LAPIN AMK
Lapland University of Applied Sciences

Lapin sairaanhoitopiirin käyttövaltuushallinnon käyttöönoton esimääritykset

Kreivi Markus
Koskiniemi Janne

Opinnäytetyö
Liikenteen ja tekniikanala
Tieto- ja viestintätekniikka
Insinööri (AMK)

2017

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Liikenteen ja tekniikanala
Tieto- ja viestintätekniikka
Insinööri (AMK)

Tekijät Markus Kreivi, Janne Koskiniemi Vuosi 2017
Ohjaaja Erkki Mattila
Toimeksiantaja Lapin sairaanhoitopiiri
Työn nimi Lapin sairaanhoitopiirin käyttövaltuushallinnon käyttöönoton esimääritykset
Sivu- ja liitesivumäärä 37

Opinnäytetyön tavoitteena oli luoda esimääritysdokumentaatiot Lapin sairaanhoitopiirin käyttövaltuushallinnon käyttöönottoa varten. Esimääritysdokumentaatiot koostuivat Lapin sairaanhoitopiirin toimintaympäristön kuvaamisesta prosessikuvina ja käyttövaltuushallinnon käyttöönottoon vaadittavasta vaatimusmäärittelydokumentaatiosta. Työn merkitys alalle on suuri, koska suurien hankintaprojektien yleisimpiä yksittäisiä syitä epäonnistumiseen ovat huonosti laaditut esiselvitykset ja niiden dokumentointi.

Opinnäytetyössä kohdattiin runsaasti haasteita. Keskeisimpänä ongelmana olivat Lapin sairaanhoitopiirin eri organisaatioyksiköiden ja niiden henkilöstöiden kiireet, jolloin tarvittavien tietojen saanti viivästyi.

Opinnäytetyö toteutettiin osana Lapin sairaanhoitopiirin IDM/IAM-projektia, sillä näiden tuloksien perusteella Lapin sairaanhoitopiirin käyttövaltuushallinto saatiin askeleen lähemmäs käyttöönottoa. Opinnäytetyössä tuotettujen dokumenttien avulla järjestelmän tuottaja määrittelee käyttövaltuushallintojärjestelmän Lapin sairaanhoitopiirin toimintaympäristön mukaiseksi.

Tutkimusaineistona käytettiin suurimmaksi osaksi Lapin sairaanhoitopiirin IDM/IAM-projektissa tuotettuja dokumentaatiota ja julkisille tahoille suunnattuja suosituksia. Koulutuksen tuoma tieto ohjelmistohankinnasta myös auttoi dokumentaatioiden tuottamista.

Opinnäytetyön tuotoksena saatiin hyväksyntää vaille olevat prosessikuvaukset Lapin sairaanhoitopiirin toimintaympäristöstä ja vaatimusmäärittelydokumentin alustava versio. Todettiin, että riittävän hyvin toteutettujen esimääritysdokumentaatioiden tuottaminen on erittäin työläs prosessi varsinkin suuressa organisaatiossa, joten siihen tulisi varata erittäin paljon resursseja.

Avainsanat IAM, IDM, prosessikuvaus, RBAC, vaatimusmäärittely

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Technology, Communication and Transport
Degree Programme in Information and Communication Technology
Bachelor of Engineering

Author Markus Kreivi, Janne Koskiniemi Year 2017
Supervisor Erkki Mattila
Commissioned by Lapland Hospital District
Subject of thesis Predefinitions of the Implementation of the Identity and Access Management System in Lapland Hospital District
Number of pages 37

The aim of this study was to create the predefinition documentations for the deployment of the Identity and Access Management System in Lapland Hospital District. The predefinition documentations consisted of describing the environment of the Lapland Hospital District as process pictures and the requirement specification documentation required to the deployment of the Identity and Access Management System. The significance of the work for the field is considerable, because the most common individual reasons of the large acquisition projects failures are poorly drawn and documented predefinition documents.

The study was carried out as a part of the IDM/IAM project in Lapland Hospital District. The basis of these results, the Identity and Access Management System was a step closer to deployment in the Lapland Hospital District. With the help of produced predefinition documents in the study the producer of the system defines the Identity and Access Management System to be in accordance with the environment of the Lapland Hospital District. Mostly the documentation that has been produced in the IDM/IAM project of the Lapland Hospital District and the recommendations directed to the public authorities were used as a research material.

The result of the study was the process descriptions without approval and the preliminary requirement specification document from the Lapland Hospital District environment. It is very laborious to produce the predefinition documentation in a large organization.

Key words IAM, IDM, process overview, RBAC, requirements engineering

SISÄLLYS

ALKUSANAT

Haluamme kiittää Lapin sairaanhoitopiirin tietohallintoa opinnäytetyön tehtävänannosta, opastuksesta ja ohjeistuksesta. Erityinen kiitos tietohallinnon Anne Pahtakarille ja Vesa-Matti Toloselle.

Haluamme kiittää myös Citrus Secure Identity Oy:n Peik Åströmmia kehitystyön avustamisesta ja yhteistyöstä. Erityisen suuri kiitos Citrus Solutions Oy:n Ilpo Mäntykankaalle prosessikuvausten kehitystyöstä ja konsultaatiosta.

KÄYTETYT TERMIT

AM	Access Management. Pääsynhallinta
DAC	Discretionary Access Control. Harkinnanvarainen pääsynhallinta
IAM	Identity and Access Management. Identiteetin ja pääsynhallinta
Identiteetti	sähköinen identiteetti, jonka avulla käyttäjä voidaan tunnistaa (VAHTI 2006, 43.)
IdM	Identity Management. Identiteetinhallinta
JHS	julkishallinnossa käytettäväksi tarkoitettu menettelytapa, määrittely tai ohje (JHS-suositukset 2017.)
MAC	Mandatory Access Control. Pakollinen pääsynhallinta malli
Provisiointi	käyttäjä- ja käyttövaltuustietojen välittäminen palvelujärjestelmiin (VAHTI 2006, 44.)
RBAC	Role-based Access Control. Roolipohjainen pääsynhallinta
Rooli	joukko käyttöoikeuksia ja valtuuksia

1 JOHDANTO

Opinnäytetyön toimeksiantona oli kartoittaa Lapin sairaanhoitopiirin toimintaympäristö prosessikuvauksiksi ja luoda vaatimusmäärittelydokumentaatio käyttövaltuushallintojärjestelmää varten. Toimeksiannon saimme Lapin sairaanhoitopiirin tietohallinnon palvelupäälliköltä. Esimääritysdokumentaation tarkoituksena oli selkeyttää IDM-järjestelmän tuottajalle, millä tavalla järjestelmän tulee toimia Lapin sairaanhoitopiirissä.

Esimääritysdokumentaatiota luodessamme hyödynsimme mahdollisimman tehokkaasti Lapin sairaanhoitopiirissä aiemmin tuotettuja käyttövaltuushallintoon liittyviä dokumentaatioita, jotka oli tuotettu käyttövaltuushallintojärjestelmän käyttöönottoprojektissa (IDM/IAM-projekti).

Opinnäytetyön teoriaosuudessa käsitellään käyttövaltuushallinnon toimintaperiaatetta hyvinkin ylätasolla, ilman tarkempaa kuvantamista käyttövaltuushallinnon toiminnasta teknisesti. Teoriaosuudessa tutustutaan myös roolipohjaisen pääsynhallinnanmalliin RBAC, jolla tullaan toteuttamaan pääsynhallinta Lapin sairaanhoitopiirissä. Teoriaosuudessa käsitellään myös prosessikuvausten tarkoitusperää ja vaatimusmäärittelyiden tarkoitusta.

Tämän opinnäytetyön kohde organisaationa on Lapin sairaanhoitopiiri. Lapin sairaanhoitopiiri on 15 kunnan yhteisomistuksessa. Lapin sairaanhoitopiiri vastaa kuntiensa väestön perusterveydenhuollon lisäksi sosiaalihuollosta, erikoissairaanhoidosta, sekä päihdeongelmaisten hoidosta ja kuntoutuksesta. Lapin sairaanhoitopiirissä työskentelee vakituisesti 1642 henkilöä, joista suurin osa työskentelee hoito- ja tutkimushenkilöinä (v. 2016). Lapin keskussairaala sijaitsee Rovaniemellä. (Lapin sairaanhoitopiiri 2015.)

Nykyään Lapin sairaanhoitopiirissä on käytössä useita kymmeniä eri järjestelmiä, joista tärkeimmät ovat noin kymmenen pääjärjestelmää. Käyttövaltuushallinnolla saadaan sisäisten, että ulkoisten käyttäjien tiedot ajantasaiseen seurantaan. Se tarjoaa myös työkalut prosessin eri osapuolille käyttövaltuuksien hallitsemiseen ja seurantaan omasta näkökulmasta. Käyttövaltuushallintojärjestelmän käyttöönottoprojekti on aloitettu Lapin sairaanhoitopiirissä v. 2013.

2 KÄYTTÖVALTUUKSIEN HALLINTA

Käyttövaltuushallinnolla (KVH) tarkoitetaan prosessia, jolla hallitaan identiteettejä ja käyttövaltuuksia. Synonyymina käytetään myös termiä identiteetin ja pääsynhallinta. Käyttövaltuushallinto koostuu identiteetinhallinnasta ja pääsynhallinnasta. (Linden ym. 2011, 84.)

2.1 Yleistä

Käyttövaltuushallinnon tehtävänä on varmistaa, että vain oikein todennetuilla käyttäjillä on pääsy niihin järjestelmiin ja informaatioon, joihin heillä on yrityksen tietoturvapolitiikan ja hallintotavan mukaisesti oikeus. Käänteisesti voidaan todeta, että käyttäjillä ei saa olla käyttöoikeuksia järjestelmiin, joita hän ei työssänsä tarvitse. (Kunnas 2013.)

Käyttövaltuushallinto on koko organisaation järjestelmäympäristön läpäisevä kontrolloitu prosessi, jolla hallitaan keskitetysti organisaation tietojärjestelmien käyttövaltuuksia ja identiteettejä. Käyttövaltuushallintoon kuuluu myös tärkeänä osana seuranta ja raportointi, joiden avulla pystytään valvomaan ja tarvittaessa selvittämään, mitä käyttövaltuuksia kenelläkin on, kuka on valtuuttanut käyttöoikeudet, sekä käyttöoikeuksien myöntämisen aikaleima. Käyttövaltuuksien kontrolloidun hallintaprosessin ja prosessia tukevien tietojärjestelmien avulla saadaan parannettua tietoisuutta käyttövaltuuksien vastuista ja velvollisuuksista, pienennettyä lisensseistä koituvia kustannuksia, vähennettyä käyttövaltuuksien hallinnan manuaalista työtä ja edistettyä tietoturvatasoa. (Kunnas 2013.)

Käyttövaltuushallinnon tavoitetila on, että jokaisen organisaation tietojärjestelmän käyttövaltuuksien hallinnointi tapahtuisi sen avulla. Tähän tavoitetilaan ei kuitenkaan yleensä päästä, eikä sitä tavoitella varsinkaan järjestelmän käyttöönoton alkuvaiheessa, koska kaikkien tietojärjestelmän käyttövaltuuksien hallinnan integrointi käyttövaltuushallintoon pitkittäisi käyttöönottovaihetta huomattavasti. (VAHTI 2006, 29–30.)

2.2 Nykyisen hallintatavan ongelmat

Alati kasvava tietojärjestelmien määrä organisaatioissa tuottaa haasteita käyttäjien ja käyttöoikeuksien hallinnassa. Varsinkin suurissa organisaatioissa tietojärjestelmien kokonaismäärä voi ylittää jopa sadan ja näistä jokaisessa käyttäjä- ja käyttövaltuustiedot on tallennettu, joko omiin hakemistoihin tai tietojärjestelmien tietokantaan. Lopulta saavutaan tilanteeseen, jossa käyttäjä- ja käyttövaltuustietojen hallinnointi on äärimmäisen resursseja kuluttavaa. (Rinnemaa 2006.)

Nykyään hyvinkin perinteinen vallitseva tapa hoitaa käyttövaltuuksien hallintaa perustuu huonosti määriteltyihin vastuisiin ja hallintaprosesseihin. Hyvinkin usein toimintojen ja tietojärjestelmien vastuussa olevat hallintayksiköt delegoivat käyttövaltuuksien hallinnan ja jopa omistajavastuunsa täysin organisaation tietohallinnolle. Käyttövaltuuksia saatetaan antaa henkilöille liian laajasti eikä niitä kontrolloida asianmukaisesti. Yleensä päädytäänkin tilanteeseen, jossa palveluksesta poistuneet tai eri tehtäviin siirtyneiden henkilöiden oikeudet jäävät voimaan tarpeettoman pitkään, koska voimassa olevien valtuuksien asianmukaisuutta ei valvota. Tämä aiheuttaa sen, että vanhojen käyttövaltuuksien väärinkäytön riski kasvaa huomattavasti. (VAHTI 2006, 9–10.)

Perinteinen käyttövaltuuksien hallinta on erittäin työläs ja virhealtis, koska valtuuksia hallitsevat manuaalisesti useat ylläpitäjät, lukuisissa eri tietojärjestelmissä. Käyttövaltuuksien hallinnassa ei ole kunnollista seurantaa myöntämis-, muutos- ja poistamistapahtumien osalta, eikä niiden hyväksyjistä tai hakijoista jää kunnollista seurantaa dokumentaatioihin. Mahdollisten riskien toteutuessa, ei perinteinen käyttövaltuushallinto mahdollista tekijöiden jäljitystä. (VAHTI 2006, 9–10.)

2.3 Käyttövaltuushallinnon rakenne

Käyttövaltuushallinnon rakenne voidaan jakaa seuraaviin prosesseihin:

- todentaminen
- valtuutus
- käyttäjien hallinta
- keskitetty käyttäjä- ja käyttövaltuustietovarasto (VAHTI 2006, 24.)

2.3.1 Todentaminen

Todennusprosessi koostuu todentamisen- ja sessionhallinnasta, jossa riittävät kirjautumistiedot syöttävä käyttäjä pystyy tunnistautumaan järjestelmään, jolloin hän saa käyttövaltuudet ohjelmistoihin ja resursseihin. Käyttäjän todennettua itsensä luodaan istunto, johon viitataan käyttäjän ja tietojärjestelmän välisessä vuorovaikutuksessa, kunnes istunto joko lopetetaan käyttäjän kirjauduttua ulos tai istunnon katkettua muista syistä. Todennusprosessissa on yleensä integroituna salasanoja hallitseva palvelumoduuli, kun käytetään perinteisestä käyttäjätunnuksen ja salasanan yhdistelmää. (Witty, Allan, Enck & Wagner 2003, 2–3.)

Keskitetysti ylläpitäen käyttäjän istuntoja, pystyy todennusprosessi tarjoamaan kertakirjautumispalvelun (SSO, Single Sign-On), jolloin käyttäjän ei tarvitse kirjautua sisään kuin yhden kerran käyttäessään toista sovellusta tai tietojärjestelmää. Tämä onnistuu sovelluksissa ja tietojärjestelmissä, joita hallitaan samalla käyttövaltuushallinnolla. Kertakirjautuminen on mahdollista laajentaa myös käyttövaltuushallinnon ulkopuolelle, mutta se vaatii erillisen sopimuksen ja rajapinnan käyttövaltuushallinnon ja ulkopuolisen järjestelmän välille. (Linden ym. 2011, 85.)

2.3.2 Valtuutus

Valtuutusprosessi määrittää onko käyttäjällä käyttövaltuudet käyttää tiettyjä resursseja tai tietojärjestelmiä. Valtuutus suoritetaan tarkistamalla resurssien käyttöoikeuspyynnöt ja vertaamalla niitä käyttövaltuushallinnon käyttövaltuuksien keskitettyyn käyttövaltuustietovarastoon. (VAHTI 2006, 27–28.)

Valtuutusprosessi on ydinprosessi, joka mahdollistaa myös roolipohjaisen pääsynvalvonnan toteutuksen. Se tarjoaa myös mahdollisuuden monimutkaisiin kulunvalvonnan rakenteisiin, jotka voivat perustua lukuisiin ominaisuuksiin. Näitä ovat muun muassa informaatio, käytännöt, käyttäjien attribuutit, roolit ja pyydetyt resurssit. (VAHTI 2006, 27–28.)

2.3.3 Käyttäjien hallinta

Käyttäjähallintaprosessi koostuu käyttäjien-, salasanojen-, roolien- ja ryhmien hallinnoinnista, sekä käyttäjien ja ryhmien provisioinnista. Prosessi määrittelee hallinnollisten toimintojen tehtävät, joita ovat identiteetin luominen ja eteneminen, sekä käyttäjien identiteettien ja käyttövaltuuksien hallinta. Sen yksi tärkeimmistä komponenteista on käyttäjän identiteetin elinkaaren hallinta, jonka avulla organisaatio pystyy hallitsemaan elinkaarta alkuperäisestä provisioinnista loppuun asti käyttövaltuuksien poistamiseen. (Witty ym. 2003, 3–4.)

Provisiointi on käyttäjien hallinnan osaprosessi, joka välittää käyttäjä- ja käyttövaltuustiedot käyttövaltuushallinnon piirissä oleviin tietojärjestelmiin automaattisesti. Se hoitaa hallintajärjestelmien luvitusprosessien läpi käyneet käyttövaltuustiedot kohdejärjestelmiin, joko heti niiden luontihetkenä tai ajastettuna. Provisiointi ei ole aina mahdollista toteuttaa, sen toteuttaminen on liian työlästä tai tietojärjestelmän käyttäjämäärä on niin vähäinen, että sen käyttöönotto ei ole kannattavaa. Tällöin käytetään yleensä manuaalista hallintatapaa, jossa muutostiedot välitetään salattuna esimerkiksi sähköpostilla tietojärjestelmien pääkäyttäjille, jotka aktivoivat käyttövaltuudet manuaalisesti. (VAHTI 2006, 26.)

Käyttövaltuushallinto tukee myös käyttäjien hallinnan delegointia, jonka avulla organisaatiot pystyvät jakamaan tehokkaasti käyttövaltuuksien ylläpitotehtävistä koituvia työkuormia niistä hallinnoiville yksiköille, täten vähentäen tietohallintoyksiköiden kokonaiskuormitusta. Itsepalvelu on myös yksi ratkaisevista tekijöistä työkuorman vähentämiseksi. Itsepalvelun avulla yritys hyötyy ajantasaisista tietojen päivityksistä ja henkilöllisyystietojen tarkasta ylläpidosta. Eniten työkuormaa vähentävä itsepalvelun osa on salasanojen palautustyökalu. (Witty ym. 2003, 3–4.)

Keskitetty käyttäjä- ja käyttövaltuustietovarasto on käyttäjähallintaprosessin ydin. Se on keskitetty tietovarasto, joka sisältää kaikki käyttäjien ja heidän eri tietojärjestelmissä olevien käyttövaltuuksien tiedot ja toimittaa niitä tarvittaessa muille palveluille, sekä tarjoaa palvelun lähetettyjen asiakkaiden tunnistetietojen varmistamiseksi. Käytännössä tietovarasto koostuu useista eri käyttäjähakemis-

toista, tietokannoista ja tiedostoista ja esittää yhteenvedon tai loogisen näkymän yrityksen käyttäjistä ja heidän identiteeteistä. (VAHTI 2006, 25.)

2.3.4 Jäljitettävyys- ja raportointitoiminnot

Käyttövaltuushallintoon kuuluu tärkeänä osana raportointitoiminnot. Yksinkertaisuudessaan kaikesta, mitä käyttövaltuushallinto sisältää tai käsittelee, tulee pystyä saamaan ajantasaiset raportit. Raportoinnin avulla pystytään, myös isomman mittakaavan käyttöoikeuksien seurannan lisäksi seuraamaan yksittäisiä käyttäjiä, sekä laajoja käyttövaltuuksia omaavia käyttäjätietoja. Käyttövaltuuksiin kohdistuvat muutostapahtumat tulee olla jäljitettävissä ja niistä tulee selvitä kaikki osalliset. (VAHTI 2006, 26–27.)

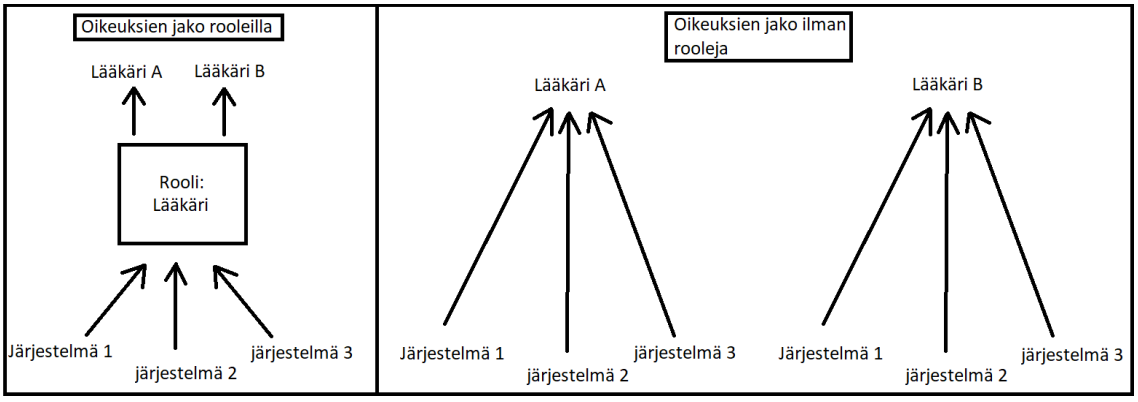
Käyttövaltuushallinnon tulee kirjoittaa lokitiedot kaikista luvitusprosessien tapahtumista, hallintajärjestelmään tehdyistä suorista muutoksista ja kohdejärjestelmiin välitetyistä tapahtumista, joiden avulla käyttövaltuuksien muutoksia ja käyttäjätietoja voidaan seurata. Käyttövaltuushallinnon tulee myös pystyä seuraamaan ja tarpeen vaatiessa varoittamaan, jos käyttäjätunnukset tai käyttöoikeudet ovat liian pitkään passiivisia. (VAHTI 2006, 26–27.)

3 PÄÄSYNHALLINTA

Tietojärjestelmät ovat suurentuneet ja monimutkaistuneet eri organisaatioissa vuosien aikana ja käytössä olevien tietojärjestelmien määrä organisaatiossa voi olla monia kymmeniä, ellei jopa satoja. Tämä on tuonut organisaatioihin monia eri haasteita toteuttaa tietojärjestelmien pääsynhallinta niin, että käyttäjillä on pääsy heille oikeutettuihin resursseihin. Näiden haasteiden ratkaisemiseen on luotu monia eri pääsynhallintamalleja, joista yksi käytetyimmistä on roolipohjainen pääsynhallinta RBAC, johon perehdymme tässä opinnäytetyössä.

3.1 Roolipohjainen pääsynhallinta

Roolipohjainen pääsynhallinta RBAC-käsite on saanut alkunsa 1970-luvulla, kun sovelluksien ja käyttäjien määrät ovat nousseet eri järjestelmissä. RBAC-mallissa käyttöoikeudet määritetään rooleille ja täten käyttäjä ei saa käyttöoikeuksia suoraan itsellensä, vaan käyttäjä sijoitetaan sopivaan roolin, josta käyttäjä saa esimääritetyt oikeudet ja valtuudet käyttöönsä (Kuvio 1). Tämä mahdollistaa sen, ettei jokaiselle käyttäjälle tarvitse lisätä oikeuksia erikseen, joka on kustannustehokkaampaa organisaation kannalta. Rooleille voidaan myöntää uusia käyttöoikeuksia ja valtuuksia, kun uusia laitteita tai sovelluksia lisätään järjestelmään. (Sandhu, Coynek, Feinsteink & Youmank 1996, 39–40.)



Kuvio 1. Oikeuksien jakaminen rooleilla, että ilman

RBAC-pääsynhallinnan yksi tärkeimmistä tavoitteista on helpottaa tietoturvan hallinnointia. RBAC-pääsynhallintamallia käyttämällä voidaan helposti seurata mitä oikeuksia ja valtuuksia käyttäjille on annettu järjestelmässä. (Sandhu ym. 1996, 39–40.)

Vuonna 1992 Ferraiola ja Kuhn toivat esille ensimmäisen RBAC-pääsynhallintamallin. Rooleihin perustuvalla pääsynhallintamallilla pyrittiin tuomaan parannusta aiemmin käytettyjen MAC- ja DAC-mallien tietoturva ongelmiin, teollisuus ja siviili ympäristöissä. MAC-malli perustuu turvallisuusetikettiin, jossa jokaiselle järjestelmän sisällä olevalle objektille annetaan turvaluokitus ja tätä verrataan käyttäjän luottamukselliseen tasoon. MAC-malli soveltuukin monitasoisen tietoturvallisuuden sisältämiin järjestelmiin, esimerkiksi puolustusvoimille. DAC-mallissa jokaisella objektilla on omistaja. Käyttäjä joka omistaa objektin, kontrolloi kenellä on oikeudet kyseiseen objektiin sekä päättää minkälainen oikeus, esimerkiksi: luku, kirjoitus tai muokkaus. DAC-mallia käytettiin teollisuuden ja siviilipuolen järjestelmissä. (Ferraiolo & Kuhn 1992, 1–2.)

3.2 Roolit

Roolien perusperiaatteena voidaan ajatella, että rooli on joukko käyttöoikeuksia ja valtuuksia. Roolilla voidaan kuvata tiettyä tehtävää organisaatiossa, kuten lääkäriä tai sairaanhoitajaa. Roolilla voidaan myös kuvata vastuuta tai auktoriteettia, kuten projektipäällikköä tai esimiestä. (Sandhu, Coynek, Feinsteink & Youmank 1995, 1–4.)

Esimerkiksi käyttäjä X voi saada roolin sairaanhoitaja, jolloin hän saa käyttöönsä esimääritetyt oikeudet ja valtuudet, johon on määritelty mitä kaikkia käyttöoikeuksia sairaanhoitajat tarvitsevat työkuvassaan. Tämä samainen käyttäjä X voi toimia myös projektipäällikkönä projektissa Y, jolloin hän saa myös roolin projektipäällikkö ja siihen sisältyvät oikeudet ja valtuudet. (Sandhu ym. 1995, 1–4.)

3.3 RBAC referenssimallit

Vuonna 1995 Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink ja Charles E. Youmank esittivät neljä RBAC-pääsynhallinnan referenssimallia: $Rbac_0$-, $Rbac_1$-, $Rbac_2$-, $Rbac_3$-mallit. (Sandhu ym. 1995, 5–6.)

$Rbac_0$-malli on perusta roolipohjaiselle pääsynhallinnalle, joka sisältää minimivaatimukset RBAC-pääsynhallinnalle. Perusmallissa kuvataan seuraavat peruskäsitteet: käyttäjät, roolit, käyttöoikeudet ja istunnot. Käyttäjät kuvaavat

RBAC-mallissa pääsääntöisesti ihmistä, mutta käyttäjällä voidaan myös kuvata muun muassa robotteja tai kiinteitä tietokoneita. Roolilla kuvataan oikeuksia ja valtuuksia, joita käyttäjät tarvitsevat suoriutuakseen työtehtävistään. Käyttöoikeudella kuvataan organisaatiossa olevaa tietojärjestelmää tai laitetta, jonka käyttämiseen käyttäjä tarvitsee luvan. Istunnolla kuvataan käyttäjän aktiivisena olevia rooleja. (Sandhu ym. 1995, 5–8.)

$Rbac_1$-malli tuo mukaan roolihierarkian. Mallissa roolit on organisoitu hierarkiarakenteeseen, jossa korkeamman aseman roolit perivät ominaisuudet matalamman tason rooleilta. Esimerkiksi käyttäjä X toimii erikoislääkärinä organisaatiossa ja organisaation roolihierarkiassa on määritelty, että rooli erikoislääkäri perii oikeudet roolilta lääkäri. Täten käyttäjä X saa käyttöönsä erikoislääkäri ja lääkäri -roolien sisältämät käyttöoikeudet ja valtuudet. (Sandhu ym. 1995, 8–9.)

$Rbac_2$-malli tuo mukanaan rajoitteet. $Rbac_2$-mallilla pyritään muodostamaan sääntöjä, ettei vaarallisia työyhdistelmiä pääse muodostumaan. Vaarallisiin työyhdistelmiin perehdymme tarkemmin luvussa 3.6. $Rbac_3$-malli tuo edellä mainitut $Rbac_0$-, $Rbac_{1-}$, $Rbac_2$-mallit yhteen. (Sandhu ym. 1995, 10–13.)

3.4 Roolien määrittely

Roolien määrittely on keskeinen osa käyttövaltuushallintoa, sillä rooleilla annetaan käyttäjille tarvittavat työkalut suoriutumaan työtehtävistä. Roolien avulla mahdollistetaan käyttöoikeuksien hallinta ryhmätasolla, täten käyttäjien oikeuksia tai velvollisuuksia ei tarvitse hallinnoida yksilötasolla. Käyttöoikeuksien ylläpitäminen on myös käytännöllisempää rooleilla, kuin yksilötasolla, sillä jos rooliin tehdään muutos tai uusi määrittely, se tulee voimaan jokaiselle rooliin asetetulle käyttäjälle. Roolien määrittely on suuri työ organisaatiossa ja se tarvitsee runsaasti suunnittelua sekä aikaa. Organisaation käyttäjien väliltä pyritään löytämään samankaltaisia työtehtäviä, joiden perusteella roolit määritellään. (Vahti 2006, 17–19.)

Onnistuneella roolien määrittelyllä saavutetaan organisaatiolle monia liiketoimintaa hyödyttäviä ominaisuuksia: käyttövaltuudet käyttäjille nopeammin ja vähemmällä työllä, käyttövaltuustietojen ymmärrettävyys ja selkeytyminen, sekä oikeuksien hallittavuus. (Kunnas 2013.)

3.5 Roolien louhinta

Roolien louhinnalla kuvataan prosessia, jossa käyttäjien ja järjestelmän käyttövaltuuksien välistä suhdetta analysoidaan ja näiden tietojen perusteella määritetään saatu informaatio roolimuodossa. Roolien louhinnalla käyttöoikeudet ja valtuudet saadaan koottua optimaalisesti määriteltyihin rooleihin, joka tukee organisaation liiketoimintaa, käyttövaltuuksien hallittavuutta ja kokonaisvaltaista tietoturvaa. (Kunnas 2013.)

Roolien louhinnassa kaksi yleisintä lähestymistapaa ovat Top-down- ja Bottom-up-menetelmät. Top-down-menetelmässä käyttäjien työtehtävät ja ominaisuudet analysoidaan, joiden perusteella tehdään roolimääritykset. Bottom-up-menetelmässä käyttäjien käyttövaltuudet järjestelmiin analysoidaan, joiden perusteella tehdään roolimääritykset. Näiden kahden edellä mainitun menettelytavan yhdistelmää kutsutaan hybridimalliksi. (Kunnas 2013.)

3.6 Vaaralliset työyhdistelmät

Vaarallisella työyhdistelmällä kuvataan sellaista tilannetta, jossa henkilö itse pystyy suorittamaan, sekä hyväksymään tekemänsä toimenpiteen. Vaarallisia työyhdistelmiä ovat esimerkiksi sellaiset tilanteet, jossa henkilö voi toimia laskun hyväksyjänä sekä maksajana. Kun käyttäjällä on käytössä monia eri rooleja, täytyy ottaa huomioon, ettei vaarallisia työyhdistelmiä pääse syntymään. (Kunnas 2013.)

Vaarallisten työyhdistelmien ennaltaehkäisy on tärkeää ja sen takia täytyy jo suunnitteluvaiheessa tiedostaa, minkälaisia mahdollisia vaarallisia työyhdistelmiä voi syntyä. Tämä tuottaa hankaluuksia pienissä organisaatioissa, sillä vaarallisten työyhdistelmien muodostumisille on suurempi riski, mitä vähemmän työntekijöitä on kyseisissä organisaatioissa. Jos vaarallisia työyhdistelmiä pääsee kuitenkin muodostumaan, on väärinkäyttöjen kannalta tärkeä tiedostaa tilanne ja varmistaa, ettei väärinkäyttöjä pääse tapahtumaan. (Kuntaliitto 2017, 1.)

Roolipohjaisessa pääsynhallinnassa vaarallisten työyhdistelmien estämiseksi voidaan asettaa rajoitteita rooleille. Esimerkiksi voidaan rajata tietty joukko rooleja, joista käyttäjä voi saada vain yhden roolin kerralla. (Sandhu ym. 1996, 44.)

4 PROSESSIKUVAUKSET

Prosessikuvauksilla on monia eri käyttötarkoituksia. Niitä voidaan käyttää muun muassa uuden työntekijän perehdyttämisessä, järjestelmien kehittämisen työkaluna tai esitysmateriaaleina eri tilaisuuksissa. Suurin käyttötarkoitus prosessikuvaksilla on kuitenkin hallita prosessit kokonaisuuksina. (JUHTA 2002, 1–3.)

Prosesseja kuvattaessa on hyvä pitää yhdenmukainen linja, sillä prosessikuvauksia käytetään organisaation eri tahoilla. Prosessikuvauksia suunniteltaessa ja piirtämisessä onkin hyvä esittää kysymys: miksi prosessi kuvataan ja millainen käyttötarkoitus kuvalla tulee olemaan. (JUHTA 2002, 3–4.)

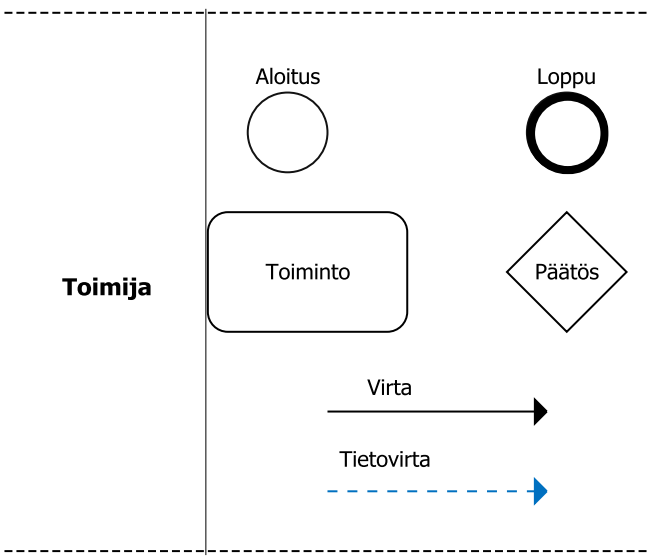
4.1 Prosessikuvausten taso

Prosesseja voidaan kuvata monella eri tasolla. Prosesseja voidaan kuvata hyvinkin yleiskatselmoidusti, jolloin jokaista prosessin pienintä yksityiskohtaa ei tarvitse kuvata omaksi toiminnoksi. Prosessit voidaan myös kuvata yksityiskohtaisesti, jolloin jokainen prosessin sisältämä tapahtuma pilkotaan omaksi toiminnoksi. Prosessikuvauksen taso määräytyy yleensä ottaen kuvauksen käyttötarkoituksesta. (JUHTA 2002, 5–6.)

JHS 152 -suosituksen mukaan prosessit voidaan jakaa neljään kuvaustasoon: prosessikartta, toimintamalli, prosessin kulku, ja työn kulku. Prosessikuvaustasoista ylimpänä toimii prosessikartta, jonka käyttötarkoituksena on kuvata organisaation kokonaiskuva, sisältäen tärkeimmät prosessit, yleiskuvauksen organisaatiosta ja sen toimintaympäristön. Seuraava prosessikuvaustaso on toimintamalli. Se kuvaa organisaation prosessihierarkian ja sitoo yhteen organisaation prosessit, tuoden esille prosesseihin vaikuttavat tekijät. Toimintamallista tarkempi kuvaustaso on prosessin kulku -taso. Prosessin kulku -taso on sisällöltään samanlainen kuin toimintamallitaso, mutta kuvaustaso on tarkempi. Se tuo mukanaan prosessiin kuuluvat työvaiheet, toiminnot ja toimijat yksityiskohtaisemmin esille. Tarkinta kuvaustasoa kutsutaan työn kuluksi. Tämän tason tarkoituksena on tuoda esille prosessien toimintojen välillä liikkuvan tiedon muoto. Työn kulku -tasolla kuvataan prosessin jokainen vaihe ja siihen liittyvät toimenpiteet. (JUHTA 2002, 6–10.)

4.2 Prosessikuvausten symbolit

Toimijan pääsääntöinen tehtävä on kuvata prosessin vastuualuetta (Kuvio 2.). Toimijalla voidaan kuvata jotain järjestelmää tai vastuuta, esimerkiksi hyväksyjää. Toimijaa nimettäessä on vältettävä käyttämästä käyttäjien työnimikkeitä, sillä käyttäjät voivat toimia prosessissa useina eri toimijoina. Prosessin aloitusta ja lopetusta kuvataan ympyrä-symbolilla, joista prosessin loppu on lihavoitu. Aloituksella kuvataan prosessin lähtökohtatilannetta ja lopetuksella kuvataan prosessin tulosta. Prosessin loppuja voi kuvauksissa olla monia, esimerkiksi jos prosessin aloituksena on: käyttäjä hakee muutoksia käyttöoikeuksiinsa. Loppuna tälle prosessille voi olla muun muassa: käyttöoikeuspyyntö ei toteuta tai käyttäjä saa uudet päivitetyt käyttöoikeudet. Toiminnolla kuvataan prosessin sisäisiä tapahtumia. Prosessin sisäisiä päätöksiä kuvataan salmiakkikuviolla. Päätöstä käytetään silloin, kun prosessin sisällä tapahtuu jonkinlainen haarautuma, joka tarvitsee päätöksen. Virran käyttötarkoituksena on yhdistää prosessin sisältämät tapahtumat, niiden suoritusjärjestyksessä. Virran symbolina käytetään yhtenäistä viivaa ja nuolta. Tietovirtaa käytetään silloin kun jokin tieto siirtyy prosessin kuuluvalta toimijalta toiselle. (JUHTA 2002, 11–12.)



Kuvio 2. Prosessikuvauksien symbolit

5 VAATIMUSMÄÄRITTELY

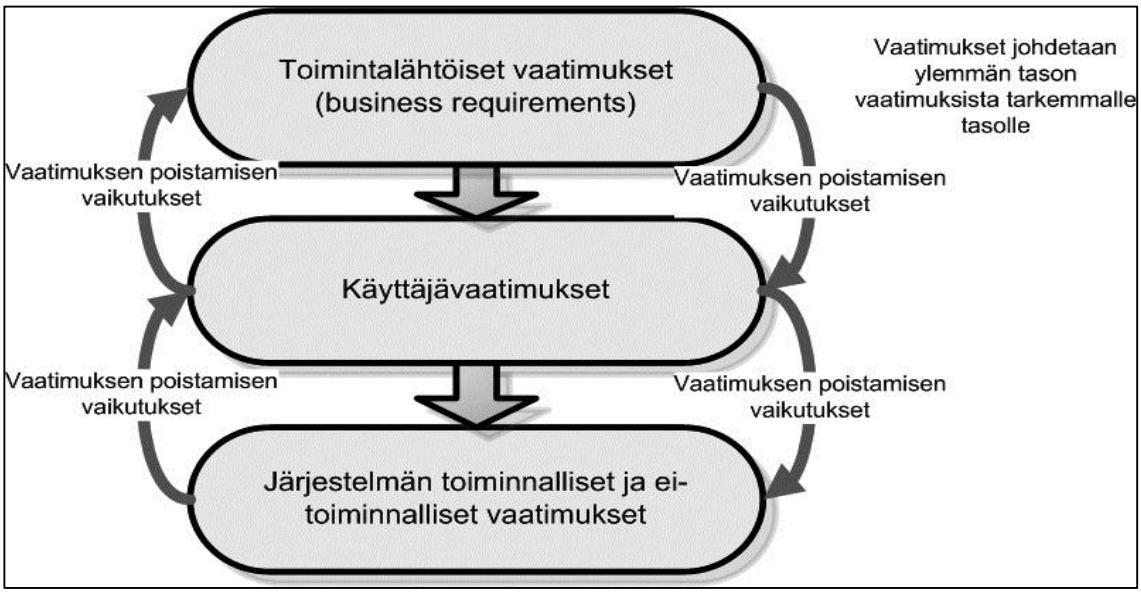
Vaatimusmäärittely on osa laajempaa kokonaisuutta, jota kutsutaan vaatimusten hallinnaksi. Vaatimusten hallinta kattaa kaikki työvaiheet tietojärjestelmien vaatimusten löytämisestä, niiden dokumentointiin ja ylläpitämiseen asti. Vaatimusmäärittely kattaa tästä järjestelmän, ohjelmiston tai palvelun vaatimusmäärittelyt, jossa listataan kaikki ominaisuudet, toiminnallisuudet ja rajoitteet hankittavalle järjestelmälle. (JUHTA 2009, 8.)

5.1 Yleistä

Vaatimusmäärittelyprosessi on olennainen osa ohjelmistohankinnan perustehtäviä. Sen tuotos vastaa kysymyksiin: miksi ja mitä ominaisuuksia hankittavan järjestelmän tulee sisältää ja mitä järjestelmältä vaaditaan. Vaatimusmäärittelyt eivät kuvaa järjestelmän toimintaa teknisellä tasolla. Vaatimusmäärittelyprosessissa syntyvät dokumentaatiot toimivat tilaajan ja järjestelmän toimittajan välisenä kivijalkana. Selkeästi ja kattavasti toteutetut vaatimukset vähentävät tilaajan riskiä hankittavan järjestelmän valinnassa ja käyttöönotossa, sekä varmistavat että hankittava järjestelmä tulee olemaan toiminnoiltaan ja ominaisuuksiltaan sellainen kuin tarvitaan. Hyvin toteutetuissa vaatimusmäärittelyissä on hahmoteltuna myös tulevaisuudessa toteutettavat toiminnallisuudet. (Kaskela 2005.)

Vaatimusmäärittelyprosessi on erittäin haastava ja resursseja kuluttava prosessi: mitä monimutkaisempi hankittava järjestelmä on, sitä enemmän siihen tulee varata resursseja. Hankintaprojektien yleisin yksittäinen syy epäonnistumiseen onkin huonosti toteutetut vaatimusten määrittelyt. Vaatimusmäärittelyprosessin epäonnistuminen tai huono toteutus voi johtua monesta eri syystä. Esimerkiksi vaatimusten keräämisestä vastaava taho ei välttämättä pääse yhteisymmärrykseen peruskäyttäjien kanssa, ohjelmiston tilaaja on yleensä eri kuin lopullista järjestelmää käyttävät tekijät tai tilaajan käsitys on poikkeava peruskäyttäjien vaatimuksista. Organisaatio voi aliarvioida vaatimustenmäärittelyyn tarvittavat resurssit, joka johtaa ongelmiin myöhemmissä vaiheissa järjestelmähankinnan vaiheissa, mahdollisesti heti järjestelmän käyttöönottovaiheessa. (JUHTA 2009, 9.)

Vaatimusmäärittelyt voidaan jaotella yleisesti ei-toiminnallisiin ja toiminnallisiin vaatimuksiin. JHS 173:ssa on laadittu kuitenkin kattavampi vaatimusmäärittelyiden jaottelu (Kuvio 3).



Kuvio 3. Vaatimusmäärittelyiden jaottelu (JUHTA 2009, 10)

Korkean tason tavoitteet eli **toimintalähtöiset vaatimukset** kuvaavat mitä organisaatio pyrkii saavuttamaan ohjelmiston tai järjestelmän hankinnalla. Usein ne perustuvat toimintaa kuvaaviin prosesseihin, joilla on kuvattu haluttu tavoitetila organisaatiossa. Toimintalähtöiset vaatimukset vastaavat kysymykseen mitä hankittavalta järjestelmältä tai ohjelmistolta halutaan ja miksi ylipäätään sen hankinta on tarpeellinen. Toimintalähtöisten vaatimuksien kuvaaminen tapahtuu yleensä projektin kokonaiskuvan näkemyksessä ja sen laajuuden tutkimisvaiheessa. (JUHTA 2009, 10.)

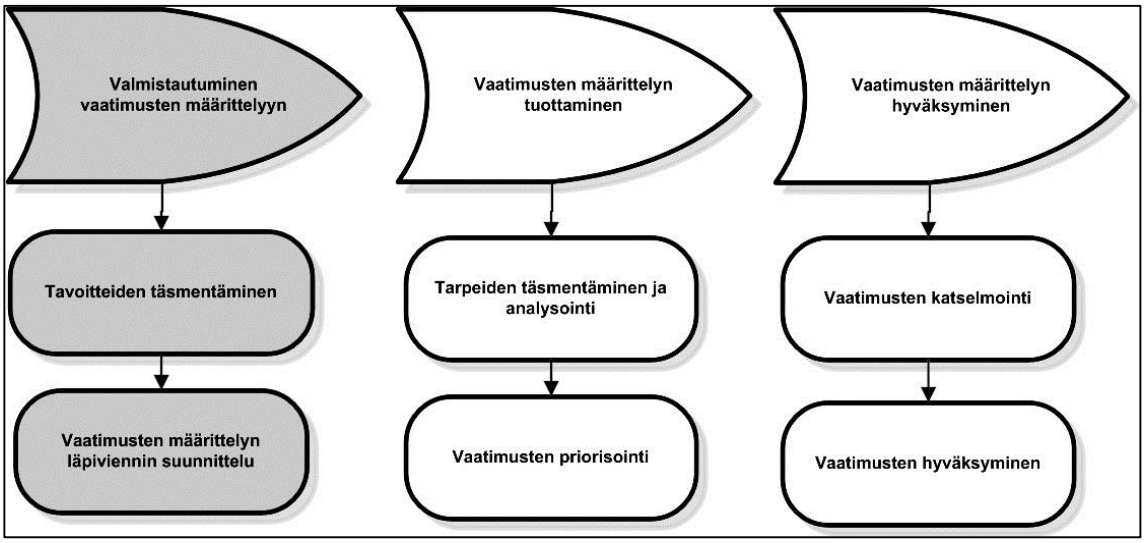
Käyttäjävaatimukset kuvaavat toimia ja toimintoja, joita järjestelmän käyttäjien pitää pystyä tekemään. Ne kuvataan yleensä käyttötapauksina tai käyttötapauskaavioina, joko esimerkki tapauksien tai hahmotelmien avulla. Käyttäjävaatimuksien vaihtoehtoinen nimitys on tarpeiden tunnistus, jonka avulla nykyisen järjestelmän ongelmat analysoidaan käytännön esimerkeillä. Hyvin tehty ja dokumentoitu kehitystarpeiden analysointi ja nykytilan ongelmien tunnistaminen antavat hyvän pohjan käyttäjävaatimuksien luonnille. Käyttäjävaatimuksien ja koko vaatimusmäärittelyprosessin teko hidastuu yleensä reilusti, jos esiselvitys-

vaiheessa ei ole toteutettu riittävän hyvin tai ollenkaan, nykytilan ongelmien tunnistamista ja kehitystarpeiden analysointia. (JUHTA 2009, 10.)

Järjestelmän vaatimuksilla määritellään järjestelmän toiminnallisuus. Järjestelmän vaatimukset jaotellaan yleensä **toiminnallisiin ja ei-toiminnallisiin vaatimuksiin**. Toiminnalliset vaatimukset vastaavat kysymykseen mitä järjestelmän tulisi pystyä tekemään ja miten tuleva järjestelmä vaikuttaa ympäristöönsä. Ei-toiminnallisilla vaatimuksilla määritetään ehtoja järjestelmälle, miten sen tulee täyttää järjestelmän toiminnalliset vaatimukset. Näitä ovat esimerkiksi luotettavuuteen, tietoturvallisuuteen ja käytettävyyteen liittyvät vaatimukset. (JUHTA 2009, 11.)

5.2 Vaatimusmäärittelyn vaiheet

Vaatimustenmäärittelyprosessi koostuu valmistautumis-, tuottamis- ja hyväksymisvaiheista (Kuvio 4). (JUHTA 2009, 11.)



Kuvio 4. Vaatimusmäärittelyprosessin vaiheet (JUHTA 2009, 11)

5.2.1 Valmistautuminen

Vaatimustenmäärittelyprosessi alkaa kehittämiskohteiden tunnistamisvaiheella. Riittävän tasoiset prosessikuvaukset tulisi olla piirrettynä hankittavasta järjestelmästä, ennen vaatimusmäärittelyprosessin aloittamista. Kehittämiskohteet ja niiden muokkaus vaatimuksiksi tukee koko järjestelmän hankinta- ja kehittämisprosessia pitkässä mittakaavassa. (JUHTA 2009, 11.)

Syy uuden tietojärjestelmän hankkimiselle selviää yleensä nykyisen tietojärjestelmän puutteen vuoksi, tietojärjestelmän vanhuuden vuoksi tai tietojärjestelmätutkimuksesta. Myös yleinen liiketoiminnan kehittäminen ja sen yhteydessä tehdyt tavoitetilaprosessit saattavat aloittaa vaatimustenmäärittelyprosessin. (Kaskela 2005.)

Tietojärjestelmää hankkivan organisaatiolla tulee olla selkeä näkemys siitä, mihin kyseistä järjestelmää tarvitaan. Alussa tunnistetut ongelmat ja puutteet eivät yleensä ole riittävän tarkkaan dokumentoitu, että järjestelmää voitaisiin niiden pohjalta lähteä toteuttamaan, joten tarve erilliselle vaatimusmäärittelyprosessille on olemassa. Vaatimusmäärittelylle muodostuu hyvä pohja kehittämiskohteiden tunnistuksessa huomatuista tarpeista ja esiselvitysvaiheessa niistä tarkennetuista käyttäjävaatimuksista. (JUHTA 2009, 11.)

5.2.2 Tuottaminen

Vaatimusmäärittelyiden tuottamisvaiheen lopputulos on saada eri osapuolien välille yhteinen ja aito näkemys hankittavasta tietojärjestelmästä, sekä sen toiminnasta. Organisaatioiden kiireiden, resurssipulien tai rahoituksen heikkouden vuoksi vaatimusmäärityksiä tehtäessä joudutaan tekemään usein eri tahojen välistä sovittelua ja jopa kompromisseja. Vaatimusmäärittelyiden onnistuminen vaatii organisaation ylimmän johdon sitoutumista ja riittävien resurssien varaamista sen työstöön, koska ilman niitä eri osapuolten välinen sovittelu on hyvin haastavaa. Vaatimusten määrittelyyn on erityisen suositeltavaa ottaa mukaan nykyisen järjestelmän käyttäjiä, koska he tietävät parhaiten peruskäyttäjän näkökulmasta tietojärjestelmän kehitystarpeista. Myös eri alueiden asiantuntijoita on hyvä käyttää apuna vaatimuksia määriteltäessä. (JUHTA 2009, 13–14.)

Vaatimusmäärittelyiden tuottamisvaiheeseen kuuluu olennaisesti vaatimuksien priorisointi eli tärkeysjärjestyksen luonti. Priorisointi on keskeinen järjestelmän hankinnan hallintatapa ajan, rahan ja ominaisuuksien suhteen. Priorisoinnin ohella on tärkeää ymmärtää, onko vaatimus nykyistä järjestelmää parantava ominaisuus vai onko se järjestelmän toiminnan kannalta välttämätön. (JUHTA 2009, 15.)

Vaatimusten priorisoinnissa on suositeltavaa pysyä yksinkertaisessa kokonaisuudessa. Esimerkiksi JHS:n suosittelema 3-tasoinen priorisointi koostuu seuraavan laisesti; 1 = pakollinen, 2 = hyödyllinen, 3 = toivottu. Vaatimusten tekijöiden ja dokumentoijien on otettava huomioon, etteivät kaikki vaatimukset ole pakollisia. Sellaisten vaatimuksien dokumentointi pakollisiksi, jotka eivät välttämättä ole tarpeellisia, suljetaan osa järjestelmän toimittajista pois mahdollisesta kilpailutuksesta. Vaatimukset ovat järjestelmän ominaisuuksia, joten mitä enemmän niitä on ja mitä monimutkaisempia ne ovat, sitä kalliimpi järjestelmän kokonaiskustannus tulee olemaan. (JUHTA 2009, 15.)

5.2.3 Hyväksyminen

Vaatimusmäärittelyiden hyväksymisellä varmistetaan vaatimusten laatu ja oikeellisuus. Määrittelyn hyväksymisessä käytetään yleensä apuna katselmointeja. Katselmoinnissa tuotetaan pöytäkirja, josta selviävät muutokset, läpikäydyt asiat, läsnäolijat, muutosten aikataulu ja vastuuhenkilö, sekä tärkeimpänä katselmoinnin tulos. Hyvin järjestetyssä katselmointitilaisuudessa päästään hyödyntämään asiakkaan näkökulmaa virheellisten vaatimusten havaitsemiseksi ja korjaamiseksi, sekä saadaan asiakkaalta hyväksyntä vaatimuksille. Asiakkaan hyväksyntä vaatimuksille sitouttaa asiakkaat ja sidosryhmät vaatimuksiin, sekä suunnitelmiin mahdollisten seurannaisvaikutuksien varalta. Katselmoinnissa keskitytään tarkastelemaan vaatimusten ymmärrettävyyttä, oikeellisuutta, yksiselitteisyyttä ja riittävää tarkkuutta. (JUHTA 2009, 15–16.)

Lopullisen hyväksynnän hyväksytyille vaatimusten määrittelydokumenteille antaa yleensä projektin ohjausryhmän vastaava tai tietojärjestelmän omistaja. Päätösselvityksen valmistelee yleensä projektipäällikkö. Päätöksentekijällä on valtuudet hyväksyä vaatimusmäärittely, keskeyttää se tai palauttaa se takaisin työstöryhmälle korjattavaksi. Vaatimukset vakiinnutetaan tietylle tasolle, joka toimii tarjouspyynnön pohjana. (JUHTA 2009, 15–16.)

6 ESIMÄÄRITTELYDOKUMENTAATIOT

6.1 Hankkeen tausta

Lapin sairaanhoitopiirissä IDM/IAM-projekti on aloitettu vuonna 2013. Projektilla on lähdetty tuomaan parannusta työntekijöiden oikeuksien ja valtuuksien hallittavuuteen, paremman tietoturvan saavuttamiseksi, taloudellisten kulujen vähentämiseksi, sekä selkeyttämään kokonaisvaltaista prosessia Lapin sairaanhoitopiirin ympäristössä. Lähtökohtana kehitettävälle käyttövaltuushallinnalle on tukea Lapin sairaanhoitopiirissä määritettyä hyvän hallinnointitavan toteutumista käyttövaltuushallinnan politiikan mukaisia periaatteita noudattaen. Käyttäjien identiteetit ja käyttöoikeudet eivät ole tällä hetkellä saatavilla keskitetyssä näkymässä. (Lapin sairaanhoitopiiri 2013.)

Tavoitteena projektille on saada keskitetty käyttövaltuuksien hallinta roolipohjaisesti IDM-järjestelmää käyttäen, jolla pystytään hallitsemaan kaikkien Lapin sairaanhoitopiirissä työskentelevien henkilöiden käyttöoikeuksia ja valtuuksia. Lapin sairaanhoitopiiriin ollaan tällä hetkellä tuomassa Citrus Secure Identity Oy:n tuottamaa IDM-järjestelmää, joka on nimeltään Datamaster. IDM-järjestelmällä pyritään toteuttamaan systemaattinen, yksinkertainen, joustava, sekä tehokas hallinnointimalli, jolla mahdollistetaan käyttöoikeuksien raportointi ja ylläpito tietoturvallisesti, sekä ajantasaisesti. Tavoitteena IDM-järjestelmällä on saada työntekijöiden tiedot kokonaisvaltaisen ja ajantasaisen seurannan piiriin, jolla helpotetaan käyttövaltuuksien hallitsemista, sekä seurantaa. (Lapin sairaanhoitopiiri 2013.)

Lapin sairaanhoitopiirin käyttöoikeushallinnan pääprosesseilla on tavoitteena hallita käyttäjien identiteettien luominen, käyttöoikeuksien hakeminen ja hyväksyminen, sekä niiden toteuttaminen käyttäjille. Työkuvan muuttuessa tähän kuuluu uusien käyttöoikeuksien hakeminen, hyväksyminen ja toteuttaminen, sekä vanhojen ja tarpeettomien käyttöoikeuksien poistaminen työsuhteen päättyessä. Järjestelmän tulee myös toteuttaa käyttäjien tunnistaminen, valtuuttaminen ja käytön seuranta asianmukaisesti. Järjestelmässä on myös toteutettava käyttöoikeuksien seuranta- ja hyväksymiskäytännöt vastuuhenkilöiden ja esimiesten osalta, sekä toteuttaa käyttöoikeuksien raportointi ja valvonta. Lapin sairaanhoi-

topiirissä työskentelee myös ulkoisia käyttäjiä. Ulkoisia käyttäjiä voivat olla esimerkiksi tutkijat, opiskelijat, vuokratyövoima ja palvelutoimittajien työntekijät. IDM-järjestelmän on pystyttävä varmistamaan heidän käyttöoikeuspyynnöt ja määräaikaisuus, sekä on myös voitava hallita, valvoa ja raportoida ulkoisten käyttäjien käyttöoikeuksia. (Lapin sairaanhoitopiiri 2013.)

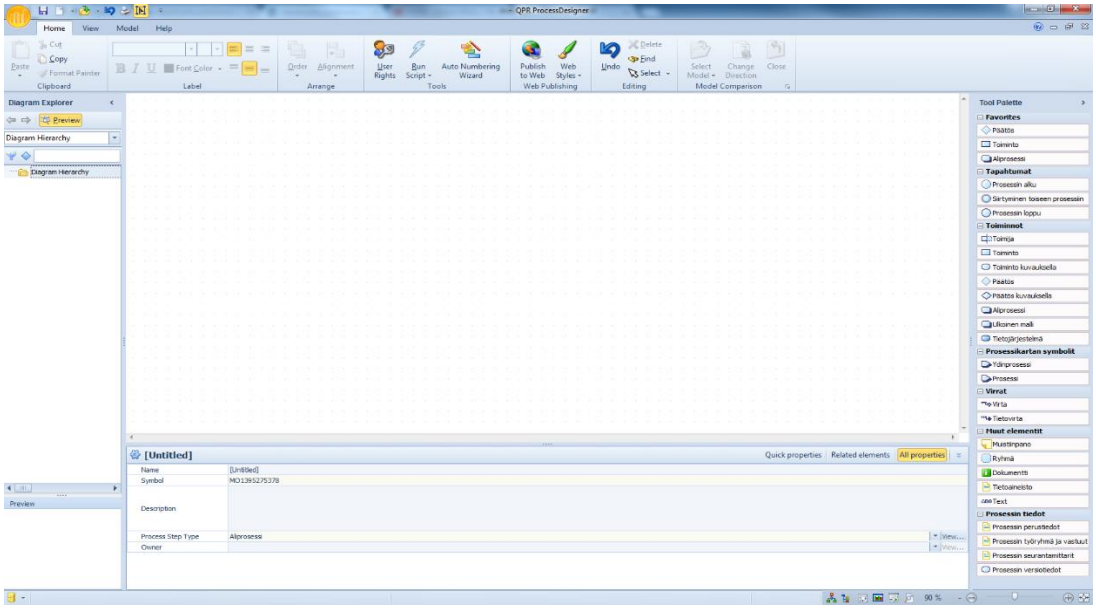
6.2 Prosessikuvaukset

Prosessikuvaukset olivat yksi tärkeimmistä prioriteeteista IDM-järjestelmän käyttöönoton kannalta. Prosessikuvissa ohjaavana tekijänä käytimme JUHTA:n laatimaa suositusta JHS 152.

Päätarkoitus tässä opinnäytetyössä oli saada oleelliset prosessikuvaukset piirrettyä. Näiden prosessikuvausten perusteella määritetään IDM-järjestelmän toiminnallisuus Lapin sairaanhoitopiirin toimintaympäristöä noudattaen.

6.2.1 Työkalut prosessikuvauksiin

Prosessikuvauksien piirtämisessä työkaluna käytimme Lapin sairaanhoitopiirissä käytettävää QPR Software Oyj:n ohjelmaa QPR ProcessDesigner (Kuvio 5). Lapin sairaanhoitopiirissä QPR:ään on määritelty pohja prosessikuvauksille, jota käytettäessä asettelut ovat yhdenmukaiset koko organisaation sisällä.



Kuvio 5. QPR piirtotyökalun perusnäkymä

QPR:n perusnäkymä on (Kuvio 5) mukainen. QPR on helppokäyttöinen ja selkeä ohjelma prosessikuvauksien laatimiseen. Lapin sairaanhoitopiirin esimääriteltyä pohjaa käyttämällä, prosessikuvaksissa tarvittavat symbolit löytyvät helposti oikeasta reunasta löytyvästä valikosta suomenkielisinä ja selkeässä järjestyksessä. Symbolien asettelu on tehty hyvin helpoksi ja käyttäjäystävälliseksi, ensin valitaan haluttu symboli valikosta ja sen jälkeen klikataan näytön keskellä näkyvää ruutua. Symboli ilmestyy ruudulle, jonka jälkeen voidaan määritellä symbolille eri ominaisuuksia, muun muassa nimi, omistaja sekä yhteydet. QPR:stä on myös mahdollista viedä prosessikuvat suoraan eri tiedostomuotoihin, kuten Word-tiedostoksi. Tämä ominaisuus tuli käytännölliseksi, kun aloimme kokoamaan prosessikuvat yhteen dokumenttiin, jonka lähetimme eri tahoille tarkasteltavaksi.

6.2.2 Prosessikuvausten laatiminen

Prosessikuvausten laatiminen oli lähtenyt projektissa liikkeelle tarvittavien prosessien tunnistamisella. Käyttövaltuushallinnon käyttöönottoa varten tarvittavat prosessit olivat koottu yhdeksi prosessilistaksi. Listalle oli tunnistettu yhteensä noin kaksikymmentä eri prosessia. Projektissa meidän tehtävänä olikin piirtää jo tunnistetut prosessit graafiseen muotoon, noudattaen Lapin sairaanhoitopiirin toimiympäristöä.

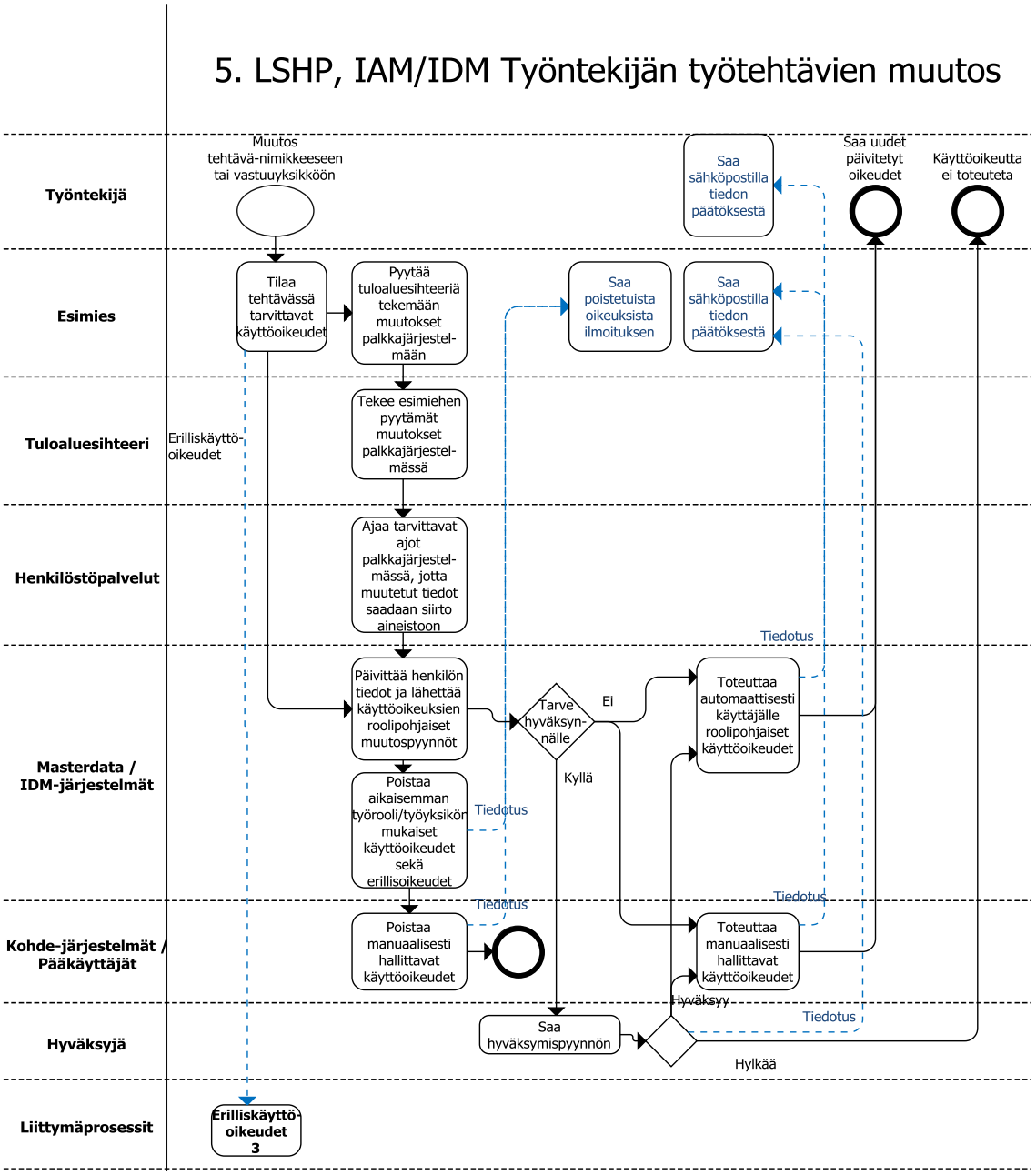
Prosessikuvauksien alustavana pohjana toimi kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri. Kuntaliitto on julkaissut viitearkkitehtuurin ohjeena yhdenmukaistamaan eri kuntien arkkitehtuurin ja käyttövaltuushallinnan prosessikuvaukset sekä toimintalogiikat. Kuntaviitearkkitehtuurin tarkoituksena ei ole tuoda valmista ratkaisuarkkitehtuurikuvausta, vaan sen pohjalta voidaan rakentaa toimiva ratkaisu eri käyttötarkoituksiin. Prosessikuvaukset kuntaviitearkkitehtuurissa ovat hyvinkin yleistasoisesti kuvattu, joten näiden prosessikuvausten perusteella piirsimme pohjat prosessikuvauksille.

Prosessikuvaukset jaoteltiin kahteen eri dokumenttiin. Organisaatiokuvaus dokumentti sisälsi kaikki prosessikartta ja toimintamalli -tason kuvaukset, sekä kulkutason dokumentti sisälsi prosessin kulku -tason kuvaukset. Kulkutason dokumentille muodostui suurempi prioriteetti, koska se oli IDM-järjestelmän

käyttöönottoa varten huomattavasti oleellisempi. Dokumentaatiossa prosessit jaottelimme hierarkiaan, josta voidaan selkeästi nähdä mitkä prosessit liittyvät toisiinsa ja näin prosessien kokonaisuudet ovat helposti havaittavissa. Hierarkian toteutimme dokumentin monitasoisen numeroidun otsikoinnin avulla.

Prosessikuvausten teknisen toimivuuden toteuttaminen ja prosessikuvien yhdenmukaistaminen toteutettiin Citrus Secure Identity Oy:n ja Citrus Solutions Oy:n kanssa noin viikon sykleissä. Tämä prosessi eteni prosessikuvausten kommentoinnilla ja näiden kommenttien perusteellä lähdimme piirtämään eri ratkaisuja prosessikuvausten toimivuuden takaamiseksi. Palavereita prosessikuvausten osalta pyrittiin pitämään viikoittain, joissa käytiin läpi prosessikuvauksiin tehdyt muokkaukset, sekä mitkä kohdat prosessikuvauksista vaativat vielä muokkausta. Näiden palaverien tarkoitus oli yhtenäistää prosessikuvausten tekninen osuus selkeäksi ja toimivaksi kokonaisuudeksi. Prosessikuvauksiin pyrittiin löytämään toimivia tapoja niin, että IDM-järjestelmään määriteltävät toiminnot toteuttavat Lapin sairaanhoitopiirin toimintaympäristön mukaiset prosessit.

Prosessikuvauksia muodostui yhteensä 28 kappaletta. Näistä kuvauksista tarkastelemme tarkemmin työntekijän työtehtävien muutos -prosessia (Kuvio 6), sekä erilliskäyttöoikeudet -prosessia (Kuvio 7).

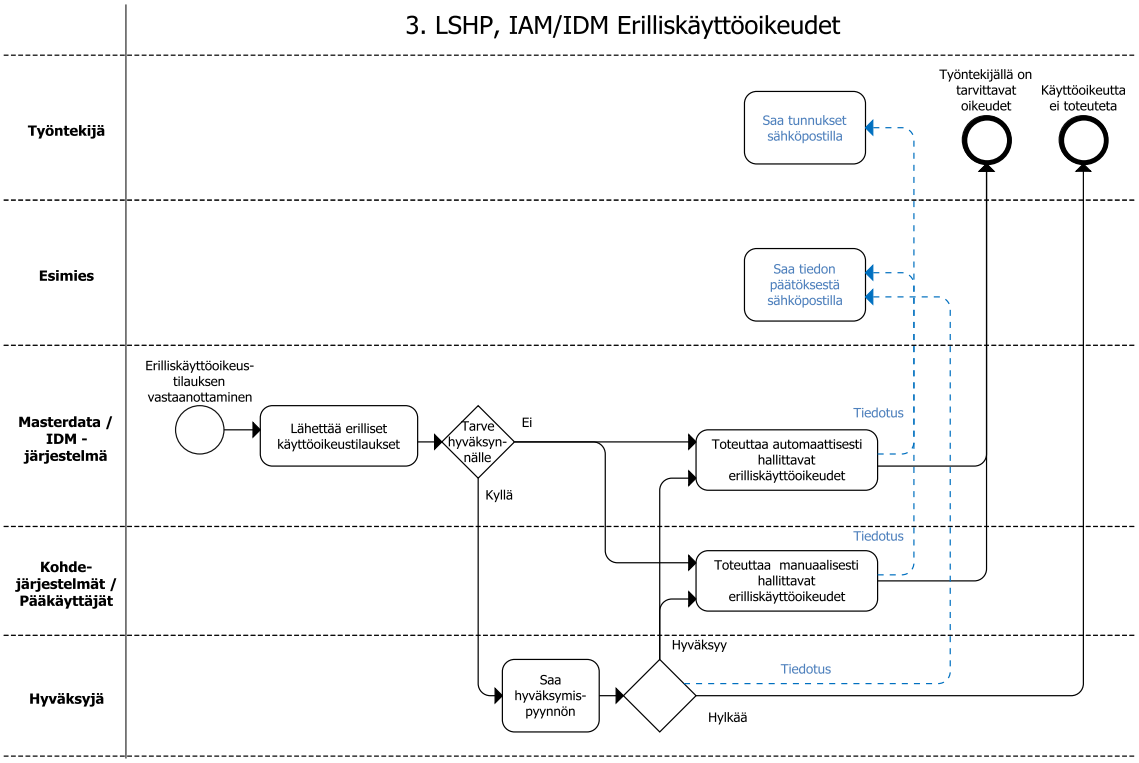


Kuvio 6. Prosessikuvaus työntekijän työtehtävien muutoksista

Työntekijän työtehtävien muutos -prosessin lähtökohtana on, kun työntekijällä tulee muutos tehtävänimikkeeseen tai vastuuyksikköön. Tämä prosessi toteutuu Lapin sairaanhoitopiirissä esimerkiksi silloin, kun työntekijä vaihtaa osastoa.

Prosessikuvauksissa tiedotukset piirsimme sinisellä katkoviivalla, sekä selkeyttävänä tekijänä muokkasimme siniset tekstit toimintoihin, joihin tietovirrat päättyvät. Harkitsimme myös tiedotusten piirtämistä omina prosessikuvauksina, koska jokaisessa prosessikuvauksessa niitä tulee olemaan paljon, mutta ajanpuutteen vuoksi sovittiin, että se jätetään tekemättä.

Prosessissa on myös liittymäprosessi: Erilliskäyttöoikeudet 3 (Kuvio 7). Tämä prosessi toteutuu, jos työntekijä tarvitsee erilliskäyttöoikeuksia uudessa työtehtävässään. Prosessi käynnistyy, kun esimies tekee erilliskäyttöoikeustilauksen työntekijän työtehtävien muutos -prosessissa, jolloin erilliskäyttöoikeusprosessin Masterdata/IDM-järjestelmä -toimija ottaa tilauksen vastaan ja jatkaa prosessia eteenpäin.



Kuvio 7. Prosessikuvaus erilliskäyttöoikeuksista

6.3 Roolit

Itse roolien määrittely ei kuulunut meille tässä projektissa, vaan meidän tavoite roolien osalta oli esittää yhdenmukainen malli, joiden perusteella roolien määrittely lähdetään toteuttamaan Lapin sairaanhoitopiirissä. Roolien määrittely on suuri projekti, sillä aikaa täytyy käyttää määrittelyihin runsaasti, jotta lopputulos olisi toimiva. Pahimmassa tapauksessa rooleja voi syntyä yhtä paljon kuin organisaatiossa on työntekijöitä, jos roolien määrittely on tehty hutaisemalla, eikä tälle prosessille ole annettu sen vaatimaa aikaa.

Lapin sairaanhoitopiirissä kaikki työntekijöiden tehtävänimikkeet ovat listattu yhteen dokumenttiin. Tästä dokumentista löytyy yli 300 eri tehtävänimikettä,

joille kaikille olisi täytynyt määritellä yksitellen käyttöoikeudet eri järjestelmiin, alkuperäisen suunnitelman mukaan. Tämä ei lopputuloksen kannalta olisi ollut järkevin vaihtoehto, sillä rooleja muodostuisi aivan liian suuri määrä, joka on ongelma tietoturvan ja roolien hallittavuuden kannalta.

Lähdimme suunnittelemaan tähän ratkaisua, jossa yhdistettäisiin tehtävänimikkeitä isompien kokonaisuuksien alle. Tämä ratkaisu olisi hallittavuuden kannalta helpoin, sillä roolien määrä pysyi matalana ja täten helposti hallittavana. Käyttövaltuushallinnon käyttöönottoa varten suunnittelimme roolituksen toteutettavan pilottivaiheessa vähäisellä rooli määrällä, jolloin roolien toiminnallisuus saataisiin helposti testattua.

6.4 Vaatimusmäärittelyt

Prosessikuvaukset saatuamme riittävälle tasolle, aloimme tuottamaan JHS 173 ohjeistuksen mukaisesti järjestelmänhankinnan seuraavaa osuutta, joka on vaatimusmäärittelyiden kartoitus ja luonti. Vaatimusmäärittelyiden luontia tuki Lapin sairaanhoitopiirin IDM/IAM-projektissa entuudestaan tuotetut dokumentaatiot kehittämistarpeiden tunnistuksesta ja nykytilan arvioinnista, sekä käyttövaltuuksien hallintatavan osalta. Työtehtävässämme vaatimusmäärittelyiden luonnin prioriteetti oli huomattavasti matalampi kuin prosessikuvausten luonnissa, joten vaatimusmäärittelydokumenttiin ei käytetty työtunteja läheskään niin paljoa kuin prosessikuvauksien dokumentteihin.

Vaatimusmäärittelyiden pohjana käytimme Kajaanin ammattikorkeakoulun laatimaa vaatimusmäärittelypohjaa, joka sisälsi vaatimusmäärittelyjä varten luotavan dokumentaation kaikki mahdolliset osa-alueet. Vaatimusmäärittelydokumentaation luonnin ensimmäinen vaihe oli määritellä, mitkä kaikki osiot olivat olennaisia Lapin sairaanhoitopiirin käyttövaltuushallinnon kannalta.

Päädyimme valitsemaan vaatimusmäärittelydokumenttiin käyttövaltuushallinnon käyttöönottoa varten vain tärkeimmät osa-alueet: vaatimusmäärittelyt, käyttötarkoitus, reunaehdot, termistö ja käyttäjien kertomat ongelmat. Vaatimusmäärittelydokumenttiin tullaan vielä lisäämään loputkin osa-alueet IDM/IAM-projektin edetessä.

Huomasimme heti vaatimusmäärittelyiden suunnitteluvaiheessa, että vaatimusmäärittelyjä syntyy suuria määriä, joten päädyimme kehittämään vaatimusmäärittelyille ryhmitystä. Ryhmittelyillä saimme selkeytettyä vaatimusten määrittelyprosessia huomattavasti. Yhden ryhmän alle oli paljon helpompi tutkia eri vaatimukset, kuin että ne olisi tutkittu sekalaisesti. Ryhmittelyn toteutimme yleisluontoisten termien avulla, joita olivat muun muassa: tietoturva, helppokäyttöisyys, arkkitehtuuri ja itsepalvelu. Ryhmiä syntyi kokonaisuudessaan noin 15 kappaletta.

6.5 Lopputulos

Projektin tavoitteena meillä oli tuottaa Lapin sairaanhoitopiirille dokumentaatiot prosessikuvausten ja vaatimusmäärittelyiden osalta käyttövaltuushallinta järjestelmän käyttöönottoa varten.

Prosessikuvausten osalta saimme tunnistetut prosessit piirrettyä QPR ProcessDesigneria käyttäen. Prosessikuvakset saimme piirrettyä tekniseltä tasolta toimiviksi ja yhdenmukaisiksi. Prosessikuvaukset jäävät vielä tässä vaiheessa odottamaan Lapin sairaanhoitopiirin eri yksiköiden viimeistä katselmointia, joiden perusteella kuvaukset saadaan hyväksymistä vaille valmiiksi. Nämä lopulliset informaatiot ovat kuitenkin todella helppo lisätä prosessikuviin, sillä prosessin hierarkia ja piirtoteknilliset toiminnallisuudet ovat jo prosessikuvissa valmiina.

Vaatimusmäärittelyiden osalta saimme tehtyä vaatimusmäärittelydokumentaation pohjamallin ja saimme listattua siihen vaatimuksia noin 80 kappaletta. Nämä vaatimukset koostuivat pääsääntöisesti toiminnallisista vaatimuksista noin 50 kappaletta ja loput noin 30 kappaletta ei-toiminnallisista. Vaatimusmäärittelydokumenttia emme saaneet täysin valmiiksi aikarajoitteiden ja prosessikuvausten suuremman prioriteetin vuoksi. Vaatimusmäärittelydokumentaation saimme JHS 173 mukaiseen määrittelyiden tuottamisvaiheeseen (Kuvio 4). Vaatimusmäärittelydokumentin työstö jatkuu Lapin sairaanhoitopiirissä eri tahojen toimesta.

6.6 IDM/IAM-projektin eteneminen

Tuottamiemme vaatimusmäärittely- ja prosessikuvausdokumentaatioiden työstäminen tulee vielä jatkumaan Lapin sairaanhoitopiirin IDM/IAM-projektissa. Dokumentaatioiden lopulliset versiot täytyy hyväksyttää Lapin sairaanhoitopiirin eri yksiköissä ja ohjausryhmissä.

Lapin sairaanhoitopiirin eri yksiköiden on määriteltävä tarvittavat roolit eri järjestelmille. Näihin roolimäärityksiin kuuluvat organisaatioroolien, työroolien ja palveluroolien määrittely. Roolien osalta on myös määriteltävä jokaisen tietojärjestelmän käytännöt, mitä käyttöoikeuksia eri roolit saavat tietojärjestelmissä käytännössä ja miten kyseiset tietojärjestelmät tukevat roolipohjaista käyttöoikeuksien hallintaa. Roolien määrittelyt ovat IDM-järjestelmän käyttöönottoa varten erittäin korkean prioriteetin omaavia, koska järjestelmän testaaminen ilman niitä, ei ole kannattavaa. Testaussuunnitelma ja itse järjestelmän testaus tulee myös toteuttaa, ennen varsinaista järjestelmän käyttöönottoa.

7 POHDINTA

Opinnäytetyön tavoitteena oli tuottaa Lapin sairaanhoitopiirille dokumentaatiot prosessikuvausten ja vaatimusmäärittelyiden osalta käyttövaltuushallinta järjestelmän käyttöönottoa varten. Dokumentaation tarkoitus on toimia ohjaavana tekijänä IDM-järjestelmän määrittelyssä, jotta se toimisi Lapin sairaanhoitopiirin toimintaympäristön mukaisesti.

Käyttövaltuushallinto terminä ei ollut meillä entuudestaan tuttu, joten varasimme hyvän ajan perehtyä asiaan ja sisäistää käyttövaltuushallinnon sisältämät eri osa-alueet, jotta pääsisimme hyvin projektiin sisälle. Lapin sairaanhoitopiirin IDM/IAM-projektissa oli syntynyt käyttövaltuushallintoa koskevia dokumentaatioita yli satoja. Näiden dokumentaatioiden tutkiminen ja analysointi oli erittäin aikaa vievää, mutta ne sisälsivät erittäin tärkeätä informaatiota, koskien Lapin sairaanhoitopiirin toimintaympäristöä ja käyttövaltuushallinnon hallintapolitiikan linjauksia.

Opinnäytetyön aikana kohtasimme erilaisia haasteita. Suurimpana haasteena olivat Lapin sairaanhoitopiirin eri yksiköiden ja niiden kiireiset aikataulut. Tämä aiheutti sen, että dokumentaatioiden tarkistusprosessit venyivät pitkiksi ja tarvittavien informaatioiden saaminen eri tahoilta oli hidasta, mutta Lapin Sairaanhoitopiirin kokoisessa isossa organisaatiossa tämä oli odotettavissa.

Opinnäytetyössä käytimme suurimman osan työajastamme prosessikuvauksien laatimiseen ja Lapin sairaanhoitopiirin toimintaympäristön kartoittamiseen, sillä nämä olivat ehdottomasti meidän suurin prioriteetti. Aliarvioimme tarvittavan työmäärän prosessikuvauksien laatimiseen, jonka vuoksi vaatimusmäärittelydokumentaatiota ei keretty tekemään läheskään suunnitellun työmäärän mukaisesti.

Kokonaisuutena opinnäytetyö oli hyvin opettavainen. Opinnäytetyöstä saimme hyvän tietopohjan käyttövaltuushallinnon eri osa-alueista ja niiden käyttöönottoon kuuluvista toimenpiteistä. Totesimme, että suurissa organisaatioissa uusien järjestelmien hankintaprosessi on erittäin aikaa ja resursseja kuluttavaa, eritoten järjestelmissä, jotka liittyvät muihin nykyisiin järjestelmiin. Saimme myös hyvän kokemuksen siitä, miten isossa organisaatiossa suuret projektit etenevät

ja miten organisaatiossa hoidetaan hankkeiden tuomat haasteet ja ongelmat, sekä miten niitä ennakoidaan.

LÄHTEET

Ferraiolo, D.F. & Kuhn, D.R. 1992. Role-Based Access Control. Viitattu 5.10.2017 https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf.

JHS-suositukset 2017. Tervetuloa JHS-järjestelmän verkkopalveluun. Viitattu 29.11.2017 http://www.jhs-suositukset.fi/web/guest/jhs.

JUHTA 2002. JHS 152 Prosessien kuvaaminen. Viitattu 20.10.2017 docs.jhs-suositukset.fi/jhs-suositukset/JHS152/JHS152.pdf.

JUHTA 2009. JHS 173 ICT-palvelujen kehittäminen: Vaatimusmäärittely. Viitattu 10.11.2017 http://docs.jhs-suositukset.fi/jhs-suositukset/JHS173/JHS173.pdf.

Kaskela, L. 2005. Vaatimusmäärittely. Viitattu 9.11.2017 https://www.tieke.fi/pages/viewpage.action?pageId=3441242.

Kunnas, J. 2013. Identiteetinhallinnan perusteet. Digital Identity Solutions Europe Oy. Luentomateriaali.

Kuntaliitto 2017. Sisäinen valvonta: työtehtävien eriyttäminen. Viitattu 13.10.2017 https://www.kuntaliitto.fi/sites/default/files/media/file/Liite%204_Ty%C3%B6teht%C3%A4vien%20eriytt%C3%A4minen.pdf.

Lapin sairaanhoitopiiri 2015. Lapin sairaanhoitopiiri. Viitattu 22.10.2017 http://www.lshp.fi/fi-FI/Sairaanhoitopiiri.

Lapin sairaanhoitopiiri 2013. Lapin sairaanhoitopiirin IDM/IAM-projektidokumentaatiot.

Linden, M., Kurtti, N., Palvalin, M., Numminen, M., Rajala, H., Holmberg, J., Mäkelä, J., Järvenpää, T., Kuusinen, J., Tuomela, M. & Vuorinen, A. 2011. Identiteetin- ja pääsynhallinta. Tampereen teknillinen yliopisto. Viitattu 26.10.2017 http://www.cs.tut.fi/kurssit/TLT-3600/iam-sem2011.pdf.

Rinnemaa, T. 2006. Identiteetinhallinta tuo uusia palasia infrakerrokseen. Viitattu 24.10.2017 http://www.tivi.fi/blogit/2006-12-01/Identiteetinhallinta-tuo-uusia-palasia-infrakerrokseen-3212129.html.

Sandhu, R.S., Coynek, E.J., Feinsteink, H.L. & Youmank, C.E. 1995. Role-Based Access Control Models. IEEE Computer. Viitattu 3.10.2017 https://csrc.nist.gov/CSRC/media/Projects/Role-Based-Access-Control/documents/sandhu96.pdf.

Sandhu, R.S., Coynek, E.J., Feinsteink, H.L. & Youmank, C.E. 1996. Role-Based Access Control Models. George Mason University and SETA Corporation. Viitattu 3.10.2017 http://www.facweb.iitkgp.ernet.in/~shamik/spring2011/i&ss/papers/RBAC%20Sandhu.pdf.

VAHTI 2006. Hyvän käyttövaltuushallinnon edellytysten luominen. Viitattu 10.10.2017 https://www.vahtiohje.fi/c/document_library/get_file?uuid=d48cbc58-d7a4-4757-a0a1-78cd860a3912&groupId=10229.

Witty, R. & Allan, A. & Enck, J. & Wagner, R. Identity and Access Management Defined. Viitattu 7.11.2017 http://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/118200/118281/118281.pdf.