



Osaamista  
ja oivallusta  
tulevaisuuden  
tekemiseen

Krista Kuusisto

# Sairaanhoitopiirin käyttövaltuusjärjestelmän sisällöllinen päivitys

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Hyvinvointiteknologia

Insinöörityö

11.11.2020

Tekijä Otsikko Sivumäärä Aika	Krista Kuusisto Sairaanhoidopiirin käyttövaltuusjärjestelmän sisällöllinen päivitys 31 sivua 11.11.2020
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Hyvinvointiteknologia
Ammatillinen pääaine	Hyvinvointiteknologia
Ohjaajat	Yliopettaja Mikael Soini, Metropolia AMK
<p>Tämän opinnäytetyön tarkoituksena oli päivittää Kanta-Hämeen sairaanhoidopiirin käyttövaltuusjärjestelmän sisältöä, jotta organisaation käyttövaltuuksien hallinnointi vastaisi paremmin organisaation tarpeita. Käyttövaltuusjärjestelmän avulla hallinnoidaan sairaanhoidopiirin henkilökunnalle jaettavia käyttöoikeuksia muun muassa työasemille ja eri järjestelmiin. Käyttövaltuushallinta koskee lähes koko henkilöstöä, järjestelmän toiminta heijastuu sairaanhoidopiirin jokapäiväiseen toimintaan.</p> <p>Opinnäytetyössä perehdyttiin käyttövaltuushallintaan tietosuojan ja tietoturvan näkökulmasta. Henkilötietojen käsittelystä säädetään tietosuojalainsäädännöllä. Tietosuojalainsäädäntöä on EU:n yleisellä tietosuoja-asetuksella (EU 2016/679) ja sitä täsmentävällä tietosuojalailla (2018/1050) uudistettu tietojärjestelmien kehitystä vastaavaksi. Taustaosuuksessa käsitellään myös käyttövaltuushallintaa ja käyttövaltuushallintajärjestelmän toimintaa.</p> <p>Käyttövaltuusjärjestelmän sisällön päivitystarvetta lähdettiin tarkastelemaan joidenkin tiedossa olleiden ongelmatilanteiden ja kehitystoiveiden perusteella. Opinnäytetyön aikana suurin työnosuus kohdistettiin identiteettien päivittämisiin ja poistoihin järjestelmästä. Identiteettien päivittämisen ohessa työssä keskityttiin käyttöoikeuksien haun päivittämiseen yhtenäistämällä käyttöoikeuksien nimeämistä ja lisäämällä haettavia oikeuksia. Suunnitellut päivittämiset jäivät osittain kesken työn aikataulun puitteissa, työn loppuun kirjattiin ehdotuksia työn jatkamiseksi.</p>	
Avainsanat	Käyttövaltuudet, Identiteetin- ja pääsynhallinta, Tietosuoja

Author Title Number of Pages Date	Krista Kuusisto Updating Content in Identity and Access Management System in Kanta-Häme Hospital District 31 pages 11 November 2020
Degree	Bachelor of Engineering
Degree Programme	Health technology
Professional Major	Health technology
Instructors	Mikael Soini, Principal Lecturer
<p>The aim of this thesis was to update the content of the access authorisation system used in Kanta-Häme hospital district so that the management of access rights corresponds better to the needs of the organisation. The identity and access management (IAM) system is used to administer permits given to manage the access rights allocated to the hospital district staff, for example to workstations and various systems.</p> <p>The theoretical section discusses information security and data protection. The processing of personal data is regulated by the data protection legislation consisting of General Data Protection Regulation (GDPR) and Data Protection Act (1050/2018). The legislation needed updating due to improvement in information systems.</p> <p>The need to update the content of the access control system derived from problems noticed earlier and improvement suggestions. During the study, most of the work was focused on updating and deleting identities from the system. In addition to updating identities, the work focused on updating the search by harmonising the naming of the access rights and increasing the access rights to be applied for. The planned upgrades were partly interrupted within the work schedule, and the study lists suggestions for continuing the work in future.</p>	
Keywords	Access rights, IAM, Data protection

## Sisällys

### Lyhenteet

1	Johdanto	1
2	Työn tilaaja	2
3	Tietoturvallisuus	3
3.1	Tietosuoja ja tietoturva	3
3.2	Tietoturvan osa-alueet	5
3.3	EU:n yleinen tietosuoja-asetus	6
3.4	Tietosuojaperiaatteet	7
3.5	Tietosuojalaki	9
3.6	Muita tietosuojaa koskevia lakeja	10
4	Käyttövaltuushallinta	11
4.1	Identiteetin- ja pääsynhallinta	11
4.2	Identiteetin- ja pääsynhallinnan hyödyt	14
4.3	Käyttövaltuushallintajärjestelmä	16
5	Työn tavoitteet	19
5.1	Työn tavoitteiden rajaaminen	19
5.2	Käyttövaltuushallinnon ongelmatilanteita	20
6	Sisällön päivittäminen	21
6.1	Ylimääräisten identiteettien poistaminen	21
6.2	Lisäoikeuksien päivittäminen ajantasaiseksi	23
6.3	Kehitysehdotukset käyttövaltuusjärjestelmän toimintaan	25
6.4	Jatkoehdotuksia käyttövaltuusjärjestelmän päivittämisprosessiin	26
7	Yhteenveto	27
	Lähteet	29

## Lyhenteet

AM	Access Management. Pääsynhallinta eli käyttövaltuushallinta.
GDPR	General Data Protection Regulation. Euroopan unionin yleinen tietosuoja-asetus.
IAM	Identity and Access Management. Identiteetin ja pääsynhallinta.
IdM	Identity Management. Identiteetin hallinta.
KHSHP	Kanta-Hämeen sairaanhoitopiiri.
KVH	Käyttövaltuushallinta.
VAHTI	Valtiovarainministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä.

## 1 Johdanto

Tämän opinnäytetyön tavoitteena oli päivittää Kanta-Hämeen sairaanhoitopiirin (KHSHP) käyttövaltuusjärjestelmän sisältöä. Käyttövaltuusjärjestelmän avulla hallinnoidaan henkilöstölle jaettavia käyttöoikeuksia organisaation eri järjestelmiin, työasemille ja esimerkiksi sähköposteihin. Opinnäytetyön aikana tarkasteltiin käytössä olevan käyttövaltuusjärjestelmän toimintaa ja tiedossa olleiden ongelmatilanteiden ja kehitystoiveiden perusteella ryhdyttiin päivittämään järjestelmän sisältöä, jotta sen toiminta olisi organisaatiolle mahdollisimman sujuvaa.

Sairaanhoitopiirin palveluksessa työskentelee noin 1900 henkilöä, joista suurin osa kuuluu hoitohenkilökuntaan [1]. Järjestelmän kautta hallinnoidaan henkilöstön päivittäisessä käytössä olevien järjestelmien oikeuksia sekä hoidollisella puolella että hallinnollisella puolella, joten järjestelmän toimivuus vaikuttaa sairaanhoitopiirin päivittäiseen toimintaan.

Käyttöoikeuksien hallinta alkaa, kun uusi työsuhde kirjataan ja käyttövaltuusjärjestelmään päivittyy uuden työntekijän tiedot henkilöstöhallinnon järjestelmästä. Käyttövaltuusjärjestelmä luo tietojen pohjalta työntekijälle yksilöllisen sähköisen identiteetin, jonka avulla henkilö voidaan luotettavasti tunnistaa tietojärjestelmissä. Jokaiselle organisaation työntekijälle luodaan automaattisesti työasematunnus, sähköpostiosoite ja työsuhteen kustannuspaikan eli yksikön perusteella annettavia automaattisia käyttöoikeuksia. Automaattisesti määräytyvien käyttöoikeuksien lisäksi esimies voi hakea työntekijälle työtehtäviin tarvittavat lisäoikeudet muihin järjestelmiin, kansioihin ja tiedostoihin. Käyttöoikeuksien hallinta, muokkaus ja poisto tapahtuvat saman järjestelmän kautta, johon identiteetti luodaan. Työsuhteen päättyessä tiedot päivittyvät käyttövaltuusjärjestelmään, identiteetti sekä identiteetille lisätyt oikeudet passivoidaan ja lopulta poistetaan.

Opinnäytetyön taustaosuudessa käsitellään tietoturvallisuutta ja tietosuojaa, jotka sääntelevät järjestelmän toimintaa ja käyttöoikeuksien hallinnointia. Tietosuojan avulla varmistetaan henkilötietojen asianmukainen käyttö. Henkilötietojen käsittelyä säädetään monessa laissa ja niiden käsittelyyn tulee aina olla jokin laillinen peruste. Käyttövaltuusjärjestelmässä henkilötietojen käsittely on automatisoitua, mutta siihen pätevät samat

lait. Tietoturvan avulla varmistetaan tietosuojan oikeanlainen toteutuminen [2]. Tietoturvallisuudella suojataan sekä organisaation tietoja, että sen henkilöstön yksityisyyteen liittyviä henkilötietoja. Tietojärjestelmissä, jotka käsittelevät henkilötietoja, tietoturvallisuuden merkitys korostuu entisestään [3].

Taustaosuus käsittelee myös identiteetinhallintaa ja käyttövaltuushallintaa. Identiteetin hallinnan avulla käyttövaltuusjärjestelmän luomalle käyttäjän sähköiselle identiteetille luodaan tarvittavia yksilöitäviä tunnisteita, jonka avulla identiteetti ja työntekijä voidaan luotettavasti yhdistää toisiinsa. Yksilöivät tunnisteet voivat perustua henkilötunnukseen, työntekijänumeroon tai muuhun yksilöityyn tunnisteeseen. Käyttövaltuushallinnassa puolestaan määritetään henkilön sähköiselle identiteetille tarvittavat roolit, joiden avulla käyttöoikeudet muodostuvat. Roolit voivat olla työtehtävien tai yksikön perusteella muodostettuja ryhmiä, joille on asetettu ryhmänmukaisia käyttöoikeuksia. [4.]

Opinnäytetyössä keskitytään käyttövaltuusjärjestelmän sisällöllisiin muutoksiin. Järjestelmän päivittäiskäytössä on huomattu epäkohtia, jotka heikentävät järjestelmän toimintaa ja vähentävät sen käyttömukavuutta. Opinnäytetyötä suunniteltaessa päätettiin keskittyä ylimääräisten identiteettien poistoon ja käyttöoikeuksien haun muokkaamiseen järjestelmän sisällä. Identiteettien poistaminen priorisoitiin suunniteltaessa ensimmäiseksi tehtäväksi ja muita suunniteltuja tehtäviä tehdään niin paljon kuin opinnäytetyön ajan puitteissa ehditään. Opinnäytetyön loppuun kirjataan kehitysehdotuksia ja jatkosuunnitelmaehdotuksia käyttövaltuusjärjestelmän päivittämisen jatkamiseksi.

## 2 Työn tilaaja

Työn tilaajana toimii Kanta-Hämeen sairaanhoitopiirin tietotekniikkapalvelut. Tietotekniikkapalvelut vastaavat sairaanhoitopiirin käyttövaltuushallinnasta ja osallistuvat sen kehittämiseen. Suurin osa käyttövaltuushallinnoinnista organisaatiossa on tällä hetkellä tietotekniikkapalveluiden hallinnoitavana.

Kuntien muodostamat sairaanhoitopiirit vastaavat erikoissairaanhoidon järjestämisestä omilla alueillaan. Sairaanhoitopiireistä ja niiden tehtävistä säädetään erikoissairaanhoidon

tolaissa (1026/1989). Erikoissairaanhoitolain mukaan sairaanhoitopiirit tuottavat ne erikoissairaanhoidon palvelut, joita ei ole tarkoituksenmukaista tuottaa perusterveydenhuollolla. Sairaanhoitopiirejä Suomessa on Ahvenanmaa mukaan lukien 21. Osa sairaanhoitopiireistä tuottaa erikoissairaanhoidon palveluita yliopistosairaaloiden erikoisvastuualueiden pohjalta. Erikoisvastuualueet pohjautuvat valtioneuvoston asetukseen sairaanhoidon erityisvastuualueista (156/2017). [5.] Kanta-Hämeen sairaanhoitopiirin alueeseen kuuluu kokonaisuudessaan Kanta-Hämeen maakunta [6]. Sairaanhoitopiirin yksiköissä Hämeenlinnassa ja Riihimäellä hoidetaan vuosittain noin 65 000 ihmistä [7].

Käyttövaltuusjärjestelmän avulla hallinnoidaan sairaanhoitopiirin henkilöstön käyttöoikeuksia muun muassa organisaation työasemille ja tietojärjestelmiin. Kanta-Hämeen sairaanhoitopiirin palveluksessa työskentelee henkilökuntaa erikoissairaanhoidon lisäksi muun muassa hallinnon, tietotekniikan ja sairaalahuollon toimialoilla. Yhteensä sairaanhoitopiiri työllistää noin 1900 työntekijää [1]. Käyttövaltuusjärjestelmän kautta lähes jokaiselle organisaation työntekijälle jaetaan työasematunnus, sähköpostiosoite ja yksikön mukaiset automaattiset käyttöoikeudet, joten sen toiminta koskettaa koko henkilöstöä. Käyttövaltuuksia hallinnoidaan järjestelmän kautta ja voidaan tarvittaessa muokata työtehtävien muuttuessa aina työsuhteen päättymiseen asti, joten se on tärkeä työväline koko työsuhteen ajan. Käytössä oleva käyttövaltuusjärjestelmä lukee jokaisen työsuhteen omaksi identiteetikseen, joten hallittavia identiteettejä on enemmän kuin työntekijöitä sairaanhoitopiirillä. Sairaanhoitopiirin tietoturvapolitiikan mukaisesti käyttövaltuuksien hallinnointiin ja tietosuojan ylläpitämiseen kiinnitetään jatkuvaa huomiota lainsäädännön mukaisesti.

### **3 Tietoturvallisuus**

#### **3.1 Tietosuoja ja tietoturva**

Tietosuoja ja tietoturva perustuvat kansallisiin ja kansainvälisiin lakeihin ja asetuksiin. Perustana olevat kansainväliset ihmisoikeussopimukset ja kansalliset perusoikeussopimukset ohjaavat alempiasteisia säännöksiä. [3.] Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioimista, sen avulla on tarkoitus turvata tiedon



kohteen yksityisyys ja oikeusturva sekä varmistaa henkilötietojen käsittelyä koskevien vaatimusten toteutuminen. Tietoturvalle tarkoitetaan niitä toimenpiteitä, joiden avulla tietosuoja toteutuminen varmistetaan. Tietoturvallisuutta organisaatioissa määrätään eri lakien ja standardien avulla. [2.] Tietosuoja-lainsäädännön muodostavat tietosuoja-asetus, tietosuoja-laki ja tapauskohtaisesti erityislainsäädäntö sekä julkisuuslaki [8]. Lakien lisäksi organisaatiot voivat määritellä organisaatiokohtaisia ohjeistuksia tietosuoja toteuttamiseksi.

Perinteisessä tiedon arvoon perustuvassa määritelmässä tietoturvallisuus koostuu kolmesta tekijästä, jotka ovat luottamuksellisuus, eheys ja käytettävyys. Näiden toteutuminen tulee varmistaa organisaatioissa sekä hallinnollisilla että teknisillä toimilla. Luottamuksellisuudella viitataan siihen, että tiedot ja tietojärjestelmät ovat vain niihin oikeutettujen henkilöiden käytettävissä. Tämän toteutumista voidaan organisaatioissa valvoa käyttövaltuushallinnan avulla. Eheydellä turvataan tiedon oikeellisuus ja käytettävyydellä tarkoitetaan sitä, että tiedot ovat saatavissa oikeutetuille henkilöille riittävän nopeasti ja oikeassa muodossa [9, s. 4-5].

Laajennettuun tietoturvallisuuden määritelmään osatekijöiksi, luottamuksellisuuden, eheyden ja käytettävyyden lisäksi, on lisätty kiistämättömyys ja pääsynvalvonta. Kiistämättömyydellä tietoturvallisuusmääritelmässä tarkoitetaan tietojärjestelmän kykyä tunnistaa järjestelmää käyttävän henkilön tiedot. Siihen pyritään käyttämällä erilaisia luotettavia tunnistusmekanismeja, kuten henkilökohtaista toimikorttia tai henkilön biometrisia tunnisteita, kuten sormenjälkeä. Pääsynvalvonnalla tarkoitetaan menetelmiä, joilla rajoitetaan luvaton laitteiden tai tietoliikenneverkon käyttö vain oikeutetuille henkilöille. [9, s. 5-6.]

Kanta-Hämeen sairaanhoitopiirin Tietoturvapoliittika-julkaisussa kirjataan sairaanhoitopiirin käytäntöjä tarvittavan tietoturvatason saavuttamiseksi. Käytännöt perustuvat lakeihin ja säädöksiin sekä tukevat sairaanhoitopiirin strategiaa ja arvoja. Keskeisimpinä lakeina tietojen käsittelyn kannalta ovat EU:n tietosuoja-asetus, julkisuuslaki, laki potilaan asemasta ja oikeuksista sekä laki potilastietojen sähköisestä käsittelystä. Tietoturvapoliittikan tarkoituksena on luoda organisaatiolle ohjeet, joiden avulla tietoturvatyötä tehdään. Tietoturvapoliittika koskee koko organisaatiota ja sen henkilöstöä, kumppaneita ja palveluntoimittajia, jotka työskentelevät yhteistyössä sairaanhoitopiirin kanssa. [10.]

Sairaanhoitopiirin Tietoturvapoliittikka-julkaisussa mainittuja tietoturvakäytäntöjä ovat muun muassa keskitetty sairaanhoitopiirin järjestelmien käyttöoikeus- ja pääsynhallinta. Tietoturvatason varmistamiseksi sairaanhoitopiiri valvoo ohjelmistoja, laitteita ja tiedostomuuotoja, jotka ovat organisaation käytössä ja tarvittaessa rajoittaa tai estää niiden käytön. Tietoturvatasoa valvotaan säännöllisesti ja siitä raportoidaan sisäisen valvonnan ja muiden tarkastusten yhteydessä. Palveluntuottajien ja muiden kumppanien on sitouduttava noudattamaan sairaanhoitopiirin tietoturvavaatimuksia. [10.]

### 3.2 Tietoturvan osa-alueet

Tietoturva voidaan jakaa eri osa-alueisiin, jotka tulee huomioida, jotta tietoturva toteutuu riittävällä tasolla. Osa-alueisiin kuuluvat tietoaineiston turvallisuus, ohjelmistoturvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, fyysinen turvallisuus, henkilöstöturvallisuus, käyttöturvallisuus ja hallinnollinen turvallisuus. [9, s. 10.] Kaikkien osa-alueiden hallitseminen helpottaa riskien analysoimista ja ennakoinnista [11].

Tietoaineiston turvallisuudella tarkoitetaan tietojärjestelmässä olevien tietojen ja tiedostojen suojaamista [9, s. 11]. Organisaatioiden kannattaa luokitella tietoaineisto niiden suojaustason mukaisesti. Karkeasti tietoaineisto voidaan jakaa kahteen luokkaan, julkiseen ja salattuun, mutta tarkempaakin luokittelua on suositeltua käyttää. [11.]

Ohjelmistoturvallisuudella turvataan tietojärjestelmän ohjelmistot luvattomalta käytöltä sekä ylläpidetään lisenssejä [9, s. 11-12]. Ohjelmistoturvallisuuteen kuuluu organisaation tietokoneiden ja puhelinten lisenssien ja ohjelmistojen hallinta sekä niiden säännöllinen päivittäminen [12]. Tietoliikenneturvallisuus turvaa järjestelmän tietoliikennettä sisäisessä ja ulkoisessa verkossa. Sen päätavoitteena on suojata tiedon eheys, luottamuksellisuus ja saatavuus dataverkossa liikkuesssa. Laitteistoturvallisuuden ja fyysisen turvallisuuden avulla suojataan tietojärjestelmän laitteet ja ne fyysiset tilat, joissa tietojärjestelmä sijaitsee. [9, s. 12.]

Henkilöstö- ja käyttöturvallisuuden huomiointi suojaa tietojärjestelmää käyttäjien toiminnan aiheuttamilta uhilta. Tietoturvariskejä voi aiheutua inhimillisistä virheistä tai tietä-

mättömyydestä. Tietoturvariskiä lisäävät liian laajat ja tarpeettomat käyttöoikeudet. Hallinnollisella turvallisuudella johdetaan tietojärjestelmän kaikkia tietoturvan eri osa-alueita. Hallinnollisen tietoturvan tavoitteena on varmistaa ja valvoa osa-alueiden toteutuminen organisaatiolle riittävällä tasolla. [11.]

### 3.3 EU:n yleinen tietosuoja-asetus

Henkilötietoja koskeva Euroopan unionin yleinen tietosuoja-asetus (EU 2016/679) hyväksyttiin vuonna 2016 ja kahden vuoden siirtymäajan jälkeen se tuli sovellettavaksi kaikissa EU:n jäsenmaissa. EU:n tietosuojalainsäädäntöä lähdettiin uudistamaan vuonna 2012 teknologian kehittymisen perusteella. Kehityksen takia tietosuoja säännökset tarvitsivat uudistusta ja ne piti muuttaa teknologiavaatimuksia vastaavaksi. [13; 14.] Digitaalisten palveluihin toimintaympäristöjen takia yksilöillä tulee olla oikeus valvoa tehokkaasti henkilötietojaan ja tietosuoja-asetuksen avulla pyrittiin luomaan lainsäädäntöpohja, jotta digitaaliset palvelut olisivat jäsenmaille luotettavia ja niitä kannattaisi kehittää [15]. Tietosuoja-asetuksessa on kansallista liikkumavaraa, jota täydennetään Suomessa tietosuojalailla. [16.] Sääntelyn tarkoituksena on harmonisoida lainsäädäntöpohja ja tulkintamiskäytännöt EU:n jäsenvaltioissa [11].

Yleinen tietosuoja-asetus edellyttää kaikilta henkilötietoja käsitteleviltä organisaatioilta asetuksen seuraamista. Asetusta sovelletaan myös henkilötietojen käsittelyyn, joka on joko osittain tai kokonaan automaattista ja käsiteltävät tiedot muodostavat rekisterin osan. Tietosuoja-asetuksesta käytetään lyhennettä GDPR (General Data Protection Regulation). Asetusta sovelletaan, jos organisaatio sijaitsee EU:ssa, riippumatta siitä missä henkilötietojen käsittely tapahtuu. Jos yritys tai organisaatio sijaitsee EU:n ulkopuolella, on sen nimettävä EU:ssa toimiva edustaja, joka huolehtii, että asetuksen määräyksiä seurataan käsittelyssä. [13.] Henkilötiedoiksi luetaan kaikki tiedot, joiden perusteella yksityinen henkilö on mahdollista tunnistaa ja sellaiset tiedot, jotka on mahdollista palauttaa takaisin tunnistettavaan muotoon. Henkilötietoja voivat olla esimerkiksi nimi, henkilötunnus tai sijaintitieto. Asetus suojaa henkilötietoja riippumatta siitä mitä tekniikkaa tietojen käsittelyssä käytetään tai millainen säilytystapa tietojen säilyttämiseen on käytössä. [15; 17.]

Tietosuoja-asetuksella pyritään parantamaan yksityishenkilöiden yksityisyyden suojaa. Asetus edellyttää, että henkilötietojen kerääminen on asianmukaista ja rajoittuu vain käsittelyn kannalta tarpeellisiin tietoihin. Niiden kerääminen on minimoitava käsittelyn kannalta olennaisiin tietoihin. [15; 19.] Rekisteröidylle on tarjottava selkeästi mahdollisuus hyväksyä tai kieltää tietojen kerääminen. Kun henkilö on hyväksynyt henkilötietojensa käsittelyn, tietoja voidaan käyttää vain siihen tarkoitukseen, johon suostumus on annettu. Organisaatioiden on pyydettäessä pystyttävä antamaan yksityishenkilölle tiedot, jotka ovat tallennettuina sen rekistereissä ja rekisteröidyllä on oikeus saada tiedot oikaistuiksi tai täydennetyiksi, jos tieto on virheellistä tai puutteellista. Tietosuoja-asetuksen mukaan henkilö voi myös pyytää henkilötietojensa poistamista rekisteristä. Tietojen poistaminen ei kuitenkaan ole pakollista, jos niiden käsittely on välttämätöntä esimerkiksi lakisääteisen velvoitteen täyttämiseksi. [15; 17.] Tietosuojaperiaatteet on määritelty EU:n yleisessä tietosuoja-asetuksessa.

### 3.4 Tietosuojaperiaatteet

Henkilötietoja käsitellessä tulee noudattaa tietosuojaperiaatteita. Tietosuojaperiaatteet annetaan Euroopan parlamentin ja neuvoston yleisessä tietosuoja-asetuksessa (EU 2016/679). Tietosuojaperiaatteita on noudatettava koko henkilötietojen käsittelyn ajan suunnittelusta keräämiseen, käsittelyyn ja tietojen poistamiseen asti ja niitä on sovellettava kaikkiin tietoihin, joista yksityinen henkilö on tunnistettavissa. [13.] Tietosuojaperiaatteisiin kuuluvat lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, eheys ja luottamuksellisuus sekä osoitusvelvollisuus. [14, s. 88-89.]

Yksi tietosuojaperiaatteista on henkilötietojen käsittely lainmukaisesti. Lainmukainen käsittely toteutuu, kun henkilötietojen käsittely perustuu johonkin lakiin, kuten EU:n yleiseen tietosuoja-asetukseen tai muuhun henkilötietojen käsittelystä määrävään lainsäädäntöön. Käsittelyperusteet henkilötietojen käyttämiseen ovat henkilön suostumus, sopimus, rekisterinpitäjän lakisääteinen velvoitteen noudattaminen, yleistä etua koskevan tehtävän suorittaminen, rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen tai oikeutettujen etujen toteutuminen. Myös sopimukseen perustuvan henkilötietojen käsittelyn tulee olla lainmukaista. [14, s. 89-90.]

Kohtuullisuuden periaatteella tarkoitetaan, että rekisterinpitäjän on otettava tietoja käsitellessään huomioon rekisteröidyn henkilön edut ja odotukset, eikä tietoja saa käyttää väärin tarkoituksiin. Periaate suojaa rekisteröityä salassa tapahtuvalta tietojen keräämiseltä ja muulta käsittelyltä. Kohtuullisuuden periaatteen mukaisesti rekisteröidyn tulee tietää käsittelyn luonne ja tarkoitus. [14, s. 90.]

Läpinäkyvyyden periaatteen mukaisesti henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän pitää olla selkeää, helposti saatavilla ja ymmärrettävissä. Ennen käsittelyä rekisteröidylle pitää ilmoittaa tietojen käsittelyyn liittyvistä riskeistä ja säännöistä, tietojen käsittelyä koskevista suojatoimista ja rekisteröityä koskevista oikeuksista. Rekisterinpitäjän on pystyttävä jälkikäteen todistamaan, että suostumus henkilötietojen käsittelyyn on annettu. Läpinäkyvyys edellyttää, ettei rekisteröidyn tarvitse etsiä tarpeellista tietoa käsittelystä vaan informaatio on löydettävissä helposti. Avoin viestintä ja informointi parantavat tietojen käsittelyn lainmukaisuutta, koska rekisterinpitäjä joutuu silloin tarkastelemaan tietosuojakäytäntöjään. [14, s. 90-92.]

Käyttötarkoitussidonnaisuuden periaate rajoittaa tietojen käyttämistä. Henkilötiedot on kerättävät osoitettua laillista tarkoitusta varten ja eikä niitä saa käsitellä myöhemmin toisessa yhteydessä. Käyttötarkoitussidonnaisuus ei estä käyttämästä tietoja myöhemmin toista tarkoitusta varten, jos käyttötarkoitus on yhteensopiva alkuperäisen tarkoituksen kanssa. Käyttötarkoitussidonnaisuus ei myöskään koske tieteelliseen tai tilastolliseen tarkoitukseen kerättyä tietoa. [14, s. 92.]

Tietojen minimoinnin periaatteen mukaisesti rekisterinpitäjän keräämien henkilötietojen pitää olla olennaisia ja rajoittua vain välttämättömiin tietoihin käsittelyn kannalta. Olennaisten tietojen kerääminen edellyttää käsittelyn tarkoituksen määrittelyä ja suunnittelua. Henkilötietoja tulee käsitellä vain, jos käsittelyn tarkoitusta ei pystytä toteuttamaan muilla tavoin. Rekisterinpitäjän tulee säännöllisesti tarkastaa henkilötiedot ja huolehtia, että henkilötiedot ovat täsmällisiä ja päivitettyjä sekä kohtuullisin toimin poistettava tai korjattavat epätarkat ja virheelliset tiedot rekisteristä. Henkilötietojen säilytysaika täytyy olla mahdollisimman lyhytaikaista ja niiden säilyttämiselle täytyy olla koko ajan jokin peruste. Laki saattaa velvoittaa rekisterinpitäjää säilyttämään henkilötietoja pitkänkin ajan, mutta kun säilyttämiselle ei ole enää perustetta lain puolesta, ne tulee poistaa. [14, s. 93.]

Eheyden ja luottamuksellisuuden periaate tarkoittaa, että henkilötietoja käsiteltäessä on varmistettava, että tietojen eheys ja luottamuksellisuus toteutuvat eikä asiattomilla ole pääsyä tietoihin. Eheydellä viitataan tietojen oikeanmukaisuuteen. Rekisterinpitäjän tulee varmistua, ettei tietoja ole muutettu ilman rekisterinpitäjän suostumusta. Tiedot on suojattava lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Tietojen eheys pitää varmistaa käyttämällä asianmukaisia teknisiä ja hallinnollisia toimia. Organisaatioiden tulee tarkastella työtehtäviä ja arvioida, millaista henkilötietojen käsittelyä työtehtävät vaativat ja mihin tietoihin työntekijällä tulee olla pääsy tehtäviensä mahdollistamiseksi. [14, s. 94-95.]

Osoitusvelvollisuuden periaatteen mukaisesti henkilötietojen oikea käsittely ja kaikkien edellä mainittujen tietosuojaperiaatteiden toteutuminen tulee pystyä todentamaan. Periaatteiden noudattaminen voidaan osoittaa dokumentoimalla toimenpiteitä ja laatimalla lainsäädännön edellyttämistä käsittelytoimenpiteistä selosteet. Dokumentoinnin laajuus riippuu tietojen luonteesta ja käsittelyn tarkoituksesta. Osoitusvelvollisuudella pyritään kannustamaan organisaatioita luomaan käytännölliset ja tehokkaat keinot henkilötietojen suojan toteuttamiseksi. Rekisterinpitäjällä on osoitusvelvollisuus koko tiedon elinkaaren ajan, kunnes tieto hävitetään. [14, s. 95.]

### 3.5 Tietosuojalaki

1.1.2019 voimaan tullut tietosuojalaki (2018/1050) täydentää EU:n yleisen tietosuojasetuksen kansallista soveltamista. Tietosuojalaki kumosi aiemmin voimassa olleen henkilötietolain sekä lait tietosuojalautakunnasta ja tietosuojavaltuutetusta. Tietosuojalaki ei itsessään muodosta kattavaa sääntelykokonaisuutta, vaan sitä sovelletaan tietosuojasetuksen kanssa rinnakkain ja sen avulla säädetään asetukseen joitakin kansallisia poikkeuksia ja täsmennyksiä. Lailla säädetään valvontaviranomaisesta ja eräistä henkilötietojen käsittelyn erikoistilanteista. [17.] Tietosuojalaissa säädetään lapsiin sovellettavasta ikärajasta, henkilötietojen käsittelystä journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten, henkilötunnuksen käsittelystä ja tilanteista, joissa yleinen etu on perusteena henkilötietojen käsittelylle sekä rajoituksista rekisteröidyn oikeuksiin. [18.]

Tietosuoja-asetuksessa määrättyä kansallisenä valvontaviranomaisena toimii tietosuojavaltuutettu. Tietosuojalaissa tarkennetaan tietosuoja-asetuksen mukaisia hallinnollisia seuraamusmaksuja. Lain mukaan seuraamusmaksua ei voi Suomessa määrätä valtion tai kunnan viranomaisille. Muita seuraamuksia, kuten varoitukset ja huomautukset sekä henkilötietojen käsittelyn rajoittaminen sovelletaan tietosuoja-asetuksen mukaisesti. [8.] Organisaatioiden sisäiset tietosuojavastaavat seuraa henkilötietojen käsittelyä ja auttaa noudattamaan tietosuojasäännöksiä. Tietosuojavastaava antaa tietoa ja neuvoja velvollisuuksista, jotka tulee huomioida henkilötietoja käsitellessä. Tietosuojavastaava toimii tietosuojavaltuutetun toimiston yhteyshenkilönä ja tekee yhteistyötä tietosuojavaltuutetun kanssa. [19.]

Henkilötietojen käsittelyyn säädetään tietosuojalaissa poikkeuksia, kun kyse on sananvapauden turvaamisesta tai henkilötietojen käsittelystä journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten. Poikkeukset merkitsevät sitä, ettei rekisteröidyllä ole oikeutta tarkistaa itseään koskevia tietoja. [17.]

Tietosuojalaissa säädetään lapsiin sovellettavasta ikärajasta, kun tarjotaan tietoyhteiskunnan palveluita. Tietoyhteiskunnan palvelujen tarjoaminen suoraan lapselle edellyttää, että lapsi on vähintään 13-vuotias. Rekisterinpitäjän on huolehdittava, että alle 13-vuotiaalla on vanhempien suostumus olemassa. Ikäraja on Suomessa alempi kuin tietosuoja-asetuksessa säädetty 16 vuotta. [17.]

### 3.6 Muita tietosuojaa koskevia lakeja

Henkilötietojen käsittelystä säädetään laajasti monissa eri laissa. Voimassa olevassa lainsäädännössä on tietosuoja-asetuksen ja tietosuojalain lisäksi useita muita henkilötietojen käsittelyä koskevia lakeja ja säännöksiä. Henkilötietojen käsittelystä säädetään esimerkiksi työelämän suojalaissa (759/2004), sähköisen viestinnän palveluista säätävässä laissa (917/2014), työelämän tietosuojalaissa (759/2004, muutokset 347/2019) ja Suomen perustuslaissa (739/1999). Korpisaari ym. esittämien laskelmien mukaan henkilötiedoista säädetään noin kahdeksassa sadassa säädöksessä. Henkilötietolainsääd

dännön hajanaisuus aiheuttaa epätietoisuutta yksityisyyttä ja julkisuutta koskevan sääntelyn keskinäisistä suhteista. Sääntelyn pirstaleisuus vaikeuttaa tietosuojan sisällöllistä osaamista ja lain oikeaa soveltamista. [14, s. 3; 20.]

## 4 Käyttövaltuushallinta

### 4.1 Identiteetin- ja pääsynhallinta

Käyttövaltuushallintaa ohjaa sitä koskeva lainsäädäntö sekä organisaatioiden sisäiset määräykset ja ohjeet. Valtiovarainministeriön Valtiohallinnon tietoturvallisuuden johtoryhmän (VAHTI) julkaisemassa Käyttövaltuushallinnon periaatteet ja hyvät käytännöt – ohjeistuksessa suositellaan, että jokaisen organisaation tulisi huolehtia käyttöoikeuksien hallinnoinnista ja määritellä organisaation sisäiset käyttövaltuushallinnan perusteet. Organisaatioiden tulee määritellä ja hallinnoida tietojärjestelmien, sovellusten ja henkilörekisterien osalta niiden käyttöön oikeutetut henkilöt, oikeutettujen henkilöiden käyttöoikeuksien laajuus ja sisältö sekä käyttöoikeuksien voimassaoloaika. [21.]

Käyttövaltuushallinnalla määritellään käyttäjän identiteettiin perustuvat oikeudet haluttuihin tietojärjestelmiin tai toimintoihin. Rooliin perustuvassa käyttövaltuusvalvonnassa käyttäjälle annetaan rooleja, joiden mukaan käyttöoikeudet jaetaan. Tietojärjestelmien käyttöoikeuksista puhuttaessa rooleilla tarkoitetaan usein organisaatiossa määriteltä työnkuvaa, jonka avulla määritellään henkilön oikeudet ja velvollisuudet. Samalla henkilöllä voi olla useita eri rooleja organisaation sisällä. [4.] Yksikön lisäksi muita perusteltuja rooleja voivat olla esimerkiksi esimiesasema tai sihteerityö, jolloin oikeudet ovat tavanomaista laajemmat. Monesti käyttövaltuuksien hallinta aloitetaan organisaation sisäisten identiteettien hallinnasta ja laajennetaan sen jälkeen tarvittaessa ulkoisten identiteettien hallintaan.

Identiteetin- ja pääsynhallinta on jaettavissa neljään osaan: autentikointiin, auktorisointiin, administroidiin ja auditointiin. Autentikointilla eli identiteetin todentamisella käyttäjän identiteetti varmistetaan. Todennus voidaan suorittaa salasanalla tai muulla varmistus-



keinolla. Auktorisoinnissa käyttäjän todennetulle identiteetille myönnetään roolin tai tehtävän mukaisesti käyttövaltuudet. Rooliin perustuvassa käyttövaltuusvalvonnassa käyttäjälle annetaan rooli tai rooleja esimerkiksi työtehtävien mukaan. Administroinnilla hallinnoidaan käyttövaltuushallinnan kokonaisuutta ja toimivuutta. Auditoinnilla valvotaan, että käyttövaltuushallinnalle asetetut vaatimukset ja säädökset toteutuvat käytännössä. [22.]

Vähimmän käyttövaltuuden periaatteen mukaan käyttäjälle annetaan vain niin laajat oikeudet kuin hän työtehtävien hoitamiseen tarvitsee [13]. Organisaatioissa, joissa käyttöoikeuksien jakamista ja käyttöä ei hallinnoida selkeästi, on vaarana, että kokonaiskuva jaetuista käyttöoikeuksista ei ole tiedossa. Hajanainen hallinnointi voi aiheuttaa sen, että käyttöoikeuksia jaetaan liian laajalti tai liian pitkäksi aikaa tai ne voivat jäädä avoimiksi työsuhteen päättyessä. Hallittu käyttövaltuuksien jakaminen ovat perustus tietosuojan toteutumiselle.

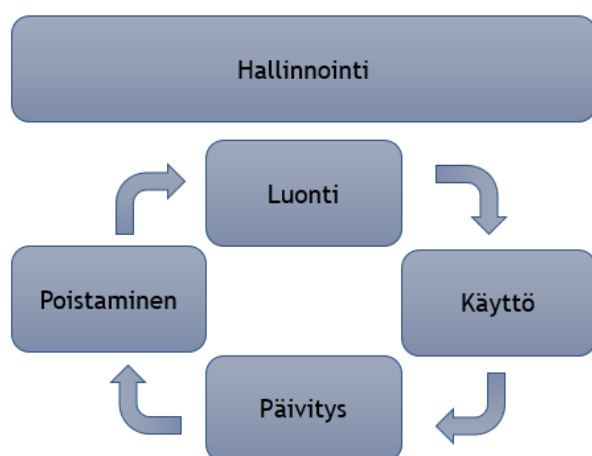
Identiteetin- ja pääsynhallinnan käsite (Identity and Access Management, IAM) koostuu kahdesta osasta: identiteetinhallinnasta (Identity Management, IdM) ja pääsynhallinnasta (Access Management, AM). Tässä opinnäytetyössä pääsynhallintaan viitataan myös käyttövaltuushallintana. Identiteetin- ja pääsynhallintaan viitataan usein myös termillä käyttövaltuushallinta (KVH). [22.]

Identiteetinhallinnalla (Identity Management, IdM) tarkoitetaan prosessia, jossa käyttäjä esitetään digitaalisena identiteettinä tietojärjestelmissä. Tietotekniikassa sähköinen identiteetti tarkoittaa kohdetta kuvailevien ominaisuuksien eli attribuuttien kokoelmaa. Muillakin kuin ihmisillä voi olla identiteetti, kuten organisaatioilla tai verkkoon kytketyillä tietokoneilla, mutta tavallisesti identiteetin- ja pääsynhallinnassa keskitytään kuitenkin ihmisten identiteetteihin. Identiteetinhallinta on usein käyttäjän kannalta näkymättömissä tapahtuvaa käyttäjätiedon hallintaa. [4.]

Identiteetinhallinnan ensimmäisessä vaiheessa käyttäjälle luodaan identiteetti, jolle määritetään tarvittavia yksilöitäviä tunnisteita, joiden avulla käyttäjä voidaan luotettavasti tunnistaa. Tarpeelliset käyttäjään liitettävät ominaisuudet vaihtelevat tarkoituksen ja ylläpi-

täjän mukaan. Yksilöitävien attribuuttien avulla käyttäjä voidaan erottaa muista käyttäjistä. Tyypillisiä yksilöitäviä tunnisteita voivat olla käyttäjätunnus, sähköposti, työtekijänumero, henkilötunnus tai passin numero. [4.]

Identiteetin elinkaaren aikana identiteetti käy läpi tiettyjä vaiheita. Kuvassa 1 on esitetty identiteetin elinkaari, joka voidaan jakaa neljään eri osioon: identiteetin luominen, käyttö, päivittäminen ja poistaminen. Identiteettiä hallinnoidaan sen koko elinkaaren ajan.



Kuva 1. Identiteetin elinkaari [23.]

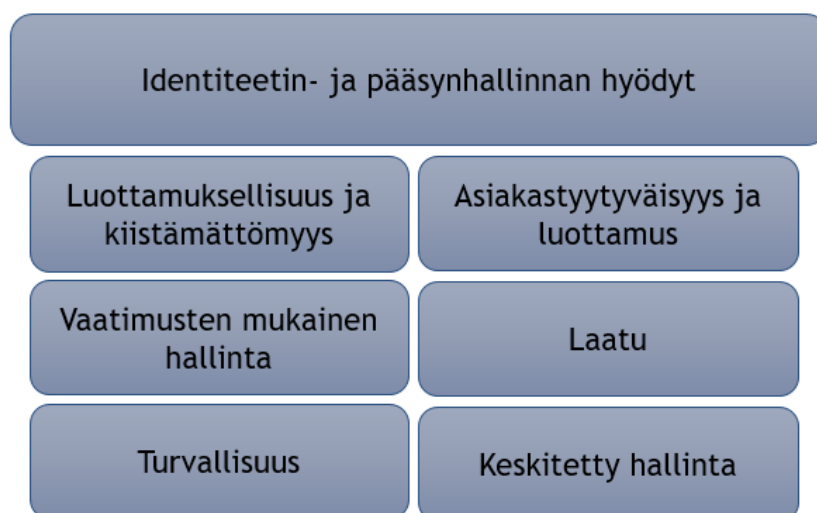
Elinkaari alkaa identiteetin luomisesta ja uuden identiteettitiedon välittämisestä kohdejärjestelmille. Kohteet käyttävät tietoja eri järjestelmiin tunnistautumiseen ja oikeuttavat niillä erilaisia toimintoja. Identiteetit päivittyvät ajoittain, kun niille määrätty attribuutit muuttuvat. Identiteetin päättyessä tiedot identiteetistä ja sille myönnetty oikeudet poistetaan ja elinkaari päättyy. [24.]

Pääsynhallinnalla (Access Management, AM) viitataan prosessiin, jossa tietojärjestelmän käyttäjä tunnistetaan ja tunnistuksen perusteella hyväksytään tai evätään käyttäjän pääsy tietojärjestelmään. Pääsynhallinta näkyy käyttäjälle useimmiten käyttäjätunnuksen ja salasanan kysymisellä. Identiteetinhallinta ja pääsynhallinta kuvataan usein omina kokonaisuuksinaan, mutta käsitteiden välinen raja ei ole aina selkeä. [4.] Pääsynvalvonta on keskeinen osa pääsynhallintaa ja se sisältää lisäksi käyttäjien käyttövaltuuksien hallinnan.

Identiteetin luomisen jälkeen se pitää pystyä todentamaan. Identiteetin todentaminen eli autentikointi tarkoittaa, että identiteetin ja henkilön välille luodaan kytkös, jonka avulla tietojärjestelmä pystyy varmistamaan henkilön. Identiteetin todentamiseen on erilaisia menetelmiä ja välineitä. Todentamiseen käytetyt menetelmät vaihtelevat luotettavuudeltaan. Mahdollisesti käytetyin todentamisen tapa on salasana tai PIN-koodi. Salasanan ja PIN-koodin luotettavuus ovat paljolti riippuvaisia käyttäjästä; liian heikko salasana tai salasanan kirjoittaminen paperille muistiin heikentää sen luotettavuutta merkittävästi. Salasana on kuitenkin helppo ja edullinen tapa toteuttaa autentikointi. Toimikorttien, toimivaimien, pankkikorttien tai muiden henkilöllä hallussa olevien laitteiden avulla todennuksesta on mahdollista tehdä salasanatodennusta luotettavampi. Niiden käyttämiseen kuitenkin tarvitaan usein muita laitteita ja se aiheuttaa lisäkustannuksia ja on käyttäjän kannalta hankalampaa. Biometrinen tunnistus perustuu johonkin ihmisen yksilölliseen ominaisuuteen, kuten sormenjälkeen. Yleisesti autentikointia pidetään vahvana, jos vähintään kaksi turvatekijää eri ryhmistä on käytössä samaan aikaan. [4.]

#### 4.2 Identiteetin- ja pääsynhallinnan hyödyt

Identiteetin- ja pääsynhallinnan avulla saavutetaan monia hyötyjä organisaatioissa. Toimivalla käyttövaltuusjärjestelmällä on mahdollista saavuttaa hyötyjä, jotka parantavat tietosuoja ja tietoturvan toteutumista sekä järjestelmän käyttäjäystävällisyyttä. Kuvassa 2 on esitetty käyttövaltuushallinnan hyötyjä. Hyötyjä ovat luottamuksellisuus ja kiistämättömyys, vaatimusten mukainen hallinta, turvallisuus, asiakastyytyväisyys ja luottamus, laatu sekä keskitetty hallinta. [25.]



Kuva 2. Identiteetin- ja pääsynhallinnan hyödyt [25].

Pääsynhallinnan ollessa suunnitelmallista ja hallittua, sitä voidaan pitää luottamuksellisena. Autentikoinnin kulkiessa käyttövaltuusjärjestelmän kautta kaikkiin järjestelmiin oikeuksien luottamuksellisuus paranee entisestään. Identiteetin- ja pääsynhallinnan seuraaminen ja raportointi lisäävät järjestelmän kiistämättömyyttä. Raportoinnin avulla käyttöoikeuksia on mahdollista seurata vaivattomammin. Vaatimusten mukaisessa hallinnassa huomioidaan organisaation vaatimukset käyttövaltuusjärjestelmän valinnassa ja muokkaamisessa sekä toteutetaan EU:n tietosuoja-asetuksen ja muun tietosuojalainsäädännön määäämiä vaatimuksia. [25.]

Käyttövaltuusjärjestelmän käyttö tuo prosessien ja toimintojen automatisoinnilla lisäturvaa tietojenkäsittelyyn. Ylläpitäjien määrää on mahdollista vähentää ja inhimillisten virheiden mahdollisuus pienenee. Järjestelmän käytöllä tietosuojan taso paranee. Käyttäjälle käyttövaltuusjärjestelmän hyödyntäminen organisaatiossa tuo turvaa käytäntöjen parantumiselle ja yhtenäistymisellä, jolloin tiedot ja oikeudet ovat luotettavammin ajan tasalla. [25.]

Käyttövaltuusjärjestelmä lisää asiakastyytyväisyyttä palveluiden helpottumisena. Se myös lisää luottamusta järjestelmiin. Käyttövaltuusjärjestelmän avulla esimerkiksi esimiehen tehtävät helpottuvat. Tietosuojalainsäädännön mukaisesti käyttäjä voi pyytää

selvityksen omista tiedoistaan, jotka ovat tallennettuna järjestelmiin. Tietojen läpinäkyvyys lisää luottamusta järjestelmän toimintaan. [25.]

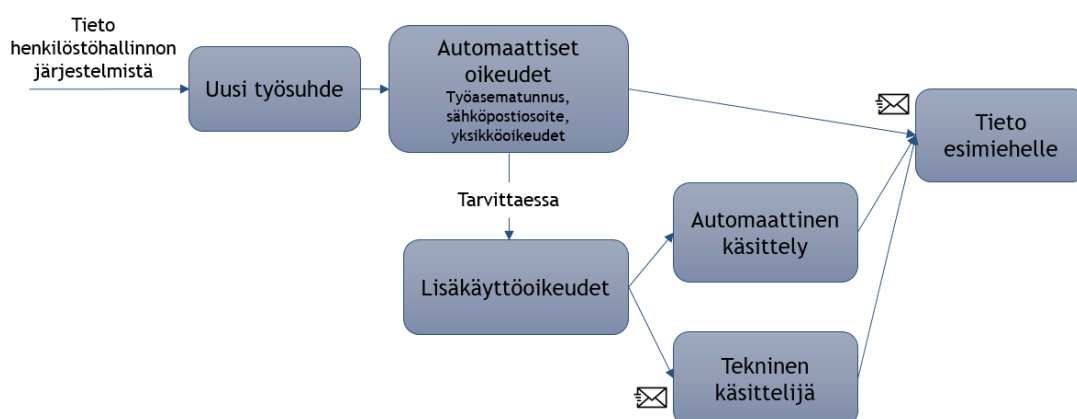
Laatu on käyttäjille tärkein kriteeri arvioitaessa käyttövaltuusjärjestelmää. Järjestelmän käytettävyyden on yksi sen tärkeimmistä ominaisuuksista käyttäjän näkökulmasta. Keskitetty hallinta nopeuttaa ja parantaa tiedonsaantia ja ongelmatilanteiden hallitsemista. Keskitetyn hallinnoinnin avulla identiteetteihin on mahdollista tehdä sujuvasti muutoksia. [25.]

#### 4.3 Käyttövaltuushallintajärjestelmä

Toimiakseen käyttövaltuushallintajärjestelmät vaativat tietoja muilta järjestelmiltä, usein tiedot käyttövaltuusjärjestelmään tulevat organisaation henkilöstöhallinnon järjestelmien kautta. Työsuhteen alkaessa henkilön uusi työsuhte luodaan henkilöstöhallinnon järjestelmään, jonka tietojen perusteella käyttövaltuusjärjestelmä luo henkilölle identiteetin ja luo identiteetille työasemien käyttäjätunnuksen ja sähköpostiosoitteen. Käyttäjätunnukseen liitetään usein automaattisesti työntekijän yksikön mukaan käyttöoikeuksia. Muut tarvittavat oikeudet esimies tai työntekijä itse hakevat järjestelmän käyttöliittymän kautta. [26, s.120-122.]

Järjestelmän luotua uuden tunnuksen, tieto tunnuksesta lähetetään työntekijän esimiehelle ja esimies pääsee hakemaan työssä tarvittavat lisäoikeudet sekä oikeuksien hyväksymisen jälkeen luovuttamaan ne työntekijälle. Määräaikaisen työsuhteen jatkuminen tai muut työsuhdetta koskevat muutokset päivittyvät automaattisesti henkilöstöhallinnon järjestelmästä ja työsuhteen päättyessä kokonaan käyttövaltuusjärjestelmä saa siitä tiedon, jolloin lopettaneen tunnus suljetaan ja tarvittavat poistopyynnöt käyttöoikeuksista ilmoitetaan eteenpäin. [26, s.120-122.]

Sairaanhoitopiirin käyttövaltuusjärjestelmä toimii perinteisen käyttövaltuushallintajärjestelmän tavoin. Kuvassa 3 on kuvattu uuden työntekijän identiteetin ja käyttöoikeuksien hallinnointi työsuhteen alkaessa, alkaen uuden työsuhteen välittymisestä käyttövaltuusjärjestelmään.

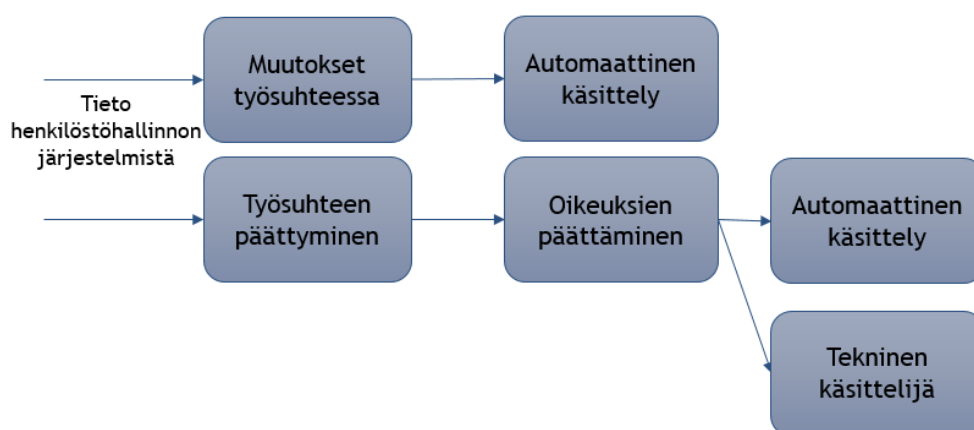


Kuva 3. Uuden työntekijän käyttöoikeuksien hallinnointi

Tieto uudesta työsuhteesta välittyy henkilöstöhallinnon järjestelmästä käyttövaltuusjärjestelmään, jolloin käyttövaltuusjärjestelmä luo työntekijälle uuden identiteetin. Identiteetille lisätään työasematunnus, sähköpostiosoite ja määritettyjä lisäoikeuksia työntekijän yksikön mukaan. Organisaation sisällä yksiköjen väliset oikeudet vaihtelevat työtehtävien mukaan. Loput työssä tarvittavat oikeudet, kuten potilastietojärjestelmän ja muiden järjestelmien käyttöoikeudet sekä yksikkökohtaiset kansio-oikeudet, esimies hakee ennen työsuhteen alkua tai heti sen alkaessa. Työntekijä voi työsuhteen alettua tarvittaessa itse hakea uusia oikeuksia, jolloin pyyntö käyttöoikeuksista menee ensin esimiehen hyväksyttäväksi. Esimiehen hyväksynnällä pyritään rajoittamaan turhien oikeuksien käsittelyä.

Manuaalisesti lisättävien oikeuksien pyynnöt, eli käytännössä muiden järjestelmien käyttöoikeudet, järjestelmä ilmoittaa määrätuille teknisille käsittelijöille. Tekninen käsittelijä on usein kohdejärjestelmän pääkäyttäjä, jonka vastuulla on järjestelmän oikeuksien hallinnointi. Pyyntöön saatuaan tekninen käsittelijä lisää tunnuksen tai oikeuden kohdejärjestelmään ja vahvistaa sen lisäyksen käyttövaltuusjärjestelmään. Vahvistus käyttöoikeuksista toimitetaan esimiehen tai oikeutta hakeneen henkilön sähköpostiin. Sähköpostista käy ilmi tarvittavat tiedot kohdejärjestelmään kirjautumiseen.

Käyttövaltuusjärjestelmä muuttaa työntekijän identiteettiä järjestelmässä henkilöstöhallinnon järjestelmistä saatavien tietojen mukaisesti. Kuvassa 4 on havainnollistettu mahdollisia muutoksia, joita henkilöstöhallinnon järjestelmistä voi identiteetille tulla. Muutokset voivat koskea joko työsuhteen muutoksia, jotka järjestelmä käsittelee automaattisesti, tai työsuhteen päättymistä, joka käsitellään osin manuaalisesti teknisten käsittelijöiden osalta ja osin automaattisesti järjestelmän osalta.



Kuva 4. Työsuhteen muutoksien käsittely järjestelmässä

Ideaalisti toimiessaan järjestelmä huomioi työsuhteella tapahtuneet muutokset, esimerkiksi vaihtuneen yksikön tai määräaikaisen työsuhteen jatkoon ja käsittelee tiedon automaattisesti. Tieto työsuhteen päättymisestä käsitellään käyttöoikeuskohtaisesti joko järjestelmässä automaattisesti tai lähettämällä tieto päättyneestä työsuhteesta toisen järjestelmän tekniselle käsittelijälle, joka päättää tunnuksen tai käyttöoikeuden kohdejärjestelmässä.

Käyttövaltuusjärjestelmässä on organisaatiokohtaisesti pyritty huomioimaan sosiaali- ja terveysalan erityistilanteita, kuten päällekkäiset työsuhteet organisaation sisällä ja jatkuvien keikkalaisten tunnuksien ja käyttöoikeuksien hallinta. Niiden käsittely poikkeaa jonkin verran muiden työsuhteiden käsittelystä käyttövaltuusjärjestelmässä. Muutoksien avulla on helpotettu käyttöoikeuksien hallintaa edellä mainituissa tilanteissa.

## 5 Työn tavoitteet

### 5.1 Työn tavoitteiden rajaus

Idea opinnäytetyön aiheeseen lähti käyttövaltuusjärjestelmän päivittäisessä käytössä ilmenneistä ongelmatilanteista ja työtä suunniteltaessa listattiin käyttöä vaikeuttavia tilanteita sekä toivottuja sisällöllisiä päivityksiä, joita järjestelmä kaipasi. Suurimmaksi ongelmaksi toiminnan kannalta todettiin järjestelmään auki jääneet identiteetit eli työsuhteiden loputtua ja työntekijän lähdettyä organisaatiosta, järjestelmän kautta annetut käyttöoikeudet eivät sulkeutuneet toivotusti. Tähän päätettiin suunnata suurin huomio työosuudesta. Ylimääräisten identiteettien kasaantuminen lisää turhaan järjestelmän käyttökustannuksia ja saattaa vaarantaa organisaation tietoturvallisuutta. Opinnäytetyön yksi pää-tavoitteista oli ylimääräisten identiteettien poistaminen järjestelmästä järjestelmän tuen kanssa yhteistyössä mahdollisuuksien mukaan joko järjestelmän toimintaa muuttamalla tai poistamalla tiedot manuaalisesti.

Toiseksi tavoitteeksi opinnäytetyötä suunnitellessa valittiin käyttövaltuusjärjestelmän sisällöllinen päivittäminen. Sisällön päivittämisen tavoitteena oli poistaa vanhentuneet tai tarpeettomat käyttöoikeudet ja lisätä järjestelmään haettavaksi tarvittavat kansio- ja järjestelmäoikeudet, jotka sieltä puuttuivat. Puuttuvat oikeudet ja muuttunut kansiorakenne aiheutti päivittäin oikeuksien käsittelyä ja hallinnointia järjestelmän ulkopuolella, jolloin tieto käyttöoikeuksista käyttövaltuusjärjestelmässä ei vastannut todellisuutta eikä niitä pystynyt luotettavasti seuraamaan tai auditoimaan.

Suunniteltaessa työtä päätettiin kirjata kehitysideoita, joilla käyttövaltuusjärjestelmän toimintaa ja käyttövaltuuksien hallinnointia saataisiin parannettua, jos niitä tulisi esille. Kehitysideat kirjattiin työhön omaksi osuudekseen, mutta niitä ei opinnäytetyön aikataulun puitteissa lähdetty toteuttamaan.



## 5.2 Käyttövaltuushallinnon ongelmatilanteita

Käyttövaltuusjärjestelmän päivittäisessä käytössä oli havaittu joitakin ongelmatilanteita, joita opinnäytetyön aikana pyrittiin selvittämään tarkemmin. Käyttövaltuusjärjestelmän toimintaan kuuluu käyttöoikeuksien kopioituminen työsuhteelta toiselle. Järjestelmää käyttöön ottaessa ei oltu tarpeeksi huomioitu organisaation toimintatapoja, joihin kuuluu, että samalla työntekijällä voi olla avoimena useampi työsuhde. Käyttövaltuusjärjestelmä tulkitsee jokaisen työsuhteen omaksi identiteetiksi. Järjestelmän toimintaan kuuluu, että se kopioi käyttöoikeudet uudelle työsuhteelle edellisen päättyessä, mutta koska aikaisempi työsuhde saattaa jäädä avoimeksi, eivät käyttöoikeudet kopioitu uudelle työsuhteelle toivotusti.

Toinen ongelmatilanne, joka on kytköksissä edelliseen, muodostuu, kun henkilöstöhallinnon järjestelmien ja käyttövaltuusjärjestelmän välillä tiedot työsuhteiden muutoksista ja niiden päättymisistä eivät aina päivyty käyttövaltuusjärjestelmään. Tällöin käyttöoikeudet eivät ole aina ajan tasalla ja esimerkiksi joitakin yksikön käyttöoikeuksia saattaa jäädä puuttumaan työsuhteen muuttuessa. Myös esimerkiksi esimiestietoja on jäänyt päivittymättä, jolloin käyttöoikeuksien käsittely ja hyväksyminen on mennyt väärälle henkilölle. Osa työsuhteisiin ja käyttöoikeuksiin liittyvistä ongelmista todettiin aikaisessa vaiheessa johtuvan enemmän organisaation toimintatavoista ja alan hektisyydestä kuin käyttövaltuusjärjestelmän ongelmista.

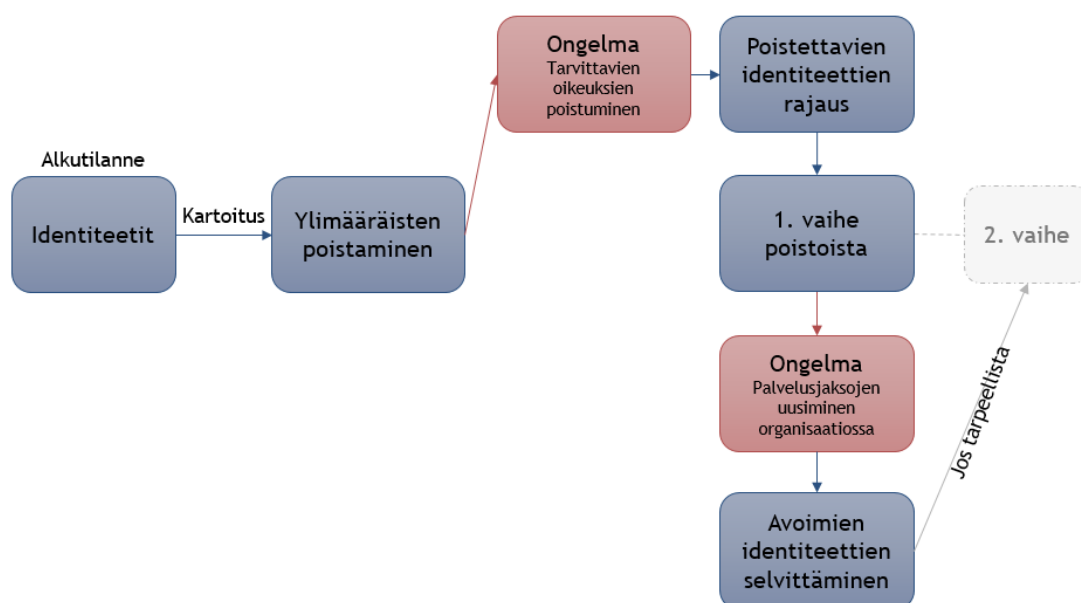
Kolmas työtä aloittaessa tiedossa ollut ongelmakohta käyttövaltuusjärjestelmän toiminnassa oli ulkopuolisten toimijoiden sekä keikkalaisten tai opiskelijoiden käyttöoikeuksien ja työsuhteiden hallinta. Käyttöoikeuksien hallinnoinnissa ei ollut selkeää toimintatapaa niiden myöntämiseen tai päättämiseen pääosin siksi, että työsuhteiden hallinnointi on jakautunut organisaatioiden yksiköihin eikä kukaan hallinnoi kokonaiskuvaa. Opinnäytetyössä on lyhyesti kirjattu kehittämis ehdotuksia käyttöoikeuksien hallintaan kyseisissä tapauksissa.

## 6 Sisällön päivittäminen

### 6.1 Ylimääräisten identiteettien poistaminen

Käyttövaltuusjärjestelmän sisällöllinen päivitys aloitettiin ylimääräisten identiteettien poistamisella järjestelmästä. Käyttövaltuusjärjestelmä lukee jokaisen työsuhteen omaksi identiteetikseen ja organisaation ja toimialan käytäntöjen mukaisesti yhdellä työntekijällä voi olla saman aikaisesti useampia voimassaolevia työsuhteita. Päällekkäisten työsuhteiden takia identiteettien määrä käyttövaltuusjärjestelmässä on suurempi kuin työntekijöiden määrä organisaatiossa. Tieto työsuhteista, uusista ja päättäneistä, tulee käyttövaltuusjärjestelmään henkilöstöhallinnon järjestelmistä automaattisesti.

Avoimet identiteetit aiheuttavat lisäkustannuksia organisaatiolle järjestelmän kustannusten muodossa ja esimerkiksi turhien lisenssien maksuissa. Ylimääräisissä käyttöoikeuksissa on aina tietoturvariskin mahdollisuus. Identiteettien kerääntymisen käyttövaltuusjärjestelmään aiheuttaa aiemmin mainittu työsuhdetietojen päivittyminen henkilöstöhallinnon järjestelmistä, joka ei syystä tai toisesta toimi oikein. Kuvassa 5 on esitetty työvaiheet identiteettien poistamisissa. Alkuperäisen hyvin suoraviivaisen suunnitelman mukaan kaikki identiteetit oli tarkoitus poistaa kerralla vertaillen käyttövaltuusjärjestelmän tietoja ja henkilöstöhallinnon järjestelmien tietoja keskenään.



Kuva 5. Identiteettien poistojen työvaiheet

Työn alussa identiteettien määrä ja kokonaistilanne pyrittiin arvioimaan järjestelmän tuen avulla. Avoimia identiteettejä vertailtiin henkilöstöhallinnon kautta saatuihin työsuhtetietoihin ja ylimääräisiä työsuhteita alettiin vertailun perusteella suunnitelman mukaan poistaa käyttövaltuusjärjestelmästä. Ensimmäinen ongelma identiteettien poistoissa havaittiin nopeasti, sillä käyttöoikeuksien puutteellinen kopioituminen aiheutti monia turhia poistopyyntöjä ja henkilöstön käyttöoikeuksien poistumisia, jonka takia identiteettien poistaminen lopetettiin nopeasti asian selvittämiseksi. Järjestelmän tuen kanssa selvitettiin mistä ongelma voisi johtua ja päätettiin identiteetit, joiden poistaminen oli turvallista ilman, että se vaikutti henkilöstön työskentelyyn. Nämä 1. vaiheen poistot onnistuivat hyvin, mutta identiteettien poistaminen oli suunniteltua hitaampaa kahden järjestelmän tietoja vertailtaessa. Etukäteen päätettyjen niin sanottujen turvallisten identiteettienkin poistot aiheuttivat poistopyyntöjä ja niistä johtuvia kyselyjä teknisten käsittelijöiden ja esimiesten osalta, mutta työ saatiin suoritettua loppuun päätettyjen identiteettien osalta. Ensimmäisellä kierroksella identiteettejä poistettiin noin 6% kokonaismäärästä. Ensimmäisen vaiheen poistojen jälkeen tarkoitus oli kartoittaa loput poistettavista identiteeteistä ja niiden käsittelyä suunniteltiin yhdessä järjestelmän tuen kanssa. Todettiin, että tuki suorittaa käyttöoikeuksien kopioimisen kaikille identiteeteille, jolloin käyttöoikeudet

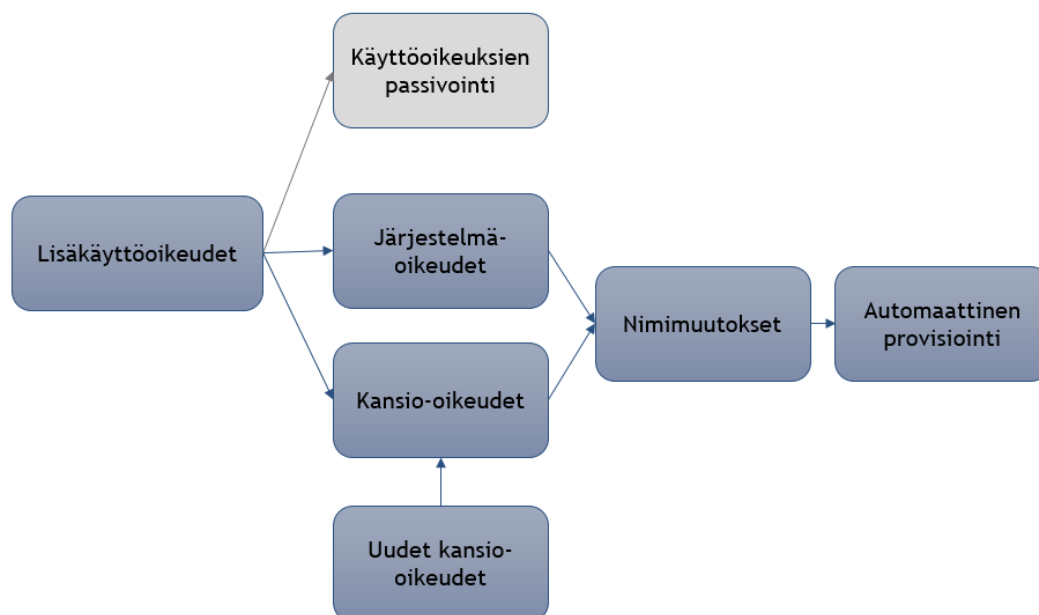
eivät katkeaisi poistoja suorittaessa. Kopioiminen suoritettiin, jotta loput ylimääräiset identiteetit päästäisiin poistamaan, mutta se ei poistanut ongelmaa ja poistot keskeytettiin.

Opinnäytetyön loppupuolella suurta osaa organisaation työntekijöistä koskeva työehtosopimuksen muutos osui identiteettien käsittelyä koskien erittäin huonoon kohtaan. Muutoksien takia suurelle osalle työntekijöitä aloitettiin uusi palvelusjakso ja edellinen päätettiin. Koska juurisyytä identiteettien kertymiselle ei ehditty ennen muutoksia selvittää ja korjata, uusien työjaksojen takia identiteettien määrä käyttövaltuusjärjestelmässä kasvoi reilusti alkuperäisestä ja työ palasi alkutekijöihin. Työsuhteiden muutokset eivät päivittyneet toivotusti käyttövaltuusjärjestelmään. Uuden palvelusjakson käyttövaltuusjärjestelmä täysin oikein tulkitsi uudeksi identiteetiksi, mutta tuntemattomasta syystä vanhat palvelusjaksot eli järjestelmässä identiteetit jäivät sulkeutumatta. Alkuperäisen suunnitelman 2. vaiheen sijaan päätettiin keskittyä uudempaan ongelmaan ja sen selvittämiseen, sillä kokonaisuuden kannalta sillä oli enemmän merkitystä identiteettien määrään. Uudempi ongelma oli myös helpompi hallita, sillä työsuhteilla oli yhteisenä tekijänä palvelusjakson loppumispäivämäärä. Henkilöstöhallinnon ja järjestelmän tuen kanssa yhteistyössä selvitettiin poistettavat identiteetit ja järjestelmän tuki suoritti niiden poistot erillisenä työpöytätyönä. Opinnäytetyön ajan puitteissa identiteettien poistoa ei ehditty suorittaa kokonaan loppuun, vaan suunnitellut 2. vaiheen poistot jäivät suorittamatta.

## 6.2 Lisäoikeuksien päivittäminen ajantasaiseksi

Käyttövaltuusjärjestelmän automaattisten toimintojen lisäksi järjestelmästä on haettavissa erikseen muita tarvittavia lisäkäyttöoikeuksia. Järjestelmän kautta haetaan oikeuksia muihin organisaation järjestelmiin sekä yhteiskäytössä oleviin kansioihin ja tiedostoihin. Organisaatiossa jaettavia käyttöoikeuksia on pystyttävä hallinnoimaan ja tarvittaessa auditoimaan. Järjestelmästä puuttuvat oikeudet hankaloittavat käyttöoikeuksien kokonaisuhallinnointia. Opinnäytetyössä keskityttiin lisäkäyttöoikeuksien päivittämiseen vanhentuneiden oikeuksien passivoimisella ja järjestelmäoikeuksien sekä kansio-oikeuksien päivittämisellä. Joitakin uusiakin kansio-oikeuksia lisättiin järjestelmään. Käyttövaltuusjärjestelmän sisällä lisäkäyttöoikeuksien muutokset koskivat lähinnä nimeä-

mistä ja oikeuksien automaattisen provisioinnin lisäämistä. Automaattinen provisiointi lisää käyttöoikeuteen tarvittavat käyttöoikeusryhmät automaattisesti käyttäjän työasema-tunnukselle. Kuvassa 6 on käyty läpi lisäkäyttöoikeuksia koskevat työvaiheet.



Kuva 6. Lisäkäyttöoikeuksien päivittämisen työvaiheet

Käyttövaltuusjärjestelmän sisällön päivitys aloitettiin vanhentuneiden ja ylimääräisten käyttöoikeuksien passivoimisella. Passivoitaessa käyttöoikeudet, ne jäivät käyttöön henkilöille, joille käyttöoikeus on aiemmin myönnetty, mutta uusia käyttöoikeuksia ei ole mahdollista hakea. Passivoidut käyttöoikeudet olivat pääasiassa kansio-oikeuksia, jotka organisaatiomuutosten takia eivät olleet enää käytössä. Käyttöoikeudet päätettiin passivoida poistamisen sijaan siksi, ettei kaikkien käyttöoikeuksien linkittymistä toisiinsa tiedetä eikä jonkin tarpeellisen oikeuden poistamisella haluttu vaikeuttaa henkilöstön toimintaa.

Työn aikana tarpeellisten kansio-oikeuksien nimeämisestä pyrittiin yhtenäistämään ja ryhmittelemään selkeämmin. Joitakin uusia kansio-oikeuksia lisättiin käyttövaltuusjärjestelmään työn aikana. Käyttöoikeuksien provisiointi oli jätetty monen oikeuden kohdalla ma-

nuaaliseksi, joten kansio-oikeuksien automaattinen provisiointi lisättiin kaikkiin oikeuksiin, joihin se oli mahdollista lisätä. Aiemmin tarvittava käyttöoikeus lisättiin manuaalisesti käyttäjän työasematunnukselle ja automatisoinnilla vähennetään manuaalisesti tehtävää työtä huomattavasti, järjestelmän käyttö on nopeampaa ja sujuvampaa eikä se sido järjestelmän pääkäyttäjää oikeuksien käsittelyyn. Automaattinen provisiointi myös poistaa käyttöoikeuden työasematunnukselta työsuhteen muuttuessa tai päättyessä.

Käyttövaltuusjärjestelmän kautta haettavat muiden järjestelmien oikeudet olivat pääosin kunnossa, joten niihin tehdyt muutokset olivat lähinnä automaattisen provisioinnin lisäämistä käyttöoikeuskäsittelyyn tai oikeuksien nimeämistä koskevia. Työn aikana järjestelmien päivittämiseen ei jo olemassa olevien oikeuksien muokkaamisen lisäksi ehditty keskittyä.

### 6.3 Kehitysehdotukset käyttövaltuusjärjestelmän toimintaan

Opinnäytetyötä suunniteltaessa päätettiin kirjata ylös kehitysideoita, joita työn aikana mahdollisesti tulisi esiin. Kehitysehdotuksia vastaanotettiin henkilöstön puolelta ja tietotekniikan puolelta, vaikkei mitään varsinaista kyselyä tehtykään. Palautteet koskivat järjestelmän päivittäisen käytön helpottamista ja käyttöoikeuksien haun selventämistä.

Henkilöstön puolelta kehitysehdotuksia tuli lisäoikeuksien haun selventämiseen. Opinnäytetyön aikana lisättiin haettavia lisäkäyttöoikeuksia järjestelmään, mutta kaikkia oikeuksia ei ole lisätty järjestelmään. Palautetta tuli myös käyttöoikeuksien ryhmittelyyn, kansiorakennetta järjestelmässä olisi hyvä kehittää esimerkiksi yksiköittäin tai muun yhdistävän tekijän perusteella. Myös nimeämisen samankaltaisuuteen on hyvä kiinnittää jatkossa huomiota, sillä nykyisin nimeämiskäytäntöjä on useita ja se vaikeuttaa tiettyjen oikeuksien hakemista luettelosta. Palautetta henkilöstön puolelta tuli myös sähköpostiryhmien käyttöoikeuksien hausta. Tällä hetkellä ryhmäsähköposteja ei hallita käyttövaltuusjärjestelmän kautta, vaan erikseen tietotekniikan kautta. Sähköpostiryhmiin liittyen myös turvapostien hallinnointi olisi hyvä lisätä käyttövaltuusjärjestelmään. Hallinnointikin olisi helpompaa, kun tiedot löytyvät samasta paikasta ja kun oikeuksien haku on yhtenäistä.

Tietotekniikkapalvelujen näkökulmasta käyttövaltuusjärjestelmän kehittämiseksi tulisi kiinnittää huomiota käyttövaltuuksien hallinnoinnin kokonaiskuvaan. Kaikki organisaatiossa olevat järjestelmät tulisi listata ja käyttövaltuuksien hallintaa pitäisi johdonmukaistaa organisaation sisällä. Hajanainen hallinnointi lisää tietoturvariskejä ja vaikeuttaa kokonais kuvan tarkastelua. Järjestelmien listaamisen lisäksi pääkäyttäjien ja järjestelmien tuen yhteystietojen kokoaminen yhteen paikkaan helpottaisi toimintaa ongelmatilanteissa. Käyttövaltuuksien hallinnointi vaatisi avoimempaa yhteistyötä eri yksiköiden välillä käytäntöjen yhtenäistämiseksi.

Käyttövaltuusjärjestelmän käyttämisen kannalta ohjeistukset järjestelmän käyttöön pitäisi saada ajan tasalle ja käyttövaltuusjärjestelmän olemassaolo paremmin henkilökunnan tietoisuuteen. Nykyisin osa käyttöoikeuksista haetaan järjestelmän kautta, osa tietotekniikkapalveluiden helpdeskin kautta ja käyttäjälle ei ole aina selvää mitä tapaa pitäisi käyttää. Henkilöstölle ei myöskään aktiivisesti tuoda esiin käyttövaltuusjärjestelmän toimintoja, joka myöskin työllistää helpdeskin työntekijöitä.

Käyttövaltuusjärjestelmän pääkäyttäjien kannalta käyttöoikeusryhmät pitäisi selkeyttää, esimerkiksi nimeämiskäytännöt ovat vaihtelevia. Päällekkäiset oikeudet pitäisi joko poistaa tai yhdistää tarpeen mukaan. Nykyisellään järjestelmän käyttö on pääkäyttäjille hitaampaa kuin käyttöoikeuksien lisääminen suoraan työasematunnukselle.

Käyttövaltuusjärjestelmän kehittämistä hidastaa tällä hetkellä päätös kilpailutetaanko nykyinen järjestelmä vai jatketaanko nykyisen kehittämistä. Ennen päätöstä järjestelmän toiminta päättynee takaisin päivittäiskäyttöön ja siihen kaavaillut toimintojen parantamiset odottavat tulevaisuutta.

#### 6.4 Jatkoehdotuksia käyttövaltuusjärjestelmän päivittämisprosessiin

Käyttövaltuusjärjestelmän päivittämistyön loppuunsaattamiseksi, loput identiteetit tulisi käydä läpi ja tarpeettomat poistaa tai päivittää. Järjestelmän tuen kanssa tulee selvittää, mistä identiteettien kertyminen johtuu ja mitä sen välttämiseksi vastaisuudessa tulee tehdä. On mahdollista, että ongelmat tietojen päivittämisessä johtuvat käyttövaltuusjär-

jestelmän omista asetuksista tai henkilöstöhallinnon järjestelmän ja käyttövaltuusjärjestelmän rajapinnasta, jolloin asian selvittäminen pitää laajentaa kummankin järjestelmän tuen ja tietotekniikkapalveluiden yhteistyöhön. Käyttövaltuusjärjestelmää olisi mahdollista kehittää ulkoisten työntekijöiden identiteettien ja käyttöoikeuksien hallintaan. Nykyisellään testikäytössä olevaa lisäosaa olisi mahdollista laajentaa koskemaan kaikkia ulkopuolisia työntekijöitä ja opiskelijoita, nykyisen pelkän opiskelijahallinnan lisäksi. Käyttövaltuuksien hallinnointi pitäisi myös saada samalle yksikölle kuin muu käyttöoikeushallinta tai yhteistyötä eri yksiköiden välillä parantaa.

Käyttövaltuusjärjestelmän sisällön päivittäminen jäi kesken. Päivittämisessä kannattaa kiinnittää huomiota palautteen perusteella oikeuksien ryhmittelyyn. Kansio-oikeuksia jäi puuttumaan suunnitellusta opinnäytetyön aikataulullisista syistä. Kun kansio-oikeudet ovat ajan tasalla, tulisi kiinnittää huomiota käyttöoikeusryhmien ja järjestelmän tietojen yhtenäisyyteen.

## 7 Yhteenveto

Opinnäytetyössä pyrittiin päivittämään ja selkeyttämään sairaanhoitopiirin käyttövaltuusjärjestelmän toimintaa. Suunnitelmana oli päivittää ja poistaa järjestelmän identiteetit, sekä niiden poistojen ohessa päivittää järjestelmän muuta sisältöä helpommin käytettäväksi. Käyttövaltuusjärjestelmän sisältöä päivitettiin käyttövaltuushaun osalta käyttövaltuuksien nimeämistä yhtenäistämällä ja ryhmittelemällä käyttövaltuuksia selkeämmiksi kokonaisuuksiksi. Työn aikana havaittiin, että käyttöoikeusryhmien hallinta on osittain hankalaa siksi, että ne ovat osittain päällekkäin, eri nimeämiskäytännöillä ja organisaatiomuutosten takia jääneet ylimääräiseksi tai yhdistämisen tarpeessa. Järjestelmäoikeuksien hallintaa vaikeuttaa se, että käyttöoikeuksia hallinnoidaan eri yksiköiden alla. Tästä johtuen esimerkiksi pääkäyttäjien ja järjestelmätukien yhteystiedot eivät ole kaikkien asian parissa työskentelevien tiedossa.

Opinnäytetyötä suunniteltaessa suurin huomio päätettiin suunnata identiteettien poistoon. Ilman työehtosopimusmuutoksia alkuperäinen suunnitelma olisi ollut mahdollista suorittaa aikataulun puitteissa. Muutokset kuitenkin hidastivat toimintaa, joten identiteet-



tien poistaminen jäi kesken. Lisätyön takia myös suunnitellut käyttöoikeuksien päivittämiset jäivät vähemmäksi kuin olisi ollut toivottua. Opinnäytetyön aikana vastaanotettiin palautetta henkilökunnan puolelta, joka kannattaa ottaa huomioon työtä jatkettaessa. Identiteettien hallinnointia kannattaa laajentaa myös ulkopuolisten toimijoiden ja opiskelijoiden sekä keikkailijoiden lisäämiseksi järjestelmään, jotta hallinnointi olisi yhtenäisempää.

Koska käyttövaltuushallinnointi ovat tärkeä organisaation toimintaa ja kytkeytyy vahvasti tietoturvan ja tietosuojan toteutumiseen, kannattaa organisaatioiden panostaa toimivaan käyttövaltuusprosessiin. Tietosuojalainsäädännön uudistuksien myötä, tietojärjestelmien tietoturvaa on syytä tarkastella uudelleen. EU:n yleinen tietosuoja-asetus ja tietosuoja-laki uudistavat tietosuojakäytäntöjä ja siten myös käyttövaltuusjärjestelmien käyttäjien tulee kiinnittää huomiota järjestelmän toimintaan. Käyttövaltuuksien hallinnointi parantaa tietosuojan toteutumista organisaatioissa.

## Lähteet

- 1 Rekrytointi. Verkkoaineisto. Kanta-Hämeen Keskussairaala. <<https://www.khshp.fi/rekry/>>. Luettu 15.9.2020.
- 2 Tietosuoja. Verkkoaineisto. Tietosuojavaltuutetun toimisto. <<https://tietosuoja.fi/tietosuoja>>. Luettu 15.9.2020.
- 3 Ruohonen, Mika. 2002. Tietoturva. 1. painos. Porvoo. Docendo.
- 4 Linden, Mikael. 2012. Identiteetin- ja pääsynhallinta. Tampereen teknillinen yliopisto. <[https://trepo.tuni.fi/bitstream/handle/10024/116698/linden\\_identiteetin\\_ja\\_paasynhallinta.pdf?sequence=1&isAllowed=y](https://trepo.tuni.fi/bitstream/handle/10024/116698/linden_identiteetin_ja_paasynhallinta.pdf?sequence=1&isAllowed=y)>. Luettu 25.10.2020.
- 5 Sairaanhoidopiirit ja erityisvastuualueet. Verkkoaineisto. Sosiaali- ja terveysministeriö. <<https://stm.fi/sairaanhoitopiirit-erityisvastuualueet>>. Luettu 15.9.2020.
- 6 Hallinto. Verkkoaineisto. Kanta-Hämeen Keskussairaala. <<https://www.khshp.fi/hallinto/>>. Luettu 15.9.2020.
- 7 Sinua kuunnellen. Verkkoaineisto. Kanta-Hämeen Keskussairaala. <<https://app.artcloud.fi/khshp/sinua-kuunnellen/>>. Luettu 30.11.2020.
- 8 Tietosuojalaki. 2019. Verkkoaineisto. Kuntaliitto. <<https://www.kuntaliitto.fi/laki/julkisuus-ja-tietosuoja/tietosuoja-asetus/tietosuojalaki>>. Luettu 18.10.2020.
- 9 Hakala, Mika; Vainio, Mika; Vuorinen, Olli. 2006. Tietoturvallisuuden käsikirja. 1.painos. Jyväskylä: Docendo.
- 10 Tietoturvapoliittikka. 2018. Verkkoaineisto. Kanta-Hämeen sairaanhoidopiirin ky. <[https://www.khshp.fi/wp-content/uploads/2018/05/Tietoturvapoliittikka\\_2018.pdf](https://www.khshp.fi/wp-content/uploads/2018/05/Tietoturvapoliittikka_2018.pdf)>. Luettu 19.10.2020.
- 11 Ollila, Maria. 2019. Tietoturvasuunnitelma pk-yritykselle. Opinnäytetyö. Oulun ammattikorkeakoulu. Theseus-tietokanta.
- 12 Ohjelmistoturvallisuus. Verkkoaineisto. Tietojesiturvaksi.fi. <<https://tietojesiturvaksi.fi/tietoturvasuunnitelma/ohjelmistoturvallisuus>>. Luettu 25.10.2020.
- 13 Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. 2016.

- 14 Korpisaari, Päivi; Pitkänen, Olli; Warma-Lehtinen, Eija. 2018. Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.
- 15 Turunen, Leila. 2017. Tietosuojavastaava Euroopan unionin yleisen tietosuojasetuksen mukaan. Opinnäytetyö. Saimaan ammattikorkeakoulu. Theseus-tietokanta.
- 16 Tietosuojasetus. Verkkoaineisto. Pro-pilvipalvelut. <<https://www.tietosuojasetus.org/>>. Luettu 19.10.2020
- 17 Oikeusministeriö. 2018. Uusi tietosuojalaki voimaan vuoden 2019 alusta. Verkkoaineisto. Oikeusministeriö. <<https://oikeusministerio.fi/-/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta>>. Luettu 20.10.2020
- 18 Tietosuojalaki. Verkkoaineisto. Tietosuojavaltuutetun toimisto. <<https://tietosuojafi.fi/tietosuojalaki>>. Luettu 20.10.2020.
- 19 Tietosuojavastaavat. Verkkoaineisto. Tietosuojavaltuutetun toimisto. <<https://tietosuojafi.fi/tietosuojavastaavat>>. Luettu 30.10.2020.
- 20 Työelämän tietosuojan käsikirja. Päivitetty 18.6.2020. Verkkoaineisto. Tietosuojavaltuutetun toimisto. <<https://tietosuojafi.fi/documents/6927448/8214540/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+2020+-+Tietosuojavaltuutetun+toimisto.pdf/3b506e9f-ae9a-c3fd-919a-df1c901ea6b8/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+2020+-+Tietosuojavaltuutetun+toimisto.pdf?t=1594205444944>>. Luettu 19.10.2020.
- 21 VAHTI. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. 2006. Valtiovarainministeriö. <[https://www.suomidigi.fi/sites/default/files/2020-06/main-book\\_9\\_2006.pdf](https://www.suomidigi.fi/sites/default/files/2020-06/main-book_9_2006.pdf)>. Luettu 20.9.2020.
- 22 Identiteetin ja pääsynhallinta (IAM). Verkkoaineisto. Itewiki. <<https://www.itewiki.fi/opas/kayttajahallinta-iam/>>. Luettu 20.10.2020.
- 23 Niemi, Jari. 2020. Case: Uuden käyttäjän identiteetti- ja käyttövaltuushallinnan kehittäminen organisaatiossa. Opinnäytetyö (YAMK). Laurea. Theseus-tietokanta.
- 24 Heikkinen Teemu. 2014. Identiteetinhallinnan käyttöönotto Kainuun ammatitopistossa. Kajaanin ammattikorkeakoulu. Opinnäytetyö.

- 25 Manninen, Kati. 2018. Identiteetin- ja pääsynhallintajärjestelmä sekä EU:n tietosuoja-asetus. Opinnäytetyö (YAMK). Lahden ammattikorkeakoulu. Theseus-tietokanta.
- 26 Andreasson, Ari. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.