiselle pääsy omiin potilas/terveystietoihin ja lokitietoihin sekä kehittämällä interaktiivisia sähköisiä palveluita. (Iivari, Ruotsalainen, 2007, 3.) Suomen tavoitteet ovat pääosin yhteneväiset komission linjaamien EU-tason tavoitteiden sekä muiden EU:n jäsenmaiden kansallisten tavoitteiden kanssa. Suomalaiselle toteutukselle on ominaista tietoturvan ja tietosuojan korostaminen sekä kehittämistyön toteuttaminen eettisesti ja juridisesti kestävällä tavalla. Suomen linjausten mukaan terveystietojen tallettaminen ja käyttö perustuu verkotettuihin tietoturvallisiin tietovarantoihin. eTerveyden perusinfrastruktuuri on Suomessa tällä hetkellä jo melko kattava. (Iivari, Ruotsalainen, 2007, 3.)

Iivari (2003, 20) näkisi, että uusien teknologioiden käyttöönotto on yksi ratkaisuvaihtoehto Suomen terveydenhuollon kustannuskriisiin ja vanhenevan väestön hoidon ongelmiin. Hän uskoo myös, että käyttöön otettavalla informaatioteknologialla pystytään tehostamaan hoitoa, lyhentämään hoitoketjuja, parantamaan ter-

veydenhoidon organisaatioiden yhteistyötä ja tuomaan kustannussäästöjä. Edellä mainitun terveydenhuollon tietojärjestelmien integraatio on noussut yhä selvemmin keskeiseksi tekijäksi terveydenhuollon prosessien kehittämisessä.

Aluetietojärjestelmät ja terveydenhuollon tietoturvallisen kommunikaatioalustan käyttöönotto asettavat paljon vaatimuksia tietojärjestelmien yhteentoimivuudelle niiden käyttöympäristössä. Iivari ja Ruotsalainen (2007, 15) näkisivät, että Suomessa on vahvasti panostettu yhteisten ns. ydintietojen määrittelyyn ja tekniseen yhteistoiminnallisuuteen. Tarkoituksena on pyrkiä määrittämään sellaiset standardien mukaiset määritykset, joilla voitaisiin jatkossa helpommin kehittää sosiaali- ja terveydenhuollon asiakirjahallintoa ja tietojärjestelmien välistä tiedonsiirtoa sekä tietojen yhteistä käyttöä. Vahvasti on noussut esille, että arkkitehtuuri ei saa myöskään riippua kunta/aluerakenteesta tai palveluiden tuotantorakenteesta.

Sosiaali- ja terveysministeriö julkaisi Sosiaali- ja terveydenhuollon tiedonhallinnan Internet-sivuillaan:

> Terveydenhuollossa tietojärjestelmien ensisijainen käyttötarkoitus on potilaan hoidon tukeminen. Terveydenhuollossa asiakassuhde perustuu aina luottamukseen, jolloin asiakkaan on voitava olla varma, että hänen tietojaan käytetään asianmukaisesti. Peruslähtökohtana on, että tietojen käyttö edellyttää aina hoito- tai asiakassuhdetta. Käyttöoikeuksien hallinta, varmenneratkaisut, suostumukseen perustuva tietojen luovutus, lokitietojen valvonta sekä asiakkaan oikeus tarkistaa lokitiedot ovat keinoja vahvistaa asiakkaan luottamusta ja parantaa samalla myös ammattilaisen oikeusturvaa. (STM, 2007).

Sosiaali- ja terveydenhuollossa hyödynnettävälle tietoteknologialle asettavat omat erityisvaatimuksensa käsiteltävien potilas- ja asiakastietojen arkaluonteisuus. Tämän vuoksi terveydenhuollon tietojärjestelmän käytön täytyy olla sopusoinnissa lainsäädännön kanssa. Samalla kun tiedon käyttömahdollisuudet laajenevat, tulee entistä paremmin huolehtia tietoturvasta ja potilaan yksityisyyden suojasta myös arkipäivän toiminnan tasolla (STM, 2007).

Terveydenhuollon organisaation käyttöoikeuspolitiikan muodostumiseen vaikuttavia tekijöitä ovat lainsäädäntö ja suositukset. Siihen, miten käyttöoikeuspolitiikka lopulta toteutuu, vaikuttavat organisaatiossa laaditut käyttöoikeusmääritykset

sekä käytössä olevat tekniset ratkaisut pääsynvalvontaan, auktorisointiin ja auditointiin. Käyttöoikeuksien hallinnassa ja käyttäjähallinnassa terkoitushan on, että sovellusten käyttäjät saavat käyttöönsä vain ne resurssit, joihin heille on nimenomaisesti myönnetty pääsy. Tämä koskee käyttöjärjestelmän resursseja kaikilta sellaisilta osin, joihin pääsy voidaan hallinnoida. Pääsy hallinnoidaan sopivilla menetelmillä esimerkiksi käyttöjärjestelmä-, sovellus- ja käyttöliittymätasoilla sekä ottamalla käyttöön kertakirjautuminen ja siihen mukaan liitettävä tunnistautuminen. Jos käyttöoikeuksia myönnetään organisaation ulkopuolisille henkilöille, kuten esimerkiksi terveydenhuollon opiskelijoille, noudatetaan erityistä varovaisuutta ja riittäviä tarkastus- ja valvontamenettelyitä pääsynhallinnoinnissa.

1.2 Työn rakenne

Opinnäytetyön luvussa 1 kerrotaan johdanto työn aiheeseen ja esitetään opinnäytetyön tavoite. Tämän lisäksi luvussa yksi on taulukko opinnäytetyössä käytetyistä tietoteknisistä ja terveydenhuollon käsitteistä

Luvussa 2 käsitellään terveydenhuollon tietojärjestelmien käytössä huomioitavaa lainsäädäntöä, asetuksia ja standardeja. Terveydenhuollossa käsitellään nykyisin yhä enenevässä määrin sähköisessä muodossa olevia arkaluontoisia ja salassa pidettäviä tietoja. Terveydenhuollossa on kuitenkin pystyttävä noudattamaan standardeja ja muita voimassa olevia sääntöjä ja ohjeita, joilla ohjataan organisaatioiden toimintaa ja terveydenhuollon toimialaa. Säännöt ja ohjeet voivat muuttua hyvin nopeastikin, ja niitä on määrällisesti melko runsaasti.

Luvussa 3 tuodaan esille tunnistamisen ja todentamisen määrittelyt ja niiden eri menetelmiä. Luvussa käsitellään myös terveydenhuollon eri varmenteita.

Luvussa 4 tuodaan esille terveydenhuollon tietojärjestelmien käyttöympäristöä sekä käyttöoikeuksien hallinnan malleja ja määrittelyn periaatteita.

Luvussa 5. käsitellään.pääsynhallinnan ja käyttäjähallinnan menetelmiä sekä rooliperusteisia pääsynhallinnan malleja.

Luku 6 sisältää pohdintaa ja yhteenvedon opinnäytetyössä esitettyjen teoriatietojen käytäntöön soveltamista terveydenhuollon toimintaympäristössä.

1.3 Opinnäytetyön tavoite, tutkimusongelma ja työn rajaus

Tämä opinnäytetyö on osa laajempaa esiselvitystyötä terveydenhuollon käyttöoikeuksien hallinnan ja käyttäjän hallinnan muutoksesta. Opinnäytetyössä tarkastellaan myös terveydenhuollon keskeisempiä tietojärjestelmien käytössä huomioitavia lakeja, suosituksia, asetuksia ja standardeja, jotka vaikuttavat käyttäjän hallinnassa. Työssä tarkastellaan terveydenhuollon toimintaympäristön käyttöoikeuksien hallintaan ja käyttäjän hallintaan esitettyjä suositeltavia toimintatapoja tai -malleja käyttöoikeuksien määrittelyyn. Lisäksi työssä selvitetään pääsynhallintaan ja käyttäjähallintaan liittyviä tekijöitä, sekä autentikoinnin ja identifioinnin toteuttamisessa esiin tulevia vaatimuksia, myös terveydenhuollon tietojärjestelmien näkökulmasta tarkasteltuna.

Työn tavoitteena oli löytää malliratkaisuehdotuksia, joita voisi soveltaa käyttöoikeuksien hallinnassa ja käyttäjän hallinnassa terveydenhuollossa. Opinnäytetyön tutkimusongelma on osata soveltaa esitetyistä teoriatiedoista toimiva malliratkaisu. Johtopäätöksissä tulen esittämään oman ratkaisuehdotukseni terveydenhuollon toimintaympäristöön soveltuvasta käyttöoikeuksien hallintaan sopivasta mallista tai niiden mahdollisesta yhdistämisestä käytettynä terveydenhuollon organisaation käyttöoikeuksien hallinnassa ja käyttäjän hallinnassa. Työn rajaamiseksi, olen käsitellyt aihetta julkishallinnon terveydenhuollon näkökulmasta tarkasteltuna. Työstä on rajattu pois Stakesin vastuulla olevat luokitukset ja koodistot, apteekkien vastuulla olevat apteekkijärjestelmät ja terveydenhuollon organisaatioiden vastuulla olevien tietoliikenteen, kortinlukijoiden ja tietojärjestelmien tarkempi tutkiminen. Näin on jouduttu tekemään, sillä KANTAan liittyvän muutoksen kokonaisvaltainen käsittely olisi ollut liian laaja aihekokonaisuus opinnäytetyöhön.

1.4 Tietoteknisiä ja terveydenhuollon käsitteitä

Attribuutti	1)ominaisuus tai määre 2) oliota tai dokumentin rakenneosaa kuvaavaa tietoa sisältävä nimetty kenttä 3) relaatiomallissa sama kuin taulun sarake
Auktorisointi	Valtuuttaminen; prosessi, jolla myönnetään oikeuksia päästä järjestelmään ja käyttää sen palveluja määrätyillä säännöillä.
Autentikointi	Todentaminen; toimenpide, jolla todistetaan ja tunnistetaan määrätty informaatio esimerkiksi käyttäjän identiteetti. (Ahtonen 2003)
Entiteetti	Entiteetti on yleisnimitys, joka kattaa yhtä lailla oliot, oliojoukot ja ainemäärät, niin konkreettiset kuin abstraktit.
Hakemistopalvelu (directory service)	Kokoelma ohjelmia, laitteistoja, prosesseja, menetelmiä ja hallinnollisia toimia, joita käytetään hakemistoon talletetun tiedon järjestämiseen ja jakamiseen käyttäjille
HL7 CDA R1/R2 HL7/v3	CDA R1/R2, potilaskertomustietojen siirtomäärityksstandardi HL7v3 sanomanvälitys, tiedonsiirto, semanttisen sisällön implementointi, sanomanvälitys viestistandardi
Identifiointi	Tunnistus; prosessi, jolla voidaan varmistua jonkun henkilön identiteetistä.
Identiteetti	Joukko ominaisuuksia, jotka kuvaavat käyttäjää ja joiden avulla käyttäjä voidaan tunnistaa.
Julkisen avaimen järjestelmä (PKI, Public Key Infrastructure)	Julkisen avaimen järjestelmässä nimetty varmentaja tuottaa käyttäjille avainparit, varmentaa ne digitaalisella allekirjoituksellaan, takaa varmenteen haltijan henkilöllisyyden ja jakaa varmenteet käyttäjille, ylläpitää varmennehakemistoa ja sulkulistaa sekä mahdollisesti antaa muita järjestelmän käyttöön liittyviä palveluja. Julkisen avaimen järjestelmässä kullakin käyttäjällä on

	kaksi toisiinsa liittyvää avainta. Toinen avainparin avaimista on julkinen, toinen on vain avainparin käyttäjän hallussa ole-va yksityinen avain. Yksityisellä avaimella sähköisesti allekirjoitettu tiedon aitous voidaan todentaa vain vastaa-valla julkisella avaimella, ja vastaavasti tiedon välittämisessä vastaanottajan julkisella avaimella salattu tieto voidaan muuttaa selväkieliseen muotoon vain vastaanotta-jan yksityisellä avaimella.
Komponentti	Itsenäinen, uudelleenkäytettävä ja selvästi rajattu ohjelmisto-osa, jota käytetään pienempänä osana tietojärjestelmän rakentamisessa. Komponentti tarjoaa palveluitaan (suorittaa tiettyjä tehtäviä) rajapintojen kautta.
Konversio tai Konvertoida	muuntaminen, konvertointi
Käyttäjä	Henkilö, joka työssään tai muussa toiminnassaan on välittömästi tekemisissä atk- laitteen kanssa esimerkiksi ohjaten järjestelmän toimintaa, syöttämällä tietoja, tekemällä kyselyjä tai olemalla keskustelukäytön osapuolena.
Käyttäjän hallinta	Palvelu, jolla ylläpidetään käyttäjien ominaisuuksia ja tietoa siitä minkä tyyppinen käyttäjä voi käyttää palvelua. Käyttäjän hallinnan palveluihin kuuluu myös käyttäjien lisääminen ja poistaminen.
Käyttäjäprofiili	Ohjelmiston tai palvelun käyttäjäkohtaiset asetukset. Näillä asetuksilla säädellään mm. käyttäjän oikeuksia ja tälle tarjottuja toimintoja ohjelmistossa tai palvelussa.
Käyttöoikeus	Käyttöoikeus on oikeus käyttää tietojärjestelmän tiedostoja ja ohjelmia tietyillä tavoilla, esimerkiksi lukemalla, päivittämällä tai muiden käyttöoikeuksia muuttaen.
LDAP	Lightweight Directory Access Protocol. X.500-hakemistomallin kanssa yhteensopiva yksinkertainen protokolla, jota käytetään mm. julkisiin avaimiin WWW:n kautta pääsemiseksi.
Olio	Yleisesti: ympäristöstä erottuva kokonaisuus. Tietokokonaisuus, joka tarjoaa myös palveluja sisältämiensä tietojen käsittelyyn. Luokan ilmentymä.

PKI	Public Key Infrastructure, julkisen avaimen järjestelmä (Atk-sanakirja 2001). Luotettavan kolmannen osapuolen palvelujen mm. varmennepalvelujen avulla julkisen avaimen teknologiaan perustuvaa tietoturvaa tukeva järjestelmä.
Rajapinta	Kahden fyysisen tai abstraktin olion välinen tai ne yhteen liittävä käytäntö. Tässä opinnäytetyösssä tarkoitetaan sovellusliittymää, jonka kautta ohjelmisto tarjoaa tai käyttää toisen (varus- tai sovellusohjelmiston) palveluja. Ohjelmointirajapinta on rajapinta, jota sovelluksen rakentaja käyttää sovelluksen rakentamisessa.
RBAC-arkkitehtuuri	Role Based Access Control, rooliperustainen pääsynvalvonta
Rekisteröijä (RA, Registration Authority)	Julkisen avaimen järjestelmässä luotettu taho, joka varmentajan valtuuttamana ja auditoimana toteuttaa rekisteröijän tehtäviä. Rekisteröijä ylläpitää varmentajan lukuun yhtä tai useampaa RA-pistettä.
Rooli	Toimijalle määritellyt ominaisuudet, joiden perusteella toimija voi saada tiettyjä oikeuksia esim. järjestelmän tai sen piirteiden käyttöön. Yhdellä toimijalla voi olla useita rooleja ja sama rooli voidaan antaa usealle toimijalle. Käyttäjäroolit liittyvät yleensä henkilön tehtäviin organisaatiossa.
Semanttinen (web)	semanttinen web (semantic Web), toiselta nimeltään merkitysten verkko, on ATK-sanakirjan määritelmän mukaan visio, joka tähtää webin kehittämiseen liittämällä sen sisältöön metatietoa tietojen merkityksistä
Sulkulista (CRL, Certificate Revocation List)	Sulkulista on luettelo peruutetuista varmenteista. Varmenne peruutetaan, kun varmenteen haltija pyytää peruuttamista, menettää varmenteeseen merkityn ammatti-oikeuden, varmennekortti ja avaustunnusluku ovat kadonneet tai anastettu tai varmenteen haltija on kuollut.
Terveydenhuollon ammatti henkilö	Terveydenhuollon ammattihenkilöistä annetun lain (559/1994) 2 §:n 1 momentin mukaan terveydenhuollon ammattihenkilöllä tarkoitetaan henkilöä, joka lain nojalla on saanut ammatinharjoittamisoikeuden (laillistettu am-mattihenkilö) tai ammatinharjoittamisluvan (luvan saanut ammattihenkilö) sekä henkilöä, jolla lain nojalla on oike-us käyttää asetuksella säädettyä terveydenhuollon am-mattihenkilön ammattinimikettä (nimikesuojattu ammatti-henkilö). Tässä varmennepolitiikassa terveydenhuollon ammattihenkilöllä tarkoitetaan myös terveydenhuollon ammattihenkilöistä annetun lain 2 §:n 3 momentissa tar-koitettua opiskelijaa.

Todennus	toimenpide, jolla varmistetaan henkilön tai muun osapuolen aitous. Todennus tapahtuu esim. tunnistetietoon liittyvän salasanan, kertakäyttösalasanan tai PKI:n mukaisen avainparin avulla.
Toimihenkilö	Tietojärjestelmien kannalta palvelujen tuottaja on organisaatio tai yksittäinen henkilö, joka saa aikaan palveluja. Tässä toimihenkilöllä tarkoitetaan palvelujen tuottajaa yksittäisenä henkilönä, joka tuottaa tietojärjestelmän käyttötarkoituksen mukaisia palveluja.
Toimija	Käyttäjää laajempi käsite, joka voi tarkoittaa myös esimerkiksi organisaatiota. Autentikaation kannalta toimija on se kohde, joka tunnistetaan luotettavasti.
Toimiyksikkö	Tässä tarkoitetaan toimintayksikköä, joka on organisaatioyksikkö tai sen osa, joka on tehtäviensä hoitamisessa hallinnollisesti ja taloudellisesti itsenäinen. Sosiaali- ja terveydenhuollon toimintayksiköitä ovat esimerkiksi julkiset ja yksityiset sairaalat, terveyskeskukset sekä niiden osat. Tietojärjestelmien kannalta toimintayksikkö on tietojärjestelmää käyttävä organisaatio tai sen osa, jolla on vaikutusta tietojärjestelmän toimintaan. Organisaatiotiedot muodostavat tietojärjestelmissä erilaisia hierarkioita.
Tunnistus	Menettely, jolla yksilöidään tietojärjestelmän käyttäjä tai toimija. Tunnistus voi tapahtua esim. käyttäjätunnuksen, pankkitilin numeron tai vaikka henkilötunnuksen avulla.
Varmenne (Certificate)	Julkisen avaimen järjestelmää käyttävän palveluverkon toimijan kuten terveydenhuollon ammattihenkilön tai palveluntuottajan julkisesta avaimesta ja tunnistetiedoista muodostettu tietokokonaisuus, jonka varmentaja on muodostanut ja allekirjoittanut yksityisellä avaimellaan. Varmenteen aitous on todennettavissa varmentajan julkisella avaimella (varmentajan varmenteella).
Varmennehakemisto	Varmennehakemisto on julkinen tietokanta, johon varmentaja tallettaa varmentajan varmenteet, terveydenhuollon ammattihenkilöiden todentamisvarmenteet sekä sulkulistat.
24H/7d-periaate terveydenhuollossa	Potilastiedot käytettävissä kaikissa tilanteissa, tieto saatavissa ajasta ja paikasta riippumatta.

1.5 Käyttäjien hallinta

Käyttäjät ja heille myönnettävät valtuudet on määriteltävä riittävän turvallisesti, tehokkaasti ja tarkasti, jotta niillä voidaan toteuttaa tietojen ja tietojärjestelmien turvatason edellyttämät vaatimukset. Lisäksi Tammisalo (2005, 73) toteaa, että käyttäjien hallinnointi on määriteltävä tarkoin etukäteen. Tammisalon mukaan hallinnointimenetelmät voivat olla tietojärjestelmäkohtaisia, mutta yksinkertaisuuden saavuttamiseksi ja virhemahdollisuuksien vähentämiseksi menetelmien on oltava keskenään mahdollisimman yhdenmukaisia..

Käyttäjän hallinnointi sisältää määritykset käyttäjien hallintaan:

- kuinka ja millä menetelmillä tietojärjestelmien käyttäjät rekisteröidä
- millaista rekisteriä käyttäjistä pidetään
- millaisia ominaisuuksia kustakin käyttäjästä kirjataan (esimerkiksi käyttäjälle myönnettävän varmenteen attribuuteiksi)
- kuinka hallinnoidaan, että kukin käyttäjä saa nimenomaan hänelle kuuluvat käyttövaltuudet tietoihin.
- Lisäksi luonnollisesti käyttäjien ja käyttövaltuuksien poistaminen on osa käyttäjien hallinnointia. (Tammisalo, 2005, 71).

Käyttäjien hallinnassa tulee vastaan tilanteita, joissa käyttäjälle myönnetään laajoja käyttövaltuuksia, kuten järjestelmänhoitajat. Tällaisiin tilanteisiin tulee kiinnittää erityinen huomio oikeuksien hallinnointiprosessin kulkuun ja siihen, että laajat valtuudet eivät kirjaudu sellaiselle henkilölle, jolla ei ole niihin oikeutta. Tammisalon (2005, 74) mukaan tulee tällaisten valtuuksien käyttöä tarkkailla tarvittaessa tehostetusti. Myös vastuut kannattaa jakaa tarvittaessa osiin ja eriyttää ne eri henkilöille. Näin ehkäistään mahdollisuus liian suurten vastuiden kasautuminen yksittäisille henkilöille, ja voidaan vähentää tästä aiheutuvaa riskiä tärkeiden ja kriittisten tietojen väärinkäyttöön ja huolimattomuuteen tietojen käsittelyssä. Tammisalo esittää, (2005, 71), että esimerkiksi vastuut tietojärjestelmien ja tietoliikenneverkkojen hoidossa on syytä eriyttää.

2 LAIT, ASETUKSET JA STANDARDIT

Stakes julkisti vuonna 2006 terveydenhuollon alalle ohjeluonnoksen, jossa Taipale ja Ruotsalainen (2006, 1-4) ohjeistavat käsittelemään terveydenhuollon luottamuksellisia henkilötietoja ja huomioimaan samalla luovutusta säätelevät useat eri lait. Näitä mainittuja lakeja ovat muun muassa kansanterveyslaki (66/1972), potilasvahinkolaki (585/1987), erikoissairaanhoitolaki (1062/1989), laki potilaan asemasta ja oikeuksista (785/1992), laki terveydenhuollon ammattihenkilöistä (559/1994), henkilötietolaki (523/1999), laki viranomaisten toiminnan julkisuudesta (621/1999), Suomen perustuslaki (731/1999), laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002), hallintolaki (434/2003), laki sähköisestä asioinnista viranomaistoiminnassa (13/2003), laki sähköisestä allekirjoituksesta (14/2003), sähköisen viestinnän tietosuojalaki (516/2004), laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), sekä monet terveydenhuollon erityislait ja asetukset. Terveydenhuollon toimintaympäristöä säätää ja määrää runsas lainsäädäntö, mutta tässä opinnäytetyössä tarkastellaan lähinnä Kanta-järjestelmään liittyvää käyttöoikeuksien hallinnan ja käyttäjähallinnan lainsäädäntöä.

2.1 Lait

2.1.1 Henkilötietolaki (523/1999)

Terveydenhuollossa henkilötietojen käsittelyä säätelee lainsäädäntö. Henkilötietolaki edellyttää tietojen käyttöön asiayhteyttä ja siten käyttöoikeuden olemassaolo ei ole itsessään riittävä peruste terveystietojen käytölle tai luovutukselle. Tiedon omistajuus ei ole terveydenhuollossa ei ole aina selkeää eikä tiedon käytöstä ja luovutuksesta päättäminen voi perustua pelkästään omistajuuteen. Henkilötietojen käsittelyyn tarkoitetuissa tietojärjestelmissä, etenkin potilastietojärjestelmissä, tie-tosuoja- ja tietoturvavaatimukset ovat keskeisessä asemassa. Potilastietojen käsittelyä varten on lisäksi oma erityislainsäädäntönsä. Se asettaa yhdessä muiden terveydenhuollon toimialan piirteiden, muun muassa hoitavan henkilöstön vaihtu-

vuuden ja kiireen kanssa, erityisiä vaatimuksia tietojärjestelmän käyttöoikeuksien yksityiskohtaiselle määrittelylle, pääsynvalvonnalle ja auktorisoinnille, sillä hoidon sujumisen kannalta potilastietojen tulisi olla helposti ja nopeasti saatavilla. Käyttöoikeuksien määrittely tulisi voida tehdä käyttäjäkohtaisesti, työtehtävän mu-kaan sekä tietokokonaisuus- ja operaatiokohtaisesti. Henkilötietojen käsittelyyn ja luottamuksellisen viestinnän suojaan liittyviä säännöksiä on lukuisissa eri laissa. EU:n tietosuojadirektiivi muodostaa puitelainsäädännön. Terveydenhuollossa oi-keudesta käsitellä arkaluontoisia ja salassa pidettäviä tietoja on säädetty henkilötietolaissa. (Taipale, Ruotsalainen, 2006, 1-4).

2.1.2 Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)

Finlexissä Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), kutsutaan nimellä Asiakastietolaki, määritellään seuraavasti:

> Tämän lain tarkoituksena on edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä. Lailla toteutetaan yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjestelmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi. (Finlex 159/2007).

Edellä mainitun lainkohdan 5 §:ssä todetaan, että käytön ja luovutuksen seurannassa sosiaali- ja terveydenhuollon palvelujen antajan tulee pitää rekisteriä omien asiakastietojärjestelmiensä ja asiakasrekisteriensä käyttäjistä sekä näiden käyttöoikeuksista. Lisäksi palvelujen antajan tulee kerätä asiakasrekisterikohtaisesti kaikesta asiakastietojenkäytöstä ja jokaisesta asiakastietojen luovutuksesta seurantaa varten lokitiedot lokirekisteriin, joista muodostuvat käyttölokirekisteri ja luovutuslokirekisteri. (Finlex 159/2007).

Saman lain 4 luvussa 14 §:ssä todetaan, että Kansaneläkelaitos (Kela) hoitaa terveydenhuollon palvelujen antajien lukuun potilasasiakirjojen säilytystä ja käyttöä varten olevaa arkistointipalvelua sekä sen osana potilasasiakirjojen luovutusta varten hakemistopalvelua ja suostumuksenhallintapalvelua. Kansaneläkelaitos hoitaa luovutuslokirekisterien säilytyksen osana arkistointipalvelua. Kansaneläke-

laitos voi hoitaa osana arkistointipalvelua myös käyttölokirekisterien säilytyksen. (Finlex 159/2007).

2.1.2.1 Asetus sähköisestä lääkkeenmääräyksestä ja lääkkeen määräämisestä annetun asetuksen muuttamisesta (485/2008 ja 490/2008) ja sähköistä lääkemääräystä koskevaa laki (61/2007)

Sosiaali- ja terveysministeriön (STM) Tiedonhallinnan ajankohtaista linkissä todetaan, että sosiaali- ja terveysministeriön asetus sähköisestä lääkemääräyksestä (485/2008) on vahvistettu ja julkaistu 16.7.2008 säädöskokoelmassa ja asetus (490/2008) annetun asetuksen muuttamisesta lääkkeen määräämisestä on vahvistettu ja julkaistu säädöskokoelmassa 18.7.2008. Asetukset astuvat voimaan 1.8.2008.

Edellä mainitusta asetuksesta sähköisestä lääkkeenmääräyksestä käytetään terveydenhuollon toimintaympäristössä nimeä eResepti-asetus. Finlexin lakikokoelma linkissä todetaan, että eReseptillä tarkoitetaan toimintamallia, jossa lääkäri kirjoittaa potilaalle lääkemääräyksen potilaskertomusjärjestelmässä ja lähettää sen sähköisesti keskitettyyn tietokantaan. Potilas voi mennä mihin tahansa apteekkiin noutamaan hänelle osoitetun lääkemääräyksen. Sähköistä lääkemääräystä koskevaa laki (61/2007) tuli voimaan 1.4.2007. Lain mukaan Kansaneläkelaitos hallinnoi valtakunnallista reseptikeskusta. Kansaneläkelaitos on aloittanut valmistelut valtakunnallisesti levitettävän toimintamallin käyttöönottamiseksi. (Finlex 2008).

2.2 Standardit

2.2.1 Standardointiorganisaatiot

Terveydenhuollon informatiikan (Health Informatics) alueella toimivia keskeisiä kansainvälisiä standardisointiorganisaatioita ovat ISO, CEN, ANSI, ASTM ja HL7.Nämä organisaatiot tuottavat terveydenhuoltospesifisiä standardeja niissä tapauksissa, joissa yleiset tietotekniikan standardit eivät sellaisenaan sovellu alalle

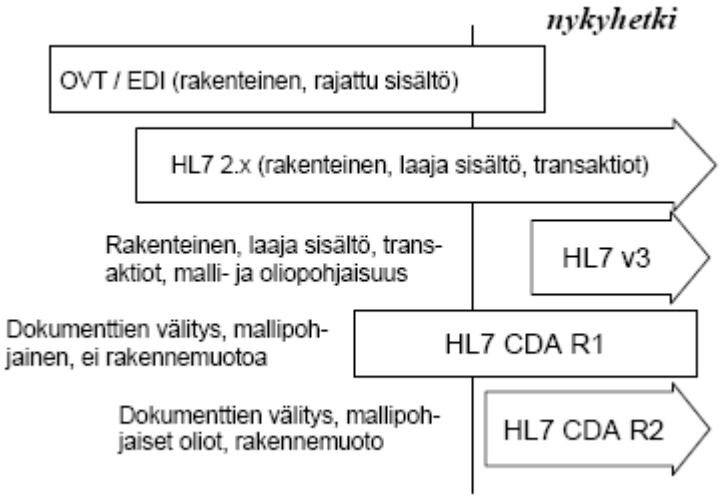
tai niitä ei ole. Terveydenhuolto käyttää laajasti yleisiä tietotekniikan standardeja, joita tuottavat sellaiset organisaatiot kuin IETF, ITU-T, W3C, OASIS ja OMG. (Suomen Standardoimisliitto)

2.2.2 Standardoinnin tasoja

De jure standardit ovat virallisen standardointiorganisaation laatimia, kuten CEN 251:n, ISO TC 215:n, ASTM:n ja IEC:n. Kansainvälinen kattostandardointiorganisaatio on ISO (International Standardisation Organisation), jonka TC 215 komiteassa toteutetaan terveydenhuollon tietotekniikan standardointia. Merkittäviä amerikkalaisia standardointiorganisaatioita terveydenhuollon alalla ovat muun muassa ACR/ NEMA, ASTM ja HL7, jotka ovat Yhdysvaltain kansallisen standardointielimen (ANSI) akreditoimia organisaatioita. Terveydenhuollon tietojärjestelmien standardisoimistyötä on Euroopassa tehty jo yli kymmenen vuoden ajan CEN:in (Commité Européen de Normalisation) perustamassa teknisessä komiteassa TC251. Se tuottaa sekä ns. esistandardeja että virallisia standardeja terveydenhuollon käyttöön. (STM, 2003, 20-23) RBAC-arkkitehtuurin (role based access control) palveluita määrittelevät ASTM E31.20 ja ITU X.509-standardit. (Ruotsalainen, 2006, 36)

De facto standardit puolestaan ovat jonkin epävirallisen ryhmän tai yrityksen luoma käytäntö, josta on tullut standardi, kuten HL7 ja DICOM. Merkittävää de facto –standardointityötä on Suomessa tehnyt Suomen HL7-yhdistys, joka on paikallistanut kuviossa 1 esitetyn mukaisesti suuren joukon Suomessa terveydenhuollossa hallitsevia HL7 -standardeja. Suomen HL7-yhdistyksessä on jäsenenä useita yrityksiä ja terveydenhuollon organisaatiota. Näitä HL7-standardeja käytetään hyvin yleisesti mm. laboratoriotutkimuspyyntöjen ja –vastausten siirrossa. HL7:n XML-pohjainen CDA-standardi otettiin käyttöön saumattoman palveluketjun kokeilulain yhteydessä palvelemaan tietojen katselua viitetietojärjestelmän avulla. Tämä standardi HL7 CDAR2 määrittelee sähköisen potilaskertomuksen rakenteen ja sen käyttö tulee yleistymään siirryttäessä Kanta-järjestelmään. Standardin avulla potilaskertomuksen ja potilasasiakirjojen ulkoasua voidaan muokata sisältöä muutta-

matta. Standardi on myös käytettävissä vuosikymmenien ajan ja se on helposti konvertoitavissa. (STM, 2003, 20-23).



KUVIO 1. Tiedonsiirtostandardien nykytila ja ennustettu elinkaari (STM, 2003)

3 TUNNISTAMINEN JA TODENTAMINEN

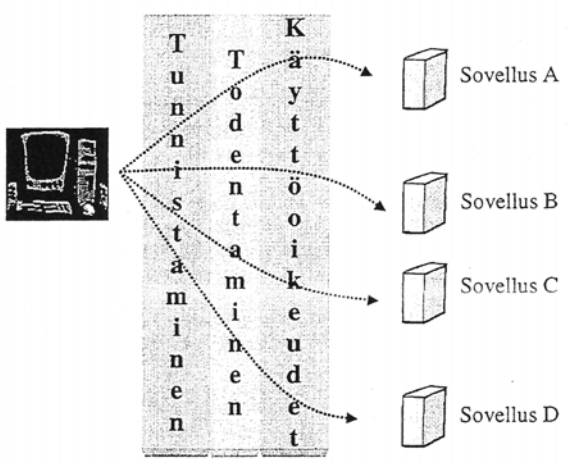
3.1 Tunnistaminen ja todentamisen menetelmiä

Käyttäjän tunnistusta tarvitaan, kun myönnetään ja hallitaan käyttöoikeuksia ja –valtuuksia. Sitä tarvitaan lisäksi mm. kertakirjautumisen periaatteen toteuttamisessa, sillä käyttäjän tunnistusjärjestelmän avulla tulee voida yksikäsitteisesti tunnistaa yksittäinen käyttäjä. Taipale ja Ruotsalainen (2006, 1-4) ohjeistavat Stakesin näkemyksen mukaan, että identiteetti on niiden ominaisuuksien joukko, joiden perusteella käyttäjä, entiteetti tai prosessi voidaan tunnistaa. Tunnistaminen tulee pitää erillään todentamisesta, käyttöoikeuksien hallinnasta ja tietojen käytön hallinnasta. Tunnistamisessa yksilöidään identiteetti, todentamisessa vakuuttaudutaan identeetin oikeellisuudesta.

Ruotsalainen (2002, 19) toteaa vuonna 2002 tehdyssä julkaisussa, että termejä tunnis-taminen ja todentaminen käytetään yleisesti jokseenkin vapaasti ristiin. Lienee helpompaa mieltää niiden ero, jos ajatellaan, että käyttäjä tunnistetaan käyttäjätunnuksen tai vaikka henkilötunnuksen avulla. Tunnistettu käyttäjäidenti-

teetti todennetaan käyttäen jotain todentamismenetelmää. Sellaisia ovat mm. kiinteä salasana, kertakäyttöinen salasana, haastelukulaskin (ns. SecurID-laskuri), Public Key Infrastructure -varmenne (PKI, julkisen avaimen järjestelmä), biometrinen todentaminen, televerkon kautta tehtävä tunnistus tai luotetun kolmannen osapuolen varmennus.

Todentaakseen henkilöllisyytensä ja oikeutensa käyttäjän on todistettava identiteettinsä käyttäen luotettavaa ja varmaa todentamisen menetelmää voidakseen vakuuttaa, että hän on se kuka väittää olevansa. Todentaminen on luotettava, jos siinä voidaan luottaa todentamisen välineen myöntäjään, silloin voidaan uskoa tunnistusasiakirjan autenttisuuteen eli aitouteen. Usein käytetään kolmatta osapuolta, joka takaa tunnistustiedon oikeellisuuden. Lisäksi tavallista on käyttää haaste-vaste-menettelyä, jossa tunnistava osapuoli lähettää tunnistettavalle haasteen, johon tämän on osattava reagoida ja vastata oikealla yhdessä sovitulla tavalla. Tunnistava osapuoli tarkistaa tämän vastauksen. Luotettava todentaminen perustuu siihen, että yhteyden kummassakin päässä käytetään tunnettujen varmentajien myöntämiä varmenteita, joiden allekirjoittaja ja sulkulistat tarkistetaan ja joiden salaiset avaimet ainakin käyttäjän osalta ovat toimikortilla. Todentamisessa voidaan käyttää standarditekniikoita, joita ovat mm. IPSec, SSL ja haaste-vaste-menetelmät. Tunnistamista ja todentamista hyväksikäytetään määriteltäessä käyttöoikeuksia eri sovelluksiin ja järjestelmiin. Ruotsalainen (2002, 20) kertoo, että pääsynvalvonnan tukena tarvitaan kuviossa 2 esitetyn mukaisesti käyttäjähakemisto tai –tietokanta, jonka on sisällettävä tiedot palvelujen käyttöön oikeutetuist käyttäjistä. (Ruotsalainen 4/2002, 19-20).



KUVIO 2. Asioitaessa verkossa käyttäjä tarvittaessa tunnistetaan, todennetaan ja hän saa pääsynvalvonnassa identiteetilleen ja roolilleen määritellyt käyttöoikeudet (Ruotsalainen, 2002)

Pääsynvalvonnassa käytetään menettelyinä tunnistamista, todentamista ja käyttäjäoikeuksia. Kun tieto on luottamuksellista tai sitä halutaan jakaa vain valikoidulle käyttäjäryhmälle, silloin otetaan käyttöön pääsynvalvonta. Ruotsalainen (2002, 20) sanoo, että pääsynvalvontaa ei tarvita, jos tarjolla on anonyymipalveluita, toisin sanoen sellaisia palveluita, joiden sisältämistä tiedoista ei voida tunnistaa tai yksilöidä henkilöä. Terveydenhuollossa ei anonyymipalveluita yleensä käytetä tietojen arkaluonteisuuden takia.

3.1.1 Heikko tunnistaminen

Heikolla tunnistamisella tarkoitetaan IT-alan sanaston mukaan tunnistamismenetelmää, joka perustuu vain yhteen seuraavista kolmesta tekijästä:

- mitä henkilö on
- mitä henkilöllä on tiedossaan
- mitä henkilöllä on hallussaan.

Esimerkiksi käyttäjätunnukseen tai tunnussanaan tai -lukuun perustuva tunnistaminen on ns. heikko tunnistaminen.

3.1.2 Vahva tunnistaminen

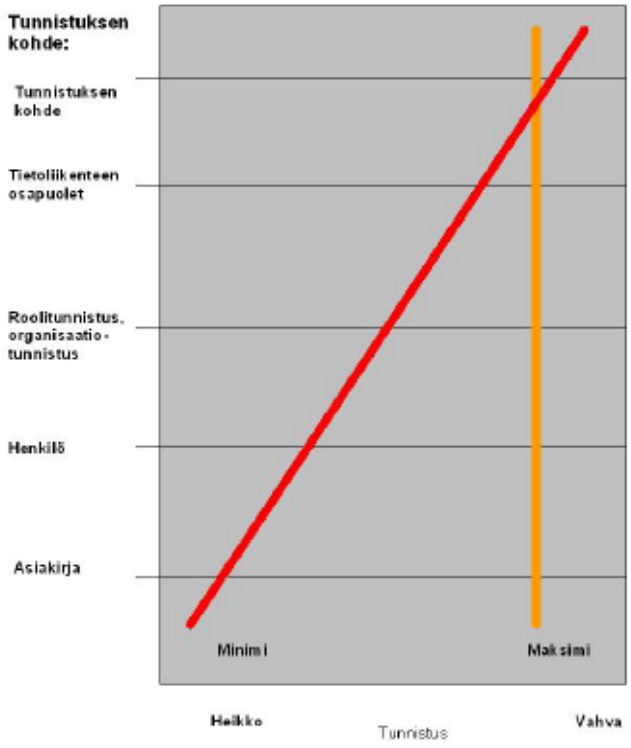
Vahva tunnistaminen tapahtuu vähintään kahden tekijän perusteella (ns. two factor authentication). Vahvasta tunnistamisesta puhutaan, kun halutaan tunnistaa käyttäjä varmasti. Vahva tunnistaminen voi perustua esimerkiksi siihen, mitä käyttäjä omistaa, todentamiseen vaaditaan jotain avainlaitetta ja kolmannessa (biometriset tunnisteet) tutkitaan käyttäjän henkilökohtaisia ominaisuuksia, kuten sormenjälkiä. Jokaiseen luokkaan on tarjolla lukuisia vaihtoehtoisia periaateratkaisuja ja keskenään kilpailevia tuotteita. (VIRTU, 2007, 4-5.)

Biometriset tunnistusmenetelmät pyrkivät tunnistamaan käyttäjän jonkin tämän fyysisen ominaisuuden – somrenjäljen, äänen, kasvonpiirteiden, tai silmän – perusteella. Tunnistettava käyttäjä antaa näytteen tunnistettavasta fyysisesta ominaisuudesta esimerkiksi sormenjälki, jota verrataan käyttäjästä aiemmin otettuun näytteeseen. Jos annettu näyte on tarpeeksi lähellä tallennettua näytettä, tunnistus hyväksytään. (Ruohonen, 2002, 154)

3.2 Tunnistusmekanismit

Tunnistus ulottuu yksittäisestä asiakirjasta tietoliikenteen useisiin osapuoliin. Tun-nistuksen vahvuus voi vaihdella eri tehtävissä. Asiakirjan tunnistusta ei tarvita ai-na lainkaan, mutta esimerkiksi reseptin tunnistus on tehtävä aina vahvasti. Kuviossa 3 on esitetty, miten tunnistuksen vahvuuden tarve kasvaa tunnistuksen kohteen mukaan. Toisaalta, mitä vaativampiin tietoteknisiin ympäristöihin siirrytään, sitä suuremmat vaatimukset on tunnistuksen luotettavuudelle asetettava. Yhtä ai-noaa, kaikkiin tilanteisiin sopivaa tunnistusratkaisua ei käytännössä ole olemassa. (VIRTU, 2007, 4-5.) Tietoverkossa asioitaessa on mahdollista eri menetelmin tun-nistaa toinen osapuoli. Se voidaan tehdä ns. heikkojen tai vahvojen tunnistusmenetelmien avulla, riippuen osapuolten haluamasta turvatasosta ja luo-

tettavuudesta. Järjestelmän vahvuuden tai heikkouden määrittelevät osapuolet kulloistenkin turvatarpeensa tasosta. Yleisesti voidaan sanoa, että kryptografisesti vahvat järjestelmät ovat vahvoja tunnistusmenetelmiä. (Ruotsalainen, 2002, 19.)



KUVIO 3. Tunnistuksen periaatekuva (VIRTU, 2007)

Tunnistusmekanismin piiriin kuuluvat muun muassa:

- Salasanat (kuten käyttäjäkohtaiset salasanat, Tupas, Katso jne.)
- Avainlaitteet (kortit, sim -kortit, usb-väyläiset tokenit)
- Biometriset tunnisteet

Ensimmäisessä tunnistusmekanismissa (salasanat) käyttäjän henkilöllisyys todennetaan kysymällä henkilön tiedossa olevaa salasanaa. Toisessa (avainlaitteet) henkilöllisyys todennetaan esim. toimikortille tallennetulla salakirjoitusavaimella. Vahva tunnistaminen voi perustua myös siihen, mitä käyttäjä on kuten biometriset menetelmät, esimerkiksi sormenjälkitunnistus. Vahvinta tunnistamista vaativissa tilanteissa voidaan käyttää yhdistelmää eri menetelmistä. (Valtiovarainministeriö, 2008).

3.3 Tunnistaminen terveydenhuollossa

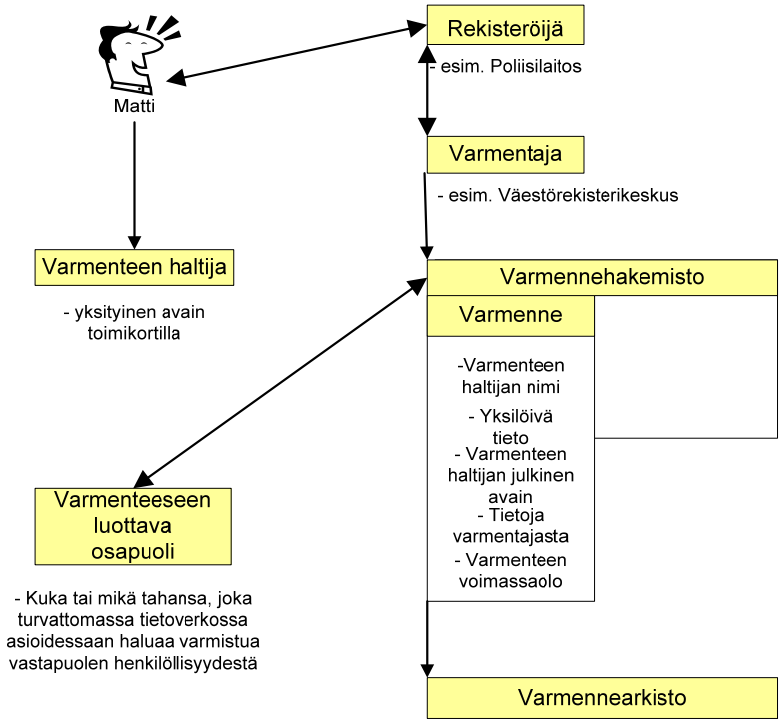
Terveydenhuollossa käyttäjän tunnistus perustuu vielä tällä hetkellä pääsääntöisesti eri järjestelmien omiin tunnistusmekanismeihin, yleisemmin käyttäjätunnuksen ja salasanan käyttöön. Terveydenhuollon ammattilaisilla voi olla käytössään joukko salasanoja eri järjestelmiin, ja salasana kysytään yleensä aina jokaisen järjestelmän käynnistyksen yhteydessä. Käytössä on myös osastokohtaisia tunnuksia, joilla useat käyttäjät pääsevät järjestelmään ilman, että tarvitsee kirjautua uudelleen esim. henkilökohtaisen käyttäjätunnuksen ja salasanan avulla. (Ruotsalainen, 2002, 23)

Terveydenhuollon potilastietojärjestelmiä ja arkistopalveluja käyttävät ammattihenkilöt tulee voida tunnistaa ja todentaa luotettavasti, siirryttäessä KANTAan. Tämän johdosta suositellaan määriteltäväksi käyttäjien tunnistamisen menetelmistä ja käytettävistä tunnisteista oma politiikka. Vain riittävän vahvat ja turvalliset menetelmät hyväksytään. Tunnisteina hyväksytään vain sellaiset, joiden väärentäminen ei ole mahdollista ja joiden avulla tietojärjestelmiä ei voi väärinkäyttää. Ammattihenkilön tunnistamisen ja sähköisen allekirjoituksen osalta tukeudutaan Terveydenhuollon oikeusturvakeskuksen (TEO) ammattivarmennepalveluun ja toimintayksiköissä toteutettuun käyttöoikeuksien hallintaan. (Sormunen, Porrasmaa, Silvennoinen, Mykkänen, Savolainen ja Rannanheimo, 2004, 20).

Terveydenhuollossa tulee roolipohjaisella tunnistatumisella tulevaisuudessa olemaan suuri merkitys. Saman organisaation sisällä saattaa esimerkiksi lääkärillä olla yhden päivän aikana useita dynaamisesti muuttuvia rooleja. Lisäksi hänellä voi olla käytössään sekä julkisen sektorin että yksityisen sektorin roolit samanaikaisesti. Ruotsalainen (2002, 23) esittää, että sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuurissa terveydenhuollon tunnistautumisen tulee tulevaisuudessa tapahtua lähtökohtaisesti roolipohjaisena.

3.4 PKI-järjestelmä

PKI-järjestelmäksi (PKI, Public Key Infrastructure), joka on kuvattu kuviossa 4,kutsutaan varmenteiden myöntämiseen, jakeluun, hallinnointiin ja ylläpitoon kuuluvaa kokonaisuutta. Järjestelmässä avain ja tieto avaimen haltijasta sidotaan yhteen, jolloin saadaan varmenne.Varmenteiden laajamittainen käyttö puolestaan edellyttää PKI-järjestelmää. Varmenne sisältää tietoja siitä, kenelle varmenne on myönnetty. PKI:ssa käytetään digitaalista avainparia, joista toinen on julkinen ja toinen yksityinen, ja järjestelmä perustuu asymmetriseen salaukseen. Allekirjoittaja tekee allekirjoituksen omalla, yksityisellä avaimellaan, joka on vain hänen tiedossaan. Allekirjoituksen vastaanottaja voi todentaa allekirjoituksen aitouden ja viestin eheyden varmenteessa olevan julkisen avaimen avulla. (Ruotsalainen, 2002, 19.)



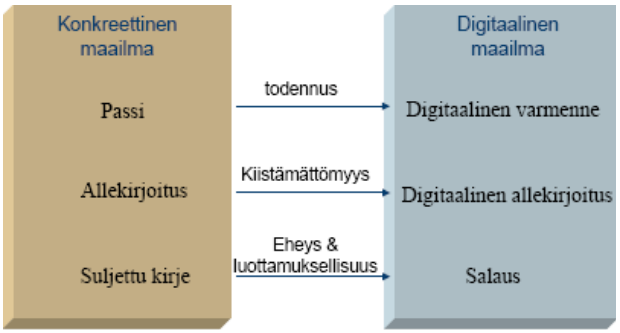
KUVIO 4. PKI:n osapuolet (Porali, Ensio, 2005)

PKI-järjestelmän ytimenä toimii varmenteiden myöntäjä (Certification Authority, CA). Kun henkilö haluaa itselleen varmenteen, hän luo itselleen julkisen ja yksityisen avaimen, ja toimittaa ne myöntäjälle. Myöntäjä tarkistaa tiedot ja allekirjoittaa ne omalla yksityisellä avaimellaan. Sen jälkeen henkilöllä on sähköinen todistus siitä, kuka hän on. Jos henkilö ei osaa tai halua luoda avainparia, silloin tehtävä jää varmenteen myöntäjälle, johon henkilön on voitava luottaa. Myöntäjä luo avaimet ja lisättyään julkisen avaimen varmenteeseen, antaa hän sekä varmen-

teen että avaimet henkilölle. Käyttännön syistä varmenteen myöntäjä saattaa olla eri taho kuin tietojen tarkistaja. Erillisestä tarkistajasta käytetään nimitystä rekisteröijä (Registration Authority, RA). (Järvinen, 2003,159-166).

Varmennehakemisto päivittyy säännöllisesti, mikä varmistaa ajan tasalla olevan hakemiston kaikista myönnetyistä varmenteista. PKI-järjestelmän käyttäjät voivat etsiä hakemistosta muiden varmenteita ja noutaa niitä omaan käyttöönsä. PKI-järjestelmään liittyy kiinteästi sulkulistapalvelut (Certificate Revocation List, CRL). Listalle lisätään niiden varmenteiden sarjanumerot, jotka on jouduttu mitätöimään ennen normaalia vanhenemista. Sulkulistaa varten on määritelty kymmenen erilaista syykoodia. (Järvinen 2003, 166.) Ruotsalainen (2002, 11) sanoo, että PKI-järjestelmää käytetään tietoturvapalveluna, koska se on osoittautunut tehokkaaksi menetelmäksi ylläpitää luottamus ja kiistämättömyys sähköisessä asioinnissa.

PKI-infrastruktuuri tarjoaa kuviossa 5 esitetyllä tavalla neljä luotettavaa ja tehokasta turvallista palvelua. Näitä ovat



KUVIO 5. PKI-järjestelmän luottamuksen taso (Ruotsalainen 4/2002)

- Vahva tunnistaminen eli todennetaan varmasti asioiva osapuoli (esim. henkilö, laite tai ohjelmisto).
- Tiedon eheys eli osoitetaan, että osapuolten välisessä viestissä mitään ei ole muutettu.
- Luottamuksellisuus eli taataan, että kukaan muua kuin vastaanottaja ei voida saada selville viestin sisältöä.

- Kiistämättömyys digitaalisella allekirjoituksella eli varmennetaan, että lähetetty viesti on lähettäjän lähettämä ja muuttumaton. (Ruotsalainen, 2002, 11).

3.5 Varmenne

Varmenne eli sertifikaatti (certificate) on sähköinen todistus, joka on myös standardimuodossa kerrottu tieto. Se sisältää joukon tietoja, jotka varmenteen myöntäjä on tarkistanut ja todennut oikeiksi. Sen jälkeen hän on laskenut tiedoista tiivisteen ja allekirjoittanut sen digitaalisesti. Henkilö, jolle varmenne esitetään, tarvitsee varmenteen myöntäjän julkisen avaimen purkaakseen tiivisteen ja verratakseen sitä itse laskemaansa. Jos tulokset täsmäävät, varmenteessa kerrottua tietoa voidaan pitää uskottavana. Varmenne on pelkkä tiedosto, jossa ei itsessään ole mitään erityistä. Tiedosto sisältää halutut tiedot kenttinä, aivan kuten kortistossa tai tietokantaohjelmassa. Jotta eri tahojen myöntämät varmenteet olisivat yhteensopivia, tarvitaan standardi määrittelemään kenttien nimet, koodaustapa ja muuta perustietoa. (Järvinen 2003, 159-163).

Varmenteen kertomiin tietoihin voidaan luottaa, mikäli seuraavat ehdot täyttyvät:

- Varmenteen myöntäjään luotetaan. On voitava olla varma siitä, että myöntäjä on todella tarkistanut tietojen aitouden ennen todistuksen myöntämistä.
- Varmenteen myöntäjän yksityisen avaimen on pysyttävä salassa. Jos avain paljastuu, ulkopuolinen hyökkääjä pystyy luomaan esteettä väärennettyjä varmenteita. Aitous lepää täysin salauksen varassa.
- Varmenteen myöntäjän julkinen avain on saatu turvallista kanavaa pitkin, joten se on varmasti aito ja siksi luotettava.
- Varmenteessa käytetty salaustekniikka on riittävän turvallista (algoritmit, avain pituudet). (Järvinen, 2003, 159).

3.6 TEO-varmenteet

3.6.1 TEO-Ammattivarmenteet

TEO myöntää todentamis- ja salausvarmenteita sekä allekirjoitusvarmenteita terveydenhuollon ammattihenkilöistä annetussa laissa (559/1994) tarkoitetulle terveydenhuollon palvelujen antajien henkilöstölle, jotka eivät ole terveydenhuollon ammattihenkilöitä (jäljempänä terveydenhuollon muu henkilö). (TEO, 2008 1b, 8)

Varmenteen hakija tunnistetaan henkilökohtaisesti rekisteröintipisteessä varmennetta haettaessa voimassa olevasta poliisin myöntämästä virallisesta henkilöllisyysasiakirjasta (passi tai 1.3.1999 jälkeen myönnetty henkilökortti). Muut kuin Suomen kansalaisuuden omaavat henkilöt tunnistetaan voimassaolevasta passista tai EU-henkilökortista. (TEO, 2008 1b, 8)

Terveydenhuollon henkilövarmenteita käytetään varmenteen haltijan sähköiseen tunnistamiseen, tiedon salaamiseen sitä viestitettäessä tai tallennettaessa ja sähköiseen allekirjoittamiseen eli digitaalisen dokumentin tai muun tiedon (esimerkiksi potilasasiakirjamerkintä, sähköinen lääkemääräys) aitouden, eheyden ja kiistämättömyyden varmistamiseen. (TEO, 2008 1b, 8)

1. Todentamiseen/tunnistautumiseen/salaukseen
    - 1024bit RSA-avain
    - Rekisterinumero
    - Suku- ja etunimi
    - Voimassa 5 vuotta (tai vähemmän, esim. lupa toimia)
    - UPN-nimi (@teonet.fi), todentamisvarmenteissa UPN-nimi esim. Windows AD-kirjautumista varten 12345678901@teonet.fi) (ammattihenkilöiden varmenteissa) (TEO 1a, 2008).
2. Allekirjoittamiseen
    - Kuten todentamisvarmenne, lisäksi:
    - 2048bit RSA-avain

- Ammattioikeuskoodi, tekstinä suomeksi ja ruotsiksi
- SV-numero (lääkäreillä)
- Ei UPN-nimeä (TEO 1a,2008).

3.6.2 TEO-Muut henkilövarmenteet

Kaksi varmennetta

1. Todentamiseen/tunnistautumiseen/salauksee
    - 1024bit RSA-avain
    - Yksilöivä tunnus (997/998…)
    - Suku- ja etunimi
    - Voimassa 5 vuotta (tai vähemmän)
    - Organisaatio ja optiona organisaatioyksikkötiedot
    - Sähköpostiosoite
    - UPN-nimi (@teonet.org), (muun henkilöstön varmenteissa 99812345678@teonet.org) (TEO 1a, 2008)

2. Allekirjoittamiseen
    - Kuten todentamisvarmenne, lisäksi:
    - 2048bit RSA-avain
    - Ammattinimike, 997/998+tekstinä suomeksi ja ruotsiksi
    - Ei UPN-nimeä (TEO 1a, 2008)

3. Avaimet luodaan sirulla (ei kopioita) (TEO 1a, 2008)

3.6.3 TEO-palveluvarmenteet

1. Palvelimien todentamiseen ja tl-salaukseen
    - Organisaatio ja optiona organisaatioyksikkötiedot
    - Yksilöivä tunnus (OID-tunnus)
    - 1024/2048bit RSA-avain (TEO 1a, 2008)

2. Järjestelmäallekirjoitusvarmenteet järjestelmäallekirjoituksille

   - Organisaatio ja optiona organisaatioyksikkötiedot
   - Yksilöivä tunnus (OID-tunnus)
   - 2048bit RSA-avain (TEO 1a, 2008)

3. Sähköpostipalveluvarmenteet sähköpostien salaamiseen ja/tai allekirjoittamiseen

   - Organisaatio ja optiona organisaatioyksikkötiedot
   - Yksilöivä tunnus (OID-tunnus)
   - 1024/2048bit RSA-avain
   - Sähköpostiosoite (helpdesk, ajanvaraus, kirjaamo, valvomo, yms. ei-henkilökohtainen) (TEO 1a, 2008).

3.7 Sähköinen allekirjoitus

Kehittynyt ja/tai turvallinen sähköinen allekirjoitus tarkoittaa laatuvarmenteisiin (TEO:n, VRK:n varmenteet) ja lakiin perustuvaa kiistämätöntä allekirjoitusta. (TEO 1a, 2008). Järvinen (2003, 171) kommentoi, että tällainen sähköinen allekirjoitus voidaan rinnastaa oikeustoimissa tavalliseen, kynällä tehtyy allekirjoitukseen.

Terveydenhuollon kansallinen ohjelma ja lainsäädäntö edellyttävät, että Kanta-järjestelmään siirrettävät asiakirjat tulee olla sähköisesti allekirjoitettu. Sähköinen allekirjoitus on sopimusperusteista ja luottamukseen perustuvaa. (TEO 1a, 2008).

Sähköisiä allekirjoitusmuotoja ovat:

- Henkilön tai viranhaltijan allekirjoitus, esimerkiksi kansalaisen suostumus-allekirjoitus ja lääkärin allekirjoittama potilasasiakirja

- Moniallekirjoitus, joka esimerkiksi on useamman henkilön allekirjoittama yksi ja sama asiakirja kuten viranhaltijapäätös
- Sarja-allekirjoitus, joka esimerkiksi on yhdellä allekirjoituksella usea asiakirja kuten resepti (TEO 1a, 2008).

Terveydenhuollossa käsiteltävä informaatio on useimmiten salassa pidettävää, ja tällöin informaation laatineen ammattilaisen allekirjoitus tarvitaan. Varmenneympäristö on ainoa oikea tapa vakuuttua allekirjoittajasta ja allekirjoitetun tiedon muuttumattomuudesta. Varmenteiden luottamusketjun perusteella voidaan löytää luotettava kolmas osapuoli, jonka todistukseen henkilön identiteetistä ja sen oikeellisuudesta voidaan luottaa. Silloin kun terveydenhuollon sähköiseen asiointiin sisältyy salassa pidettävien asiakas/potilastietojen siirtoa tai käyttöä, on perusvaatimuksena, että kyetään tunnistamaan luotettavasti palveluntuottajat, niiden alaorganisaatiot, ammattilaiset, asiakkaat/potilaat, tietojärjestelmien palvelimet ja tarvittaessa käytettävät ohjelmistot. (Ruotsalainen, 2002, 23.)

Väestörekisterikeskus on tällä hetkellä Suomessa ainoa ns. laatuvarmentaja, joka pystyy tarjoamaan sähköisistä allekirjoituksista annetun lain vaatimukset täyttäviä ja EU-direktiiviin pohjautuvia yleiseurooppalaisia, korkean tietoturvan ja oikean henkilöllisyyden sisältäviä varmenteita. (Väestorekisterikeskus)

3.8 TEO:n tunnistekortti

Ruotsalainen näkee (2002, 10), että Terveydenhuollon oikeusturvakeskus (TEO) on kansallisesti vastuullinen toimija, sillä se toimii terveydenhuollon palvelujen antajien sekä näiden palvelujen antamiseen osallistuvien henkilöiden ja tietoteknisten laitteiden varmentajana. Kansaneläkelaitos on reseptikeskuksen ja reseptiarkiston rekisterinpitäjä. Valtakunnalliseen arkistointipalveluun ja e-reseptijärjestelmään voi tunnistautua ainoastaan TEO:n varmenteella. Varmennettavia ovat terveydenhuollon ammattihenkilöt, muut potilasasiakirjoja käsittelevät toimihenkilöt, julkiset ja yksityiset palvelujen antajat sekä tietotekniset laitteet. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) eli ns.

asiakastietolaki, vastuuttaa TEO:n hallinnoimaan terveydenhuollon ammattihenkilöiden varmennepalvelua. Varmennepalvelu perustuu toimikorttiin ja kansalliseen PKI-ratkaisuun. Jo yli puolessa sairaanhoitopiireissä on suunniteltu otettavan käyttöön vahvan tunnistamisen mahdollistava ammattikortti. Tulevassa valtakunnallisessa arkkitehtuurissa TEO:n varmennepalvelun käyttö on pakollista. Käyttövaltuuksien määrittäminen ja hallinta jää paikallisella tasolla toteutettavaksi. Tavoitteena on ottaa käyttöön rooli- ja sääntöpohjainen valtuuksien hallinta, joka perustuu kansainvälisiin ISO-standardeihin. Paikallisella tasolla tulee toteuttaa myös kertakirjautuminen (SSO-työpöytäintegraatio). Alueellisella tasolla tarvitaan myös alueellista, hakemistopohjaista käyttöoikeuksien hallintaa (LDAP). (Iivari, Ruotsalainen, 2007, 17.)

4 KÄYTTÖOIKEUDET

4.1 Käyttöoikeus- ja valtuushallinta

Käyttöoikeus- ja valtuushallinta käsittää järjestelmien käyttöoikeusperiaatteiden määrittelyn. Siinä otetaan huomioon tietojärjestelmien käytölle tarvittavat käyttäjäkohtaiset rajoitukset. Käyttöoikeudet ja -valtuudet myönnetään kunkin tietojärjestelmän osalta erikseen peruskäyttäjille ja pääkäyttäjille. Oikeuksista ja valtuuksista tulee pitää rekisteriä. Oikeuksien ja valtuuksien muuttamis- ja poistamismenettelyt tulee ohjeistaa. (STM 2007, 33-34). Käyttövaltuuksien määrittely tarkoittaa käyttöoikeuksien kytkemistä käyttäjien työrooleihin. Palvelujärjestelmien käyttöoikeudet tai osa niistä saattaa olla koottu joukoksi järjestelmän rooleja, joihin työroolit kytketään siten, että halutut käyttövaltuudet syntyvät. Jos rooleja ei ole määritelty järjestelmään, niin työrooleihin kytketään asianmukaiset yksittäiset käyttöoikeudet. (VM, 2006, 20).

Käyttöoikeudet ovat yksi tietoturvan tärkeimpiä yksittäisiä osa-alueita. Käyttöoikeudet määräävät, kuinka tietty käyttäjä voi käyttää määrättyä resurssia (tiedosto, hakemisto, tulostin tms.), eli mitä lupia käyttäjällä on tähän rerurssiin. Luvat, joita käyttäjälle voidaan antaa, riippuvat resurssin tyypistä. Resurssin jokainen lupa

voidaan joko sallia käyttäjälle, kieltää käyttäjältä, tai jättää määrittämättä. Käyttäjällä on resurssiin kaikki ne luvat, jotka hänelle on jossain yhteydessä myönnetty, ja joita ei missään yhteydessä ole kielletty. Jos lupa kielletään käyttäjältä jossain yhteydessä, käyttäjä ei saa tätä lupaa, vaikka se olisikin hänelle jossain toisessa yhteydessä myönnetty. (Ruohonen, 2002, 157)

4.2 Käyttöoikeuksien hallinnan periaatteet

Suositeltavia periaatteita käyttöoikeuksien määräämisessä ovat Ruohosen (2002, 165) mukaan samat periaatteet kuin palomuurin sääntöjen määräämisessä. Käytettäviä periaatteitava ovat:

- Sääntöjä tulee olla mahdollisimman vähän.
- Sääntöjä tulee rajoittaa resurssien käyttöä mahdollisimman paljon.
- Säännöt eivät saa estää käyttäjien normaalia työskentelyä.

Käyttäjille tulee antaa vain ne luvat, joita he tarvitsevat. Käyttäjäryhmät kannattaa perustaa käyttäjien työtehtävien ja/tai sijaintien mukaan. Käyttäjätunnukset kannattaa ja-kaa käyttäjäryhmiin siten, että käyttöoikeukisen antaminen halutuille käyttäjille on mahdollisimman helppoa ja joustavaa. (Ruohonen, 2002, 166). Hallintajärjestelmässä, jossa käyttövaltuudet ovat työroolikohtaisia, työroolin omistajan tehtävänä on hankkia työroolille sen edellyttämät käyttövaltuudet sopimalla asiasta ao. kohteen omistajien kanssa. Pääperiaatteena työroolin käyttövaltuuksien määrittelyssä tulee pitää todellista tarvetta, ts. rooliin ei tule kiinnittää kaiken varalta laajempia valtuuksia kuin mitä rooli käytännössä edellyttää. Tilapäiset laajemmat tietotarpeet tai muut käsittelyvaltuudet tulee hoitaa käyttäjälle esimerkiksi määräajaksi aktivoitavalla työroolilla, johon on liitetty tarvittavat valtuudet. (VM, 2006, 20).

Arkaluonteiseen tietoon voidaan myöntää myös yksityiskohtaisempia valtuuksia, esimerkiksi potilastietoihin pääsy vain hoitoprosessissa mukana oleville henkilöille. Tällaisia valtuuksia määritettäessä on kuitenkin kiinnitettävä erityinen huomio

siihen, että tietoihin pääsyä ei estetä liikaa. Usein pelkkä valvonta saattaa tuottaa riittävät keinot torjumaan tietoihin kohdistuvat uhkat. Tämä myös takaa, että kiireellisessä tilanteessa välttämättömät toimenpiteet voidaan suorittaa viiveettä, kun tietoihin on pääsy, eikä yksittäisiä käyttöoikeuksia tarvitse erikseen myöntää tai olemassa olevia käyttövaltuuksia määritellä ylitettäväksi. (Tammisalo, 2005, 75)

Organisaatioiden on suunniteltava, kenellä on valtuudet myöntää käyttäjille oikeuksia tietojärjestelmiin ja miten oikeuksia hallinnoidaan. Käyttöoikeuksien myöntäminen on oltava ennalta tarkkaan määritelty prosessi, jossa on päätetty menetelmät, miten käyttäjälle myönnetään hänelle kuuluvat oikeudet. Verkkopalveluiden ja kriittisten järjestelmien käytöstä on oltava oma politiikka, jossa määritellään käyttäjille ja käyttäjäryhmille pääsy ainoastaan niihin resursseihin joihin on tarve. Organisaatioiden on huolehdittava, että myönnettyjä käyttövaltuuksia arvioidaan ja päivitetään säännöllisesti ennalta määritellyn prosessin mukaan. Tarvittaessa organisaation jokaiselle tietojärjestelmälle on määriteltävä oma pääsynhallintapolitiikka riippuen järjestelmän tietoturvatasosta. (Tammisalo, 2005, 72-73)

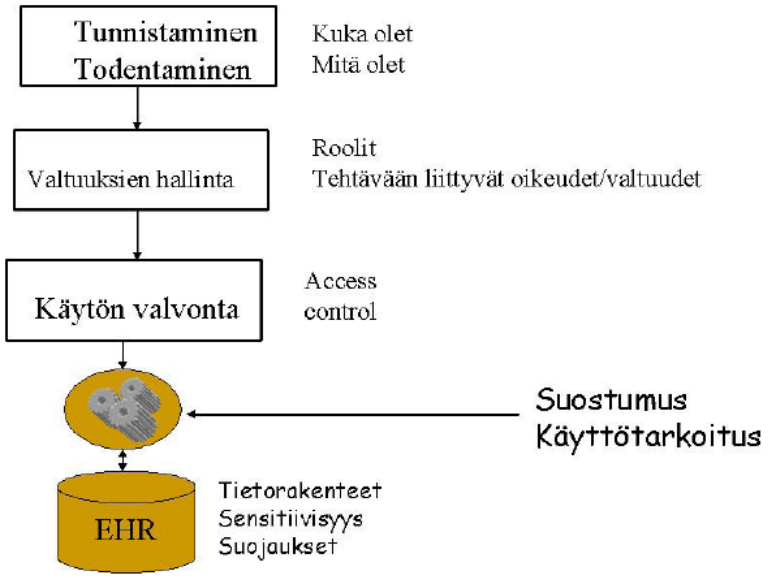
Käyttöoikeuksien hallintaperiaatteeseen kuuluu, että henkilöille ja järjestelmässä oleville olioille annetaan vain sellaiset oikeudet, jotka tehtävien suorittamisessa tarvitaan. Paavilaisen (1998, 217) mukaan käyttöoikeuksia voidaan antaa monella eri tavalla. Yleensä oikeudet määräytyvät käyttöoikeustaulukon avulla, jossa määritellään roolit ja niiden saamat luku-, kirjoitus- ja muutos- ja muut mahdolliset oikeudet.

4.3 Terveydenhuollon käyttöoikeudet

Käyttäjän hallinnan ja käyttöoikeuksien periaatemalli on esitetty kuviossa 6, jolla Ruotsalainen (2006, 53-54) kuvaa, terveydenhuollon tietoja käsittelevän tietojärjestelmän. Sillä tulee olla käytössä järjestelmät, jotka tuottavat:

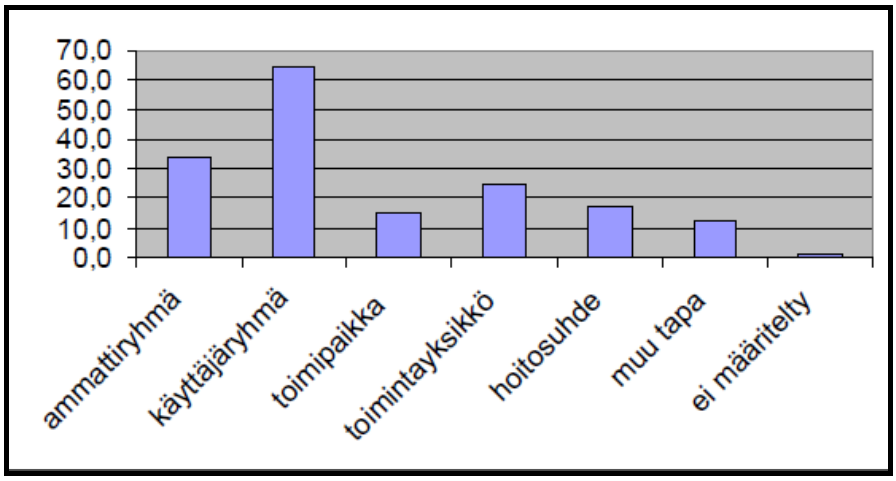
- käyttäjien hallinnan ja tunnistamisen palvelut
- käyttöoikeuksien hallinnan tietojärjestelmäpalvelut

- tietojen käytön hallinnan tietojärjestelmäpalvelut (access controll services).



KUVIO 6. Käyttäjän hallinnan ja käyttöoikeuksien periaatemalli (Ruotsalainen, 2006)

Terveydenhuollon tietojärjestelmien käyttöympäristössä käyttöoikeudet määritellään kuvion 7 mukaan yleisimmin käyttäjäryhmittäin (65 %), ammattiryhmittäin (34 %) ja asiakas-hoitosuhteen mukaan (17 %). Käyttöoikeuksia voidaan määritellä myös toimipaikoittain, toimintayksiköittäin tai muulla tavoin. Organisaation koolla ei ollut merkitystä kuin käyttöoikeuksien määrittelyssä toimintayksiköiden perusteella. Suurissa organisaatioissa käyttöoikeuksia jaettiin pieniä enemmän toimintayksiköiden perusteella, koska niissä on enemmän erillisiä toimintayksiköitä kuin pienissä. Käyttöoikeuksien valvonta tapahtuu lokikirjanpidon avulla. Tässä vuonna 2002 tehdyssä kyselyssä vastauksena käyttöoikeksien valvonnasta tuli, että potilastietojen käytön valvonta oli laiminlyöty peräti 17 %:lla vastaajista. Tämä on selkeä epäkohta, joka tulisi korjata, sillä lokikirjanpito on lakisääteinen tehtävä, josta tulee pystyä raportoimaan rikkomusepäilyissä. (Hartikainen, Kuusisto-Niemi, Lehtonen, 1/2002, 57)



KUVIO 7. Käyttöoikeuksien jakoperusteet (Hartikainen & muut 1/2002)

Terveydenhuollon asiakkaiden tietojen käyttötarkoitus on potilaan tutkimusten ja hoidon järjestäminen, toteuttaminen ja seuranta. Potilastietojen käsittelyyn tarkoitettua tietojärjestelmää suunniteltaessa ja toteutettaessa on huomioitava tietosuojavaatimukset ja potilaan sekä henkilökunnan oikeusturvan toteutuminen. Käyttöjärjestelmätasolla oikeudet tulee määritellä hyvin tarkkaan. Jotta jokaiselle käyttäjälle ei tarvitsisi määritellä oikeuksia yksi kerrallaan, oikeudet on niputettu ryhmiin. Windowsissa Administrators-ryhmällä on kaikki oikeudet tietokoneeseen, kun taas Users-ryhmällä on vain ohjelmien käytössä tarvittavat perusoikeudet. Kun käyttäjä sijoitetaan ryhmän jäseneksi, hän saa ryhmään liittyvät oikeudet. Henkilö voi kuulua useaan ryhmään yhtäaikaisesti. (Järvinen, 2006, 195-196)

4.4 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 keskeisempiä. (Ruotsalainen, 2006, 57).

4.4.1.1 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 käyttöoikeuksien kunkin toimintayksikön henkilökunnalle niiden omiin tietojärjestelmiin. Tietosuojan ja tietoturvan näkökulmasta muun kuin oman toimintayksikön työntekijän suorittama tietojen katseleminen teknisellä yhteydellä merkitsee tietojen luo-vuttamista toimintayksikön ulkopuolisille henkilöille tai prosesseille nostaakin esille useita tietoturvan ja tietosuo-jan hallintaan liittyviä ongelmia. Koska tietoja luovuttavalla toimintayksiköllä on aina vastuu siitä, että tietojen luovutuksen edellytykset ovat olemassa, ei edellä kuvatun kaltainen salasanojen ja käyttäjätunnustenantaminen toimintayksikön henkilökunnan ulkopuolisille käyttäjille ole tietosuojan ja tietoturvan näkökulmasta suositeltava menetelmä. (Ruotsalainen, 2006, 57-58).

4.4.2 Dokumenttimalli (Document Model)

Mallin lähtökonta on se, että prosessit, roolit, käyttöoikeudet jne. ensin dokumentoidaan ja sitten varmennetaan. Varmentaminen tapahtuu siten, että auditoinnin jälkeen kummatkin osapuolet allekirjottavat 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.

4.4.3 Politiikkamalli (Policy Model)

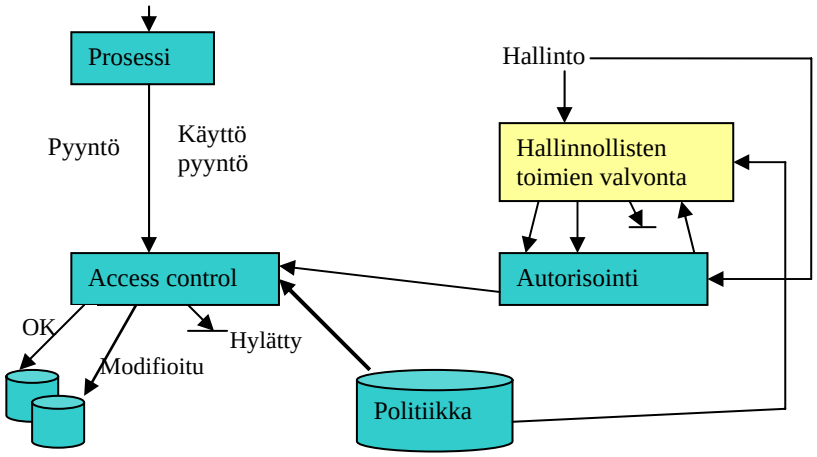
Tietoturvapolitiikka on monimutkainen lakiperustainen, eettinen, sosiaalinen, organisatorinen, psykologinen, toiminnallinen ja tekninen keino synnyttää luottamus tietojärjestelmissä. Tietoturvapolitiikka kuvaa mm. lakiympäristön säännöt ja säädökset, toiminnallisen ympäristön, tavoitteet ja periaatteet. 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 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

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

Käyttöoikeuksien hallinnan malllin eli PMAC-mallin periaate on esitetty kuviossa 8. Jos PMAC-mallia käytetään uasean organisaation käyttöoikeuksien hallintaan, tarvitaan hakemisto, joka sisältää kaikki ne henkilöt, joille on annettu rooleja. Lisäksi tarvitaan säännöt, jotka koskevat koskien politiikan hyväksymiä henkilöitä. (Ruotsalainen, 2006, 60-61).



KUVIO 8. PMAC-malli (Ruotsalainen, 2006)

4.4.4 Delegointimalli (Delegation Model)

Delegointimallilla tarkoitetaan menetelmää, jossa toimintayksikön määrittelemiä käyttöoikeuksia delegoidaan sähköisesti edelleen uusille organisaatioille/käyttäjille. On myös mahdollista, että käyttöoikeuksien vastaanottaja delegoi saamiaan käyttöoikeuksia seuraaville organisaatioille/käyttäjille, mikä johtaa käyttöoikeuksien delegoinnin ketjuttamiseen. Tässä mallissa jokainen uusi käyttöoikeuksien saaja toimii käyttöoikeuksien omistajan puolesta. Mallissa tarvitaan seuraavat toimijat:
(Ruotsalainen, 2006, 58).

- käyttöoikeuksien haltija
- käyttöoikeuksien tarkistaja
- valtuuksien antaja
- luotettu kolmas osapuoli (ns. attribute authority, AA), joka toimii oikeuksien lähteenä. (Ruotsalainen, 2006, 58).

Yleisesti käytetty käyttöoikeuksien jakamisen malli perustuu roolipohjaiseen käytön hallintaan (ns. RBAC-arkkitehtuuri). Roolipohjainen pääsynvalvonta on tun-

nustettu pääsynvalvontamalli, jossa tietojärjestelmien käyttöoikeudet kytkeytyvät organisaation funktionaalisiin rooleihin käyttäjien sijaan. Työntekijöille määritellään roolit heidän tehtäviensä mukaisesti, jolloin työntekijät saavat tehtäviensä mukaiset käyttöoikeudet tietojärjestelmiin. Tarvittavien yhteyksien määrä vähenee, josta seuraa roolipohjaisen pääsynvalvonnan hallinnollinen tehokkuus ja alhaisemmat hallinnointikustannukset. (Ruotsalainen, 2006, 58).

4.5 Usean toimintayksikön yhteisen käyttäjän ja käyttöoikeuksien hallinnan toteuttamistapoja

Usean toimintayksikön yhteisn käyttäjän ja käyttöoikeuksien hallinnan toteuttaminen kuvataan seuraavassa yksityiskohtaisemmin kolmea erilaista menetelmää. (Ruotsalainen, 2006, 63).

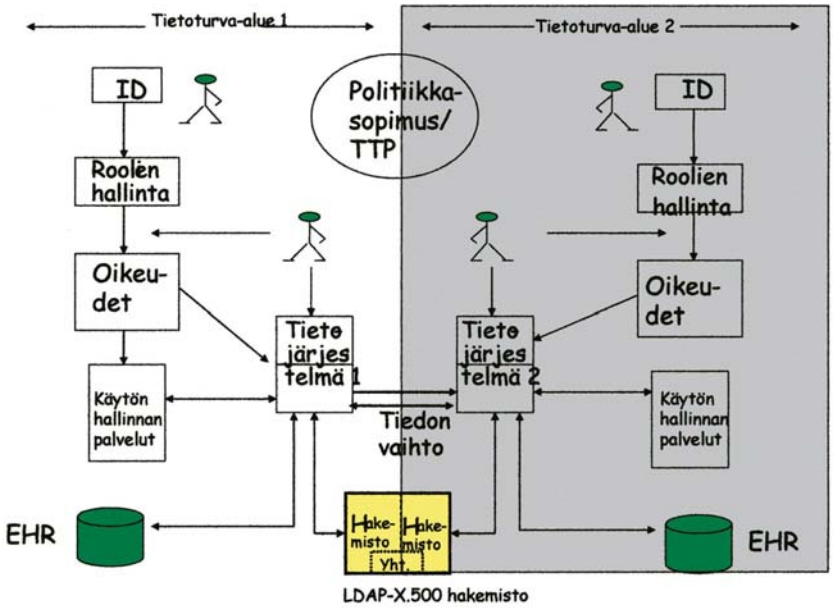
1. Yhteiseen/jaettuun LDAP-hakemiston käyttöön perustuva ratkaisu
2. PMI-arkkitehtuuriin perustuva ratkaisu
3. Identiteetin hallinnan järjestelmän käyttöön perustuva ratkaisu.

4.5.1 Jaettuun LDAP-hakemistoon perustuva malli

Usean eri toimintayksikön käyttöoikeuksia on mahdollista hallinnoida yhteisen/jaetun käyttäjähakemiston avulla. Tämä yhteinen tiedonlähde sisältää tietoa käyttöoikeuksista, niiden poistamisesta, rooleista ja muuta yksityiskohtaista käytön hallinnan ohjaustietoa. Hakemiston avulla voidaan myös toteuttaa ns. Single Sign On-ratkaisu (SSO). Tällainen hakemisto kykenee tarvittaessa toimimaan yhdessä PKI-järjestelmän kanssa. (Ruotsalainen, 2006, 64).

Kuviossa 10 esitetään jaettuun LDAP-hakemistoon perustuvan mallin periaate. Toimintayksiköllä tulee olla samantasoinen tietoturvapolitiikka ja sen lisäksi niilla

on joko kokonaan yhteinen tai osaksi jaettu LDAP-hakemisto, jonka avulla käyttöoikeuksia voidaan hallita ja välittää käyttöoikeustietoa hakemiston piirissä oleville. (Ruotsalainen, 2006, 64).



KUVIO 10. Käyttöoikeuksien hallinta LDAP-hakemiston avulla (Ruotsalainen, 2006)

ITU-T X.500 standardi määrittelee edellä mainitun 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. (Ruotsalainen, 2006, 64).

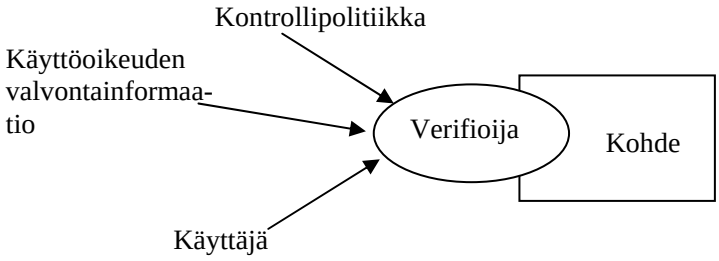
Yksi terveydenhuollon erityispiirteistä on se, että sama ammattihenkilö voi toimia usean eri organisaation puolesta siten, että hänellä on kussakin organisaatiossa erilaiset työtehtävät. Terveydenhuollon ammattihenkilöillä voi olla samassakin organisaatiossa useita eri rooleja. Vastaavasti terveydenhuollon asiakkaat voivat olla samanaikaisesti usean eri organisaation potilaina. Terveydenhuollon ammattihenkilöt voivat myös olla asiakkaita, ja siksi heidän asiakasidentiteettinsä ja ammatti-identiteettinsä pitää voida pitää erillään toisistaan. ISO TC215 standardiluonnos on ottanut nämä piirteet huomioon. Tämän standardiluonnoksen laatimi-

sen laajennusten avulla terveydenhuollon tunnisteet ja roolit sekä varmenneorganisaatioita, rekisteröintiorganisaatioita ja attribuuttisertifikaatteja hallinnoivaa organisaatiota kuvaavat tiedot voidaan julkaista laajennetussa LDAP-hakemistossa. Tämän standardiehdotuksen avulla voidaan ITU-T X.500 hakemistoa käyttää terveydenhuollossa useiden organisaatioiden käyttöoikeuksien hallinnnan toteuttamiseen. (Ruotsalainen, 2006, 64).

4.5.2 PMI-malli (Privilege Management Infrastructure Model)

PMI-arkkitehtuurin lähtökohtana on se, että pelkkä identiteetti ei 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 X509 standardiin perustuen terveydenhuollon tarpeisiinsoveltuvan PKI-arkkitehtuurin vaatimukset. Tiiviistettynä voidaan sanoa, että PMI-arkkitehtuuri hallinnoi käyttöoikeuksia ja tarjoaa yhdessä PKI-palvelujen kanssa kattavat käyttöoikeuksien hallintapalvelut. (Ruotsalainen, 2006, 65).

Sekä PKI-arkkitehtuurin että PMI-arkkitehtuurin PMI-arkkitehtuurin peruskonseptit ovat samanlaiset, mutta PKI-arkkitehtuurin keskittyessä todentamiseen on PMI-arkkitehtuurin kohteena käyttöoikeudet. PMI-arkkitehtuuri käyttää kuviossa kuvattua valvonta-mallia. PMI-arkkitehtuuri koostuu alla olevassa kuvassa esitetyistä viidestä komponentista. Käyttöoikeuksien liittämisellä käyttäjään varmistetaan, että hän noudattaa valtuuksien lähteen määrittelemää tietoturvapolitiikkaa.



KUVIO 11. 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 delegointia alla olevan kuvion 12 mukaisesti. (Ruotsalainen, 2006, 66).

4.5.3 Identiteetin hallintamenetelmä (Identity Management Method, IM)

IM-menetelmän keskeinen palvelu on identiteetin siirtäminen, mutta myös käyttäjien todentaminen Ja valtuuksien antaminen voidaan liittää mukaan tarjottaviin palveluihin. Menetelmällä pyritään hallinnoimaan samalla kertaa sitä, kenelle tiedon käyttö on sallittua ja 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). IM-järjestelmässä käyttöoikeudet voidaan julkaista myös LDAP-hakemiston kautta. Vaihtoehtoinen toteutustapa käyttöoikeuksien hallintaan on käyttää ns. Virtual Directory palvelua. Tällöin identiteetin jakamispyyntö voi tulla joko LDAP-hakemistosta tai esimerkiksi Web-palvelusta. IM-toteutus voi perustua federaatio-palvelimen (Federation Server) käyttöön.

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

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

5 PÄÄSYN HALLINTA

5.1 Pääsyn hallinta

Pääsyn hallinnan kokonaisuuteen kuuluvat pääsyn hallinnointi, käyttäjien hallinta ja käyttäjien tunnistaminen ja todentaminen. Tammisalo (2005, 71) näkee, että terveydenhuollossa pääsyn hallinnassa kuuluu määrittää millaisia politiikkoja, sääntöjä ja käytäntöjä hallinnointiin on käytettävissä ja käytettävä. Pääsyn hallinnointi käsittää esimerkiksi oikeuksien määrittelyn eli millaisia pääsyoikeuksia tietoihin luodaan ja millaisia oikeuksia voidaan valtuuttaa erityyppisille käyttäjille ja käyttäjäryhmille. Tehokkaalla ja hyvin määritellyllä pääsyn hallinnalla sekä asianmukaisella käyttäjien ja heille myönnettävien valtuuksien hallinnoinnilla voidaan tehokkaasti ehkäistä niitä uhkia, joita syntyy valtuudettomasta tietoihin pääsystä. Sellaisten henkilöiden, jotka eivät ole niihin valtuutettuja, päästessä käsiksi tietoihin ja tietojärjestelmiin, voi tietojen luottamuksellisuuden menetyksen lisäksi aiheutua vakavia uhkia myös tietojen olemassaololle ja oikeellisuudelle. Pääsyn hallintaan liittyvät määrittelyt ja toimenpiteet ovat yksi tietoturvallisuuden oleellisimmista osa-alueista. Näissä määrittelyissä todetaan, kuinka tietojärjestelmien ja niissä olevien tietojen käyttö ja käyttäjät määritellään, kuinka käyttöoikeuksia ja käyttövaltuuksia hallitaan ja millaisilla menetelmillä käyttäjät tunnistetaan ja heidän henkilöllisyytensä todennetaan. (Tammisalo, 2005, 71)

Pääsynhallinta perustuu ja noudattaa organisaation tietoturvapolitiikkaa. Pääsyn hallinnalla kontrolloidaan käyttäjien oikeuksia tiedonkäsittelyyn ja ohjelmistojen käyttöön sekä mahdollistetaan ylläpitäjille keinot seurata ja valvoa tietojärjestelmien käyttöä. Terveydenhuollon organisaatioissa on useita eri sovelluksia ja käyttäjiä. Tämän vuoksi organisaation tulee määritellä tarkat politiikat, säännöt ja käytännöt millaisia pääsyoikeuksia tietoihin luodaan sekä millaisia oikeuksia (esimerkiksi luku, kirjoitus, muutos, poisto, suoritus ja hallintaoikeus) voidaan valtuuttaa eri käyttäjille ja käyttäjäryhmille. Lisäksi organisaation on määriteltävä, millä menetelmillä käyttäjät tunnistetaan, millaisia yhteyksiä tietojärjestelmiin sallitaan ja miten tietojärjestelmien käyttöä seurataan. Käytettävien pääsynhallin-

tamenetelmien on oltava riittävän vahvoja ja turvallisia, jotta voidaan varmistaa tietojärjestelmien turvatasojen täyttyminen. (Tammisalo, 2005, 71-72)

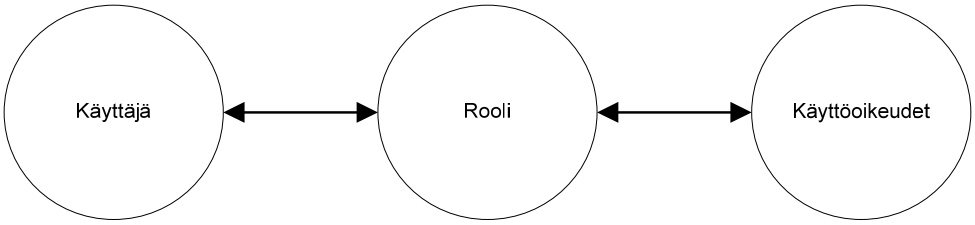
Pääsyn hallinnoinin menetelmät on hyvä määritellä Tammisalon (2005, 72) mukaan tarkoin etukäteen, sillä niiden vahvuuden ja turvallisuuden on vastattava tietojärjestelmien ja tietojen turvatasoa. Tarvittaessa jokaiseen tietojärjestelmään on määriteltävä erillinen politiikka, jossa määritellään käyttäjien tunnistamisen menetelmät, millaisia tunnisteita käytetään, millaisia yhteyksiä tietojärjestelmiin on käytössä ja miten tietojärjestelmien käyttöä tarkkaillaan. Kaikista laadittujen politiikkojen ja ohjeiden mainitsemista menetelmistä ja teknisistä yksityiskohdista ilmenee tarkkaan, onko kyseessä pakollinen ominaisuus, suositus tai hyväksyttävä (mutta ei suositeltava) vaihtoehto.

Tammisalo (2005, 73) näkee tärkeänä, että verkkopalveluiden ja -yhteyksien käytöstä määritellään myös oma politiikkansa. Tällöin organisaation käyttäjät pääsevät vain niihin verkkoihin ja verkkoyhteyksiin, joihin heille on nimenomaisesti myönnetty pääsy. Tarvittaessa arkaluonteisiin tietoihin pääsystä verkkoyhteyksien takaa määritellään yksityiskohtaiset säännöt ja ohjeet. Tietojärjestelmien käyttäjät voidaan jakaa tarvittaviin ja sopiviin käyttäjäryhmiin, joille määritellään yhdenmukaiset valtuudet tietoihin. Tällä voidaan sekä vähentää inhimillisiä virheitä esimerkiksi valtuuksien määrittelyssä ja käytön seurannassa että helpottaa käytännön hallinnointityötä. Jos käyttövaltuuksia myönnetään organisaation ulkopuolisille henkilöille (muiden organisaatioiden työntekijät, asiakkaat ja potilaat), noudatetaan eri-tyistä varovaisuutta ja riittäviä tarkastus- ja valvontamenettelyitä

5.2 Roolit ja pääsynvalvonta

Käyttäjän henkilöllisyyden todentamisen jälkeen käynnistyy pääsynvalvonta, joka rajoittaa tietojärjestelmän laillisen käyttäjän toimintoja tai operaatioita. Pääsynvalvonta voi perustua esimerkiksi rooleihin. Rooli on tiettyyn työtehtävään liittyvä tehtävien ja vastuiden joukko. Jokaiseen rooliin liittyy tietyt käyttöoikeudet. Käyttäjät luokitellaan rooleihin ja he pääsevät vain rooliensa oikeuttamiin tietoihin. Rooleihin perustuva pääsynvalvonta on esitetty yksinkertaistettuna kuviossa

9. Käyttöoikeuksia määriteltäessä käytetään hyväksi tunnistamista ja todentamista. Henkilöt, jotka osallistuvat potilaiden hoitoon, saavat käsitellä potilasasiakirjoja vain työtehtäviensä edellyttämässä laajuudessa. Hoitohenkilökunnan sekä muiden henkilöiden, joilla on pääsy potilasasiakirjoihin, käyttöoikeudet potilasasiakirjoihin sisältyviin tietoihin tulee olla yksityiskohtaisesti määritelty. (Porali., Ensio, 2005, 5).



KUVIO 9. Rooleihin perustuva pääsynvalvonta, mukailtu (Porali, Ensio, 2005)

Tietyllä käyttäjällä voi olla yksi tai useampi rooli ja tietty rooli voi olla yhdellä tai useammalla käyttäjällä. Porali ja Ensio (2005, 5) toteavat, että käyttöoikeudet ovat rooliin liitettyjä oikeuksia. Terveydenhuollossa roolien käyttäminen käyttöoikeuksien määrittelyssä on luontevaa, koska erilaisia työtehtäviä on paljon ja samalla henkilöllä voi olla useita työtehtäviä. Rooliin saadaan niputettua useita tehtäviä. Roolipohjaisen käyttöoikeuksien määrittelyn avulla voidaan myös varmistaa, ettei esimerkiksi osastolla A töissä oleva hoitaja pääse katsomaan osastolla B hoidettavana olevan potilaan tietoja.

5.3 Roolit terveydenhuollossa

Stakes näkisi, että RBAC-arkkitehtuuri (RBAC, Role Based Access Control, rooliperustainen pääsynvalvonta) olisi terveydenhuoltoon sopiva menetelmä. Sosiaali- ja terveydenhuollon henkilötietojen käsittelyn näkökulmasta tarkasteltuna, ei ole suositeltava menettely luoda käyttöoikeuksia "potentiaalisille" käyttäjille. Stakes kyseenalaistaa myös, täyttääkö tällainen menettely henkilötietolain asiayhteysvaatimuksen. Stakesin näkemyksen mukaan käyttöoikeuksia ei tule luoda

potentiaalisille käyttäjille varmuuden vuoksi eikä pelkän koulutukseen tai virka-asemaan perustuvan roolin perusteella automaattisesti. Tämä on erityisen tärkeää tapauksissa, joissa tietojärjestelmä ei kykene varmistamaan organisaation ulkopuolisen henkilön asiayhteyttä tai muuta laista johtuvaa perustetta organisaation hallinnoimien tietojen käyttämiseen tai luovuttamiseen. (Stakes 2008)

Rooleille on tyypillistä se, että samalla henkilöllä ei pitäisi samalla hetkellä olla useita rooleja. Toisaalta jotkin roolit voivat olla sellaisia, että niissä ei voi samalla hetkellä olla useita henkilöitä. Alla mainitussa luettelossa on seikkoja, joita rooleilla voidaan saavuttaa:

- Roolin mukaan personoitu käyttöliittymä.
- Satunnaisten virheiden vaikutus saadaan pienemmäksi, kun voimakkaammissa rooleissa ollaan vain vähän aikaa.
- Vastaavasti mahdollisesti turvattoman koodin aiheuttamat ongelmat saadaan rajatuksi, kun sellaista ajetaan vain oikeuksiltaan rajatussa roolissa.
- Monimutkaisia politiikkoja. (Stakes, 2008)

Stakesin näkemyksen mukaan identiteetti on niiden ominaisuuksien joukko, joiden perusteella käyttäjä, entiteetti tai prosessi voidaan tunnistaa. Tunnistaminen tulee pitää erillään todentamisesta, käyttöoikeuksien hallinannasta ja tietojen käytön hallinnasta. Stakesin näkemyksen mukaan terveydenhuollon asiakastietojen käytön hallinta (access control) tulisi toteuttaa sääntöpohjaisesti. Terveydenhuollon tietojärjestelmissä roolien (ns. structural role and fuctional role) hallinnan tulisi Stakes näkemyksen mukaan perustua ASTM E31.20 ja ISO 22600 standardeihin. (Stakes, 2008)

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) säätää, että kaikista järjestelmien ja käyttäjien tekemistä toimista on jäätävä sellainen tieto järjestelmään, että myöhemmin voidaan todeta mitä ja milloin on tehty ja kenen toimesta. Tammisalo näkee, että organisaation tulee rakentaa selkeät kontrollit, joilla pystytään seuraamaan lokitietojen avulla tietojärjestelmien ja käyttäjien toimintaa. Kontrollit tukevat tietoturvasta vastaavien henki-

löiden toimintaa ja ylläpitävät prosessien käyttämien tietojen turvallisuutta (Finlex 2007).

5.4 Rooliperustainen pääsynhallinta

5.4.1 Rooliperustainen pääsynhallinta

Tietojärjestelmien käyttöoikeuksista puhuttaessa rooleilla tarkoitetaan organisaatiossa määriteltyä työnkuvaa, jossa määritellään roolin mukaisissa tehtävissä toimivan henkilön käyttöoikeudet ja ja velvollisuudet. On kuitenkin huomattava, että henkilön kompetenssi eroaa näistä. Se. mitä henkilö pystyisi tekemään, on eri asia kuin mitä henkilön on hyväksyttävää tehdä tai mitä hänen odotetaan tekevän. Tämä on eräs syy siihen, miksi pääsynhallintaa tarvitaan. (Sandhu, Coyne, Feinstein ja Youman, 2006, 38-47).

5.4.2 Rooliperustainen pääsynhallintamalli, perustaso $RBAC_0$

Rooliperusteinen (Role-based Access Control) perustaso koostuu neljästä perusryhmästä, jotka järjestelmän tulee toteuttaa mahdollistaakseen rooliperustaisen pääsynhallinnan perustason. Nämä perusryhmät ovat: käyttäjät, roolit, oikeudet ja istunnot. (Sandhu ja muut 2006, 38-47).

Oikeudella tarkoitetaan pääsyoikeutta yhteen tai useampaan tiettyy obejktiin järjestelmässä. Ne ovat luonteeltaan positiivisia, eli ne tuovat jonkin oikeudet lisää järjestelmässä, mutta eivät lisää rajoitteita. Yhteen rooliin voi liittyä useita oikeuksia ja yksittäinen oikeus voi liittyä useaan rooliin. Oikeuksien ja roolien sitomisesta käytetään termiä oikeuttaminen. (Sandhu ja muut 2006, 38-47).

Istunto kuvaa ne käyttäjän roolit, jotka ovat kyseisellä ajanjaksolla aktiivisina. Jokainen istunto sitoo yhden käyttäjän yhteen tai useampaan aktiiviseen rooliin.

Tästä käytetään termiä roolittaminen. Aktiivisena olevat roolit voivat muuttua kesken istunnon. (Sandhu ja muut 2006, 38-47).

5.4.3 Rooliperustainen pääsynhallintamalli, hierarkiset roolit $RBAC_1$

Perustasolla roolit ovat toisistaan riippumattomia. Jokaiseen rooliin voi kuulua useita käyttäjiä ja jokainen käyttäjä voi kuulua useaan rooliin. $RBAC_1$ laajentaa $RBAC_0$:ia lisäämällä rooleille mahdollisuuden periä toistensa ominaisuudet. Joissakin tapauksiaa kaikkien oikeuksien periytyminen ei ole toivottavaa, vaan periytymistä halutaan rajoittaa. (Sandhu ja muut 2006, 38-47).

5.4.4 Rooliperustainen pääsynhallintamalli, rajoitemalli $RBAC_2$

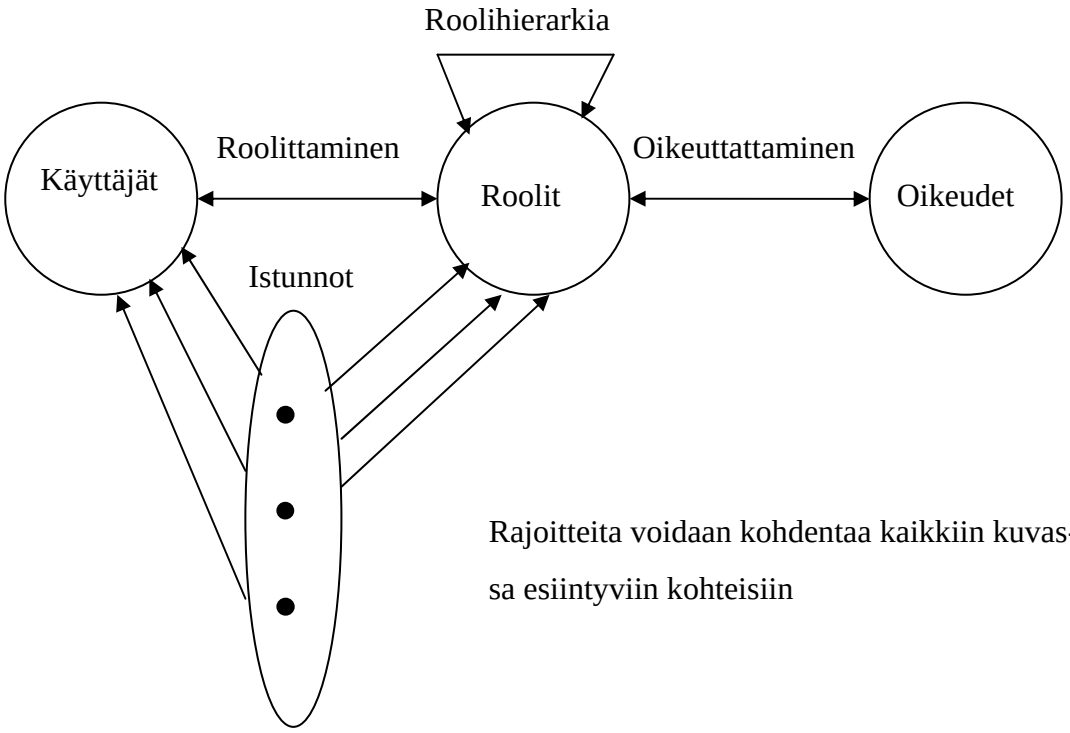
Kohdassa 5.4.2 kerrottiin oikeuksista, jotka ovat luonteeltaan positiivisia, eli oikeuden saaminen kasvattaa aina käyttäjän pääsyoikeuksia. Usein on kuitenkin tarvetta asettaa sääntöjä, jotka rajoittavat oikeuksien saamista. Tällöin on kyse rajoitteista. Tällainen tilanne voi olla yrityksessä, jossa tehdään tilauksia ja tehdyt tilaukset tarkastetaan. Tällöin on luonnollista, ettei sama henkilö voi toimia sekä tilaajana että hyväksyjänä. Tällaisesta vastuista rajaavasta rajoitteesta käytetään englanniksi nimitystä separation of duties, johon viitataan usein pääsynhallintaa koskevassa kirjallisuudessa. Käyttöoikeuksista huolehtivan järjestelmän täytyykin tarkistaa, ettei käyttäjän roolittamisessa myönnetä käyttäjälle kiellettyjä rooliyhdistelmiä. Tällaisia rajoitteita voidaan tehdä mm. luomalla roolijoukkoja, joista ainoastaan yksi rooli voi olla kerrallaan roolitettuna käyttäjälle. Roolittamista voidaan rajoittaa myös muillakin säännöillä. Kardinaliteettisäännöllä voidaan asettaa lukumäärärajoitteita siihen, kuinka monta käyttäjää voi enintään olla roolitettuna samaan rooliin samanaikaisesti. Rooleille voidaan asettaa myös edellytysvaatimuksia, niin että käyttäjän on täytettävä tietyt ehdot, jotta hänet voidaan roolittaa tiettyyn rooliin. (Sandhu ja muut 2006, 38-47).

Rajoitteet voivat kohdentua myös roolihierarkiaan, jolloin tiettyjen oikeuksien peritytyminen roolilta toiselle on kiellettyä. Myös istunnoille voidaan asettaa ra-

joitteita muun muassa siten, että käyttäjä saa olla liitettynä useampaan tiettyyn rooliin, mutta yhden istunnon aikana aktiivisina saa olla ainoastaan tietyt roolit. Organisaation tulee määritellä käytettävät rajoitteet ja niitä tulee soveltaa roolien määrittelyssä. (Sandhu ja muut 2006, 38-47).

5.4.5 Rooliperustainen pääsynhallintamalli, Yhdistetty malli $RBAC_3$

Yhdistetty malli kerää edellä esitetyt pääsynhallintamallit ($RBAC_1$, $RBAC_2$ ja $RBAC_3$) yhteen. Tämä kokonaisuus on esitettynä kuviossa 10, joka on tehty Sandhun ja muiden (1996) artikkelissa esitety kuvan pohjalta.



KUVIO 10. RBAC-malli

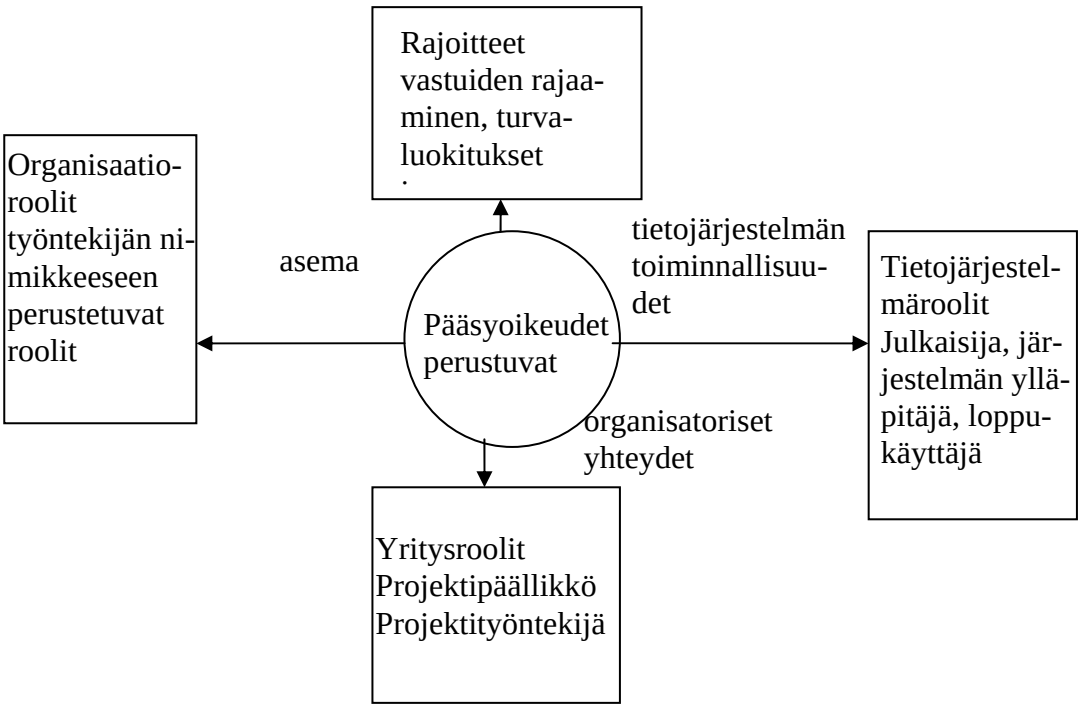
Nykyaikaisten pääsynhallintajärjestelmien tulisi täyttää vähintään edellä kuvattujen pääsynhallintamallien vaatimukset. RBAC on saanut vuoden 1996 jälkeen useampienkin kirjoittajien laajennuksia. Pääsynhallintajärjestelmää suunniteltaessa tai kehitettäessa kannattaa tutustua myös muihin RBAC-mallin laajennuksiin. RBAC-malli on myös Stakesin suosittelema malli terveydenhuollon käyttöoikeuksien hallintaan.

5.5 Komposiittimalli

Laajoissa tietojärjestelmissä voidaan tarvita satoja tai jopa tuhansia rooleja. Vastaavasti organisaation koon kasvaessa erilaisten tehtävänkuvien ja niiden välisten riippuvuuksien kompleksisuus kasvaa. Näistä syistä roolienhallinta tulee sitä haastavammaksi, mitä laajemmasta organisaatiosta tai tietojärjestelmästä (tai tietojärjestelmäkokonaisuudesta) on kyse. Suurien organisaatioiden roolienhallinnan helpottamiseksi on kehitetty komposiittimalli (Composite RBAC approach). Komposiittimallin perusideana on eriyttää organisatoriset ja tietojärjestelmiin liittyvät roolirakenteet ja tarjota toimiva linkitys näiden välille. (Park, Costello, Neven, Diosomito, 2004,163-172).

5.5.1 Roolien luokittelu komposiittimallissa

Park ja muut ovat esittäneet roolien jaottelun kolmeen eri rooliluokkaan: Organisaatioroolit, Yritysroolit ja Tietojärjestelmäroolit. Kuviossa 11 esitetään tämä luokittelu.



KUVIO 11. Roolien luokittelu (Park ja muut, 2004)

Kuviossa 11 ylimpänä esitetyistä rajoitteista on kerrottu kohdassa 5.4.4. Edellä mainittujen rajoitteiden lisäksi keskeinen rajoite on usein sovellettu vähäisimpien oikeuksien periaate. Tällä tarkoitetaan sitä, että kullekin käyttäjällä myönnetään vain ne käyttöoikeudet, joita hän työssään todella tarvitsee. Park ja muut (2004, 163-172) mainitsevat yhdeksi rajoitteeksi myös tiedon turvaluokituksen. Turvaluokitusta voidaan käyttää joko lainsäädännön valvoitteesta tai organisaation omasta tahdosta. Tällainen luokitus voi jakaa tiedot esim. luottamuksellisiin ja salaisiin tietoihin.

Organisaatioroolit perustuvat henkilön asemaan organisaatiossa. Organisaatiorooleja voivat olla muun muassa Toimitusjohtaja ja Osastopäällikkö. Tällaiset roolit ovat helposti poimittavissa organisaatiokaaviosta. Nykyisin työskentely organisaatiossa on kuitenkin projektiluonteista. Yhteen projektiin voidaan koota työntekijöitä niin organisaation eri yksiköistä kuin myös ulkopuolisista organisaatioista esimerkiksi konsultti. Tällöin projektihenkilöstö muodostaa tavallaan oman virtuaalisen organisaationsa, joka toimii perinteisistä organisaatiorajoista riippumatta. Tätä tarkoitusta varten on mahdollista käyttää yritysrooleja. (Park ja muut 2004, 163-172).

Yritysroolit ovat läheistä sukua organisaatiorooleille, jotka kuvaavat tiettyyn organisaatioyksikköön kuuluvan henkilön asemaa. Tämä yksinkertainen malli ei kuitenkaan yksinään riitä useimpien organisaatioiden tarpeisiin, sillä organisaatioissa tehdään usein organisatioyksiköiden välistä yhteistyötä. Yleinen esimerkki tällaisesta toiminnasta ovat projektit, joihin osallistuu henkilöstöä useasta eri organisaatioyksiköstä. Yritysroolien tärkeys korotuu etenkin silloin, kun projektihenkilöstö on valittu rinnaikaisista yksiköistä. Tällöin hierarkiaan perustuvat organisaatioroolit eivät enää välttämättä päde projektin sisäisessä hierarkiassa ja tarvitaan yritysrooleja. Näistä rooleja voivat olla muun muassa Projektipäällikkö ja Projektihenkilö. (Park ja muut 2004, 163-172).

Edellä on tarkasteltu Parkin ja muiden (2004, 163-172) esittämää roolien jaottelua kolmeen eri rooliluokkaan. Oikeiden roolien löytäminen ja määrittely on haastava tehtävä identiteetinhallintajärjestelmän käyttöönotossa. Mitä suurempi organisaa-

tio on kyseessä, sitä vaikeammaksi roolien määrittely tulee. Suuret ja kompleksiset organisaatiot tarvitsevat työkaluja roolien määrittelyyn ja ylläpitoon, jotta työmäärä pysyisi kohtuullisena. Rooleja voidaan jaotella useampaankin rooliluokkaan ja laajennettuja malleja roolijaottelusta löytyy lisää, mutta rajatakseni opinnäytetyötäni en tutki niitä opinnäytetyössäni enempää. Mahdollinen jatkoselvitys olisi hyödyllistä tehdä, jossa tutkittaisiin tarkemmin roolimalleja ja niiden ratkaisuvaihtoehtoja valitulle toiminta-alueelle..

6 YHTEENVETO

6.1 Pohdinta

Opinnäytetyön aiheeseen käyttöoikeuksien ja käyttäjä hallinnan muutos terveydenhuollossa kuuluvat olennaisena osana identiteetinhallinta ja rooliperustainen pääsynhallinta. Tässä pohdinnassani tulen esittämään oman näkemykseni julkisen terveydenhuollon organisaation käyttöoikeuksien hallinnasta ja käyttäjä hallinnasta. Opinnäytetyössäni olen kuvannut useita eri teoriamalleja vaihtoehdoiksi käyttöoikeuksien hallinnan arkkitehtuuriksi. Vahvasti esiin nousi roolien merkitys käyttöoikeksien hallinnan määrittelyssä. Halutun käyttäjien ja käyttöoikeuksien hallinnan arkkitehtuurin toteuttaminen vaatii tehtäväksi ensin hyvän määrittelytyön. Tärkeässä roolissa tässä määrittelytyössä voin sanoa olevan työprosessien kartoituksen ja mallinnuksen. Käyttöoikeuksia määriteltäessä ei ole käytännöllistä eikä järkevää tarkastella käyttäjiä yksilötasolla, vaan tulee pyrkiä löytämään käyttäjäryhmiä, joiden jäsenillä on samantyyppiset työtehtävät. Näin ollen heillä on samanlaiset tietotarpeet ja toimintavaltuudet eli samanlainen toiminnallinen rooli. Käyttöoikeuksista muodostuu henkilötietolain tarkoittama henkilörekisteri, jonka tietojen käsittelyssä tulee ottaa huomioon henkilötietolain vaatimukset. Käyttäjärekisteriä koskevat siten myös henkilötietolain suojaamis- ja huolellisuusvelvoitteet.

Roolien määrittelemisessä käyttäjähakemistossa on tallennettuna organisaation sähköiset identiteetit ja niihin liittyvät käyttäjätunnukset. Käyttäjähakemistona

voidaan käyttää esimerkiksi Microsoft Active Directorya. Käyttäjähakemisto kuvaa koko organisaation käyttäjäkunnan. Toinen tärkeä hakemisto käyttöoikeuksien hallinnassa on roolihakemisto, joka voidaan toteuttaa monella tavalla esimerkiksi LDAP-hakemistona tai relaatiotietokantana. Organisaation tulee tallentaa kuvaustiedot kaikista pääsynhallintaan käyttämistään rooleista. Pääsynhallinnan kannalta roolihakemiston tulisi toteuttaa seuraavat ominaisuudet:

- Roolihakemistosta tulee löytyä kaikkia organisaation roolit.
- Jokainen rooli on kuvattuna ja dokumentoituna riittävälle tasolle saakka.
- Jokaiselle roolille on tallennettu luokkatieto.
- Roolien kuvaukset, rooleihin liittyvät rajoitteet ja suhteen muihin rooleihin ovat dokumentoituna.

Näiden roolikuvaustietojen avulla roolienhallinta helpottuu, joka tehostaa käyttöoikeuksen ja käyttäjä hallintaa.

Identiteettiin voidaan sitoa myös tiettyjä rooleja esimerkiksi sen mukaan, mihin yksikköön tai millä työnimikkeellä uusi työntekijä on rekrytoitu. Vastaavasti roolien ja tunnuksen voimassaolo voidaan sitoa tällaisiin päättelysääntöihin. Identiteetinhallintajärjestelmiin voidaan liittää päättelysääntöjä, joiden avulla järjestelmä automaattisesti luo sekä sulkee käyttäjätunnuksia. Tällaisien päättelysääntöjen hyödyntäminen vähentää manuaalista ylläpitotyötä. Jotta tällaisten sääntöjen käyttäminen on mahdollista, tulee sääntöjen käsittelemien tietojen olla oikein. Toisin sanoen mikäli HR-järjestelmää käytetään tunnusten luomisessa ja roolittamisessa, täytyy HR-järjestelmästä aina löytyä kaikkien työntekijöiden tiedot oikein tallennettuna. Tämä tarkoittaa käytännössä sitä, että käyttöoikeuksien anomisessa työnkulut toimivat siten, että käyttäjä kirjautuu organisaatio intranetiin ja avaa tätä kautta käyttöoikeuksien hakemista varten luodun sivun. Sen kautta työntekijä anoo itselleen työntehtävissään tarvitsemia käyttöoikeuksia, joita hänelle ei ole jo aiemmin myönnetty. Käyttöoikeuspyyntö voidaan ohjata työnkulun avulla työntekijän esimiehelle, joka tarkistaa, että anomus on asianmukainen. Esimiehen tekemän hyväksynnän jälkeen anomus voidaan automatisoidusti ohjata sille ylläpitä-

jälle, joka vastaa sen tietojärjestelmän käyttöoikeuksista, jonka oikeuksia anomus koskee. Kun ylläpitäjä on hyväksynyt pyynnön, käyttöoikeus astuu voimaan.

Esittelin työssäni pääsyn hallinnan teoriamalleja, joista terveydenhuollon laajaan ja kompliksiseen toimintaympäristöön parhaiten sopivana pidän komposiittimallin RBAC-mallia. Siinä mallissa erotetaan organisaatio- ja tietojärjestelmätasot toisistaan ja niiden välille muodostetaan toimiva linkitys. Tämä malli voisi olla toimiva myös terveydenhuollon toimintaympäristössä, koska terveydenhuollon organisaatioilla on käytössään useita tietojärjestelmiä, joihin kullakin käyttäjällä on eritasoisia käyttöoikeuksia. Tietojärjestelmäroolien käyttäminen muiden roolien ja järjestelmien käyttöoikeuksien välissä tehostaisi roolienhallintaa. Tämä voidaan perustella sillä, että kun tietojärjestelmäroolit on luotu, näiden avulla käyttöoikeuksien sitominen rooleihin helpottuu. Tällöin kaikkien ylläpitäjien ei tarvitse tuntea kaikkien järjestelmien käyttöoikeuksia yksityiskohtaisesti. Ylläpitäjät voivat poimia tietojärjestelmäroolit roolihakemistosta muita uusia rooleja muodostaessaan.

Terveydenhuollon organisaatiot suunnittelevat lähiaikoina identiteetinhallintajärjestelmän hankkimisen käynnistämistä. Identiteetinhallintajärjestelmän voidaan todeta hallitsevan käyttöoikeuksien hallinnassa pääsynhallinnan kerrosta. Järjestelmä voidaan valjastaa luomaan uusi käyttäjätunnus automaatisesti, kun organisaation HR-järjestelmään lisätään uusi työntekijä. Tällöin järjestelmä luo käyttäjän sähköisen identiteetin ja käyttäjätunnuksen. Tässä prosessissa on huomioitava, että uutta henkilöä rekrytoitaessa, on hänen tietonsa tallennettava mahdollisimman pian HR-järjestelmään. Uuden työntekijän käyttöoikeuksien voimaan tulo on riippuvainen HR-järjestelmän henkilötiedoista.

6.2 Johtopäätökset

Nykyisistä organisaatiokohtaisista tietojärjestelmistä ollaan siirtymässä alueelliseen tietojenkäsittelyyn ja asiakkaan palveluiden suunnitteluun. Aluetietojärjestelmän web-portaalin avulla voidaan jakaa muuta sosiaali- ja terveydenhuoltoon liittyvää tietoa sekä eri toimintayksiköiden välillä että kansalaisille. Tulevaan

kansalliseen terveydenhuollon arkistopalveluun liitetään vain auditoidut ja sertifioidut luotettavat osapuolet. Tämä tarkoittaa muun muassa, että KANTA-palvelulla on luottosuhde siihen liittyviin potilastietojärjestelmiin eli ne tunnistavat käyttäjänsä ja rajoittavat kansallisen arkistopalvelun käyttöä käyttöoikeuksien puitteissa. Kansallinen arkisto tarkastaa, että sille saapuvan sanoman on lähettänyt luotettu (varmennettu) osapuoli.

Tavoitteena on luoda sosiaali- ja terveydenhuoltoon taloudellinen ja toimintavarma tietotekninen infrastruktuuri, joka mahdollistaa potilasturvallisuuden, hoidon jatkuvuuden ja laadun parantamisen sekä kustannustehokkaampien toimintamallien käyttöönoton. Tietojärjestelmäarkkitehtuurin toimeenpanon pohjana on sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskeva laki, joka velvoittaa kaikki terveydenhuollon julkiset toimijat liittymään siirtymäajan kuluessa kansalliseen sähköiseen potilasasiakirjojen arkistopalveluun sekä sähköistä lääkemääräystä koskeva laki, jonka mukaan sovitun siirtymäajan kuluessa kaikilla terveydenhuollon organisaatioilla sekä apteekeilla on oltava valmius eReseptiin. Lainsäädännön toimeenpano edellyttää, että sähköiset potilasasiakirjajärjestelmät sekä apteekkijärjestelmät täyttävät kansalliset vaatimukset. Lisäksi rakennetaan valtion rahoituksella kansalliset tietojärjestelmäpalvelut eArkisto, eResepti/Kela, varmennepalvelu/TEO ja koodistopalvelu/Stakes.

Uuden teknologian, erityisesti tieto- ja tietoliikenneteknologian laajamittaisen käyttöönoton vaikutukset ulottuvat kaikille inhimillisen elämän lohkoille. Muutoksen tuloksena nähdään vuorovaikutteisesti toimiva verkottunut tietoyhteiskunta. Verkostoituminen ja uuden teknologian käyttöönotto muuttaa sosiaali- ja terveydenhuollon tuotantoprosesseja, asiakkaan ja ammattihenkilöstön suhdetta, lisää asiakkaiden omatoimisuutta ja osallistumista sekä tekee monet nykyisistä hallintorakenteista tarpeettomiksi

Käyttöoikeuksien hallinnassa tavoitetilana on, että käyttöoikeuksien määrittely tehtäisiin käyttäjäkohtaisesti, työtehtävän mukaan sekä tietokokonaisuus- ja operaatiokohtaisesti. Tavoitteena on saada organisaation henkilökunta aktiivisesti mukaan muutoksenhallintaan järjestämällä tulevista muutoksista riittävä tiedotta-

minen. Kriittisten tietojärjestelmien käyttöjärjestelmä- ja muiden resurssien käytöstä määritellään tarvittaessa politiikka. Sovellusten käyttäjät saavat käyttöönsä vain ne resurssit, joihin heille on nimenomaisesti myönnetty pääsy. Tämä koskee käyttöjärjestelmän resursseja kaikilta sellaisilta osin, joihin pääsy voidaan hallinnoida (muistin, levytilan ja prosessoriajan käyttö, verkkotulostimien ja oheislaitteiden käyttö ym.). Pääsy hallinnoidaan sopivilla menetelmillä esimerkiksi käyttöjärjestelmä-, sovellus- ja käyttöliittymätasoilla sekä ottamalla käyttöön kertakirjautuminen ja siihen mukaan liitettävä tunnistautuminen ja todentaminen. Käyttöoikeuksien hallinasta ja käyttäjän hallinnasta terveydenhuollossa olisi hyvä tehdä jatkoselvitystyö laajennettujen mallien roolijaottelusta. Mahdollisessa jatkoselvitystyössä tutkimusongelmana tarkasteltaisiin tietojärjestelmäroolien käyttämistä muiden roolien ja järjestelmien käyttöoikeuksien välissä.

7 LÄHTEET

Kirjalliset lähteet:

Järvinen, P., 2003, Salausmenetelmät, Porvoo, WS Bookwell

Järvinen, P., 2006, Paranna tietoturvaasi, Porvoo, WS Bookwell

Paavilainen, J., 1998, Tietoturva, Jyväskylä, Gummerus Kirjapaino Oy

Ruohonen, M., 2002, Tietoturva, Porvoo, WS Bookwell

Salminen, H., 1997, Tietoturvallisuus etätyössä, Jyväskylä, Gummerus

Tutkimusraportit:

Hartikainen, K., Kuusisto-Niemi, S., Lehtonen, E. Sosiaali- ja terveydenhuollon tietojärjestelmäkartoitus 2001, 2002, Osaavien keskusten verkoston julkaisuja, 1/2002

Iivari, A., Ruotsalainen, P., 2007, Sosiaali- ja terveysministeriön selvityksiä 2007:14, Suomen eTerveys–tiekartta, STM

Iivari, A., STM:n työryhmämuistioita 2003:38, Sähköisten potilasasiakirjajärjestelmien valtakunnallinen määrittely ja toimeenpano, STM, Helsinki 2004

Kopra, P., Lindblad-Ahonen, A., Keskinarkaus, J., Allen, S., Oikarinen, T. & Kettunen E., 2007, Kuntaliiton ja Sisäasiainministeriön KuntaIT -yksikön yhteistyöprojekti 2007, Kuntien työntekijöiden tunnistaminen ja käyttövaltuuksien hallinta VIRTU(K)-raportti

Liikenne- ja viestintäministeriö, 2003. Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve. Liikenne- ja viestintäministeriön julkaisuja 44/2003

Mykkänen, J., Häyrinen, K., Savolainen, S. & Porrasmaa J., 2004, Plugit-hankkeen selvityksiä ja raportteja 3, Standardien arviointi j a valintaterveydenhuollon sovellusintegraatiossa, Kuopion yliopisto Savonia-ammattikorkeakoulu, Kuopio, Kopijyvä Oy

Porali, M., Ensio, A., 2005, Tietoturvallinen potilasasiakirjojen käsittely, Avointaprojekti, Kysely yrityksille, Kuopion yliopisto, Terveyshallinnon ja - talouden laitos, Shiftec-tutkimusyksikkö Anne Eerola, Kuopion yliopisto, Tietojenkäsittelytieteen laitos

Ruotsalainen, P. 2002, Ehdotus Sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi – terveydenhuollon PKI-arkkitehtuuri, Osaavien keskusten verkoston julkaisuja 4/2002, Helsinki, Stakesin monistamo

Ruotsalainen, P., 2006, Suositukset terveydenhuollon asiakastietojen tietoturvalliselle sähköiselle arkistoinnille – Usean toimintayksikön yhteinen käyttäjän ja käyttöoikeuksien hallinta - periaatteet ja suositukset, Stakesin raportteja 4/2006, Helsinki

Sormunen, M., Porrasmaa, J., Silvennoinen, R., Mykkänen, J., Savolainen, S. & Rannanheimo, J., 2004, HIS-tutkimusyksikkö, Kuopion yliopisto, Plugit-hankkeen selvityksiä ja raportteja 9, Terveydenhuollon avoimet sovellusrajapinnat - käyttäjä – ja käyttöoikeusrajapinnat, Kuopion Yliopisto, Savonia-Ammattikorkeakoulu, Kuopio, Kopijyvä Oy

Sosiaali- ja terveysministeriö, 2006, Terveydenhuollon kansallisen tietojärjestelmäarkkitehtuurin määrittelyprojekti, KANTA – Kokonaisarkkitehtuuri, STM Arkkkitehtuurimäärittely 28.2.2006

Sosiaali- ja terveysministeriön julkaisuja 2007:19, Helsinki 2007, STM, Tietoturvallisuussuunnitelman laatiminen, Opas sosiaali- ja terveydenhuollon toimintayksiköille, 2007, Helsinki, Yliopistopaino

Taipale, V., Ruotsalainen, P., 2006, Stakesin lausunto identiteetti- ja käyttövaltuushallinnon periaatteet ja hyvät käytännöt –ohjeluonnoksesta, 24.2.2006

Tammisalo, T. ,Stakes, 2007, Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi, Periaatteer ja menetelmät, Helsinki, Valopaino Oy

Tammisalo, T., Stakes, 2005, Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt, Ohje sosiaali- ja terveydenhuollon organisaatioille ja toimintayksiköille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi, Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus, Helsinki, Stakesin monistamo

Terveydenhuollon kansallisen tietojärjestelmäarkkitehtuurin määrittelyprojekti KANTA – tunnistaminen ja sähköinen allekirjoitus, Vaatimusmäärittely, 28.2.2007

Terveydenhuollon kansallisen tietojärjestelmäarkkitehtuurin määrittelyprojekti, KANTA – Viestinvälitys, Vaatimusmäärittely 28.2.2007

Terveydenhuollon oikeusturvakeskus 1b, TEOPKI – P1 Varmennepolitiikka terveydenhuollon ammattivarmennetta varten, Versio 1.01, 3.6.2008

Valtiovarainministeriö, Hallinnon kehittämisosasto, Valtion IT- johtamisyksikkö, Virkamiehen tunnistaminen ja käyttöoikeuksien hallinta – hankkeen esitutkimusraportti 19.6.2007

Valtiovarainministeriö, Tunnistaminen julkishallinnon verkkopalveluissa, 2006, Helsinki, Edita Prima Oy

Valtiovarainministeriö, Virkamiehen tunnistaminen ja käyttöoikeuksien hallinta – hanke (Virtu)

Valtiovarainministeriö, 9/2006, Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, 2006, Helsinki, EDITA Prima

Aikakausiartikkelit:

Ahlblad J., Suomen Lääkärinlehti, 13.6.2008

Muu materiaalit:

Terveydenhuollon oikeusturvakeskus 1a TEO Workshop 18.1.2008 –kalvot

Elektroniset lähteet

Caelli W., Rhodes A., Implementation of Active Role Based Access Control in a Collaborative Environment [viitattu 18.7.2008]. Saatavissa internetissa: *http://www.isi.qut.edu.au/research/publications/technical/qut-isrc-tr-1999-005.pdf*

FINLEX ®, Lainsäädäntö, Sähköinen säädöskokoelma 2008 [viitattu 20.7.2008]. Saatavissa internetissa: *http://www.finlex.fi/fi/laki/kokoelma/2008/*

FINLEX ® - Valtion säädöstietopankki [viitattu 15.7.2008]. Saatavissa internetissa: *www.finlex.fi*

Health Services Specification Project (HSSP), HL7 SOA SIG & OMG HDTF, SOA. Glossary of Key Concepts and Definitions, Draft Version 0.3. [viitattu 20.7.2008]. Saatavissa internetissa: *http://hssp-infrastructure.wikispaces.com/space/showimage/Microsoft+Word+-+HSSP+SOA+Key+Concepts+and+Definitiions+v0.3.pdf*

HL7 Finland r.y. [viitattu 17.7.2008]. Saatavissa internetissa: *http://www.hl7.fi/*

JUHTA - Julkisen hallinnon tietohallinnon neuvottelukunta, JHS 133 Hakemistotiedot ja niiden ylläpito, Versio: 2.11.2006 [viitattu 25.7.2008]. Saatavissa internetissa: *http://docs.jhs-suositukset.fi/jhs-suositukset/JHS133/JHS133.pdf*

Park J., Costello K., Neven T., Diosomito J., A composite rbac approach for large, complex organizationsa, USA, 2004. Saatavissa ACM Portalilta: http://portal.acm.org/citation.cfm?id=990036.990063

Sandhu R.,Coyne E.,Feinstein H., Youman C., Role-Based Access Control Models, IEEE Computer, Volume 29, Number 2, pages 38-47, 1996. [viitattu 23.8.2008] Saatavissa internetissa: *http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.49.5912*

Sosiaali- ja terveysministeriö, Sosiaali- ja terveydenhuollon tiedonhallinta, Ajankohtaista 22.7.2008 [viitattu 23.7.2008]. Saatavissa internetissa: *http://www.stm.fi/Resource.phx/vastt/tietoh/ajankoht.htx*

Suomen Standardisoimisliitto SFS ry [viitattu 18.7.2008]. Saatavissa internetissa: *http://www.sfs.fi/it/aihealueet/terveydenhuolto/standardit/*

Stakes, Ajankohtaista, Lausunnot 2006, [viitattu 19.7.2008]. Saatavissa internetissa: *http://www.stakes.fi/FI/ajankohtaista/lausunnot/2006/060224.htm*

Valtiovarainministeriö, VAHTI-tietoturvasanasto, [viitattu 11.6.2008]. Saatavissa internetissa: *http://www.vm.fi/tietoturvasanasto/sisallys.htm*

Väestörekisterikeskus, Sähköinen henkilöllisyys ja varmenteet [viitattu 16.6.2008]. Saatavissa: *http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/0B0AD53D8A8B1A0BC225721800294CFD?opendocument*

Väestörekisterikeskus, Varmenteet [viitattu 24.7.2008]. Saatavissa internetissa: *http://www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/1C341F7393DD8D06C2256FFF003A84EA#Varmenteet*

Väestörekisteri keskus, Kansainvälisen Porvoo-ryhmän 10. konferenssi Porvoo 2.–3.11.2006 [viitattu 25.7.2008]. Saatavissa internetissa: http://www.porvoo10.net/p10/Porvoo10.pdf