HAAGA-HELIA
ammattikorkeakoulu

Käyttöoikeuksien hallintaprosessien kehittäminen, case: Yritys X

Sini Peltonen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

4.5.2014

Tietojenkäsittelyn koulutusohjelma

Tekijä tai tekijät Sini Peltonen	**Ryhmätunnus tai aloitusvuosi** 2010
Raportin nimi Käyttöoikeuksien hallintaprosessien kehittäminen, case: Yritys X	**Sivu- ja liitesivumäärä** 35 + 1
Opettajat tai ohjaajat Jarmo Harmonen	

Tässä opinnäytetyössä esitetään kehittämisehdotuksia Yritys X:n käyttöoikeuksien hallintaprosesseihin kuvaamalla ja analysoimalla käyttöoikeuksien hallintaprosessien yhteydet HR-prosesseihin Yritys X:ssä. Tämä opinnäytetyö tehtiin Yritys X:n toimeksiantona.

Opinnäytetyön teoriaosuudessa käsitellään käyttöoikeuksien hallintaa, käyttöoikeuksien hallintaan liitettyä problematiikkaa sekä identiteetinhallintaan käyttöoikeuksien hallinnan menetelmänä.

Opinnäytetyö sisältää myös case-osuuden Yritys X:stä. Case-osuudessa kuvataan ja analysoidaan HR-prosessien yhteydet käyttöoikeuksien hallintaprosesseihin Yritys X:ssä. Lisäksi case-osuudessa esitetään kehittämisehdotuksia Yritys X:n käyttöoikeuksien hallintaprosesseihin nykytilan kuvauksen ja analyysin pohjalta.

Opinnäytetyö tehtiin vuoden 2013 ja kevään 2014 aikana. Opinnäytetyön tuloksena saatiin aikaan kehittämisehdotuksia Yritys X:n käyttöoikeuksien hallintaprosesseihin, jotka tukivat käyttöoikeushallinnan omistajan määrittelemiä tavoitteita käyttöoikeuksien hallinnan automatisoinnista, manuaalisen työn vähentämisestä sekä tietoturvallisuuden parantamisesta.

Asiasanat
Kehittäminen, käyttöoikeus, hallinta

HAAGA-HELIA
University of Applied Sciences

Abstract

4 May 2014

Degree Programme in Information Technology

Authors Sini Peltonen	**Group or year of entry** 2010
The title of thesis **DEVELOPMENT OF USAGE RIGHT MANAGEMENT PROCESSES, CASE: COMPANY X**	**Number of pages and appendices** 35 + 1
Supervisor(s) Jarmo Harmonen	

This thesis includes development suggestions for usage right processes to the Company X through current state analysis of the connections between usage right processes and HR-processes. This thesis was made as an assignment for the Company X.

The theory part of the thesis includes information about usage right management and problems associated with it and also identity management as a method to manage usage rights.

This thesis also includes a case study about the Company X. The case study consists of the description and the analysis of the current state of the usage right processes and their connections with HR-processes within the Company X. This thesis resulted in various development suggestions based on the aforementioned analysis.

The thesis was written during the year of 2013 and the Spring of 2014. The thesis resulted in development suggestions that reached the goals of the owner of usage right management in Company X. The goals were to automatize usage right management, reduce manual labor and improve of data security.

Key words
Development, usage right, management

Sisällys

1 Johdanto

Erityisesti tietojenkäsittelypainotteisilla aloilla toimivissa organisaatioissa työntekijöiden päivittäinen tekeminen on riippuvaista ajantasaisista käyttöoikeuksista työssä tarvittaviin resursseihin, jotka voivat olla esimerkiksi tietojärjestelmiä tai sovelluksia. Käyttöoikeudella tarkoitetaan tässä opinnäytetyössä yksilöityä oikeutta käyttäjälle tai käyttäjäryhmälle määritellyn resurssin käyttöön. Käyttöoikeuksien hallinta on usein sitä haastavampaa mitä enemmän yrityksessä on työntekijöitä ja eri resursseja, joita työntekijät työssään tarvitsevat. Käyttöoikeuksien hallinta onkin monissa yrityksissä osoittautunut haasteelliseksi ja käyttöoikeuksien hallinnassa on monenlaisia ongelmia. Huonosti toteutetusta käyttöoikeuksien hallinnasta on haittaa sekä työnantajalle että työntekijöille. (Valtiovarainministeriö 2006, 9-10.)

Identiteetinhallinta on menetelmä, jolla voidaan hallita käyttöoikeuksia ja sen avulla voidaan ratkaista ongelmia, joita käyttöoikeuksien hallintaan tyypillisesti liitetään. Identiteetinhallinnalla tarkoitetaan tässä yhteydessä käyttäjän sähköisen identiteetin sekä identiteettiin liitettyjen käyttöoikeuksien hallintaa sekä identiteetti- ja käyttöoikeustietojen välittämistä eri järjestelmiin. Identiteetinhallintajärjestelmän identiteettitiedon lähteenä on tyypillisesti henkilöstöhallinnon järjestelmä, jolloin organisaation henkilöstöhallinnolla ja HR-prosesseilla on myös merkittävä rooli käyttöoikeuksien hallintaprosesseissa. (Kasanen 2010, 1.)

Yritys X on Suomessa toimiva keskisuuri yritys, jonka henkilöstön lukumäärä on noin 4000 työntekijää. Tämän lisäksi Yritys X:ssä toimii paljon ulkopuolista työvoimaa eli konsultteja, vuokratyöntekijöitä sekä harjoittelijoita. Yritys X:n toimiala on tietojenkäsittely painotteista, joten Yritys X:n työntekijät tarvitsevat pääsyn useisiin Yritys X:n sisäisiin resursseihin, joiden kautta tietoa käsitellään eri tarkoituksia varten. Yritys X:ssä käyttöoikeuksien hallintaa on osin keskitetty ja automatisoitu käyttäen identiteetinhallintaa ja identiteetinhallintajärjestelmää. Identiteetinhallintajärjestelmän auktoritaarinen lähde on Yritys X:n henkilöstöhallinnon ylläpitämä HR-tietojärjestelmä. Yritys X:ssä on käynnissä hanke käyttöoikeuksien hallinnan uudistamisesta ja tässä opinnäytetyössä esitetään kehittämisehdotuksia Yritys X:n käyttöoikeuksien hallintaprosesseihin käyttö-

oikeuksien hallintaprosessien ja HR-prosessien yhteyksien kuvauksen ja analyysin perusteella.

Liitteessä Liite 1 esitellään opinnäytetyössä vastaan tulevat keskeiset käsitteet.

1.1 Tavoitteet ja rajaus

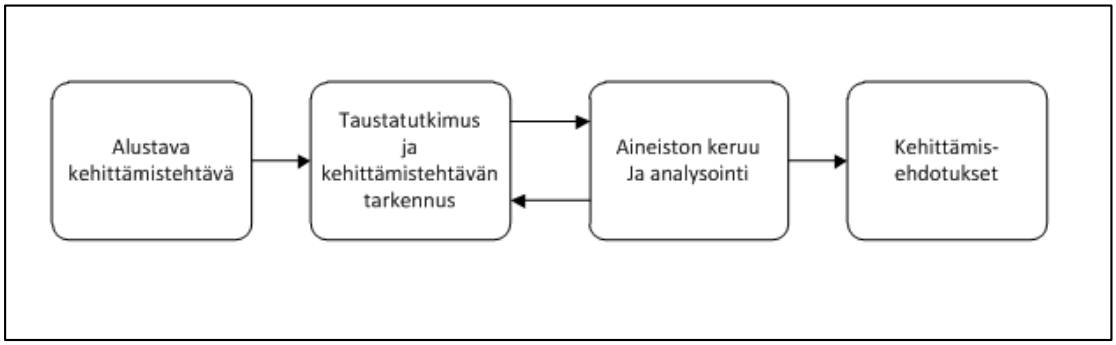
Tämän opinnäytetyön tavoitteena on kuvata ja analysoida käyttöoikeuksien hallintaprosessien yhteydet HR-prosesseihin Yritys X:ssä. Kuvauksen ja analysoinnin pohjalta esitetään kehittämisehdotuksia käyttöoikeuksien hallintaprosesseihin. Tavoitteena on, että kehittämisehdotukset tukevat toimeksiantajana olevan käyttöoikeushallinnan omistajan määrittelemiä tavoitteita käyttöoikeuksien hallinnan automatisoinnista, manuaalisen työn vähentämisestä sekä tietoturvallisuuden parantamisesta. Lisäksi opinnäytetyön tavoitteena on se, että opinnäytetyöstä myös muut yritykset voisivat saada ehdotuksia omien käyttöoikeuksien hallintaprosessiensa kehittämiseen. Omia tavoitteinani opinnäytetyölle ovat opinnäytetyön aikana oppia prosessien kehittämisestä, käyttöoikeuksien hallinnasta sekä käyttöoikeuksien hallinnan ja HR-prosessien yhteyksistä. Tavoitteenani on lisäksi oppia projektityöskentelystä.

Käyttöoikeuksien hallintaprosessit, joita tässä opinnäytetyössä tutkitaan, rajataan koskemaan vain niihin käyttöoikeuksien hallintaprosesseihin, joilla on yhteys HR-prosesseihin. Opinnäytetyössä tutkitaan vain käyttöoikeuksien hallintaprosessien ja HR-prosessien loogisia yhteyksiä eli yhteyksiä, joissa Yritys X:n HR-tietojärjestelmästä välittyy identiteettitietoa identiteetinhallintajärjestelmään.

1.2 Tutkimusmenetelmä

Tutkimusmenetelmäksi tähän opinnäytetyöhön valittiin tapaustutkimus, koska se soveltuu tutkimusmenetelmäksi erinomaisesti kehittämistöihin, joissa on tavoitteena saada aikaan kehittämisehdotuksia ja kehittämisen kohteena on esimerkiksi yritys, sen toiminta tai prosessi (Ojasalo, Moilanen & Ritalahti 2009, 52). Tapaustutkimuksessa tutkimukselle asetetaan alustava kehittämistehtävä ja kehittämistyö aloitetaan perehtymällä aihe-alueeseen tutustumalla lähdekirjallisuuteen ja lähdeaineistoihin sekä samankaltai-

siin tutkimuksiin. Taustatutkimuksen aikana useimmiten myös kehittämistyön kehittämistehtävä tarkentuu, kun kehitettävästä aiheesta on saatu lisää tietoa. (Kuvio 1.)



Kuvio 1. Tapaustutkimuksen vaiheet (Ojasalo ym. 2009, 54-55)

Lisäaineistoa tutkimukseen voidaan kerätä erilaisin menetelmin, kuten haastatteluin ja kyselyin, joita analysoimalla saadaan aikaan uutta tietoa kehittämistyötä varten. Tutkimuksen tässäkin vaiheessa voidaan vielä tarkentaa kehittämistehtävää. Tapaustutkimukseen yhdistetään vahvasti kvalitatiiviset eli laadulliset aineistonkeruumenetelmät, mutta siinä voidaan soveltaa myös kvantitatiivisia eli määrällisiä menetelmiä. Taustatutkimuksen ja aineiston keruun sekä analysoinnin pohjalta tehdään kehittämisehdotukset. (Kuvio 1.)

Tutkimusmenetelmän valinnassa harkittiin myös toimintatutkimuksen valitsemista tutkimusmenetelmäksi sillä myös toimintatutkimuksen menetelmät olisivat sopineet tämän tutkimuksen tekemiseen. Toimintatutkimus pyrkii ratkaisemaan käytännön ongelmia ja löytämään niihin ratkaisuja, jotka saavat aikaan paremman toimintatavan. Tutkimusmenetelmäksi valittiin kuitenkin tapaustutkimus, koska tapaustutkimus päätetään kehittämisehdotuksien esittämiseen, kun taas toimintatutkimuksessa kehittämisehdotuksia testataan syklisesti käytännössä, kunnes saavutetaan toivottu lopputulos. (Ojasalo ym. 2009, 54-55).

2 Käyttöoikeuksien hallinta

Työntekijä voi työssään tarvita pääsyn useaan eri resurssiin, jotta hän pystyy suoriutumaan hänelle osoitetuista työtehtävistä. Resurssi voi olla esimerkiksi jokin tietojärjestelmä tai sovellus, joihin työntekijöiden pääsyä hallitaan käyttöoikeuksilla. Työntekijälle ei kannata antaa käyttöoikeuksia kaikkiin yrityksen resursseihin eikä kaikille työntekijöille kannata myöntää samoja käyttöoikeuksia yhteen resurssiin. Yhdelle työntekijälle saattaa riittää pelkät katseluoikeudet, kun taas toinen työntekijä tarvitsee työssään muutosoikeudet. Työntekijöille tulisi siis antaa käyttöoikeudet vain niihin resursseihin, joita he välttämättä tarvitsevat ja käyttöoikeudet tulisi rajata vain työtehtävien puitteissa välttämättä tarvittaviin toimintoihin. Menetelmä tunnetaan yleisesti englanninkielisellä nimellä Principle of Least Privileged (POLP). Näin voidaan ehkäistä mahdollisimman paljon tietoturvariskejä, jotka liittyvät käyttöoikeuksien väärinkäyttöön ja yrityksen salaisen sekä luottamuksellisen tiedon vaarantumiseen. (Ferraiolo & Kuhn 1992, 9.)

Suuressa yrityksessä, jossa voi olla tuhansia tai kymmeniä tuhansia työntekijöitä ja lukuisia eri resursseja, joita työntekijät työtehtävissään tarvitsevat, tulee käyttöoikeuksien hallinnan olla hyvin suunniteltu ja toteutettu. Työntekijöiden puutteelliset käyttöoikeudet aiheuttavat monenlaista haittaa sekä työnantajalle että työntekijöille. Tyypillisesti käyttöoikeuksien hallinnassa on ongelmia erityisesti käyttöoikeuksien päättämisessä. Lisäksi käyttöoikeuksia ylläpidetään usein hallitsemattomasti useasta eri paikasta eri järjestelmävastaavien toimesta, mikä voi helposti johtaa siihen, että työntekijöillä on liikaa sekä liian laajoja käyttöoikeuksia kuin työtehtävässä olisi tarpeen. (Valtiovarainministeriö 2006, 10.)

Identiteetinhallinta on tapa, jolla voidaan automatisoida ja keskittää käyttöoikeuksien hallintaa. Identiteetinhallinta perustuu identiteettitietoon, joka koostuu käyttäjä- ja käyttöoikeustiedoista, ja niiden välittämisestä eri järjestelmiin. Identiteetinhallintajärjestelmän avulla voidaan automatisoida käyttöoikeuksien päättelyä ja hallintaa välitysrajapinnan kautta esimerkiksi henkilöstöhallinnon järjestelmästä, joka toimii identiteettitiedon lähteenä. Identiteetinhallintajärjestelmä automaattisesti siirtää eli provisioi käyttäjä- ja käyttöoikeustiedot identiteetinhallintajärjestelmän piirissä oleviin kohdejärjestelmiin, joita työntekijät työssään hyödyntävät. (Kasanen 2010, 1.)

2.1 Ongelmat

Käyttöoikeuksien puutteellinen hallinta voi pahimmillaan estää työntekijöiden päivittäisen tekemisen kokonaan, mistä aiheutuu myös liiketappiota työnantajana toimivalle yritykselle. Lisäksi ongelmat käyttöoikeuksien hallinnassa voivat aiheuttaa vakavia tietoturvariskejä, jotka voivat johtaa esimerkiksi salaisen tai luottamuksellisen tiedon vaarantumiseen. Ongelmat käyttöoikeuksien hallinnassa usein johtuvat tavalla tai toisella siitä, että käyttöoikeuksien hallintaprosesseja ei ole suunniteltu tarpeeksi tarkalla tasolla ja vastuut prosesseista ovat epäselvät. (Valtiovarainministeriö 2006, 10.)

Käyttöoikeuksien hallinta on yrityksissä usein jätetty lähes kokonaan tietohallinnon vastuulle. Se ei ole paras mahdollinen ratkaisu, koska useimmiten paras tietämys siitä, mitä käyttöoikeuksia työntekijä työssään tarvitsee, on liiketoiminnan puolella eli esimiehillä ja organisaatioyksiköiden sisällä. Työtehtävien edellyttämien käyttöoikeuksien määrittely voi kuitenkin olla erittäin työlästä ja liiketoiminnalta liikaa aikaa vievää, joten se usein jää muiden kiireiden takia tekemättä. Tämä usein johtaa siihen, että esimiehet tilaavat tarpeettomia tai liian laajoja käyttöoikeuksia ikään kuin varmuuden vuoksi, koska esimiehet eivät ole varmoja, mitä käyttöoikeuksia tulisi tilata. (Valtiovarainministeriö 2006, 10.)

Käyttöoikeuksien hallinnassa on usein ongelmia myös käyttöoikeuksien päättämisessä. Kun työntekijän tarve käyttöoikeuksille päättyy, esimerkiksi työtehtävien vaihtuessa tai projektin päätyttyä, jää työntekijälle usein voimaan käyttöoikeuksia, joita ei enää tarvittaisi. Jopa työntekijöille, joiden työsuhde on jo päättynyt, voi jäädä järjestelmiin voimaan käyttöoikeuksia ja käyttäjätunnuksia. (Valtiovarainministeriö 2006, 10.) Työntekijän työtehtävien vaihtuessa esimiehillä on usein suurempi mielenkiinto siihen, että työntekijä saa tarvittavat käyttöoikeudet uusista työtehtävistä suoriutumiseen kuin siihen päätetäänkö tarpeettomaksi tulleet käyttöoikeudet. Käyttöoikeuksien hallinnassa voi aiheuttaa ongelmia myös se, että käyttöoikeuksien hallintaprosesseja ei ole automatisoitu tarpeelliselle tasolle. Pienessä yrityksessä voidaan vielä pärjätä, jos käyttöoikeuksien hallinta perustuu esimiesten tekemiin käyttöoikeustilauksiin, mutta suuressa yrityksessä on lähes pakollista automatisoida käyttöoikeuksien hallintaa, koska käyttöoikeuksien manuaalinen hallinta on hidasta ja virhealtista työtä.

2.2 Lainsäädäntö

Käyttöoikeuksien hallinnassa käsitellään suojattavia henkilötietoja, joten käyttöoikeuksien hallinnassa ja sen suunnittelussa tulee ottaa huomioon lainsäädäntö. Suomessa käyttöoikeuksien hallintaa koskevia lainsäädäntöjä ovat esimerkiksi julkista puolta koskeva julkisuuslaki (621/1999) ja myös yksityistä puolta koskeva henkilötietolaki (523/1999). (Valtiovarainministeriö 2006, 11-12.) Henkilötietolain tarkoitus on turvata henkilöiden yksityiselämää sekä toteuttaa hyvän tietojenkäsittelyn kehittämistä sekä noudattamista. Henkilötietolaki määrää muun muassa edellytyksistä, velvoitteista, oikeuksista sekä madollisista sanktioista, jotka liittyvät henkilötietojen käsittelyyn sekä henkilötietojen käsittelyyn henkilötietolain vastaisesti. (Tietosuojavaltuutetun toimisto.)

Laissa on lisäksi yleisvelvoitteita, kuten tarpeellisuus- ja virheettömyysvaatimukset sekä huolellisuus- ja suojaamisvelvoitteet, jotka on otettava huomioon, kun käsitellään henkilötietoja (Tietosuojavaltuutetun toimisto). Lisäksi joillain toimialoilla on erilaisia, myös ulkomaisia, toimialakohtaisia lainsäädäntöjä, joihin tulee perehtyä toimialakohtaisesti (Propentus Oy).

2.3 Identiteetinhallinta

Identiteetinhallinnalla (Identity Management, IdM) voidaan automatisoida ja keskittää käyttöoikeuksien hallintaa. Identiteetinhallinnalla tarkoitetaan tässä yhteydessä käyttäjän sähköisen identiteetin ja identiteettiin liitettyjen käyttöoikeuksien hallintaa sekä identiteetti- ja käyttöoikeustietojen välittämistä eri järjestelmiin. (Kasanen 2010, 1.) Tässä opinnäytetyössä käyttäjällä tarkoitetaan yrityksen sisäistä tai ulkopuolista työntekijää, mutta käyttäjä voisi olla myös esimerkiksi yrityksen asiakas tai jokin tietojärjestelmä.

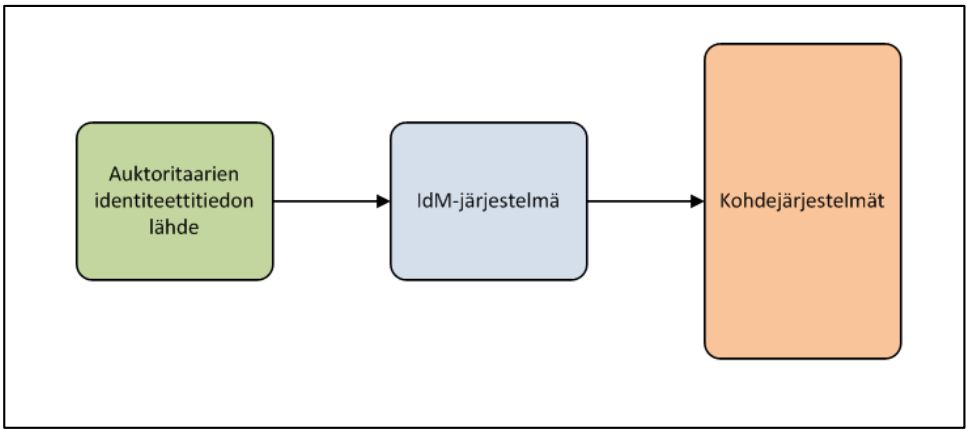
Identiteetinhallinnassa ollaan kiinnostuneita käyttäjistä, käyttäjien erilaisista tarpeista eri resursseihin sekä, siitä kenellä on oikeus hyväksyä käyttäjien pääsy resurssiin. Identiteetinhallinta on kokonaisuus, joka koostuu sekä IT-pohjaisista ratkaisuista, ihmisistä, toimintatavoista että prosesseista. Identiteetinhallinta usein sekoitetaan identiteetin- ja pääsynhallintaan (Identity and Access management, IaM), joiden erona on se, että iden-

titeetinhallinta ei ota kantaa pääsynhallintaan eli käyttäjän tunnistamiseen liittyviin asioihin. (Kasanen 2010, 1.)

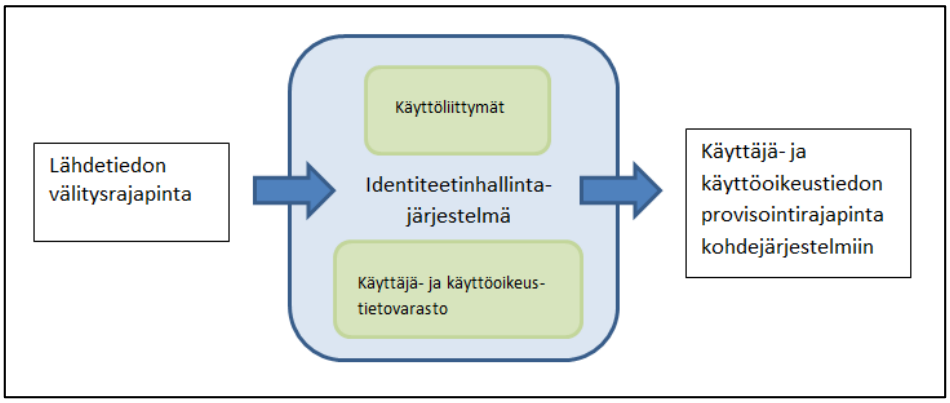
Identiteetinhallinta palveluna sisältää (Kasanen 2010, 2) usein seuraavia toimintoja

- identiteetin elinkaaren hallinnan (esim. luoti, poisto yms.)
- attribuuttien generoinnin (esim. käyttäjätunnukset, sähköpostiosoitteet yms.)
- käyttöoikeuksien mallintamisen (esim. säännöt, rajoitteet yms.)
- käyttöoikeuspyyntöjen hallinnan ja automatisoinnin
- raportointi- ja jäljitettävyystoiminnot
- identiteettitiedon eli käyttäjä- ja käyttöoikeustietojen provisioinnin eri järjestelmiin.

Identiteetinhallinnan yleinen arkkitehtuuri koostuu identiteettitiedon auktoritaarisesta lähteestä, identiteetinhallintajärjestelmästä, sekä identiteetinhallintajärjestelmän piirissä olevista kohdejärjestelmistä (kuvio 2). Identiteetinhallintajärjestelmä, IdM-järjestelmä, koostuu useammasta toiminnallisesta osasta eli lähdetiedon välitysrajapinnasta, keskitetystä käyttäjä- ja käyttöoikeustietovarastosta, käyttöliittymistä sekä käyttäjä- ja käyttöoikeustiedon provisointirajapinnasta kohdejärjestelmiin (kuvio 3).



Kuvio 2. Identiteetinhallinnan arkkitehtuuri (Kasanen 2010, 3)



Kuvio 3. Identiteetinhallintajärjestelmän toiminnalliset osat (Kasanen 2010, 3)

IdM-järjestelmä saa tarvittavan tiedon käyttäjistä välitysrajapinnan kautta identiteettitiedon auktoritaarisesta lähteestä, joita voi olla yksi tai useampi. Tyypillisesti lähdetieto tulee henkilöstöhallinnon HR-tietojärjestelmästä, jossa ylläpidetään henkilöstötietoa. (Kasanen 2010, 3.) Lähdetiedon välitysrajapinnan avulla voidaan hallita käyttäjä- ja käyttöoikeustietoja koko työsuhteen elinkaaren ajan. IdM-järjestelmä saa tiedon esimerkiksi työntekijän työsuhteen päättymisestä HR-tietojärjestelmästä ja päättää automaattisesti käyttäjän käyttöoikeudet kaikista kohdejärjestelmistä.

HR-tietojärjestelmä (Human Resource Information System, HRIS) on käsitteenä laaja ja tässä opinnäytetyössä HR-tietojärjestelmällä tarkoitetaan IT-pohjaisia tietojärjestelmiä ja sovelluksia, joita käytetään yleisesti henkilöstöhallinnollisiin tarkoituksiin. HR-tietojärjestelmä voi olla tietojärjestelmä, verkkopohjainen sovellus, tai se voi olla näiden kahden yhdistelmä. (Bondarouk, Ruel & Looise 2011, 26.) HR-tietojärjestelmät voivat sisältää hyvin erilaisia toimintoja, mutta HR-tietojärjestelmät ovat karkeasti jaettu kolmeen eri ryhmään: toiminnallisiin, suhteellisiin sekä muuntautuviin. (Bondarouk ym. 2011, 27.)

Toiminnallista HR-tietojärjestelmää käytetään useimmiten tavallisten HR-toimintojen suorittamiseen, kuten palkanlaskentaan ja henkilöstötietojen hallintaan. Suhteelliset HR-tietojärjestelmät sisältävät hieman kehittyneempiä toimintoja, jotka sisältävät HR-tietojärjestelmän ja henkilöstön välistä kommunikointia, kuten rekrytointi ja koulutusjärjestelmät. Muuntautuvat HR-tietojärjestelmät sisältävät usein hyvin kehittyneitä toimintoja, joiden tarkoitus on todella tukea yrityksen strategiaa. Muuntautuva HR-tietojärjestelmä voi olla esimerkiksi keskustelufoorumi henkilöstölle, ammatillisen kyky-

jen arviointisovellus tai sovellus, jonka tarkoitus on tukea henkilöstöä muutoksen hallinnassa. Pienissä ja keskikokoisissa yrityksissä löytyy useimmiten toiminnallisia ja suhteellisia HR-tietojärjestelmiä, mutta suurissa yrityksissä saattaa löytyä HR-tietojärjestelmiä jokaisesta ryhmästä. (Bondarouk ym. 2011, 26-27.)

IdM-järjestelmä tekee useimmiten käyttöoikeuksien päättelyä identiteettitietiedon lähteestä välittyvän identiteettitiedon perusteella. Lähdetiedon välitysrajapinta voidaan toteuttaa esimerkiksi liittimien (connectors), yhteys- tai välitaulujen, tai cvs- tai xml-muotoisten tiedostojen avulla. (Kasanen 2010, 3-4; Valtiovarainministeriö 2006, 25.) IdM-järjestelmä säilyttää identiteetin sisältämiä käyttäjä- ja käyttöoikeustietoja keskitetyssä käyttäjä- ja käyttöoikeustietovarastossa (kuvio 3). Tietovarasto muodostaa IdM-järjestelmän ytimen ja se voi olla esimerkiksi käyttäjähakemisto, tietokanta tai tiedosto, tai se voi koostua useammasta eri lähteestä. Tietovaraston käyttäjä- ja käyttöoikeustietoja ylläpidetään automaattisten hallintaprosessien kautta. (Valtiovarainministeriö 2006, 25.)

IdM-järjestelmä välittää eli provisioi identiteetin sisältämät käyttäjä- ja käyttöoikeustiedot IdM-järjestelmän piirissä oleville kohdejärjestelmille käyttäjä- ja käyttöoikeustiedon välitysrajapinnan kautta (kuvio 3.) Provisointi voi tapahtua reaaliaikaisesti tai ajastettuna. Käyttäjä- ja käyttöoikeustiedon välitysrajapinta kohdejärjestelmiin voidaan toteuttaa esimerkiksi SPML (Service Provisioning Markup Language) standardilla. Aina kaikkiin järjestelmiin syystä tai toisesta ei ole identiteetinhallintaa hyödyntävissä yrityksissä toteutettu provisiointirajapintaa ja provisioinnissa joudutaan tekemään myös manuaalista työtä. Tällöin IdM-järjestelmä voi välittää käyttäjä- ja käyttöoikeustiedot esimerkiksi salattuna sähköpostilla järjestelmävastaaville ja järjestelmävastaavat syöttävät tiedot manuaalisesti kohdejärjestelmään. Myös tällaisella järjestelyllä saadaan aikaan hyötyjä verrattuna käyttöoikeuksien hallintaan, jossa ei hyödynnetä lainkaan IdM-järjestelmää. (Kasanen 2010, 4; Valtiovarainministeriö 2006, 10.)

Yleensä kohdejärjestelmien auktoritatiivinen tiedonlähde on IdM-järjestelmä ja muutokset identiteettitietoihin kohdejärjestelmissä pyritään estämään kaikin tavoin, jotta IdM-järjestelmässä oleva tieto on aina paikkansa pitävää ja yhdenmukaista. Joissain tapauksissa voi olla kuitenkin tarpeellista tuoda kohdejärjestelmissä tehtyjä muutoksia

IdM-järjestelmään, mitä kutsutaan rekonsilioinniksi. Rekonsiliointi voi olla tarpeellista esimerkiksi, jos käyttäjään liittyviä tietoa, kuten puhelinnumeroa, hallinnoidaan kohdejärjestelmän kautta. Silloin kohdejärjestelmän tiedot on rekonsilioitava IdM-järjestelmään. (Kasanen 2010, 5.)

IdM-järjestelmään kuuluvat oleellisesti myös käyttöliittymät (kuvio 3). Useimmiten IdM-järjestelmään on toteutettu erilliset käyttöliittymät loppukäyttäjille ja IdM-järjestelmän parissa työskenteleville asiantuntijoille. Loppukäyttäjien käyttöliittymän kautta esimiehet voivat tarkastella ja hallita alaistensa käyttöoikeuksia ja alaiset voivat itsepalveluna tehdä käyttöoikeuspyyntöjä, jotka automaattisesti menevät esimiehelle hyväksyttäväksi. IdM-järjestelmän parissa työskentelevät asiantuntijat voivat konfiguroida IdM-järjestelmää erillisen hallintakäyttöliittymän kautta. (Kasanen 2010, 5-6.) IdM-järjestelmä mahdollistaa myös käyttöoikeuksien raportoinnin, ja se sisältää erilaisia jäljitettävyystoimintoja. IdM-järjestelmän avulla voidaan raportoida esimerkiksi käyttäjän kaikki käyttöoikeudet tai raportoida kaikki käyttäjät, joilla on käyttöoikeuksia määriteltyyn kohdejärjestelmään. Lisäksi käyttöoikeuksien hallinnoinnissa tehdyt muutostapahtumat ja niihin osallistuneet tahot ovat mahdollisia jäljittää. (Valtiovarainministeriö 2006, 26.)

Identiteetinhallinnasta voidaan yrityksissä hyötyä yrityksen toimialasta ja koosta riippumatta. Erityisen hyödyllinen identiteetinhallinta on yrityksille, joissa tapahtuu paljon sisäisiä muutoksia ja työntekijöissä on paljon vaihtelevuutta, koska tällaisissa yrityksissä käyttöoikeuksien hallinta ilman identiteetinhallintaa on hyvin haasteellista. (Propentus Oy.) Identiteetinhallinnasta saadaan eniten hyötyä ottamalla käyttöön keskitetty identiteetinhallinta, mikä tarkoittaa sitä, että kaikki yrityksen järjestelmät liitetään IdM-järjestelmän piiriin. Keskitetyn identiteetinhallinnan selkeitä hyötyjä ovat parempi kontrolli, kustannustehokkuus sekä loppukäyttäjäkokemus (Kasanen 2010, 2).

Käyttöoikeuksien hallinnassa saavutetaan parempi kontrolli, kun käyttöoikeuksia hallinnoidaan keskitetysti yhdestä toiminnosta käsin identiteetinhallinnalla eikä käyttöoikeuksia hallinnoida hajautetusti eri järjestelmienomistajien toimesta. Lisäksi, jos kaikki yrityksen järjestelmät ovat IdM-järjestelmän piirissä, ei työntekijälle voi jäädä voimaan käyttäjätunnuksia tai käyttöoikeuksia voimaan erillisesti hallinnoituihin järjestelmiin.

Myös raportointi- ja jäljitettävyystoiminnot tuovat käyttöoikeuksien hallintaan parempaa kontrollia. Käyttöoikeuksien raportointiomaisuuden avulla voidaan tarvittaessa saada tieto esimerkiksi kaikista käyttäjän käyttöoikeuksista tai kaikista käyttäjistä, joilla on tietty käyttöoikeus. Jäljitettävyystoimintojen avulla voidaan lisäksi selvittää esimerkiksi käyttöoikeuspyyntöjen hyväksyjät ja muut osalliset käyttöoikeuksienhallintatapahtumassa. Jäljitettävyys- ja raportointitoiminnot ovat erityisen tärkeitä, jos yrityksessä ilmenee käyttöoikeuksien väärinkäytöksiä. (Kasanen 2010, 2; Valtiovarainministeriö 2006, 26.)

Identiteetinhallinnan avulla voidaan saada aikaan myös taloudellisia hyötyjä kustannustehokkuudella. Työntekijät pääsevät nopeammin tuottavaan työhön, kun käyttöoikeudet ovat ajan tasalla esimerkiksi uuden työntekijän aloittaessa tai työntekijän vaihtaessa työtehtäviä yrityksen sisällä. Käyttöoikeuksien hallinnassa myös manuaalinen työn määrä vähentyy, kun käyttöoikeuksien hallinnassa hyödynnetään automatiikkaa, jonka seurauksena käyttöoikeuksien hallinnassa ei tarvita niin paljoa työvoimaa, ja tietohallinnon resursseja voidaan ohjata muihin tietohallinnon tehtäviin. Lisäksi manuaalisesta työstä johtuvien inhimillisten virheiden määrä vähenee, kun käyttöoikeuksien hallintaa automatisoidaan. (Kasanen 2010, 2.)

Keskitetty identiteetinhallinta antaa myös loppukäyttäjälle paremman käyttäjäkokemuksen. Käyttäjän kannalta parempi kokemus syntyy, koska käyttäjän kannalta on yksinkertaisempaa, että käyttöoikeudet tulevat ainakin suurimmaksi osin automaattisesti eikä kaikkia käyttöoikeuksia tarvitse tilata erikseen työntekijän tai esimiehen toimesta. Jos joitain käyttöoikeuksia kuitenkin tarvitsee tilata erikseen, ovat ne helppo tilata yhdestä paikasta eli loppukäyttäjän käyttöliittymän kautta ja samalla käyttöoikeustilauksien etenemistä pystyy seuraamaan reaaliaikaisesti. Lisäksi esimies pystyy käyttöliittymän kautta tarkastelemaan alaistensa jo voimassa olevia käyttöoikeuksia. (Kasanen 2010, 2.)

2.4 Työroolit ja käyttäjäroolit

Organisaation työrooleja voidaan hyödyntää käyttöoikeuksien hallinnassa, kun tunnistetut työroolit sekä eri järjestelmien mahdollistamat käyttäjäroolit ja kytketään ne toisiinsa. Työntekijät, joilla on organisaatiossa samanlaiset tai samankaltaiset tietotarpeet, vas-

tuut ja velvollisuudet, voidaan luokitella kuuluvan samaan työrooliin. Käyttäjä voi kuulua useampaan työrooliin ja samassa työroolissa voi olla useampia käyttäjiä. Työroolien määritys on kannattavinta aloittaa ensin karkealla koko organisaation kattavalla tasolla ja yksityiskohtaisemmat työroolit on syytä määrittää organisaation sisältämien yksiköiden tasolla. Työroolien tulee sisältää vain työssä tarvittavat käyttöoikeudet eikä työrooleihin tulisi kiinnittää mitään ylimääräisiä käyttöoikeuksia (Valtiovarainministeriö 2006, 19-20.)

Työroolien määrä organisaatiossa tulisi lisäksi säilyttää hallittavana, koska muuten työroolien määrä saattaa nousta liian suureksi ja pahimmillaan lähes jokaisella käyttäjällä olisi oma työrooli. Työroolien lukumäärä tulisi olla enimmissään sata ja mielellään alle kyseisen lukumäärän. (Kuntaliitto 2013a, 19.) Jotta työroolit ja niihin liitetyt käyttäjäroolit pysyvät hallinnassa, on käytännössä jokaisella työroolilla oltava vastuuomistaja, joka ylläpitää tietoa työroolista ja siihen liitetyistä käyttäjärooleista matriisissa (taulukko 1).

Taulukko 1. Työroolien käyttöoikeudet matriisi (Kuntaliitto 2013b)

Työroolien käyttöoikeudet matriisi			
	Työrooli 1	Työrooli 2	Työrooli 3
Järjestelmä 1	tunnukset ja oikeudet		tunnukset ja oikeudet
Järjestelmä 2		tunnukset ja oikeudet	tunnukset ja oikeudet
Järjestelmä 3	tunnukset ja oikeudet	tunnukset ja oikeudet	

Työroolitiedon kiinnitys käyttäjään tapahtuu henkilön perustietojen luonnin yhteydessä eli käytännössä henkilöstöhallinnossa henkilön palkkauksen yhteydessä, mutta jo rekrytointivaiheessa tulisi määrittää mihin työrooliin työntekijää haetaan. (Kuntaliitto 2013a, 18.) Työrooleja ei ole kannattavaa liittää suoraan esimerkiksi työntekijöiden tehtävänimikkeisiin tai yrityksen organisaatioyksiköihin sillä esimerkiksi samalla tehtä-

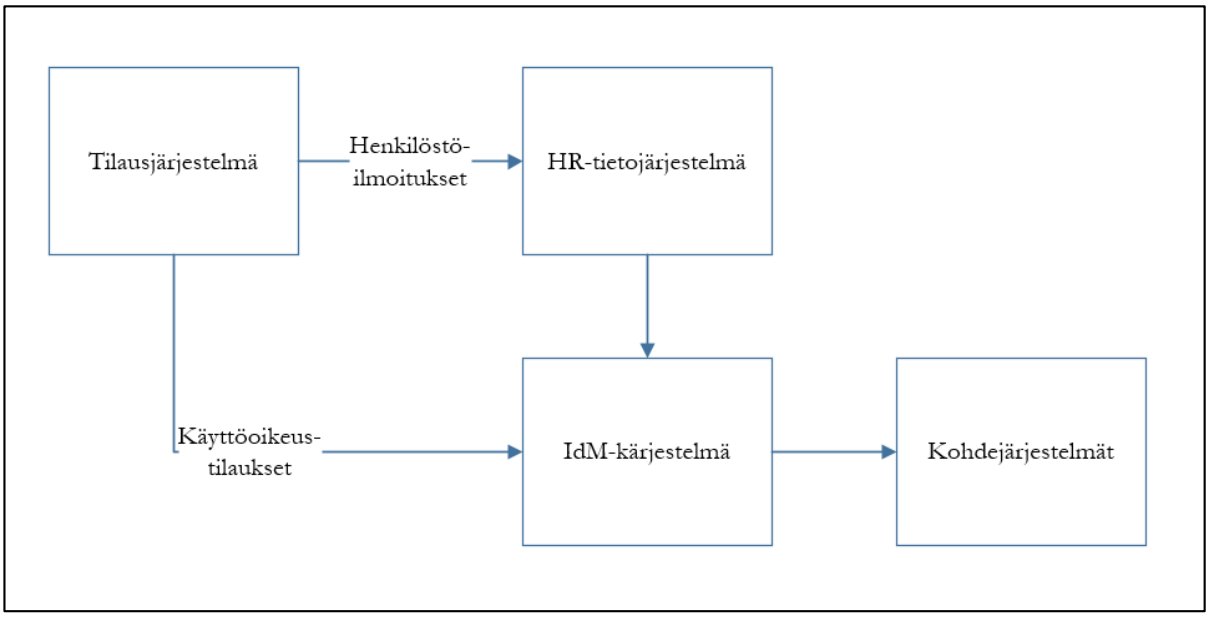
vänimikkeellä toimivat työntekijät voivat toimia hyvin erilaisissa työtehtävissä. Lisäksi yhdessä organisaatioyksikössä voi työskennellä työntekijöitä hyvin erilaisissa työtehtävissä, joten käyttöoikeuksien liittäminen organisaatioihin ei ole myöskään suositeltavaa. (Valtiovarainministeriö 2006, 19.)

3 Case: Yritys X

Yritys X:ssä käyttöoikeuksien hallinnasta tekee haasteellista henkilöstön suuri määrä ja vaihtelevaisuus, erilaisten IT-resurssien lukumäärä sekä yrityksen toistuvat sisäiset muutokset. Yritys X:ssä on kehitetty käyttöoikeuksien hallintaa hiljalleen viimeisen kymmenen vuoden aikana, mutta viimeaikaiset merkittävät sisäiset muutokset Yritys X:ssä ovat saaneet aikaan pakottavan muutostarpeen käyttöoikeuksien hallinnan ja hallintaprosessien uudistamiseksi. Tätä tarkoitusta varten Yritys X:ssä käynnistettiin syksyllä 2012 projekti, jonka tavoitteena on saada aikaan parempi käyttöoikeuksien hallinnan ratkaisu, joka palvelee yrityksen muuttuneita tarpeita.

Yritys X:ssä on käytössä IdM-järjestelmä työvälineenä käyttöoikeuksien hallinnassa. Yritys X:n identiteetinhallinnan arkkitehtuuri on toteutettu samoin kuin kappaleessa 2.3 Identiteetinhallinta kuvattu yleinen identiteetinhallinnan arkkitehtuuri. Yritys X:n identiteetinhallinnan arkkitehtuuri koostuu identiteettitiedon auktoritaarisesta lähteestä, joka Yritys X:ssä on henkilöstöhallinnon omistama HR-tietojärjestelmä, IdM-järjestelmästä sekä kohdejärjestelmistä. (Yritys X tietohallinto, 2012, 1.) Käyttöoikeuksien hallintaprosessilla tarkoitetaan tässä case-osuudessa identiteetinhallinnan tapahtumaketjua, jossa IdM-järjestelmään välittyy HR-tietojärjestelmästä uutta tai muuttunutta identiteettitietoa ja IdM-järjestelmä välittää luodun tai muuttuneen identiteettitiedon käyttäjä- ja käyttöoikeustiedot kohdejärjestelmien käyttäjä- ja käyttöoikeustietovarastoihin.

Yritys X:n IdM-järjestelmä on otettu käyttöön jo vuonna 2006 (Yritys X tietohallinto 2006, 1). Yritys X:n IdM-järjestelmässä ei ole kaikkia ominaisuuksia, joita uudemmissa IdM-järjestelmä-ratkaisuissa on. Kappaleessa 2.3 Identiteetinhallinta kuvatuista toiminnoista Yritys X:n IdM-järjestelmästä puuttuu erillinen käyttöliittymä loppukäyttäjiä varten, mutta sen puuttuminen on Yritys X:ssä korvattu erillisellä tilausjärjestelmällä. Tilausjärjestelmän kautta Yritys X:n työntekijät voivat tehdä käyttöoikeustilauksia sekä ilmoittaa henkilöstömuutoksista henkilöstöilmoituksilla. (Kuvio 4.) Tilausjärjestelmä on Yritys X:n tietohallinnon sekä henkilöstöhallinnon yhteisesti omistama järjestelmä.



Kuvio 4. Yritys X:n Identiteetinhallinnan arkkitehtuuri (Yritys X:n tietohallinto 2012, 1)

Yritys X:ssä päädyttiin IdM-järjestelmän käyttöönottoon vuonna 2006 monesta eri syystä. IdM-järjestelmän käyttöönotolla pyrittiin Yritys X:ssä ratkaisemaan yleisiä perinteiseen käyttöoikeuksien hallintaan liitettyjä ongelmia, joista kerrottiin tarkemmin kappaleessa 2.1 Ongelmat. Lisäksi käyttöönoton tarkoituksena oli, että IdM-järjestelmällä saataisiin Yritys X:ssä aikaan kustannushyötyjen lisäksi muita hyötyjä, joita eriteltiin kappaleessa 2.3 Identiteetinhallinta. Tavoitteena oli myös se, että toimialaan sidonnaiset henkilötietojenkäsittelyyn liittyvät lainsäädännön vaatimukset toteutuisivat aukottomasti. (Yritys X tietohallinto 2006, 1.)

Yritys X:n HR-tietojärjestelmä koostuu toiminnanohjausjärjestelmän HR-moduulista ja siihen liitetystä organisaatiohallintatietokannasta. Yritys X:n HR-tietojärjestelmä kuuluu kappaleessa 2.1 Identiteetinhallinta kuvatuista ryhmistä toiminnallisiin HR-tietojärjestelmiin, koska se on tarkoitettu tyypillisten HR-toimintojen suorittamiseen. HR-tietojärjestelmässä Yritys X:n henkilöstöhallinto ylläpitää keskitetysti tietoa Yritys X:n työntekijöistä, työntekijöiden työsuhteista sekä Yritys X:n organisaatiosta tilausjärjestelmän kautta tulleiden henkilöstöilmoituksien perusteella. (Yritys X:n HR-tietojärjestelmä.)

Työntekijällä tarkoitetaan tässä opinnäytetyössä sekä sisäisiä työsuhteessa Yritys X:ään olevia työntekijöitä että ulkopuolisia toisen yrityksen kautta palvelusopimuksella Yritys X:ssä työskenteleviä työntekijöitä, ellei toisin mainita. Työsuhteella tarkoitetaan sekä todellisia Yritys X:ään sidottuja työsuhteita että palvelusopimuksia. Organisaatioyksiköllä tarkoitetaan liiketoimintayksikköä, johon kuuluu esimies ja työntekijä tai työntekijöitä. Organisaatioyksikköjä voi olla eritasoisia, kuten esimerkiksi tiimi, osasto tai yksikkö. Organisaatiohierarkialla tarkoitetaan puolestaan organisaatioyksiköiden järjestystä suhteessa toisiinsa. HR-prosessi tarkoittaa Yritys X:n henkilöstöhallinnon HR-tietojärjestelmään tekemää HR-tietojen ylläpitoa.

HR-tietojärjestelmän ja IdM-järjestelmän kiinteän kytkennän, ja HR-tietojärjestelmän ollessa IdM-järjestelmän identiteettitiedon auktoritaarinen lähde, on osalla Yritys X:n HR-prosesseista suoria vaikutuksia käyttöoikeuksien hallintaprosesseihin. Tästä syystä käyttöoikeuksien hallintaprosesseja kehitettäessä Yritys X:ssä ei voida keskittyä vain käyttöoikeuksien hallintaprosessien kehittämiseen vaan on tarkasteltava HR- ja käyttöoikeuksien hallintaprosesseja kokonaisuutena. Kappale 3.1 Nykytilan kuvaus ja analyysi sisältää kokonaisuudessaan kuvauksen Yritys X:n HR-prosessien ja käyttöoikeuksien hallintaprosessien yhteyksistä toisiinsa. Kappaleessa 3.2 Kehittämisehdotukset on esitetty nykytilan kuvauksen ja analyysin pohjalta kehittämisehdotuksia Yritys X:n käyttöoikeuksien hallintaprosesseihin.

3.1 Nykytilan kuvaus ja analyysi

Yritys X:ssä HR-prosessit vaikuttavat käyttöoikeuksien hallintaprosesseihin siten, että HR-prosessin suorittaminen HR-tietojärjestelmään voi käynnistää käyttöoikeuksien hallintaprosessin. Lisäksi HR-prosessin aikana tehdyt muutokset HR-tietojärjestelmään vaikuttavat käyttöoikeuksien hallintaprosessissa IdM-järjestelmän suorittamiin hallintatoimenpiteisiin. HR-prosessien yhteydet käyttöoikeuksien hallintaprosesseihin perustuvat Yritys X:ssä siihen, että HR-prosessin aikana voidaan HR-tietojärjestelmässä luoda uutta tai tehdä muutoksia olemassa olevaan identiteettitietoon, joka koostuu HR-tietojärjestelmän tietotyypeistä.

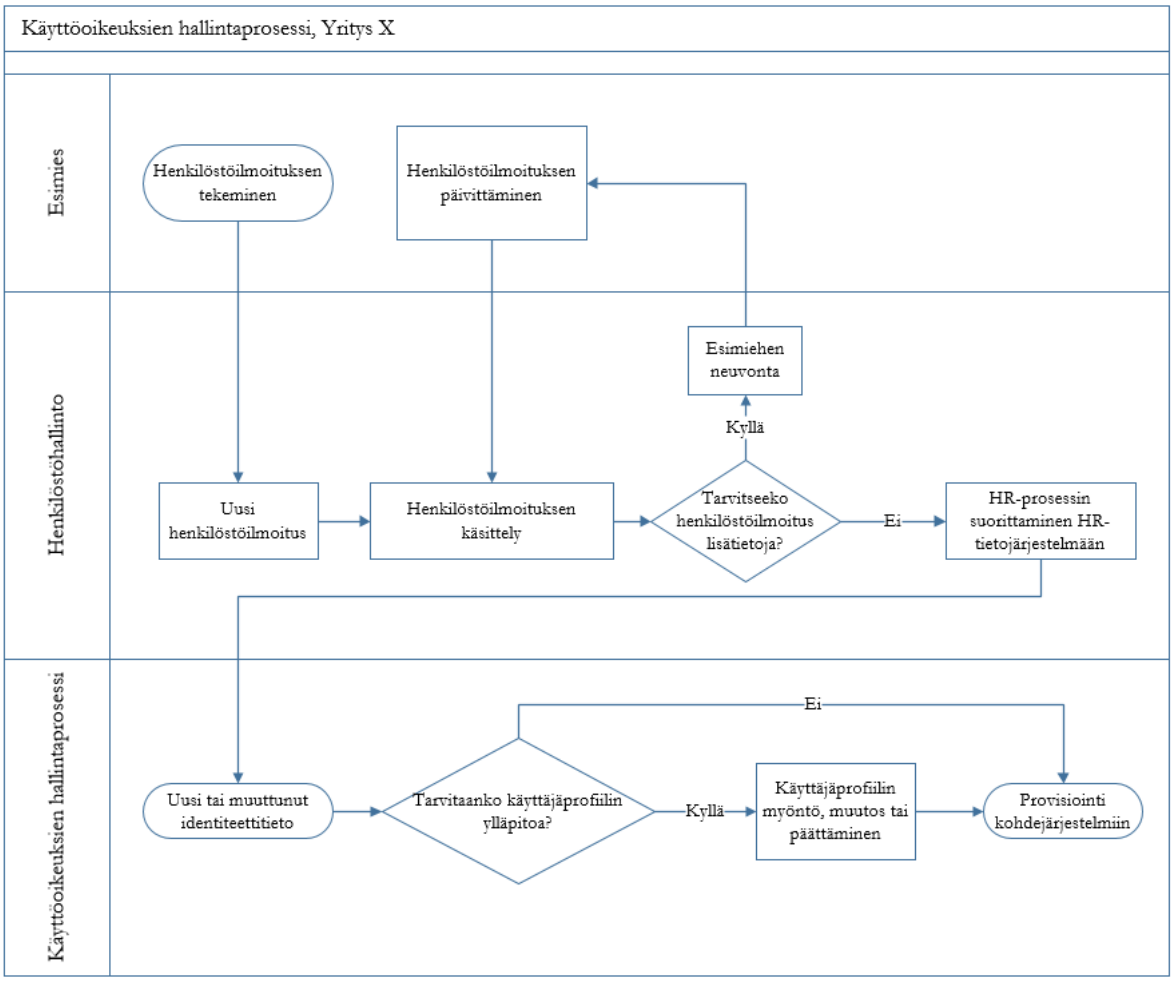
Kappaleessa 3.1.1 HR-prosessit on kuvattu HR-prosessin käynnistämä käyttöoikeuksien hallintaprosessi ja yksilöity HR-prosessit, jotka voivat käynnistää käyttöoikeuksien hallintaprosessin. Lisäksi kappaleessa on selvitetty HR-prosessien vaikutuksia käyttöoikeuksien hallintaprosessin aikana IdM-järjestelmän suorittamiin käyttöoikeuksien ylläpitotoimenpiteisiin. Kappaleessa 3.1.2 Identiteettitieto on kuvattu, mistä HR-tietojärjestelmän tietotyypeistä HR-tietojärjestelmästä IdM-järjestelmään välittyvä identiteettitieto koostuu ja selitetty tietotyyppien merkityksiä Yritys X:ssä. Kappaleessa 3.1.3 Ongelmakohdat on kuvattu ongelmatilanteet, joita HR- ja käyttöoikeuksien hallintaprosessien nykytilassa voi tapahtua käyttöoikeuksien hallinnan näkökulmasta. Kappaleessa on analysoitu myös tekijät, jotka HR- tai käyttöoikeusprosessissa vaikuttavat ongelmatilanteiden syntymiseen.

3.1.1 HR-prosessit

HR-prosessi voi käynnistää käyttöoikeuksien hallintaprosessin, kun HR-prosessin aikana tehdään muutoksia HR-tietojärjestelmään, jonka seurauksena syntyy uutta tai muuttunutta identiteettitietoa, joka välittyy IdM-järjestelmään. Jotta HR-prosessi saadaan Yritys X:n henkilöstöhallinnossa suoritettua HR-tietojärjestelmään, tulee Yritys X:ssä esimiesasemassa toimivan henkilön tehdä henkilöstöilmoitus. Uusi henkilöstöilmoitus siirtyy henkilöstöhallinnon työjonoon ja henkilöstöilmoitus otetaan henkilöstöhallinnossa käsittelyyn. Henkilöstöilmoitus toteutetaan HR-tietojärjestelmään, jos henkilöstöilmoituksessa ovat kaikki tarvittavat tiedot. Jos henkilöstöilmoituksessa ei ole ilmoitettu kaikkia tarvittavia tietoja, henkilöstöhallinto neuvoo esimiestä päivittämään henkilöstöilmoitukseen puutuvat tiedot. Henkilöstöilmoituksen päivittämisen jälkeen, kun henkilöstöhallinnolla on kaikki tarvittavat tiedot, toteutetaan henkilöstöilmoituksessa ilmoitetut muutokset HR-prosessilla HR-tietojärjestelmään. (Kuvio 5.)

Käyttöoikeuksien hallintaprosessi alkaa, kun IdM-järjestelmään välittyy HR-tietojärjestelmästä uutta tai muuttunutta identiteettitietoa. Käyttöoikeuksien hallintaprosessin aikana IdM-järjestelmä voi ylläpitää käyttäjän käyttäjäprofiilia tai pelkästään välittää identiteettitietoa kohdejärjestelmien käyttäjä- ja käyttöoikeustietovarastoihin. IdM-järjestelmä voi ylläpitää käyttäjän käyttäjäprofiilia myöntämällä, muuttamalla tai päättämällä käyttäjäprofiilin. Käyttäjäprofiilin myönnön, muutoksen tai päättämisen

jälkeen IdM-järjestelmä suorittaa aina käyttäjä- ja käyttöoikeustiedon provisioinnin. Jos käyttäjäprofiilia ei tarvitse uuden tai muuttuneen identiteettitiedon perusteella ylläpitää käyttöoikeuksien hallintaprosessin aikana, IdM-järjestelmä suorittaa vain identiteettitiedon provisioinnin kohdejärjestelmiin. (Kuvio 5.)



Kuvio 5. Käyttöoikeuksien hallintaprosessi

Käyttöoikeuksien hallintaprosessissa käyttäjäprofiilin myöntäminen tarkoittaa, että uuden tai muuttuneen identiteettitiedon perusteella käyttäjä on oikeutettu johonkin käyttäjäprofiiliin ja IdM-järjestelmä liittää käyttäjäprofiilitiedon käyttäjän käyttäjä- ja käyttöoikeustietotoihin. Käyttäjäprofiilin muuttaminen tarkoittaa, että käyttäjä on ollut oikeutettu käyttäjäprofiiliin, mutta identiteettitiedoissa on tapahtunut muutos, jonka seurauksena IdM-järjestelmä päättää nykyisen käyttäjäprofiiliin ja myöntää muuttuneen identiteettitiedon perusteella jonkin toisen käyttäjäprofiilin. Käyttäjäprofiilin päättäminen tarkoittaa, että muuttuneen identiteettitiedon perusteella käyttäjä ei ole enää oikeutettu

mihinkään käyttäjäprofiiliin ja IdM-järjestelmä päättää käyttäjäprofiilin voimassaolon käyttäjän käyttäjä- ja käyttöoikeustiedoissa.

HR-prosessit, joiden seurauksena käyttöoikeuksien hallintaprosessi käynnistyy, uuden tai muuttuneen identiteettitiedon seurauksena, ovat työsuhteen alkaminen, organisatorinen muutos, pitkäaikaiselle vapaalle lähtö, pitkäaikaiselta vapaalta paluu, työsuhteen päättyminen, uudelleen aloitus ja organisaatiomuutos. Kun HR-prosessit toteutetaan HR-tietojärjestelmään, voi käyttäjän identiteettitiedoissa tapahtua muutoksia, joiden seurauksena IdM-järjestelmä identiteettitietojen provisioinnin lisäksi ylläpitää käyttäjäprofiilia käyttöoikeuksien hallintaprosessin aikana. (Taulukko 2).

Taulukko 2. HR-prosessien vaikutus käyttäjäprofiilin ylläpitoon (Yritys X:n HR-tietojärjestelmä)

HR-prosessi	**Vaikutus identiteettiin**	**Käyttäjäprofiilin ylläpito**
Työsuhteen alkaminen	Uusi identiteettitieto	Käyttäjäprofiilin myöntö
Organisatorinen muutos	Muutos identiteettitietoon	Käyttäjäprofiilin myöntö / muutos / päättäminen
Pitkäaikaiselle vapaalle lähtö	Muutos identiteettitietoon	Käyttäjäprofiilin päättäminen
Pitkäaikaiselta vapaalta paluu	Muutos identiteettitietoon	Käyttäjäprofiilin myöntö
Työsuhteen päättyminen	Muutos identiteettitietoon	Käyttäjäprofiilin päättäminen
Uudelleen aloitus	Muutos identiteettitietoon	Käyttäjäprofiilin myöntö
Organisaatiomuutos	Muutos identiteettitietoon	Käyttäjäprofiilin myöntö / muutos / päättäminen

HR-tietojärjestelmään luodaan uuden työntekijän tiedot HR-prosessilla työsuhteen alkaminen (Yritys X henkilöstöpalvelut 2011a, 2). HR-tietojärjestelmästä kyseisen HR-prosessin seurauksena välittyy IdM-järjestelmään uusi identiteettitieto. IdM-järjestelmä voi myöntää käyttäjälle käyttäjäprofiilin identiteettitiedon perusteella käyttöoikeuksien hallintaprosessin aikana (taulukko 2). HR-tietojärjestelmään muutokset, joita työntekijälle voi tapahtua työsuhteen aikana, toteutetaan HR-prosessilla organisatorinen muutos. Muutostilanteita työsuhteen aikana ovat esimerkiksi työntekijän työtehtävien vaihtuminen tai tehtävänimikkeen muutos. (Yritys X henkilöstöpalvelut 2012a, 1.) IdM-järjestelmä voi myöntää, muuttaa tai päättää käyttäjän käyttäjäprofiilin muuttuneen identiteettitiedon perusteella (taulukko 2).

Työntekijän jäädessä pidempiaikaiselle vapaalle, kuten vanhempain-, opinto- tai toimivapaalle, toteutetaan muutos työntekijän tietoihin HR-tietojärjestelmässä HR-prosessilla pitkäaikaiselle vapaalle lähtö (Yritys X henkilöstöpalvelut 2012b). Kyseisen HR-prosessin seurauksena IdM-järjestelmä voi muuttuneen identiteettitiedon perusteella päättää käyttäjän käyttäjäprofiilin käyttöoikeuksien hallintaprosessissa, jos käyttäjä on ollut oikeutettu käyttäjäprofiiliin (taulukko 2). Kun työntekijä palaa töihin pitkäaikaiselta vapaalta, suoritetaan HR-tietojärjestelmään HR-prosessi, joka on pitkäaikaiselta vapaalta paluu (Yritys X henkilöstöpalvelut 2012c, 2). IdM-järjestelmä voi tällöin myöntää käyttäjälle käyttäjäprofiilin, jos käyttäjä on muuttuneen identiteettitiedon perusteella oikeutettu johonkin käyttäjäprofiiliin (taulukko 2).

Työntekijän työsuhteen päättyessä päätetään henkilön työsuhde HR-tietojärjestelmästä HR-prosessilla työsuhteen päättyminen (Yritys X henkilöstöpalvelut 2012d, 1). HR-prosessin suorittamisen seurauksena IdM-järjestelmä voi käyttöoikeuksien hallintaprosessin aikana päättää käyttäjäprofiilin, jos käyttäjällä on ollut käyttäjäprofiili käyttäjä- ja käyttöoikeustiedoissaan (taulukko 2). Jos työntekijä palaa Yritys X:ään työsuhteen jo päätyttyä, palkataan työntekijä uudelleen HR-tietojärjestelmään HR-prosessilla uudelleen aloitus (Yritys X henkilöstöpalvelut 2011b, 1). HR-prosessin seurauksena IdM-järjestelmä voi muuttuneen identiteettitiedon perusteella myöntää käyttäjälle käyttäjäprofiilin käyttöoikeuksien hallintaprosessissa (taulukko 2).

HR-prosesseista organisaatiomuutos eroaa muista HR-prosesseista siten, että sitä ei viedä HR-tietojärjestelmään yksittäiselle henkilölle kerrallaan vaan siinä muokataan organisaatiotietoja, joita on käyttäjien identiteettitiedoissa (Yritys X henkilöstöpalvelut 2013, 1). Organisaatiomuutos Yritys X:ssä voi tarkoittaa esimerkiksi sitä, että yritykseen luodaan uusi organisaatioyksikkö, johon siirretään työntekijöitä. Lisäksi organisaatiomuutoksessa voidaan esimerkiksi päättää organisaatioita tai muuttaa organisaatiohierarkiaa. Organisaatiomuutoksen seurauksen voi käynnistyä käyttöoikeuksien hallintaprosessi useammalle käyttäjälle kerrallaan, jossa IdM-järjestelmä voi myöntää, muuttaa tai päättää käyttäjien käyttäjäprofiileja muuttuneiden identiteettitietojen perusteella (taulukko 2).

3.1.2 Identiteettitieto

HR-tietojärjestelmästä IdM-järjestelmään välittyvä identiteettitieto koostuu HR-tietojärjestelmän tietotyypeistä, joten käyttöoikeuksien hallintaprosessin aikana tehdyt ylläpitotoimenpiteet ovat suoraan yhteydessä siihen, mitä tietotyyppejä HR-prosessien aikana ylläpidetään. Identiteettitiedon muodostavat HR-tietojärjestelmän tietotyypit luokitellaan tässä opinnäytetyössä henkilötietoihin, tunnistetietoihin, tehtävätietoihin, työsuhdetietoihin, organisaatiotietoihin sekä henkilöstötoimenpidetietoihin (taulukko 3). Osa tietotyypeistä vaikuttaa käyttäjäprofiileihin siten, että riippuen käyttäjän identiteettitiedoissa olevasta tietotyypin arvosta, käyttäjäprofiili voidaan myöntää tai estää (taulukko 3).

Käyttäjäprofiilin estämisellä tarkoitetaan, että tietotyypillä oleva arvo voi vaikuttaa IdM-järjestelmässä siten, että käyttäjälle ei myönnetä mitään käyttäjäprofiilia. Tietotyypillä oleva arvo ei kuitenkaan vaikuta siihen mikä useasta eri käyttäjäprofiilista käyttäjälle myönnetään. Käyttäjäprofiilin myöntämisellä riippuen tietotyypin arvosta tarkoitetaan, että käyttäjillä, joilla on tietotyypissä eri arvot, voidaan myöntää eri käyttäjäprofiilit. Yritys X:ssä on useampia eri käyttäjäprofiileja, joihin on liitetty erilaisia käyttöoikeuksia. Tässä opinnäytetyössä ei kuitenkaan tarkemmin kuvata, mitkä täsmälliset arvot tietotyypeissä vaikuttavat käyttäjäprofiilien myöntöön tai estoon IdM-järjestelmässä.

Taulukko 3. Identiteettitieto (xxx.idmorha liittymätaulu)

Luokitus	**Tietotyyppi**	**Vaikutus käyttäjä-profiiliin**
Henkilötiedot	Etunimi	
	Kutsumanimi	
	Sukunimi	
	Henkilötunnus	
Tunnistetiedot	Henkilönumero	
	Nimi_id	
	Cics_id	
Tehtävätiedot	Henkilöryhmä	Esto
	Henkilöstöalaryhmä	Esto
	Toiminimike	Esto
	Toiminimikeryhmä	Esto
	Vastuualue	
	Myyntikanava	Esto
	Myyntikanavaryhmä	Esto
Työsuhdetiedot	Työsuhteen alkupvm	
	Työsuhteen päättymispvm	
	Alkuyritys	
Organisaatiotiedot	Yhtiö	Myöntö / Esto
	Yksikkö	Myöntö / Esto
	Osasto	Myöntö / Esto
	Tiimi	Myöntö / Esto
Henkilöstötoimenpidetiedot	Toimenpidekoodi	
	Toimenpidekoodin alkupvm	
	Toimenpidekoodin päättymispvm	

Henkilötietoihin kuuluvat tietotyypit ovat kutsumanimi, etunimi, sukunimi ja henkilötunnus. Tunnistetietoihin kuuluvat tietotyypit ovat henkilönumero, Nimi_id ja Cics_id. (Taulukko 3.) Henkilönumero tarkoittaa HR-tietojärjestelmässä generoituvaa HR-tietojärjestelmässä henkilöitä yksilöivää numeerista tunnistetta. Nimi_id ja Cics_id ovat erillisessä järjestelmässä generoitavia tunnuksia, jotka toimivat työntekijöiden käyttäjätunnuksina Yritys X:n järjestelmissä. Nimi_id ja Cics_id generoidaan henkilön kutsuma- ja sukunimestä. Nimi_id:llä on looginen ja Cics_id:llä epälooginen yhteys henkilön kutsuma- ja sukunimeen. (Yritys X henkilöstöpalvelut 2011a, 1-2.)

Tehtävätietoihin kuuluvat tietotyypit ovat henkilöryhmä, henkilöstöalaryhmä, toiminimike, toiminimikeryhmä, vastuualue, myyntikanava sekä myyntikanavaryhmä (taulukko 3). Henkilöryhmä ilmaisee HR-tietojärjestelmässä onko henkilö Yritys X:ssä sisäinen vai ulkopuolinen työntekijä, ja onko työntekijän työsuhde aktiivinen vai passiivinen. Henkilöstöalaryhmä HR-tietojärjestelmässä ilmentää tarkemmin työntekijän työsuhteen laatua. Henkilöstöalaryhmiä ovat esimerkiksi toimihenkilö, asiantuntija, johtaja, kon-

sultti ja vuokratyöntekijä. Yritys X:ssä HR-tietojärjestelmän tehtävänimikkeet ovat jaoteltu toiminimikkeisiin ja osa toiminimikkeistä kuuluu toiminimikeryhmiin. (Yritys X:n HR-tietojärjestelmä.) Identiteettitiedoissa olevan henkilöryhmän, henkilöstöalaryhmän tai toiminimikkeen ja toiminimikeryhmän perusteella IdM-järjestelmä voi estää käyttäjäprofiilit (taulukko 3). Käyttäjäprofiilit estetään, jos tietotyyppien sisällöt viittaavat ulkopuoliseen työntekijään. Sisäisillä työntekijöillä eri arvot edellä mainituissa tietotyypeissä eivät kuitenkaan vaikuta siihen, minkä käyttäjäprofiilin IdM-järjestelmä myöntää identiteettitiedon perusteella. (Yritys X henkilöstöpalvelut, 2011c).

Tehtävän vastuualuetieto on Yritys X:ssä palkanlaskennassa käytetty tunniste kulujen kohdistamiselle. Myyntikanavaa ja myyntikanavaryhmää ylläpidetään HR-tietojärjestelmässä myyntitehtävissä toimiville työntekijöille ja kyseiset tiedot vaikuttavat esimerkiksi myynnin palkkiointiin. (Yritys X henkilöstöpalvelut 2011c, 2; Yritys X:n HR-tietojärjestelmä.) Myyntikanavassa ja myyntikanavaryhmässä olevan arvon perusteella IdM-järjestelmä voi estää käyttäjäprofiilit. Työsuhdetietoihin kuuluvat työsuhteen alku- ja päättymispäivämäärä sekä alkuyritys. (Taulukko 3). IdM-järjestelmään välittyy aina viimeisimmän työsuhteen alkupäivämäärä ja viimeisimmän työsuhteen päättymispäivämäärä, jos sellainen on viety HR-tietojärjestelmään. Alkuyritys kertoo yhtiöryhmään kuuluvan yrityksen, johon henkilö on ollut työsuhteessa viimeisimmän työsuhteensa alkaessa. (Yritys X:n HR-tietojärjestelmä.)

Organisaatiotietoihin kuuluvat tietotyypit ovat yhtiö, yksikkö, osasto ja tiimi (taulukko 3). Yhtiö-, yksikkö-, osasto-, ja tiimitiedot ilmaisevat tarkalla tasolla, miten työntekijä on organisatorisesti sijoittunut Yritys X:n organisaatioon HR-tietojärjestelmässä. Identiteettitietoihin voi mennä kaikki neljä organisaatiotietoa tai vain osa niistä. Esimerkiksi yksikönjohtajan identiteettitietoihin menee tiedot yhtiöstä ja yksiköstä, mutta ei osastosta ja tiimistä. Organisaatiotietoihin on kohdistettu IdM-järjestelmässä päättelysääntöjä käyttäjäprofiileista. IdM-järjestelmä voi myöntää tai estää käyttäjäprofiilit organisaatiotietojen perusteella (taulukko 3). Työntekijöiden, joilla on identiteettitiedoissa eri organisaatiotiedot, käyttäjäprofiilit saattavat sisältää eri käyttöoikeuksia. IdM-järjestelmä voi myös joidenkin organisaatiotiedoissa olevien arvojen perusteella estää kaikki käyttäjäprofiilit. (Yritys X henkilöstöpalvelut 2011a, 1; Yritys X henkilöstöpalvelut 2011c, 2.)

Henkilöstötoimenpidetietoihin kuuluvat tietotyypit ovat toimenpidekoodi ja toimenpidekoodin alku- ja päättymispäivämäärä (taulukko 3). Henkilöstötoimenpiteet ovat valmiita toimenpideketjuja, joiden avulla HR-prosesseja suoritetaan HR-tietojärjestelmään. Henkilöstötoimenpiteet ovat HR-tietojärjestelmässä yksilöityjä numeerisilla tunnisteilla. (Yritys X:n HR-tietojärjestelmä.) Kun HR-tietojärjestelmässä tehdään käyttäjälle henkilöstötoimenpide, välittyy henkilöstötoimenpiteeseen liitetty toimenpidekoodi ja sen alku- ja päättymispäivämäärä IdM-järjestelmään muiden identiteettitietojen lisäksi (taulukko 3).

3.1.3 Ongelmakohdat

HR-prosessien ja käyttöoikeuksien hallintaprosessien nykytilan kuvauksen perusteella voidaan havaita asioita, jotka voivat johtaa Yritys X:ssä ongelmatilanteisiin käyttöoikeuksien hallinnan näkökulmasta. Ongelmakohdat käyttöoikeuksien hallintaprosesseissa voivat aiheuttaa Yritys X:n kannalta vahingollisia tilanteita, kuten Yritys X:n luottamuksellisen ja salaisen tiedon vaarantumisen työntekijöiden liian laajojen käyttöoikeuksien takia. Tässä kappaleessa on tuotu esiin ongelmakohdat Yritys X:n käyttöoikeuksien hallintaprosesseissa ja kuvattu minkälaisia ongelmatilanteita ne voivat aiheuttaa.

Tällä hetkellä Yritys X:n IdM-järjestelmä ei saa tarpeeksi identiteettitietoa HR-tietojärjestelmästä, jotta IdM-järjestelmä pystyisi yksilöimään työntekijän työroolin Yritys X:ssä. Identiteettitiedon sisältämistä tietotyypeistä mikään tietotyyppi ei yksittäin tai yhdisteltynä yksilöi työntekijän työroolia Yritys X:ssä. Tietotyypit, joista identiteettitieto koostuu, ovat luotu HR-tietojärjestelmään henkilöstöhallinnon tarkoituksia varten. Puutteellisen identiteettitiedon vuoksi käyttäjäprofiilien päättelysääntöjä on liitetty tietotyyppeihin, jotka eivät täysin palvele käyttöoikeuksien hallinnan tarpeita, kuten organisaatiotietoihin.

Esimerkkitilanteessa HR-tietojärjestelmään on luotu organisaatioyksikkö, jonka nimi on toimisto Y ja IdM-järjestelmässä on liitetty päättelysääntö käyttäjäprofiilista kyseiseen organisaatioyksikköön. Toimisto Y:ssä toimii myyjiä, jotka myyvät erilaisia tuotteita, asiakaspalvelijoita, siivoojia ja muuta henkilökuntaa erilaisissa työtehtävissä. Kun IdM-järjestelmä myöntää Toimisto Y:ssä työskenteleville työntekijöille käyttäjäprofiilit orga-

nisaatiotietojen mukaan, saavat kaikki organisaatioyksikössä työskentelevät työntekijät saman käyttäjäprofiilin käyttäjä- ja käyttöoikeustietoihinsa ellei käyttäjäprofiilia ole työntekijöiden muun identiteettitiedon perusteella estetty.

Tässä tilanteessa toimisto Y:n asiakaspalvelija voi saada käyttäjäprofiilin kautta käyttöoikeuksia, joita tarvitaan myyjän työtehtävässä. Asiakaspalvelija voi todellisuudessa tarvita johonkin järjestelmään katseluoikeudet, mutta saa käyttäjäprofiilin kautta järjestelmään myös muutosoikeudet, joita myyjän työtehtävässä tarvitaan. Työntekijöille tulisi myöntää käyttöoikeudet niihin resursseihin, joita työtehtävien puitteissa tarvitaan ja käyttöoikeudet resurssiin tulisi rajata vain työtehtävien kannalta välttämättömiin toimintoihin (Ferraiolo ym. 1992, 9). Toinen vaihtoehto on, että käyttäjäprofiili sisältää vain käyttöoikeudet, jotka eivät ota kantaa työtehtävissä tarvittaviin käyttöoikeuksiin, jolloin työtehtävässä tarvittavat käyttöoikeudet tulee tilata erikseen. Käyttöoikeuksien hakemiseen ja käyttöoikeustilauksien käsittelyyn voi mennä aikaa, jonka työntekijä on ilman työtehtävässä tarvittavia käyttöoikeuksia.

Käyttäjäprofiilien päättelysääntöjen liittämisestä organisaatiotietoihin voi aiheutua myös muita ongelmatilanteita käyttöoikeuksien hallinnan kannalta. Esimerkiksi, jos henkilöstöhallinto päättää HR-tietojärjestelmästä organisaatioyksikön, johon on IdM-järjestelmässä viety päättelysääntö käyttäjäprofiilista. Kun organisaatioyksikkö päätetään HR-tietojärjestelmästä, päättyy organisaatiotiedon voimassaolo myös käyttäjien identiteettitiedoista IdM-järjestelmässä, joten myös mahdollisten käyttäjäprofiilien voimassaolo päättyy. Pahimmillaan tuhansilta työntekijöiltä voisi päättyä samaan aikaan käyttäjäprofiilit ja tästä voisi aiheutua merkittävää haittaa Yritys X:lle, koska työntekijöillä ei enää olisi työssä tarvittavia käyttöoikeuksia.

Käyttäjäprofiilit ovat työntekijöiltä estetty, jos identiteettitiedoissa olevan tietotyypin arvo viittaa ulkopuoliseen työntekijään, kuten henkilöstö- ja henkilöstöalaryhmä. Esimies joutuu näin ollen ulkopuoliselle työntekijälle tilaamaan käyttöoikeudet käyttöoikeustilauksilla, joiden käsittelyyn voi mennä aikaa Yritys X:n käyttöoikeustiimissä. Tästä voi aiheutua Yritys X:lle haittaa, koska ulkopuolista työvoimaa käytetään usein paikkaamaan kausittaista tai määräaikaista tarvetta lisätyövoimalle. Esimerkiksi, jos Yritys X:n asiakaspalvelukeskukseen tulisi erityisen paljon yhteydenottaja joka vuosi joulun

aikaan. Yritys X palkkaisi joulun ajaksi asiakaspalvelukeskukseen ulkopuolisia vuokratyöntekijöitä helpottamaan kiiretilannetta, jotta asiakkaita pystytään palvelemaan nopeammin. Vaikka ulkopuolisella työntekijällä on identiteettitiedoissaan samat organisaatiotiedot kuin sisäisellä työntekijällä, ei ulkopuoliselle työntekijälle identiteettitietojen perusteella IdM-järjestelmä myönnä käyttäjäprofiilia. Tästä syystä esimies joutuu tilaamaan ulkopuolisten työntekijöiden käyttöoikeudet erikseen.

Jos ruuhka-avuksi palkatun vuokratyöntekijälle tehtyjä käyttöoikeustilauksia ei pystytä käsittelemään nopeasti, voi vuokratyöntekijä olla jonkin aikaa ilman työssä tarvittavia käyttöoikeuksia. Tämä on erityisen harmillista, jos vuokratyöntekijä palkataan ruuhka-avuksi vain lyhyeksi ajaksi, esimerkiksi viikoksi, ja hän on työajasta esimerkiksi kaksi päivää ilman työssä tarvittavia käyttöoikeuksia. Yritys X:n asiakaspalvelukeskus ei saa vuokratyöntekijän palkkaamisesta huolimatta heti apua ruuhkatilanteen helpottamiseksi ja Yritys X maksaa kahdelta päivältä vuokratyöntekijästä turhaan, koska tämä ei pysty tekemään tarvittavia työtehtäviä.

Käyttöoikeuksien hallintaprosessi ei pääse Yritys X:ssä käynnistymään ennen kuin HR-prosessi on saatu päätökseen, joka voi johtaa siihen, että työntekijän käyttöoikeudet eivät ole aina ajan tasalla. Esimerkiksi tällainen ongelmatilanne voi syntyä työntekijän vaihtaessa työtehtäviä yrityksen sisällä niin, että hän vaihtaa fyysistä työpistettään toimistosta A toimistoon B. Toimistoon A ja toimistoon B kuuluvilla työntekijöillä on eri käyttäjäprofiilit johtuen erilaisista organisaatiotiedoista käyttäjä- ja käyttöoikeustiedoissa. Esimerkkitilanteessa esimies on tehnyt työntekijän työtehtävien muutoksesta henkilöstöilmoituksen, mutta ei ole ilmoittanut kaikkia henkilöstöhallinnon tarvitsemia tietoja, joten henkilöstöhallinto ei pysty tekemään muutosta HR-tietojärjestelmään. Henkilöstöhallinnosta pyydetään esimiestä päivittämään henkilöstöilmoitukseen puuttuvat tiedot ja siinä vaiheessa, kun esimies päivittää henkilöstöilmoituksen, olisi muutoksen pitänyt jo astua voimaan.

Kun HR-prosessia ei saada päätökseen ajoissa, työntekijän käyttöoikeudet eivät ole ajan tasalla johtuen siitä, että uudet organisaatiotiedot eivät ole oikeasta muutospäivämäärästä päivittyneet työntekijän käyttäjä- ja käyttöoikeustietoihin. Tämä johtaa siihen, että työntekijän perehdytys uusiin työtehtäviin vaikeutuu tai estyy kokonaan. Lisäksi työn-

tekijällä ovat vanhan organisaation mukaiset käyttöoikeudet vielä voimassa, joten työntekijä voi päästä katselemaan ja muokkaamaan tietoja, joihin hänellä ei uuden toimenkuvan puitteissa olisi enää tarvetta eikä oikeutta nähdä ja käsitellä.

3.2 Kehittämisehdotukset

Yritys X:n käyttöoikeuksien hallintaprosessien ongelmakohdat syntyivät pääsääntöisesti johtuen siitä, että IdM-järjestelmä ei saa tarpeeksi identiteettitietoa HR-tietojärjestelmästä työtehtäväkohtaisten käyttöoikeuksien päättelemiseksi. Tästä syystä opinnäytetyössä lähdettiin pohtimaan kehittämisehdotuksia erityisesti identiteettitiedon sisältöön liittyen. Toiseksi ongelmakohtia käyttöoikeuksien hallintaprosesseissa todettiin aiheuttavan se, että käyttöoikeuksien hallintaprosessi ei pääse käynnistymään ennen kuin HR-prosessi on saatu päätökseen henkilöstöhallinnossa. Tästä tosin aiheutuu ongelmatilanteita käyttöoikeuksien hallintaprosessissa vain tapauksissa, joissa HR-prosessia ei syystä tai toisesta ehditä saamaan päätökseen ajoissa todelliseen muutosajankohtaan.

Yritys X:ssä käyttöoikeuksien hallintaprosesseja tulisi kehittää niin, että IdM-järjestelmä saisi tarpeeksi identiteettitietoa tehtäväkohtaisten käyttöoikeuksien päättelemiseksi. Tämä voitaisiin Yritys X:ssä toteuttaa tekemällä määrittelyt työrooleista ja niihin kytkettävistä käyttäjärooleista, kuten kuvattiin kappaleessa 2.4 Työroolit ja käyttäjäroolit. Työroolitiedon esimies pystyisi ilmoittamaan henkilöstöilmoituksella HR-tietojen lisäksi esimerkiksi uuden työntekijän aloittaessa ja työsuhteen muutostilanteissa. Työntekijälle olisi mahdollista antaa myös useampia työrooleja. Esimies pystyisi tilaamaan työntekijälle useampia työrooleja esimerkiksi määräajaksi työntekijän sijaistaessa Yritys X:n toista työntekijää. Henkilöstöhallinto tallentaisi tiedon työntekijän työroolista HR-tietojärjestelmään, josta se välittyisi lopulta myös IdM-järjestelmään.

Työroolien tallentaminen HR-tietojärjestelmään tarkoittaisi sitä, että HR-tietojärjestelmään määriteltäisiin ja toteutettaisiin uusia tietotyyppejä. HR-tietojärjestelmään lisättäisiin tietotyypit työrooli, työroolin alkupäivämäärä sekä työroolin päättymispäivämäärä. Tietotyyppejä voitaisiin kutsua työroolitiedoiksi. Henkilöstöhallinto pystyisi ylläpitämään työroolitietoja HR-prosessin aikana samaan aikaan kuin muita HR-tietoja

tai HR-prosessista erillisesti ylläpitämällä vain työroolitietoja. Työroolitietojen ylläpito HR-prosessista erillisenä tosin vaatii sen, että työntekijän tiedot ovat jo kertaalleen luotu HR-tietojärjestelmään HR-prosessissa työsuhteen alkaminen.

Työroolitietojen myötä identiteettitiedon ei tarvitsisi koostua niin monesta HR-tietojärjestelmän eri tietotyypeistä, koska käyttöoikeuksien hallinta perustuisi työroolitietoihin. Identiteettitieto koostuisi työroolitietojen lisäksi henkilötiedoista, tunnistetiedoista, työsuhdetiedoista sekä henkilöstötoimenpidetiedoista. Työsuhdetiedoista alkuyrityksen ja organisaatiotietojen ei tarvitsisi välittyä IdM-järjestelmään identiteettitietona, koska kyseisillä tiedoilla olisi enää merkitystä käyttöoikeuksien hallinnan kannalta. (Taulukko 4.) IdM-järjestelmän tarvitsisi enää muun identiteettitiedon kuin työroolitietojen perusteella estää tai myöntää käyttöoikeuksia.

Taulukko 4. Uusi identiteettitieto

Henkilötiedot	Etunimi
	Kutsumanimi
	Sukunimi
	Henkilötunnus
Tunnistetiedot	Henkilönumero
	Nimi_id
	Cics_id
Työroolitiedot	Työrooli
	Työroolin alkupäivämäärä
	Työroolin päättymispäivämäärä
Työsuhdetiedot	Työsuhteen alkupäivämäärä
	Työsuhteen päättymispäivämäärä
Henkilöstötoimenpidetiedot	Toimenpidekoodi
	Toimenpidekoodin alkupvm
	Toimenpidekoodin päättymispvm

Kehittämisehdotuksen mukaan henkilötiedot ja tunnistetiedot välittyvät edelleen IdM-järjestelmään käyttäjien tunnistamista varten. Lisäksi on perusteltua, että työsuhdetiedoista työsuhteen alku- ja päättymispäivämäärä välittyvät yhä identiteettitiedoissa,

jotta käyttöoikeuksien hallinnassa pystytään valvomaan, että käyttäjä on oikeutettu käyttöoikeuksiin Yritys X:n järjestelmiin. Myös henkilöstötoimenpidetiedot välittyvät kehittämisehdotuksen mukaan edelleen IdM-järjestelmään, koska ne helpottavat henkilöstöhallinnon ja käyttöoikeuksia ylläpitävän toiminnon yhteistyötä. Henkilöstötoimenpidekoodeista ja sen alku- ja päättymispäivämääristä käyttöoikeuksien hallinnassa tunnistetaan tilanteet esimerkiksi miksi käyttäjän käyttöoikeudet on päätetty. (Taulukko 4.)

Kehittämisehdotuksesta saatavia hyötyjä ovat tietoturvallisuuden parantuminen ja manuaalisen työn määrän vähentyminen käyttöoikeuksien hallinnassa. Lisäksi saadaan aikaan työntekijöiden päivittäisin työn turvaamisen kannalta parempi ratkaisu. Tietoturva paranee, kun työroolien käyttöoikeussisällöt ovat kerralla työstetty yhdessä liiketoiminnan kanssa. Esimiehet eivät enää tilaa työntekijöille tarpeettomia tai liian laajoja käyttöoikeuksia, kun he eivät enää ole epävarmoja, mitä käyttöoikeuksia heidän tulisi tilata. Manuaalisen työn määrä vähentyy käyttöoikeuksien hallinnassa, koska suuri osa käyttöoikeuksista tulisi työntekijöille työroolitiedon kautta automaattisesti. Tosin, jotta työroolien määrä saadaan pidettyä hallittavana, tulee Yritys X:ssä varmasti olemaan myös erikseen tilattavia käyttöoikeuksia, joita ei sisälly työrooleihin liitettyihin käyttöoikeuksiin.

Kun HR-tietojärjestelmässä on työroolia ilmaiseva tietotyyppi, ei ole enää tarpeellista viedä käyttöoikeuspäättelyitä esimerkiksi organisaatioyksiköihin. Näin vältyttäisiin ongelmatilanteilta, joita tuotiin esiin kappaleessa 3.1.3 Ongelmakohdat. Lisäksi esimies pystyisi valitsemaan työroolin myös ulkopuoliselle työntekijälle, joten Yritys X:ssä päästäisiin eroon myös ulkopuolisiin työntekijöihin liittyvästä problematiikasta käyttöoikeuksien hallinnassa. Käyttöoikeuksien hallintaprosessin käynnistymisen ei ole työsuhteen muutos- ja päättymistilanteissa riippuvainen HR-prosessin viemisestä päätökseen henkilöstöhallinnossa, koska henkilöstöhallinnossa voidaan ylläpitää työroolitietoa, vaikka muita tarvittavia HR-tietoja ei olisi saatu ajoissa muutosajankohtaan. Työroolitietojen lisääminen identiteettitietoihin muuttaisi HR-prosessien vaikutusta käyttöoikeuksien hallintaprosesseihin myös siten, että käyttöoikeuksien kannalta riskialtis HR-prosessi organisaatiomuutos ei vaikuttaisi enää käyttöoikeuksien hallintaprosesseihin.

4 Yhteenveto

Käyttöoikeuksien hallinta on monissa yrityksissä koettu haasteelliseksi ja käyttöoikeuksien hallinnassa on usein ongelmia liittyen epäselviin prosesseihin ja vastuisiin, käyttöoikeuksien hallinnan hajautumiseen eri toimintoihin sekä työntekijöiden huonosti hallittuihin käyttöoikeuksiin. (VM 2006, 10.) Käyttöoikeuksien hallinnan perusperiaate on, että käyttäjälle tulisi antaa käyttöoikeudet vain niihin resursseihin, joita he välttämättä tarvitsevat. Lisäksi käyttöoikeudet tulisi rajata vain niiden toimintojen suorittamiseksi kuin työtehtävien puitteissa tarvitaan. (Ferraiolo ym. 1992, 9.) Sen lisäksi, että työnantajana toimivan yrityksen tulee huolehtia tietoturvasta koskien yrityksen salaista ja luottamuksellista tietoa, asettaa laki myös vaatimuksia työnantajana toimiville yrityksille. Vaatimukset työnantajaa kohtaan kohdistuvat muun muassa työntekijöiden henkilötietojen käsittelyyn, joita käsitellään myös käyttöoikeuksien hallinnassa. (Valtiovarainministeriö 2006, 11-12.)

Tämän opinnäytetyön tavoitteena oli kuvata ja analysoida käyttöoikeuksien hallintaprosessien yhteydet HR-prosesseihin Yritys X:ssä ja saada aikaan kehittämisehdotuksia, joilla käyttöoikeuksien hallintaprosesseja voidaan kehittää Yritys X:ssä. Kehittämisehdotuksien tavoitteita oli myös tukea toimeksiantajana olevan käyttöoikeushallinnan omistajan määrittelemiä tavoitteita käyttöoikeuksien hallinnan automatisoinnista, manuaalisen työn vähentämisestä sekä tietoturvallisuuden parantamisesta. Opinnäytetyölle omia tavoitteitani olivat oppia muun muassa prosessien kehittämisestä, identiteetinhallinnasta sekä HR-prosessien ja käyttöoikeuksien hallintaprosessien yhteyksistä. Tutkimusmenetelmänä opinnäytetyössä hyödynnettiin tapaustutkimusta, joka soveltuu kehittämistöihin, joiden tavoitteena on saada kehittämisehdotuksia ja kehittämisen kohteena on esimerkiksi yritys tai sen toiminta tai prosessi (Ojasalo 2009, 52).

Identiteetinhallinnalla voidaan ratkoa käyttöoikeuksien hallintaan liittyviä ongelmia keskittämällä ja automatisoimalla käyttöoikeuksien hallintaa (Kasanen 2010, 1). Identiteetinhallinnan arkkitehtuuri koostuu identiteettitiedon auktoritaarisesta lähteestä, IdM-järjestelmästä sekä kohdejärjestelmistä. Identiteetinhallintajärjestelmä, IdM-järjestelmä, koostuu useammasta toiminnallisesta osasta eli lähdetiedon välitysrajapinnasta, keskitetystä käyttäjä- ja käyttöoikeustietovarastosta, käyttöliittymistä sekä käyttäjä- ja käyttöoi-

keustiedon provisointirajapinnasta kohdejärjestelmiin. (Kasanen 2010, 3) Keskitetystä identiteetinhallinnasta saadaan aikaan hyötyä yrityksen koosta ja toimialasta riippumatta paremmalla kustannustehokkuudella, hallittavuudella sekä loppukäyttäjäkokemuksella (Kasanen 2010, 2).

Organisaation työrooleja voidaan hyödyntää käyttöoikeuksien hallinnassa, kun tunnistetut työroolit sekä eri järjestelmien mahdollistamat käyttäjäroolit ja kytketään ne toisiinsa. Työntekijät, joilla on organisaatiossa samanlaiset tai samankaltaiset tietotarpeet, vastuut ja velvollisuudet, voidaan luokitella kuuluvan samaan työrooliin. (Valtiovarainministeriö 2006, 19-20.) Työroolien määrä organisaatiossa tulisi lisäksi säilyttää hallittavana, koska muuten työroolien määrä saattaa nousta liian suureksi ja pahimmillaan lähes jokaisella käyttäjällä olisi oma työrooli. Jotta työroolit ja niihin liitetyt käyttäjäroolit pysyvät hallinnassa, on käytännössä jokaisella työroolilla oltava vastuuomistaja, joka ylläpitää tietoa työroolista ja siihen liitetyistä käyttäjärooleista matriisissa. (Kuntaliitto 2013a, 19.)

Opinnäytetyön case-osuudessa otettiin tarkasteluun Yritys X, jossa käyttöoikeuksien hallintaa on osin keskitetty ja automatisoitu IdM-järjestelmän käyttöönotolla, mutta yrityksessä tapahtuneet sisäiset muutokset ovat saaneet aikaan pakottavan muutostarpeen käyttöoikeuksien hallinnan uudistamiseksi. Yritys X:n identiteetinhallinnan arkkitehtuuri on toteutettu samoin kuin kappaleessa 2.3 Identiteetinhallinta kuvattu yleinen identiteetinhallinnan arkkitehtuuri. IdM-järjestelmän auktoritaarinen lähde on Yritys X:n henkilöstöhallinnon ylläpitämä HR-tietojärjestelmä, joten Yritys X:ssä HR-prosesseilla on kiinteä vaikutus käyttöoikeuksien hallintaprosesseihin.

Kappaleessa 3.1 Nykytilan kuvaus ja analyysi kuvattiin HR-prosessien yhteydet käyttöoikeuksien hallintaprosesseihin Yritys X:ssä. Kappaleessa tultiin niihin tuloksiin, että Yritys X:ssä HR-prosessin suorittaminen HR-tietojärjestelmään voi käynnistää käyttöoikeuksien hallintaprosessin. Lisäksi havaittiin, että HR-prosessin aikana tehdyt muutokset HR-tietojärjestelmään vaikuttavat käyttöoikeuksien hallintaprosessissa IdM-järjestelmän suorittamiin hallintatoimenpiteisiin. HR-prosessien vaikutukset käyttöoikeuksien hallintaprosesseihin perustuvat siihen, että HR-tietojärjestelmästä IdM-järjestelmään välittyvä identiteettitieto koostuu HR-tietojärjestelmän tietotyypeistä.

Kappaleessa 3.1.1 HR-prosessit yksilöitiin HR-prosessit, joiden seurauksena käyttöoikeuksien hallintaprosessi käynnistyy, uuden tai muuttuneen identiteettitiedon seurauksena. HR-prosessit, jotka käynnistävät käyttöoikeuksien hallintaprosessin ovat työsuhteen alkaminen, organisatorinen muutos, pitkäaikaiselle vapaalle lähtö, pitkäaikaiselta vapaalta paluu, työsuhteen päättyminen, uudelleen aloitus sekä organisaatiomuutos. Kun HR-prosessit toteutetaan HR-tietojärjestelmään, voi käyttäjän identiteettitiedoissa tapahtua muutoksia, joiden seurauksena IdM-järjestelmä identiteettitietojen provisioinnin lisäksi ylläpitää käyttäjän käyttäjäprofiilia käyttöoikeuksien hallintaprosessin aikana. (Taulukko 2).

IdM-järjestelmä voi myöntää käyttäjälle käyttäjäprofiilin HR-prosessien seurauksena, jotka ovat työsuhteen alkaminen, organisatorinen vaihto, pitkäaikaiselta vapaalta paluu, uudelleen aloittaminen ja organisaatiomuutos. IdM-järjestelmä voi taas muuttaa käyttäjän käyttäjäprofiilin HR-prosessien seurauksena, jotka ovat organisatorinen vaihto ja organisaatiomuutos. HR-prosessien organisatorinen vaihto, pitkäaikaiselle vapaalle lähtö, työsuhteen päättäminen ja organisaatiomuutos seurauksena IdM-järjestelmä voi puolestaan päättää käyttäjän käyttäjäprofiilin. (Taulukko 2.)

Kappaleessa 3.1.2 Identiteettitieto kuvattiin HR-tietojärjestelmän tietotyypit, jotka välittyvät identiteettitietona IdM-järjestelmään ja selvitettiin tietotyyppien merkityksiä Yritys X:ssä. Identiteettitiedon muodostavat HR-tietojärjestelmän tietotyypit luokiteltiin opinnäytetyössä henkilötietoihin, tunnistetietoihin, tehtävätietoihin, työsuhdetietoihin, organisaatiotietoihin sekä henkilöstötoimenpidetietoihin. Henkilötietoihin kuuluvat tietotyypit ovat kutsumanimi, etunimi, sukunimi ja henkilötunnus. Tunnistetietoihin kuuluvat tietotyypit henkilönumero, Nimi_id ja Cics_id. Tehtävätietoihin kuuluvat tietotyypit henkilöryhmä, henkilöstöalaryhmä, toiminimike, toiminimikeryhmä, vastuualue, myyntikanava sekä myyntikanavaryhmä. Organisaatiotietoihin kuuluvat tietotyypit yhtiö, yksikkö, osasto ja tiimi. Lisäksi henkilöstötoimenpidetietoihin kuuluvat tietotyypit toimenpidekoodi ja toimenpidekoodin alku- ja päättymispäivämäärä. (Taulukko 3.)

Tehtävätiedoista henkilöryhmän, henkilöstöalaryhmän, toiminimikkeen, toiminimikeryhmän, myyntikanavan sekä myyntikanavaryhmän perusteella IdM-järjestelmä voi es-

tää käyttäjältä käyttäjäprofiilit. Organisaatiotiedoista yhtiön, yksikön, osaston ja tiimin perusteella käyttäjältä voidaan estää käyttäjäprofiili tai sen perusteella voidaan myöntää käyttäjäprofiili. Opinnäytetyössä ei kuitenkaan tutkittu mitkä täsmälliset arvot yllä mainituissa tietotyypeissä vaikuttavat käyttäjäprofiilin estämiseen tai myöntämiseen. (Taulukko 3.)

Kappaleessa 3.1.3 Ongelmakohdat kuvattiin nykytilan kuvauksen perusteella ongelmatilanteita, joita voi tapahtua Yritys X:ssä nykyisten HR- ja käyttöoikeuksien hallintaprosessien puitteissa. Ongelmatilanteita käyttöoikeuksien hallinnassa Yritys X:ssä todettiin aiheuttavan se, että identiteettitiedoissa olevat tietotyypit eivät yksittäin tai yhdisteltynä yksilöi käyttäjän työroolia Yritys X:ssä. HR-tietojärjestelmän tietotyypit ovat luotu henkilöstöhallinnon tarpeita varten ja siksi päättelyitä käyttöoikeuksista on Yritys X:ssä viety tietotyyppeihin, jotka eivät täysin palvele käyttöoikeuksien hallinnan tarpeita. Ongelmatilanteita käyttöoikeuksien hallintaprosessissa todettiin aiheutuvan myös, jos HR-prosessia ei ole henkilöstöhallinnossa saatu toteutettua HR-tietojärjestelmään ajoissa työsuhteessa tapahtuvaan muutosajankohtaan. Tämä voi johtaa siihen, että työntekijöiden käyttöoikeudet eivät ole aina ajan tasalla.

Nykytilan kuvauksen ja analyysin pohjalta opinnäytetyössä saatiin aikaan kehittämisehdotus, joka perustui kappaleessa 2.4 Työroolit ja käyttäjäroolit esitettyyn tapaan määritellä organisaation työroolit ja yhdistää työrooleihin järjestelmien mahdollistamat käyttäjäroolit. Tämä tarkoittaisi sitä, että HR-tietojärjestelmään määriteltäisiin ja toteutettaisiin uusia tietotyyppejä. HR-tietojärjestelmään lisättäisiin tietotyypit työrooli, työroolin alkupäivämäärä sekä työroolin päättymispäivämäärä. Kyseisiä tietotyyppejä voitaisiin kutsua työroolitiedoiksi. Henkilöstöhallinto pystyisi ylläpitämään työroolitietoja HR-prosessin aikana samaan aikaan kuin muita HR-tietoja tai HR-prosessista erillisesti ylläpitämällä vain työroolitietoja HR-tietojärjestelmässä olettaen, että työntekijät tiedot ovat jo kertaalleen luotu HR-tietojärjestelmään HR-prosessissa työsuhteen alkaminen. Identiteettitieto koostuisi työroolitietojen lisäksi henkilötiedoista, tunnistetiedoista, työsuhdetiedoista sekä henkilöstötoimenpidetiedoista (taulukko 4).

Kehittämistoimista saatavia hyötyjä ovat muun muassa tietoturvallisuuden parantuminen ja manuaalisen työn määrän vähentyminen käyttöoikeuksien hallinnassa. Tietotur-

va parantuu, kun esimiehet eivät hallitsemattomasti tilaa työntekijöiden käyttöoikeuksia, kun työroolit ja niihin liitetyt käyttöoikeudet ovat määritelty yhdessä liiketoiminnan kanssa. Lisäksi manuaalisen työn määrä vähentyy, kun käyttöoikeudet tulevat pääsääntöisesti automaattisesti työroolitietojen kautta eikä esimiehen tarvitse tilata käyttöoikeuksia käyttöoikeustilauksilla, jotka käsitellään manuaalisesti. Kun HR-tietojärjestelmässä on työroolia ilmaiseva tietotyyppi, ei ole enää tarpeellista viedä käyttöoikeuspäättelyitä esimerkiksi organisaatioyksiköihin. Käyttöoikeuksien kannalta riskialtis HR-prosessi organisaatiomuutos ei vaikuttaisi enää käyttöoikeuksien hallintaprosesseihin. Lisäksi esimies pystyisi valitsemaan työroolin myös ulkopuoliselle työntekijälle, joten Yritys X:ssä päästäisiin eroon myös ulkopuolisiin työntekijöihin liittyvästä problematiikasta käyttöoikeuksien hallinnassa.

Omat tavoitteeni opinnäytetyölle oman osaamisen laajentamisesta toteutuivat ja olen oppinut paljon käyttöoikeuksien hallinnasta ja identiteetinhallinnasta käyttöoikeuksien hallinnan menetelmänä. Pystyn hyödyntämään opittuja asioita nykyisessä työtehtävässä toimiessani. Opinnäyteyöprojekti oli myös oppimiskokemus projektityöskentelystä. Lisäksi toimeksiantajana olevan käyttöoikeushallinnan omistajan määrittelemiä tavoitteet käyttöoikeuksien hallinnan automatisoinnista, manuaalisen työn vähentämisestä sekä tietoturvallisuuden parantamisesta saataisiin toteutumaan kohtuullisen hyvin opinnäytetyössä esitetyllä kehittämistoimilla.

Pian opinnäytetyöprosessin alkamisen jälkeen huomasin, että omat tietoni käyttöoikeuksien hallinnasta olivat lähtötilanteessa kovin suppeat. Erityisesti termistön ymmärtäminen oli vaikeaa ja oppiminen tapahtui yrityksen ja erehdyksen kautta. Toisaalta tapaustutkimuksessa onkin tyypillistä, että taustatutkimusta tehdessä kehittämistehtävää tarkennetaan, kun aiheesta opitaan lisää ja kehittämistehtävän tarkennus on mahdollista vielä aineiston keruun ja analysoinnin jälkeen, kuten kappaleessa 1.2 Tutkimusmenetelmä kerrottiin tapaustutkimuksesta.

Haasteellista opinnäytetyön tekemisessä oli myös lähdemateriaalin löytäminen. Opinnäytetyön teoriaosuutta varten en löytänyt kaikilta osin niin tuoreita lähteitä kuin olisi toivonut ja löysinkin lähteitä suppeammin kuin olisin toivonut. Haastavaksi koin myös opinnäytetyön aikataulutuksen, koska minulla meni opinnäytetyöprosessissa aikaa käyt-

töoikeuksien hallintaan perehtyessä. Opinnäytetyön aikatauluun olin myös yliarvioinut ajan, jota minulla oli käyttää päivittäin opinnäytetyön tekemiseen ja se vaikutti merkittävästä opinnäytetyön aikataulun venymiseen. Lisäksi opinnäytetyön ohjaajien kiireiset aikataulut vaikuttivat opinnäytetyön valmistumisen viivästymiseen.

Omasta mielestäni onnistuin hyvin kuvaamaan ja analysoimaan Yritys X:n HR-prosessien ja käyttöoikeuksien hallintaprosessien yhteydet. Olisin kuitenkin toivonut, että olisin saanut aikaan enemmän kehittämisehdotuksia. Opinnäytetyötä olisi voinut vielä kehittää tekemällä esimerkiksi haastatteluita Yritys X:n loppukäyttäjille, jolloin olisi voitu löytää lisää ongelmakohtia Yritys X:n käyttöoikeuksien hallinnasta ja prosesseista. Haastatteluista olisi voitu saada myös tietoa loppukäyttäjän näkökulmasta olisiko käyttöoikeuksien hallintaprosesseja voitu kehittää vielä muilla tavoin. Kaiken kaikkiaan opinnäytetyön tekeminen on ollut pitkä prosessi, jonka varrella olen oppinut paljon uutta liittyen opinnäytetyön aihe-alueeseen.

Lähteet

Bondarouk, T., Ruel, H. & Looise, J. 2011. Electronic HRM in Theory and Practice. Emerald Group Publishing Limited. Bingley.

Kasanen, H. 2010. Keskitetty identiteetinhallinta, referenssiarkkitehtuuri. Luettavissa: http://www.secproof.com/media/Documents/Secproof_IdM_Referenssiarkkitehtuuri.pdf. Luettu: 15.4.2013.

Kuntaliitto. 2013a. Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri. Viitearkkitehtuurin kuvaus. Luettavissa: http://www.kunnat.net/fi/asiantuntijapalvelut/tyk/kuntien-ka/tuotokset/kvh-viitearkkitehtuuri/Documents/KVH_viitearkkitehtuuri_v0_99.docx. Luettu: 20.5.2013.

Kuntaliitto. 2013b. Ohjelmisto- Rooli oikeudet matriisi (oikeudet rooleittain). Luettavissa: http://www.kunnat.net/fi/asiantuntijapalvelut/tyk/kuntien-ka/tuotokset/kvh-viitearkkitehtuuri/Documents/Liite3_Kayttajarooli-tyorooli-matriisi_v0_99.xls. Luettu: 15.3.2014.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämisen menetelmät. Uudenlaista osaamista liiketoimintaan. WSOYpro Oy. Helsinki.

Propentus Oy. Mitä on identiteetinhallinta? Luettavissa: http://www.propentus.com/fi/propentus_united_identity/mita_on_identiteetinhallinta.html. Luettu: 17.4.2013.

Tietosuojavaltuutetun toimisto. Henkilötietolaki. Luettavissa: http://www.tietosuoja.fi/1577.htm. Luettu: 1.9.2013.

Valtiovarainministeriö. 2006. Käyttövaltuushallinnon hyvät periaatteet ja käytännöt. Luettavissa: http://www.vm.fi/vm/fi/

04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/2006112 2Kaeyttoe/vahti_9_06.pdf. Luettu: 19.1.2013.

Yritys X henkilöstöpalvelut. 2011a. Uuden henkilön perustaminen. Ohje.

Yritys X henkilöstöpalvelut. 2011b. Uudelleen aloittaminen yrityksessä. Ohje.

Yritys X henkilöstöpalvelut. 2011c. ORHA-IDM -LIITTYMÄN OHJAUSTIETOJEN SELITYKSET. Ohje.

Yritys X henkilöstöpalvelut. 2012a. Muistettavaa muutostilanteista HR-tietojärjestelmässä. Ohje.

Yritys X henkilöstöpalvelut. 2012b. Pitkäaikaiselle vapaalle lähtö. Ohje.

Yritys X henkilöstöpalvelut. 2012c. Pitkäaikaiselta vapaalta paluu. Ohje.

Yritys X henkilöstöpalvelut. 2012d. Henkilön erottaminen järjestelmästä. Ohje.

Yritys X henkilöstöpalvelut. 2013. Organisaatiomuutos. Ohje.

Yritys X:n HR-tietojärjestelmä

Yritys X tietohallinto. 2012. Käyttövaltuuskokonaisuus.

Yritys X tietohallinto. 2006. YHTEENVETO KODE-PROJEKTIN MÄÄRITTE-LYSTÄ.

xxx.idmorha liittymätaulu

Liitteet

Liite 1. Käsitteet

HR-tietojärjestelmä	(engl. *Human Resource Information System*) Tarkoittaa IT-pohjaisia tietojärjestelmiä ja sovelluksia, joita käytetään yleisesti henkilöstöhallinnollisiin tarkoituksiin.
HR-prosessi	HR-prosessilla tarkoitetaan tässä opinnäytetyössä henkilöstöön tai organisaatioon liittyvää muutosta, joka toteutetaan HR-tietojärjestelmään.
IaM	(engl. *Identity and Access Management*) Lyhenne tarkoittaa identiteetti- ja pääsynhallintaa.
Identiteetinhallinta	*(*engl. *Identity Management*) Tarkoittaa käyttäjän sähköisen identiteetin ja identiteettiin liitettyjen käyttöoikeuksien hallintaa sekä identiteetti- ja käyttöoikeustietojen välittämistä eri järjestelmiin.
IdM-järjestelmä	(engl. *Identity Management*) Tarkoittaa tässä opinnäytetyössä käyttöoikeuksien hallintajärjestelmää.
Kohdejärjestelmä	Tarkoittaa IdM-järjestelmän piiriin liitettyä järjestelmää.
Käyttäjä	Tarkoitetaan tässä opinnäytetyössä yrityksen sisäistä tai ulkopuolista työntekijää, mutta käyttäjä voisi olla myös esimerkiksi yrityksen asiakas tai jokin tietojärjestelmä.

Käyttöoikeuksien hallintaprosessi	Tarkoittaa prosessia, jossa IdM-järjestelmään välittyy HR-tietojärjestelmästä uutta tai muuttunutta identiteettitietoa ja IdM-järjestelmä välittää luodun tai muuttuneen identiteettitiedon perusteella käyttäjä- ja käyttöoikeustiedot kohdejärjestelmien käyttäjä- ja käyttöoikeustietovarastoihin.
Käyttöoikeus	(engl. *Usage right*) Tarkoittaa tässä opinnäytetyössä yksilöityä käyttöoikeutta käyttäjälle tai käyttäjäryhmälle määritellyn resurssin käyttöön.
POLP	(engl. *Principle of Least Priviledged*) Tarkoitetaan periaatetta, jonka käyttäjälle tulisi antaa mahdollisimman rajatut käyttöoikeudet.
Provisiointi	Tarkoittaa tässä opinnäytetyössä IdM-järjestelmän tekemää identiteetti- ja käyttöoikeustietojen välittämistä eri järjestelmiin.
Resurssi	Tarkoittaa tässä opinnäytetyössä tietojärjestelmää tai sovellusta.
SPML	(engl. *Service Provisioning Markup Language*) SPML on ohjelmointikieli, jolla voidaan toteuttaa provisiointi eli tietojen välittäminen esimerkiksi eri sovelluksien välillä.