



**LAUREA**  
AMMATTIKORKEAKOULU

*Uuden edellä*

# Käyttäjätunnusten hallinnan kehittäminen

Linteri, Jenni

2014 Kerava



Laurea-ammattikorkeakoulu  
Laurea Kerava

## Käyttäjätunnusten hallinnan kehittäminen

Jenni Linteri  
Tietojenkäsittelyn koulutusohjelma  
Opinnäytetyö  
Syyskuu, 2014

Linteri, Jenni

### Käyttäjätunnusten hallinnan kehittäminen

Vuosi 2014 Sivumäärä 37

---

Opinnäytetyön tavoitteena oli löytää Yritys X:n käyttäjätunnusten hallinnan prosessista parannettavaa ja tarjota mahdollisia kehitysehdotuksia yrityksen tietohallinnon käyttöön. Yrityksessä oli joulukuussa 2013, eli tutkimushetkellä alle puoli vuotta aikaisemmin, siirrytty uuteen identiteetinhallintajärjestelmään. Tapaustutkimuksen tarkoituksena oli löytää käyttäjätunnusten hallinnan prosessista niitä vanhan toimintamallin jäänteitä, jotka olisivat korvattavissa uuden tietojärjestelmän tarjoamin mahdollisuuksin. Prosessia tarkasteltiin kokonaisuutena, mutta pyrkimyksenä oli huomioida sekä käyttäjätunnusten hakijan että käyttäjätunnusten hallinnan prosessin omistajan näkökulma.

Tutkimusmenetelmäksi valittiin tapaustutkimus. Kirjallisuuskatsauksen lisäksi tutkimusaineistoa kerättiin prosessin omistajan haastatteluin ja tutustumalla olemassa olevaan dokumentaatioon sekä prosessin mallintamisella. Tutustuminen sekä vanhaan toimintamalliin että uuteen identiteetinhallintajärjestelmään ja henkilöstöhallinnon järjestelmään auttoivat kokonaisuuden hahmottamisessa, vaikka tietojärjestelmät sinänsä rajattiin tutkimuksen ulkopuolelle.

Tapaustutkimus osoitti useita pieniä, mutta merkittäviä kehityskohteita. Tarkastelemalla prosessimallinnusta voitiin havaita turhaksi jääneitä työvaiheita ja manuaalisesti tehtäviä toimintoja. Karsimalla turhaa työtä ja hyödyntämällä uuden tietojärjestelmän automatiikkaa käyttäjätunnusten hallinnan prosessia voidaan merkittävästi sujuvoittaa. Esimiesten ohjeistukseen tulee kiinnittää huomiota ja viittaukset vanhaan tilauslomakkeeseen tulisi poistaa uuden prosessin vakiinnuttamiseksi ja epäselvyyksien välttämiseksi.

Tutkimus toi esiin uusia näkökulmia ja tulokset auttavat Yritys X:n tietohallintoa jatkamaan jo aloitettua työtä käyttäjätunnusten hallinnan prosessin kehittämisessä.

käyttäjätunnus, prosessi, pääsynvalvonta, tietoturva

Linteri, Jenni

### Development of User ID Management

Year	2014	Pages	37
------	------	-------	----

---

The primary aim of this case study was to provide a useful tool for Company X's IT department to improve their process of user ID management.

The company had implemented a new computer program for identity and access management in December 2013. Because of that change there was a need to review the user ID management process and focus on the possibilities of the new computer program.

The study was based on qualitative methods. It was done by interviewing the process owner and collecting documentation from the company and analyzing it.

This research ignored the architectural aspect of computer systems and focused on the process itself. It was important to take into consideration both process owner's and superior's points of views throughout the research.

Modeling the process and analyzing the interviews and documentation revealed several aspects in need of development. Some of them could be easily replaced with automation of the computer system. A few topics will need more research and development in collaboration with the provider of the computer system.

The study revealed new insights and the results will help the Company X's IT department to continue the work with user ID management in the development process.

access management, IT security, processes, user ID management

## Sisällys

Keskeiset käsitteet ja lyhenteet .....	6
1 Johdanto .....	7
2 Työn lähtökohdat .....	8
2.1 Tutkimuksen toimeksiannon taustaa.....	8
2.2 Tutkimuksen tavoite ja tutkimuskysymykset.....	9
2.3 Aihealueen rajaus .....	9
3 Kirjallisuuskatsaus ja teoreettinen viitekehys .....	10
3.1 Identiteetti- ja käyttöoikeushallinta .....	10
3.1.1 Käyttäjä- eli identiteetinhallinta.....	11
3.1.2 Pääsynhallinta .....	11
3.1.3 Käytännön ongelmia .....	11
3.1.4 Katsaus tutkimustuloksiin.....	12
3.2 Lainsäädännön luomat perusteet.....	17
3.3 Käyttäjäroolit .....	18
3.4 Vaaralliset työyhdistelmät.....	19
4 Tutkimusmenetelmä.....	20
4.1 Kvantitatiivinen tutkimus .....	20
4.2 Kvalitatiivinen tutkimus.....	21
4.3 Kvalitatiivisia tutkimusmenetelmiä .....	21
4.4 Prosessin mallinnus .....	22
4.5 Aineiston hankinta ja analyysi .....	22
4.6 Reliabiliteetti ja validiteetti .....	23
5 Tutkimuksen toteutus .....	23
6 Tutkimustulokset.....	24
6.1 Käyttäjätunnusten hakijan näkökulma .....	24
6.2 Käyttäjätunnusten hallinnan prosessin omistajan näkökulma.....	26
6.3 Henkilöstö- ja tietohallinnon yhteistyö .....	26
7 Yhteenveto ja johtopäätökset .....	27
8 Jatkokehitysehdotukset.....	28
9 Oman osaamisen arviointi .....	29
Lähteet .....	31
Kuvat .....	34
Kuviot .....	35
Liitteet.....	36

## Keskeiset käsitteet ja lyhenteet

Seuraavassa on esitelty opinnäytetyössä esiintyvät keskeiset käsitteet ja lyhenteet.

AM, access management	Pääsynhallinta on tietojärjestelmän toiminto, millä käyttäjä tunnistetaan ja sen perusteella päätetään joko hyväksyä tai hylätä pääsy tietojärjestelmään.
autentikointi	Todennuksella tarkoitetaan sitä, että käyttäjän (tai palvelun) identiteetti varmennetaan esim. salasana-, sormenjälki- tai verkkokalvotunnistuksella.
IAM, identity and access management	Identiteettien ja käyttöoikeuksien hallinnalla tarkoitetaan kokonaisuutta, jolla hallinnoidaan tietojärjestelmien asianmukaista käyttöä. Yläkäsite identiteetin- ja pääsynhallinnalle.
identiteetti	Tietotekniikan kontekstissa identiteetillä tarkoitetaan ihmisen kuvailevien ominaisuuksien kokonaisuutta. Ominaisuudet voivat olla esim. nimi, käyttäjätunnus ja valtuus.
IdM, identity management	Identiteetinhallinnalla tarkoitetaan prosessia, jolla kohteet esitetään digitaalisina identiteetteinä tietojärjestelmissä.
prosessin omistaja	Toimija, joka vastaa prosessin toiminnasta, tuloksesta ja kehittämisestä.
provisiointi	Käyttöoikeuksien luominen, poistaminen tai välittäminen kohdejärjestelmiin.
SoD, segregation of duties	Tehtävien eriyttämisellä tavoitellaan virheiden ja väärinkäytösten estämistä. Tietojärjestelmissä käyttöoikeuksien rajaamisella saavutetaan tehtävien eriyttäminen.

## 1 Johdanto

Identiteettien ja käyttöoikeuksien hallinta on keskeinen osa yrityksen riskienhallintaa. Taylor ym. painottavat tietoturvatietoisuuden yrityskulttuurin tärkeyttä riskienhallinnassa. Työntekijöiden tulee olla tietoisia mihin kaikkeen heidän toimensa, oikeat ja väärät, vaikuttavat. Perustelemattomat kiellot voivat nostaa riskiä, että työntekijät pyrkivät kiertämään sääntöjä ja tietoisesti uhmaavat asetettuja rajoituksia. (Taylor, Alexander, Finch & Sutton 2013, 86.) Jos esimerkiksi sosiaalisen median käyttö kielletään työpaikalla, on hyvä perustella työntekijöille syy tähän päätökseen. Työntekijöiden on helpompi noudattaa kieltoa, jos perusteluna ovat tietoturvakäsitykset. Ilman esitettyjä perusteluja työyhteisöön voi levitä virheellinen ajatus työnantajan halusta rajoittaa ja kontrolloida työntekijöiden toimia.

Prosessien kehittämällä pyritään yleensä toiminnan tehostamiseen, laadun ja palvelun parantamiseen ja kustannustehokkuuteen. Kehitystyön pohjana tulee olla koko yrityksen visio, strategiat ja toimintaperiaatteet. Yrityksen johdon tulee määritellä selkeät tavoitteet prosessien kehittämiseksi ja toisaalta myös luoda edellytykset tämän työn toteutukselle. Prosessien kehittämisen tulee olla jatkuvaa eikä vain kertaluonteinen projekti. (JUHTA 2012, 3.) Tämän opinnäytetyön pääasiallisena tarkastelun kohteena on tietohallinnon yksi keskeinen osaprosessi, käyttäjätunnusten hallinnan prosessi. Koska yrityksen kaikki toiminnot ovat tavalla tai toisella sidoksissa toisiinsa, aihepiiri sivuaa myös yrityksen tietoturvaa, henkilöstöhallinnon prosesseja ja hallinnollista prosessien kehittämistä. Työn keskiössä on kuitenkin käyttäjätunnusten hallinnan prosessin tarkastelu, kaikki muu on toisarvoista ja huomioidaan tässä opinnäytetyössä vain maininnan asteella.

Opinnäytetyön alussa on selitetty aihealueen keskeisimmät käsitteet ja lyhenteet. Ensimmäisessä luvussa esittelen lyhyesti yrityksen toimeksiannon taustaa ja tutkimuksen lähtökohdat. Tutkimusmenetelmäksi valikoitui tutkimuksen kohteesta ja luonteesta johtuen kvalitatiivinen eli laadullinen tutkimustapa ja näkökulmaksi tapaustutkimus. Tutkimusaineiston kerääminen haastatteluin ja olemassa olevaan dokumentaatioon pohjautuen tapahtui kevään 2014 aikana. Olemassa olevan prosessin mallintaminen (Liite 1) ja tutustuminen yrityksessä käytössä oleviin tietojärjestelmiin auttoivat hahmottamaan kokonaiskuvaa prosessin toimivuudesta.

Teoriaosassa esittelen identiteetin ja käyttöoikeuksien hallinnan keskeiset osa-alueet, kuten pääsynhallinnan ja identiteetin hallinnan ja niiden osuuden organisaation tietoturvastrategiasa. Esittelen keskeisiä tutkimustuloksia havainnollistamaan asian merkityksellisyyttä koko IT-strategian kannalta. Esittelen myös käyttäjäroolipohjaisen tunnustenhallintakäytännön etuja ja tehtävien eriyttämisen tärkeyttä. Teoriaosassa on pyrkimyksenä pitäytyä kansantajuudessa kerronnassa, eikä syventyä liian teknisiin yksityiskohtiin.

Teoriaosan jälkeen esitellään tutkimuksen toteutus ja tutkimustulokset. Tulokset on jaoteltu karkeasti käyttäjätunnusten hakijan ja käyttäjätunnusten hallinnan prosessin omistajan näkökulmaan. Luvussa on otettu lyhyesti kantaa myös henkilöstöhallinnon ja tietohallinnon yhteistyön merkitykseen käyttäjätunnusten hallinnan prosessin näkökulmasta. Tarkastelen lopuksi omaa oppimistani ja kehittymistäni opinnäytetyöprosessin aikana. Aivan viimeiseksi olen koonnut tutkimustuloksiin pohjautuvat kehitysehdotukset. Kehitysehdotusten on tarkoitus olla tiivis ja selkeä kokonaisuus, minkä pohjalta varsinaisen kehitystyön yritys X:n tietohallinnossa voi aloittaa.

## 2 Työn lähtökohdat

Tässä luvussa esittelen perustelut ja lähtökohdat tälle tapaustutkimukselle. Esittelen lyhyesti kohdeyrityksen ja sen käyttäjätunnusten hallinnan prosessin taustaa ja nykytilaa. Luvussa esittelen myös tutkimukselle asetetut ja tutkimusta ohjaavat tutkimuskysymykset. Tutkimus keskittyy prosessin tarkasteluun ja kehitysehdotuksiin ja luvun lopuksi määrittelen tutkimuksen ulkopuolelle jäävät osa-alueet.

### 2.1 Tutkimuksen toimeksiannon taustaa

Tutkimuksen toimeksiantajana on yksityinen, pääkaupunkiseudulla toimiva terveystalouden yritys. Kokoluokaltaan se sijoittuu suuriin yrityksiin, työntekijöitä yrityksessä on hieman alle 700. Yrityksessä työskentelee sekä työsuhteisia työntekijöitä että ammatinharjoittajia. Tutkimuksen sisältämien, liiketoiminnan strategian kannalta merkittävien tietojen vuoksi yrityksestä käytetään tässä tapaustutkimuksessa nimeä Yritys X.

Yrityksessä on joulukuussa 2013 siirrytty käyttämään identiteetinhallintajärjestelmää eli tutkimuksen käynnistyessä järjestelmä oli ollut käytössä alle puoli vuotta. Ennen uuden järjestelmän käyttöönottoa käyttäjätunnusten hallinnan prosessi oli huomattavasti monimutkaisempi, pitkäkestoisempi ja suurelta osin manuaalinen. Tunnustenhallinta oli aiemmin ollut ulkopuolisen palveluntarjoajan hallinnoima ja työpyynnöt lähetettiin sähköpostilomakkeella yrityksen ulkopuolelle. Uudistuksen myötä Yritys X on ottanut itse hoitaakseen koko käyttäjätunnusten hallinnan prosessin.

Uuden identiteetinhallintajärjestelmän hankinnan taustalla on, yhteen yrityksen tietojärjestelmään liittyvä, lainsäädännöllinen uudistus. Se velvoittaa yritystä tarkistamaan käyttäjätunnusten tilaa useammin ja seuraamaan oikeuksien ajantasaisuutta aikaisempaa aktiivisemmin. Keskitetty identiteetinhallinta mahdollistaa tämän toiminnon aikaisempaa helpommin. Nopea uuden tietojärjestelmän käyttöönotto on kuitenkin jättänyt käyttäjätunnusten hallinnan pro-



sessiin elementtejä vanhasta prosessista, eikä kaikkia uuden järjestelmän mahdollisuuksia ole vielä täysin hyödynnetty.

## 2.2 Tutkimuksen tavoite ja tutkimuskysymykset

Tutkimuksen tavoitteena on löytää Yritys X:n käyttäjätunnusten hallinnan prosessista selkeitä kehityskohteita. Tarkastella kriittisesti miten prosessia voidaan kehittää, toimintoja selkeyttää ja järkeistää. Tavoitteena on löytää prosessista jäänteitä vanhasta käyttäjätunnusten hallinnan prosessista, mitkä voidaan korvata uuden IdM- eli identiteethallintajärjestelmän tuomin mahdollisuuksin. Tutkimuksen tavoitteena on tuottaa selkeästi jäsenelty tutkimusraportti, jota Yritys X:n tietohallinto voi käyttää käyttäjätunnusten hallinnan prosessin kehitystyössä.

Prosessia tarkastellaan sekä tunnusten hakijan eli käytännössä esimiesten että yrityksen tietohallinnon eli järjestelmän pääkäyttäjän näkökulmasta. Prosessin eri osia tarkastellessa on tarkoitus pitää mielessä molemmat näkökulmat ja pyrkiä kehitysehdotuksissa prosessin sujuvoittamiseen molempien osapuolten kannalta. Prosessiin liittyy paljon muitakin osapuolia, kuten esimerkiksi henkilöstöhallinto. Henkilöstö- ja tietohallinnon yhteistyöhön on lyhyesti otettu kantaa, mutta muuten henkilöstöhallinnon osuuteen ei tässä tutkimuksessa syvennytä.

Pääasiallinen tutkimusongelma on: ”Miten yritys X:n käyttäjätunnusten hallinnan prosessia voidaan kehittää?” Prosessia tarkastellaan kokonaisuutena, mutta tutkimuksessa kiinnitetään huomiota sekä käyttäjätunnusten hakijan että tietohallinnon näkökulmaan prosessin sujuvuudessa. Tutkimuskysymyksenä on myös: ”Voidaanko prosessin olemassa olevia käytäntöjä yksinkertaistaa ja karsia turhia työvaiheita?” Tutkimuksessa pyritään myös vastaamaan kysymyksen: ”Voidaanko uuden IdM-järjestelmän tarjoamia mahdollisuuksia paremmin hyödyntää käyttäjätunnusten hallinnan prosessissa?”

## 2.3 Aihealueen rajaus

Yritys X:n tietohallinto saa opinnäytetyön tuloksena apuvälineen tunnustenhallinnan prosessin kehittämiseksi. Analysoimalla tutkimusaineistoa ja prosessin mallinnusta nostan esiin kehityskohteita ja esitän ehdotuksia prosessin ongelmakohtien ratkaisemiseksi. Varsinaisen uudistustyön toteutuksen rajaan opinnäytetyön ulkopuolelle.

Liiketoiminnan prosessit eivät koskaan ole täysin erillisiä kokonaisuuksia. Käyttäjätunnusten hallinnan prosessi sivuaa monessakin kohtaa henkilöstöhallinnon prosesseja. Liitoskohtien osalta ja yhteistyön sujuvuuden parantamiseksi pyrin tuomaan esille käyttäjätunnusten hal-

linnan kannalta oleellisia huomioita, mutta syvällisempi perehtyminen henkilöstöhallinnon prosesseihin rajataan työn ulkopuolelle.

IdM-järjestelmän tai HR- eli henkilöstöhallinnon tietojärjestelmän arkkitehtuuriin tai mahdollisiin teknisiin puutteisiin en tutkimuksessa ota kantaa. Käytössä oleva IdM-järjestelmä on varsin uusi ja on jo etukäteen tiedossa, että sen kehitystyö jatkuu. Tästä syystä kehityskohteiden esiin nostaminen tässä tutkimuksessa olisi varsin turhaa. Mikäli jotain merkittävää tulee selkeästi tutkimuksessa esille, mainitaan huomiot johtopäätöksissä.

### 3 Kirjallisuuskatsaus ja teoreettinen viitekehys

Tässä luvussa esitellään yleisellä tasolla identiteetti- ja käyttöoikeushallinnan käsite. Laajan kokonaisuuden osista on haluttu nostaa erityisesti tarkasteluun identiteetin- ja pääsynhallinta. Teknisten toteutusratkaisujen tasolle ei tässä yhteydessä mennä vaan tarkoituksena on selittää peruseriaatteet ymmärrettävästi. Luvussa nostetaan esiin muutamia mahdollisia käytännön ongelmia identiteetin- ja pääsynhallinnassa. Pyritään myös tuomaan lainsäädännön näkökulma käsiteltävään aiheeseen ja luvussa esitellään lain määräämät perusteet käyttäjätunnusten hallinnan järjestämiselle. Luvun lopussa on pieni katsaus käyttäjäroolipohjaiseen käyttäjätunnushallintaan ja vaarallisiin työyhdistelmiin.

#### 3.1 Identiteetti- ja käyttöoikeushallinta

Identiteettien ja käyttöoikeuksien hallinnalla tarkoitetaan kokonaisuutta, jolla hallinnoidaan tietojärjestelmien asianmukaista käyttöä. Yrityksessä käytönvalvonta tulee olla osa laajempaa riskienhallinnan strategiaa, eikä vain erillinen prosessi. Käyttöoikeuksien hallinta on oleellinen osa yritysten tieto-omaisuuteen liittyvää riskienhallintaa. (Andreasson & Koivisto 2013, 106.) Identiteetti- ja käyttöoikeushallinta on yläkäsite, joka pitää sisällään mm. käyttäjähallinnan ja pääsynhallinnan.

Identiteetti- ja käyttöoikeushallinnan tavoitteena on estää järjestelmän luvaton ja sallia luvallinen käyttö. Jordan ja Silcock (2006, 184) määrittelevät teoksessaan Strateginen IT-riskien hallinta yleisiä periaatteita valvonnan järjestämiseen. Heidän mukaan kenelläkään ei tule olla oletuksena mitään oikeuksia vaan luvat tulee myöntää keskitetysti. Jokaisella käyttäjällä tulee olla henkilökohtainen käyttäjätunnus, käyttöoikeuksien laajuus tulee riippua määritellystä käyttäjäroolista, eikä henkilökohtaisista ominaisuuksista. Käyttäjän autentikointia varten tulee olla käytössä esimerkiksi salasana, joka on vain käyttäjän itsensä tiedossa. Järjestelmässä tulisi olla käytössä aikakatkaisu siten, että määritellyn ajan käyttämättömyys vaatii uuden autentikoinnin. Järjestelmässä tulisi olla mahdollisimman vähän käyttäjiä, joilla on ns. rajoittamattomat käyttöoikeudet. Näitä käyttäjiä varten tulisi olla sisäinen valvontajärjestelmä.

### 3.1.1 Käyttäjä- eli identiteetinhallinta

Lindenin (2012, 10-11) mukaan prosessia, jossa kohteet esitetään tietojärjestelmissä digitaalisina identiteetteinä, voidaan kutsua identiteetinhallinnaksi. Kohteet voivat olla luonnollisten henkilöiden ilmentymien lisäksi myös järjestelmiä tai laitteistoja. Esimerkiksi organisaation identiteetin tunnisteena voidaan pitää yksilöivää Y-tunnusta tai tietokoneella IP-osoitetta. Kohteella voi olla useampia identiteettejä eri ympäristöissä, esimerkiksi sosiaalisen median identiteetti eroaa merkittävästi työntekijän identiteetistä, vaikka identiteettien taustalla on sama henkilö. (Bertino & Takahashi 2011, 21-23.)

Käyttäjähallinnan perusidea voidaan kiteyttää esimerkiksi tarkoitukseksi taata identiteetin eheys koko elinkaarensa ajan huomioiden tiedon saatavuus ja tietosuojanäkökulma. Identiteetinhallinnan tarpeellisuus korostuu silloin, kun yrityksessä on useita eri tietojärjestelmiä. Käyttäjätietojen eheys on vaarassa, jos tietojen muuttuessa kaikkia eri tietokantoja ei muisteta päivittää. Keskitetty identiteetinhallintajärjestelmän tarkoituksena on minimoida nämä riskit. (Bertino & Takahashi 2011, 21-23; Linden 2012, 7, 10.)

### 3.1.2 Pääsynhallinta

Pääsynhallinta on tietojärjestelmän toiminto, millä käyttäjä tunnistetaan ja sen perusteella päätetään joko hyväksyä tai hylätä pääsy tietojärjestelmään. Pääsynhallinnalla voidaan kontrolloida milloin ja miten tietojärjestelmään tai tietoverkkoon on mahdollista päästä. Liiketoiminnan näkökulmasta pääsynhallinta parhaimmillaan mahdollistaa optimaalisen resurssien jakamisen, mutta toisaalta pahimmillaan se voi turhauttaa käyttäjiä, nostaa hallinnollisia kustannuksia ja aiheuttaa arvokkaan tiedon vuotamista tai korruptoitumista. (Ferraiolo, Kuhn & Chandramouli 2007, 1-2; Linden 2012, 10-11.)

Pääsynhallinta on vain yksi osa yrityksen tietoturvapoliittikkaa, mutta käyttäjille varmasti näkyvin osa. Ferraiolon ym. mukaan pääsynhallinnan tarkoituksena on varmistaa luottamuksellisuus, eheys ja saatavuus. Tiedon on oltava saatavilla vain niille, jotka ovat siihen oikeutettuja. Vain asianmukaisten tahojen tulee voida hallitusti muuttaa tai korjata tietoja. Tiedon tulee olla oikea-aikaisesti saatavilla. (Ferraiolo ym. 2007, 2-3.)

### 3.1.3 Käytännön ongelmia

Organisoidulla käyttäjä- ja identiteetinhallinnalla pyritään estämään inhimillisiä erehdyksiä ja niistä aiheutuvia ongelmia. Pitkään yrityksessä palvelleet henkilöt keräävät usein melkein huomaamatta itselleen ajan saatossa lisää käyttöoikeuksia. Jos turhia oikeuksia ei tehtävien

muuttuessa poisteta, ollaan tilanteessa, missä joillain käyttäjillä on vapaa pääsy eri järjestelmiin ilman työtehtävien luomaa perustetta. (Jordan & Silcock 2006, 185.) Kuten seuraavassa alaluvussa kuvatussa Ponemon Instituutin tekemässä tutkimuksessa käy ilmi (Kuvio 2), monet kokevat olevansa oikeutettuja kaikkeen siihen tietoon, minkä myönnetyt käyttöoikeudet heille sallivat, vaikka perusteena olisi vain puhdas uteliaisuus (Ponemon Instituutti 2011, 6).

Usein määräaikaisten tai keikkatyöläisten kohdalla koetaan helpommaksi käyttää yhteiskäyttötunnuksia, mikäli yrityksessä ei ole tehokkaasti ratkaistu lyhytaikaisten ja ehkä yllättäenkin työhön kutsuttujen työntekijöiden käyttäjätunnusten hallintaa (Jordan & Silcock 2006, 185). Vuorotyö asettaa myös omat haasteensa käyttäjätunnusten hallinnalle. Esimiehen tai vastuhenkilön tulee ennakoida virka-ajan ulkopuolella tapahtuva henkilökunnan liikkuvuus.

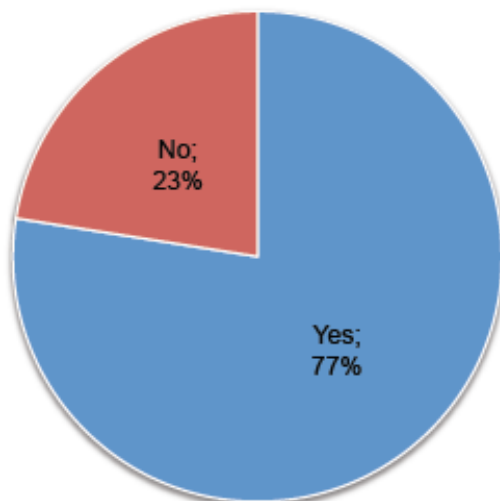
#### 3.1.4 Katsaus tutkimustuloksiin

Yhdysvaltalainen Ponemon Instituutti, jonka pääasiallisina tutkimuskohteina ovat yksityisyys, tietosuoja ja tietoturvakäytännöt, on tehnyt lukuisia kiinnostavia tutkimuksia, jotka sivuavat myös käyttäjätunnusten hallintaa. Tässä on syytä mainita, että Ponemon Instituutin toteuttamien tutkimusten kohderyhmänä ovat IT-alan ammattilaiset ja yritysten johtohenkilöt. Ns. tavallisen työntekijän näkökulma suhteessa tietoturvaan, käyttöoikeuksien ja käyttäjätunnusten hallintaan jää näissä Ponemon Instituutin tutkimuksissa kokonaan käsittelemättä. (Ponemon Institute 2014.)

Joulukuussa 2011 julkaistuun kansainväliseen tutkimukseen *Insecurity of Privileged Users* osallistui 5569 IT- ja tietoturva-alan ammattilaista 13:sta eri maasta. Kysely suunnattiin yritysten IT-alan ammattilaisille, joilla on normaalia työntekijää laajemmat oikeudet yrityksen eri tietojärjestelmiin. (Ponemon Institute 2011, 21.) Tutkimustulokset eivät suoraan ole yleistettävissä koko tietojärjestelmän käyttäjäkuntaa koskevaksi, mutta tutkimuksen tulokset ovat mielenkiintoista luettavaa käyttäjätunnusten hallinnan näkökulmasta. Tulokset vahvistavat käsitystä käyttäjätunnusten hallinnan ajantasaisuuden ja tietohallinnon aktiivisen roolin tärkeydestä.

Pääosa (77 %) tutkimukseen osallistujista sanoi käyttöoikeuksiensa olevan linjassa heidän nykyisiin työtehtäviinsä tai rooliinsa yrityksessä. Kuviossa 1 on eritelty loppujen 23 prosentin osalta, miksi heillä on erityisoikeudet, vaikka he eivät niitä tällä hetkellä työssään tarvitse. Kaksi merkittävintä syytä ovat aiemmin tarvittujen oikeuksien poistamatta jättäminen ja se, että käyttöoikeudet on myönnetty siitä huolimatta, että työssä ei niitä tarvitse.

**Pie Chart 1: Is privileged access required in order for you to complete your current job assignment or function within the organization?**

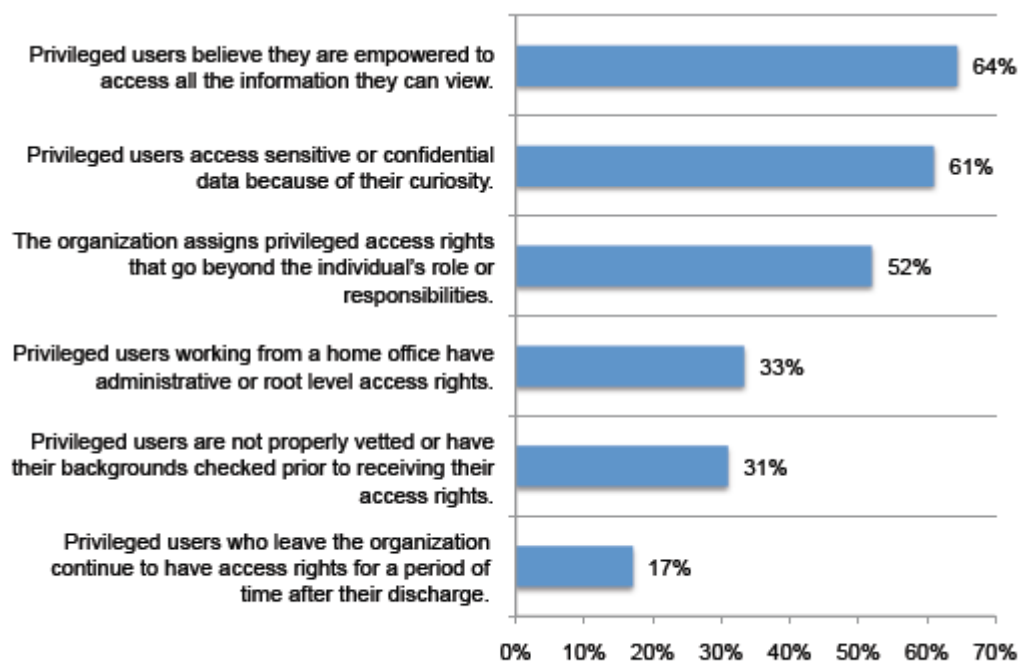


**Table 1: If you said no, what is the primary reason you still have privileged access rights? Only one choice is permitted.**

Reasons why	Pct%
I needed privileged access in a previous position and it was not revoked after my role changed	34%
Everyone at my level has privileged access even if it is not required to perform a job assignment	43%
The organization assigned privileged access rights for no apparent reason	12%
I don't know	11%
Total	100%

Kuvio 1: Vastaajien käyttöoikeuksien ajantasaisuus ja syyt eriteltynä, mikäli ne eivät ole ajantasaisia (Ponemon Institute 2011, 5).

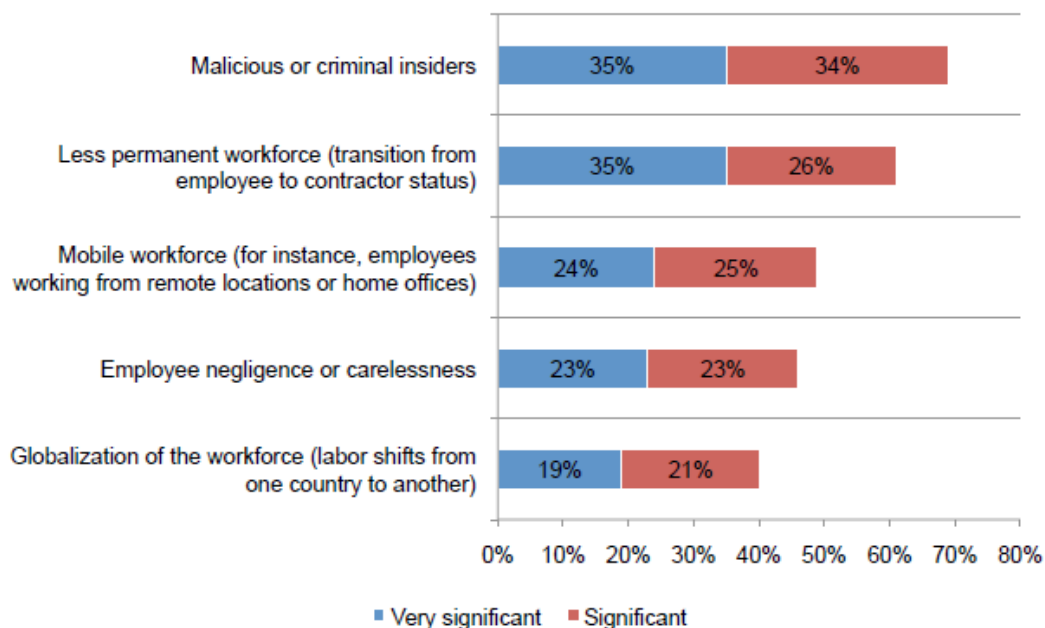
Tutkimukseen osallistujille esitettiin erilaisia väittämiä ja he arvioivat niiden esiintyvyyttä omassa yrityksessään. Tutkimuksessa kävi ilmi, että vastaajista 64 prosenttia uskoo, että on hyvin todennäköistä tai todennäköistä, että laajempien käyttöoikeuksien haltijat uskovat olevansa oikeutettuja kaikkeen siihen tietoon, mikä oikeuksien myötä on saatavilla. 61 % vastaajista uskoi oikeuksien haltijoiden pitävän oikeutenaan myös pääsyn arkaluontoiseen ja luotamukselliseen tietoon, vaikka vain uteliaisuudesta. (Kuvio 2).



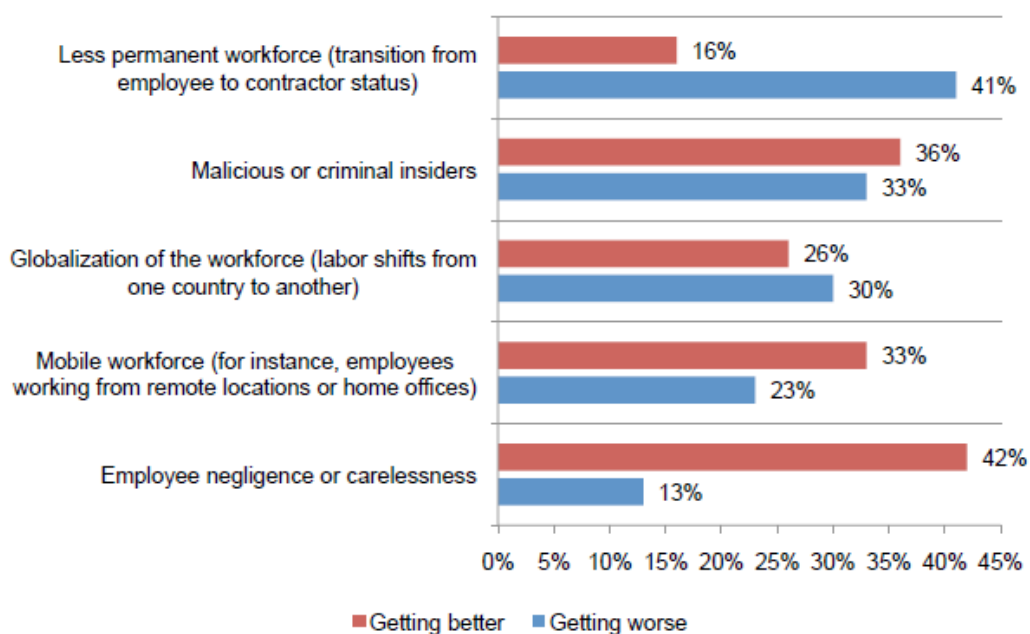
Kuvio 2: Vastajat arvioivat väittämien todennäköisyyden omassa yrityksessään (Ponemon Institute 2011, 6).

Tammikuussa 2012 Ponemon Instituutti julkaisi Future State of IT Security - A Survey of IT Security Executives -tutkimuksen, mihin osallistui 614 kokenutta it- ja tietoturva-alan ammattilaista. Tutkimuksen tarkoituksena oli kartoittaa tulevaisuuden trendejä yritysten tietoturvassa. Vastajat arvioivat minkälaiset inhimilliset tekijät vaikuttavat yrityksen tietoturvaan tällä hetkellä (Kuvio 3) ja heitä pyydettiin myös arvioimaan, mihin suuntaan kehitys menee tulevaisuudessa (Kuvio 4). Kuvioista käy ilmi, että tämän hetken suurimpana uhkana pidetään yrityksen sisäistä vahingollista tai rikollista toimintaa. Merkittävänä uhkana koetaan väliaikainen työvoima. Työntekijöiden huolimattomuus tai laiminlyönti on verrattain vähäinen uhka tällä hetkellä vastaajien mukaan ja vastaajien arvioiden mukaan osuus on tulevaisuudessa vielä merkittävästi vähenemässä. Tulevaisuuden nousevana uhkana pidetään väliaikaista työvoimaa ja sen mukanaan tuomia tietoturvauhkia. (Ponemon Institute 2012a, 2, 14.)

Nämä ovat tärkeitä huomioita käyttäjätunnusten hallinnan näkökulmasta. Esimerkiksi väliaikaisen työvoiman osalta hyvin organisoitu käyttäjätunnushallinto ehkäisee tehokkaasti tietoturvariskejä. Yrityksen tulee ennalta varautua ja linjata käytännöt keikkatyöläisten, sijaisten ja muiden väliaikaisten työntekijöiden osalle, jotta sekä työnteon sujuvuus taataan että tarpeeton tunnusten yhteiskäyttö ehkäistään.



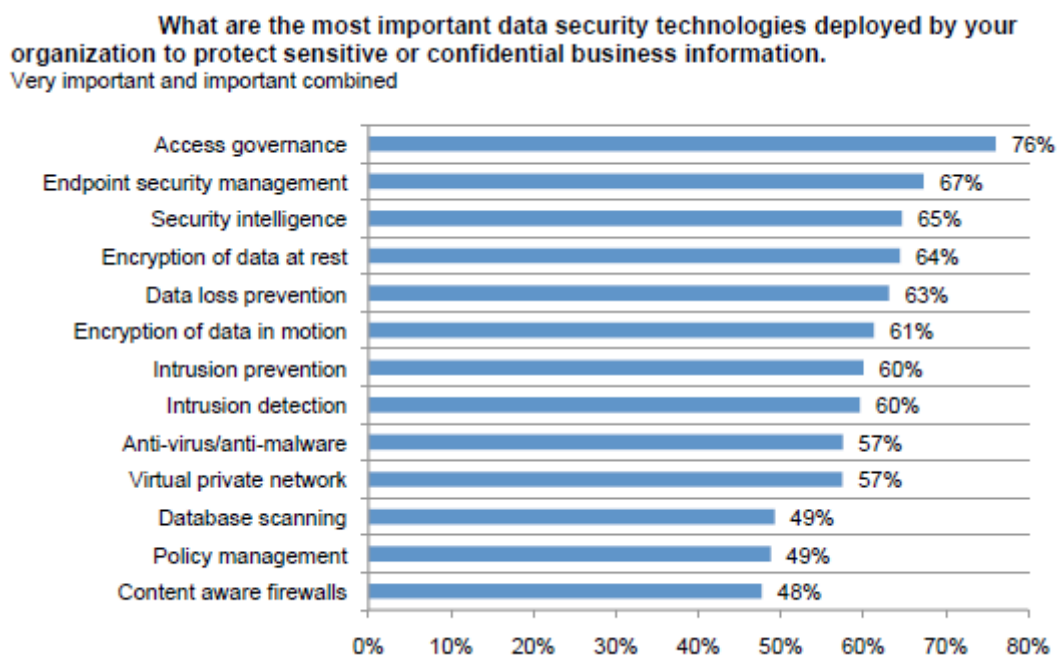
Kuvio 3: Tietoturvan kannalta merkittävimmät inhimilliset uhkatekijät vastaajien mielestä (Ponemon Institute 2012a, 14).



Kuvio 4: Tietoturvan kannalta merkittävien inhimillisten uhkatekijöiden kehitys tulevaisuudessa vastaajien mukaan (Ponemon Institute 2012a, 14).

Tammikuussa 2012 Ponemon Instituutti julkaisi tutkimuksen *The Human Factor in Data Protection*, missä keskityttiin yrityksen sisäisiin riskeihin ja keinoihin niiden välttämiseksi. Tutkimus osoitti, että sosiaalinen media ja mobiili- ja pilvipalvelut lisäävät yrityksen sisäisiä riskejä omien työntekijöiden taholta. Kuvio 5 osoittaa, että tutkimukseen osallistujat arvioivat

käyttöoikeuksien hallinnan edelleen pääasialliseksi tavaksi suojautua riskejä vastaan. (Ponemon Institute 2012b, 5.)



Kuvio 5: Vastajien mielestä organisaation tärkeimmät tietoturvateknologiat uhkia vastaan (Ponemon Institute 2012b, 5).

Tietotekniikan liiton vuosittain toteuttaman kyselytutkimuksen, IT-barometrin tarkoituksena on kartoittaa käsityksiä tietotekniikasta, sen johtamisesta ja hyödyntämisestä. Kyselyn vastaajat ovat liiketoimintajohtajia ja IT-asiantuntijoita ja -johtajia. (IT-barometri 2013, 3.)

Kuvio 6 osoittaa, että kysymykseen IT:n vaikutuksesta tulevaisuuden menestykselle vastaukset jakaantuvat melko tasaisesti. Vastauksista käy ilmi, että IT:n käyttö prosessien ohjaamiseen ja kehittämiseen ja toisaalta myös IT-riskien hallintaan nähdään tärkeänä tulevaisuudessa. Nämä ovat juuri niitä asioita, mitkä koskettavat organisoitua identiteetti- ja käyttöoikeushallintaa. Tärkeystä huolimatta IT-barometrin vastaajat uskovat, että suurin osa organisaatioista lykkää IT-hankintoja ja karsii IT-kuluja taloustaantumisen aikana. (IT-barometri 2013, 13.)





Kuvio 6: Vastaajien arvio IT:n merkityksestä yrityksen menestykselle tulevaisuudessa (IT-barometri 2013, 21).

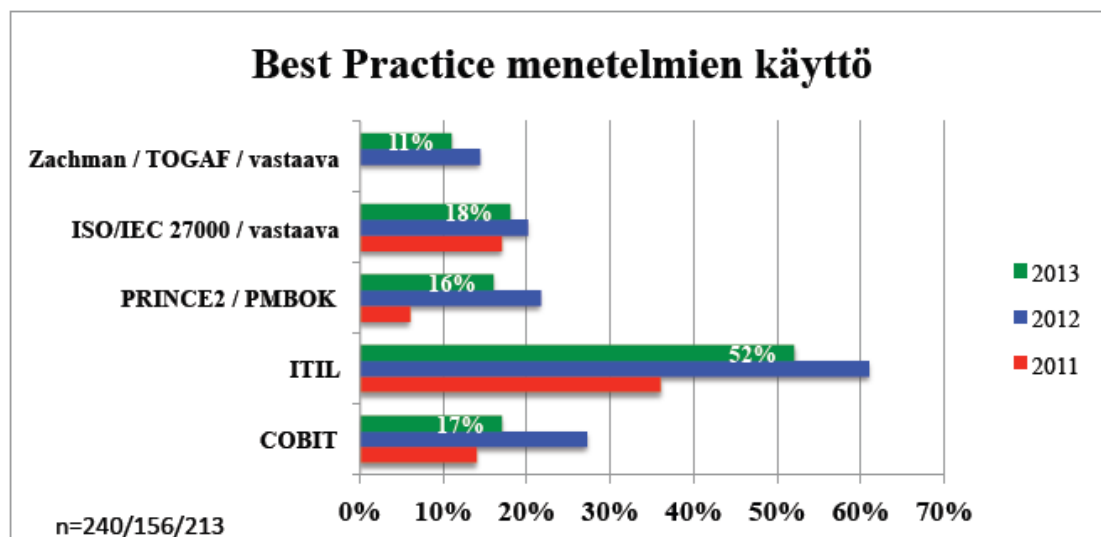
Huomion arvoista on, että kaikissa edellä mainituissa tutkimuksissa ei vielä näy viimeaikaiset laajat kyber- ja tietoturvallisuuskohut. Nämä epäilemättä suuntaavat myös yritysten panostuksia verkkohyökkäyksiä vastaan tulevaisuudessa ja pakottavat yrityksiä miettimään uudestaan tietoturvastrategiaansa uusien tietoturvaohjeiden konkretisoituessa ja heijastuessa yrityksen koko toimintaan.

### 3.2 Lainsäädännön luomat perusteet

Riippuen organisaation toimialasta ja yritysmuodosta käyttöoikeuksien hallinnan perustana on erilaisia lakeja. Esimerkiksi julkisen sektorin toimintaa ohjaa laki viranomaisen toiminnan julkisuudesta (621/1999). Organisaatiossa, missä käsitellään asiakkaiden henkilötietoja, tulee noudattaa henkilötietolain (523/1999) säädöksiä. Käyttöoikeushallinnan keinoin henkilötiedot tulee olla vain niiden henkilöiden käytettävissä, jotka työssään niitä tarvitsevat. Laki edellyttää henkilötietojen suojaamista, tietojen tarpeellisuus- ja virheettömyysvaatimuksen sekä käyttöoikeussidonnaisuuden vaatimuksen huomioon ottamista. Tämä nostaa käyttöoikeushallinnan organisoinnin tärkeään asemaan ja puoltaa roolipohjaisten käyttäjäoikeuksien käyttöä. (Andreasson & Koivisto 2013, 108-109; Valtiovarainministeriö 2006, 11.)

Erilaiset standardit ja käytännöt ohjaavat myös käyttöoikeushallintaa. Nämä ovat kuitenkin vapaaehtoisia, eivätkä lakiin ja säädöksiin rinnastettavia. Sekä Suomen standardisoimisliitto

SFS ry:n että kansainvälisen vastaavan organisaation ISO:n (the International Organization for Standardization) internetsivuilta löytyy lukuisia tieto-omaisuuden valvontaan ja käyttäjähallinnan organisointiin liittyviä standardeja. Oheisesta IT-barometrin kuviosta (Kuvio 7) käy ilmi, että selvästi suosituin IT-palveluiden hallinnan prosessikehys on ITIL (Information Technology Infrastructure Library).



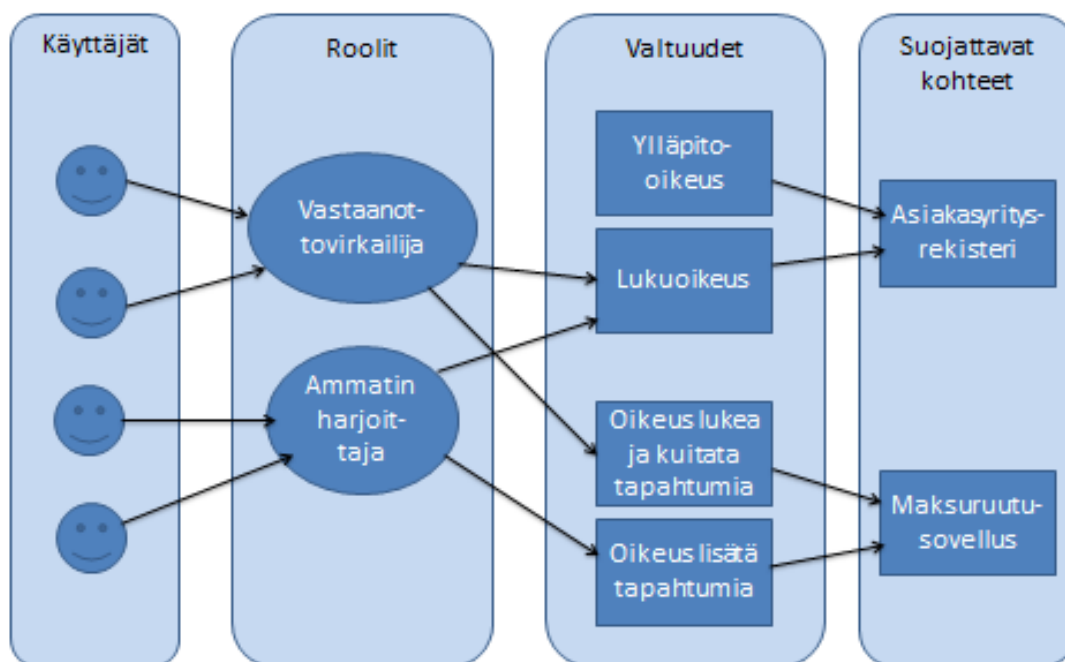
Kuvio 7: Best Practise -menetelmien käyttö vastaajien yrityksissä (IT-barometri 2013, 29).

### 3.3 Käyttäjäroolit

Lähtökohtana selkeälle ja oikeudenmukaiselle käyttöoikeuksien hallinnalle pidetään yleisesti roolipohjaista toimintatapaa. Pienissä yrityksissä yksittäisiin identiteetteihin pohjautuva käyttäjähallinta on täysin mahdollista toteuttaa, mutta suuremmissa yrityksissä käyttäjäroolipohjainen toteutustapa tekee kokonaisuudesta paljon hallittavamman. Sen sijaan, että jokaisen yksilön kohdalla määritellään tarvittavat käyttöoikeudet, määritellään työtehtäviin perustuvat käyttäjäroolit organisaatiotasolla ja sijoitetaan kukin yksilö näihin käyttäjärooleihin. Alussa suurin ja aikaa vievin työ on määritellä erilaiset käyttäjäroolit. Tämä vaatii syvällistä toimenkuvien tuntemista; kuka tekee ja mitä, tehtäväkuvauksen avaamista ja osiin pilkkomista. Tekniikoita on monia, apuna voidaan käyttää esimerkiksi ohjelmistokehityksestä tuttuja vaatimusmäärittelyn työkaluja. Kun käyttäjäroolien määrittely on huolella tehty, käyttäjätunnustenhallinta helpottuu merkittävästi ja liiketalouden näkökulmasta myös kustannustehokkuus nousee. Käyttäjäroolien ajantasaisuutta on kuitenkin hyvä seurata organisaation muuttuessa ja kehittyessä. (Andreasson & Koivisto 2013, 106; Ferraiolo ym. 2007, 213-214; Sharoni, Spaulding, Williamson & Yip 2012, 103-104.)

Kuviossa 8 on havainnollistettu käyttäjäroolien toimintalogiikkaa. Käyttäjät jaetaan työtehtävien mukaan eri käyttäjärooleihin, joille on määritelty niiden vaatimat käyttöoikeudet. Yksit-

täisellä käyttäjällä voi olla useampia käyttäjärooleja. Toiminnan muutoksissa on helpompaa lisätä ja poistaa käyttöoikeuksia käyttäjäroolilta kuin käydä jokainen yksittäinen käyttäjä läpi ja tehdä tarvittavat muutokset.



Kuvio 8: Roolien mukainen käyttäjähallinta (mukaillen Linden 2012, 31).

### 3.4 Vaaralliset työyhdistelmät

Tietojärjestelmien käyttövaltuuksissa kuten muussakin yrityksen toiminnassa vaarallisten työtehtävien eriyttäminen (segregation of duties, SoD) kahdelle tai usealle eri henkilölle ehkäisee työtehtävien hoidossa tapahtuvia erehdyksiä, virheitä ja väärinkäytöksiä. Henkilön ei tule toimia kahdessa toisiaan sivuavassa roolissa, missä roolien intressit saattavat olla keskenään ristiriidassa. Hyvä esimerkki tällaisesta ristiriitaisesta roolista on omien laskujen hyväksyminen. (Linden 2012, 34-35; Taylor ym. 2013, 89.)

Vaarallisten työtehtävien eriyttämisen käytännöt voidaan jakaa staattisiin ja dynaamisiin tapoihin. Staattinen eriyttäminen tarkoittaa sellaisten tehtävien kokonaan eriyttämistä eri henkilöille, joissa roolit voivat joutua eturistiriitaan tai on vaarana niiden sekoittuminen. Laskujen hyväksymisprosessissa henkilö ei missään tapauksessa voi toimia laskujen hyväksyjänä, jos hänellä itsellään on hyväksyttäviä laskuja. Yrityksen itsensä on määriteltävä, mitkä ovat nämä toisensa poissulkevat roolit. Dynaaminen eriyttäminen tarkoittaa edellisessä laskuesimerkissä

sitä, että henkilö voi toimia sekä laskun hyväksyjän roolissa että hyväksyttää laskujaan yrityksessä, mutta henkilön omat laskut hyväksyy joku toinen henkilö. (Ferraiolo ym. 2007, 100-101; Linden 2012, 34-35.)

#### 4 Tutkimusmenetelmä

Opinnäytetyön tarkoitus on mallintaa olemassa oleva käyttäjätunnusten hallinnan prosessi ja sitä kautta löytää vallitsevasta käytännöstä kehityskohteita ja vanhentuneita toimintamalleja. Seuraavassa luvussa esittelen sekä määrällisen että laadullisen tutkimusmenetelmän ja perustelen, miksi tutkimustavaksi valikoitui laadullinen tutkimus määrällisen tutkimuksen sijaan. Olemassa olevaan dokumentaatioon tutustuminen ja prosessin osapuolten haastattelut luovat pohjan prosessin mallinnukselle. Prosessin elementtien tunnistaminen ja niiden suhteiden kartoitus on tutkimuksen lopputuloksen ja validiteetin kannalta tärkeää. (Hirsjärvi, Remes & Sajavaara 2004, 152-155.)

##### 4.1 Kvantitatiivinen tutkimus

Määrällinen eli kvantitatiivinen tutkimus pyrkii esittämään tilastollisin menetelmin mitattua tutkimustietoa. Se pyrkii yleistämään otoksen kautta saadun tutkimustiedon laajempaan kokonaiskuvaan, tutkimuksen suunta on teoriasta käytäntöön. Määrällinen tutkimusmenetelmä voidaan valita vain, jos aiheesta on riittävästi aiempaa tutkimustietoa, mihin tuloksia voi peilata. Määrälliselle tutkimukselle on ominaista vahva teoriapohja. Termien määrittely ja hypoteesin asettelu pohjautuvat aikaisempaan tutkimustietoon. Teoriat toimivat tutkimuksen rakenteina ja ohjaavat tutkimusongelmaa ja -kysymyksiä. Teoriat tuovat yhteisen kielen tutkijoille, kaikki tietävät mistä puhutaan kun perustana on yleisesti hyväksytty teoriapohja. (Hirsjärvi, Remes & Sajavaara 2008, 136-138; Kananen 2008, 10; Kananen 2013, 49-50.)

Tämän opinnäytetyön kohdalla tutkimuksen tarkoituksena oli löytää tutkimuksen kohteena olevan prosessin ongelmakohtia ja tuoda analyysin kautta kehitysehdotuksia. Määrällisen tutkimustavan valinnan edellytys olisi, että jo tutkimuksen alkuvaiheessa voisi määrittellä, mitä lopputuloksena olisi odotettavissa. Määrällinen tutkimus voidaan nähdä vaiheittain etenevänä prosessina. Ensin on ongelma, johon lähdetään etsimään vastausta. Seuraavaksi mietitään, millä tiedolla ongelmaan saadaan vastaus. Kun tämä on selvillä, valitaan menetelmä, millä tämä tieto kerätään. Tarvittavan tiedon laatu vaikuttaa sopivan tutkimusmenetelmän valintaan ja etsittävä tieto vaikuttaa tutkimuskysymysten laadintaan. (Kananen 2008, 11-15.)

#### 4.2 Kvalitatiivinen tutkimus

Laadullisen tutkimusmenetelmän lähtökohtana on kuvata todellista elämää. Tutkimuksen kohdetta pyritään käsittelemään kokonaisvaltaisesti. Tutkimus tapahtuu tutkimuskohteen luonnollisessa ympäristössä ja tutkija on vuorovaikutuksessa tutkittavien kanssa. Tutkijan valitsema näkökulma vaikuttaa olennaisesti tutkimuksen kulkuun ja lopputulokseen. (Hirsjärvi ym. 2004, 157; Kananen 2013, 26-27.) Suomessa laadulliseen tutkimustapaan yhdistetään usein sanat pehmeä ja ymmärtävä ja toisaalta käytetään synonyyminä termiä ihmistutkimus (Tuomi & Sarajärvi 2003, 23).

Tämän opinnäytetyön lähtökohtana on mallintaa yksi organisaation sisäisistä prosesseista ja löytää tähän kehityskohteita. Jo tämä lähtötilanne poissulkee määrällisen tutkimusmenetelmän käytön, prosessin mallinnuksessa ja analyysissä ei ole numeerisesti mitattavaa tutkimustietoa saatavissa. Laadullisen tutkimusmenetelmän valintaa puoltaa myös se, että aineistoa kerätään haastatteluin, tutkimalla olemassa olevaa dokumentaatiota ja ilmiön hahmottamisen tueksi mallintamalla olemassa oleva prosessi. Tarkoituksena on tutkia prosessia kokonaisuutena, eikä esimerkiksi mitata prosessin läpimenoaikaa tms. Mikäli näin olisi, määrällinen tutkimus olisi oikea valinta tutkimusmenetelmäksi.

#### 4.3 Kvalitatiivisia tutkimusmenetelmiä

Laadullinen tutkimusmenetelmä pitää sisällään erilaisia tutkimusmetodeja. Näistä esimerkkinä mainittakoon narratiivinen, fenomenologinen ja case- eli tapaustutkimus. Narratiivisessa menetelmässä käsitellään yksittäisten ihmisten kertomuksia. Fenomenologisessa menetelmässä tutkittavia on useampia ja heistä pyritään muodostamaan yhtenäinen joukko. Yksilöiden kertomukset muodostavat kokonaisuuden. Tapaustutkimuksessa tutkimuksen kohteena on usein ilmiö, johon pyritään syvällisesti perehtymään ja lopuksi kuvaamaan kattavasti. Tapaustutkimusta lähellä olevassa kehittämistutkimuksessa on kokeellisen tutkimuksen elementtejä. Muutosta pitää pystyä mittaamaan jollain tavalla. Toimintatutkimus on luonteeltaan prosessaista. Se on sekoitus määrällistä ja laadullista tutkimustapaa. Oleellista tässä on muutoksen aikaan saaminen, tutkijan mukana oleminen ja tutkimuksellinen ote. (Kananen 2013, 28-30.)

Tähän opinnäytetyöhön tapaustutkimus sopii tutkimusmetodiksi. Tutkimuksen kohteena on tämänhetkinen ilmiö. Aineiston keräämiseen ja analyysiin tarvitaan useampia menetelmiä. Toisin kuin kehittämistutkimus, tapaustutkimus ei jatka kehitystyöhön vaan tutkimuksen lopputuloksena saadaan kehitysehdotukset ja varsinainen kehitystyö rajataan opinnäytetyön ulkopuolelle. (Kananen 2013, 54-58.)

#### 4.4 Prosessin mallinnus

Prosessin kuvaaminen on olennainen osa prosessin kehitystyötä. Prosessin kehittämislle asetut tavoitteet määrittävät prosessimallinnuksen tarkkuustason ja tarkastelun näkökulman. Tavoitteena voi olla esimerkiksi kustannustehokkuuden lisääminen, päällekkäisten työvaiheiden karsiminen tai laadun ja palvelun parantaminen. Prosessikuvaukset ovat työvälineitä päätöksenteossa sekä yritysjohdolle että lähiesimiehille esimerkiksi työnjaon ja resursoinnin suunnittelussa. Prosessimallinnus on hyödyllinen työkalu, niin laajoihin kehittämishankkeisiin kuin pienien, osaprosessien tarkasteluun. Prosessin kuvaaminen auttaa yhtenäistämään eri prosessien rajapintoja, mittaamaan kustannuksia ja arvioimaan laatua. (JUHTA 2012, 3.)

Tämän tutkimustyön perustana oli prosessin nykytilan mallinnus. Visuaalinen kuvaus prosessin eri työvaiheista ja osapuolten rooleista auttoi hahmottamaan prosessin ongelmakohtia ja näkemään vanhentuneita toimintamalleja. Myös tulevaisuudessa prosessimallinnusta voidaan käyttää apuna käyttäjätunnusten hallinnan prosessin edelleen kehittämisessä. Prosessin kuvausta ei tarvitse alusta asti tehdä uudelleen prosessin kehittyessä vaan nyt tehtyä kuvausta voidaan päivittää tarpeen mukaan.

#### 4.5 Aineiston hankinta ja analyysi

Laadulliselle tutkimusmenetelmälle tyypillisiä aineistonkeruumenetelmiä ovat kysely, haastattelu ja havainnointi. Kerätty aineisto on tekstiä, sanoja, dokumentteja ja kuvia. Tästä johdun analyysi on hieman haastavampi toteuttaa kuin määrällisen menetelmän puhtaasti laskennallinen tapa. Tarkkoja kysymyksiä ei voida määrällisen tutkimuksen tapaan esittää, koska tutkittavaa ilmiötä ei tunneta. Juuri tutkimuksen kohteen on tarkoitus avata ymmärrys ilmiöön. (Kananen 2013, 26-27.) Prosessinomistajan teemahaastattelut ja sähköpostikyselytunnusten hakijoille sekä olemassa olevaan dokumentaatioon perehtyminen ovat aineiston hankinnan välineitä tässä tutkimuksessa.

Tutkijan tulee huomioida myös eettinen näkökulma tutkimusta tehdessään. Tämä tarkoittaa laadullisen tutkimustavan osalta henkilötietojen tai nimien poistamista tai muuttamista. Nimen muuttamisessa täytyy olla varovainen, koska keksitty nimi voi olla jonkun toisen tutkittavan oikea nimi. Tutkijan tulee arvioida kerätystä aineistosta mahdollinen arkaluonteinen tieto ja poistaa tai muuttaa se tunnistamattomaan muotoon. Taustatiedot tulee esittää niin luokiteltuna, että yksittäistä tutkittavaa ei voida tunnistaa. (Kuula 2011, 214-219.) Tässä tutkimuksessa yrityksen nimi on muutettu tunnistamattomaksi, eikä yrityksessä käytössä olevien tietojärjestelmien oikeita tuotenimiä käytetä. Tutkimuksen toteutuksen ja lopputuloksen kannalta nimillä ei ole merkitystä, koska tutkimuksen kohteena eivät ole tietojärjestelmät vaan käyttäjätunnustenhallinnan prosessi kokonaisuutena.

#### 4.6 Reliabiliteetti ja validiteetti

Tutkimuksen peruslähtökohtana tulee olla pyrkimys virheettömyyteen ja puolueettomuuteen. Reliabiliteetilla tarkoitetaan tutkimuksen luotettavuutta ja sitä, kuinka hyvin tutkimus on toistettavissa. Tutkimusaineisto tulee myös olla siinä muodossa, että se on tarkastettavissa. Laadullisessa tutkimuksessa luotettavuuden arvioiminen on hieman haastavampaa kuin määrällisessä tutkimuksessa, mutta tarkka tutkimuksen kulun dokumentaatio helpottavat arviota. (Hiltunen 2009; Hirsjärvi ym. 2008, 226-227.)

Validiteetilla viitataan tutkimuksen pätevyyteen eli onko esimerkiksi tutkimusaineiston kattavuus niin hyvä, että yleistäviä päätelmiä voidaan tehdä. Jo tutkimusmenetelmän valinnassa on hyvä pitää mielessä vastaako käytetyllä tutkimusmenetelmällä saatu aineisto tutkimuskysymykseen ja onko menetelmä luotettava. Analyysivaiheessa on muistettava tutkimuksen luotettavuuden ja toistettavuuden vaatimus. Tutkimustulokset ja johtopäätökset tulee voida perustella. (Hiltunen 2009; Hirsjärvi ym. 2008, 226-227.)

#### 5 Tutkimuksen toteutus

Aloitin tutkimuksen tutustumalla tutkimuksen kannalta oleelliseen termistöön, perehtymällä alan kirjallisuuteen ja sähköisiin lähteisiin. Etsin internetistä tietoa mm. siitä, miten kaupalliset yritykset tarjoavat käyttäjätunnusten hallinnan prosessiin liittyviä palveluja ja miten he perustelevat näiden ratkaisujen tarpeellisuutta. Kun aihealue oli teoriatasolla jonkin verran selkiytynyt, aloitin tapaustutkimuksen kohdeyrityksen tilanteeseen perehtymisen. Tämän työn aloitin haastattelemalla käyttäjätunnusten hallinnan prosessin omistajaa huhti-toukokuun aikana yhteensä neljänä päivänä. Tapaamisten aikana kävimme yhdessä läpi olemassa olevan dokumentaation liittyen käyttäjätunnusten hallinnan prosessiin. Perehdyin yrityksen käyttäjätunnusten hallinnan prosessiin sekä ennen uuden IdM-järjestelmän käyttöönottoa joulukuussa 2013, että prosessin kulkuun järjestelmän käyttöönoton jälkeen. Tapaamisissa tutustuin myös Yritys X:ssä käytössä olevaan HR-järjestelmään, mikä on vahvasti liitoksissa käyttäjätunnusten hallinnan prosessiin. Prosessin omistaja esitteli myös uuden IdM-järjestelmän, jotta saisin hyvän kuvan sen tarjoamista mahdollisuuksista prosessin kehittämisen näkökulmasta.

Yritys X:n tilanteen selvittämistä ja teoriaosuuteen paneutumista tein koko ajan rinnakkain. Teoriaosan kokoamisessa oli ongelmana runsauden pula. Aiheesta on valtavasti kirjallista aineistoa etenkin englannin kielellä. Totesin jo varhain, että kovin syvälliseen ja tekniseen tarkasteluun ei ole järkevää ryhtyä tai muuten opinnäytetyö paisuu hallitsemattomasti. Tämän puolesta puhui myös se, että tutkimuksen kohteena oli käyttäjätunnusten hallinnan prosessi ja sen kehittäminen, eikä esimerkiksi pääsynhallinnan tekninen toteutus tms. Pyrin lähdeai-

neistoon pohjautuen luomaan identiteetin- ja käyttöoikeuksien hallinnan teoriasta kattavan ja kansantajuisen kokonaiskuvan, mikä tukisi prosessin kehitystyön hahmottamista.

Haastattelujen ja dokumentaation pohjalta mallinsin tämänhetkisen käyttäjätunnusten hallinnan prosessin Microsoft Wordilla (Liite 1) ja mallinnustyön edetessä olin jatkuvasti yhteydessä Yritys X:n tietohallinnon edustajaan varmistuakseni mallinnuksen oikeellisuudesta. Kesustelujen perusteella tein mahdollisia korjaustoimia prosessimallinnukseen. Mallinnuksen valmistuttua prosessin kulkua oli helpompi tarkastella ja hahmottaa siitä tärkeitä kokonaisuuksia. Prosessia tarkastelemalla tein viimeisessä luvussa esitetyt jatkokehitysehdotukset. Haastattelujen ja mallinnuksen jälkeen pidin muutaman viikon tauon ennen kuin lähdin analysoimaan tuloksia. Tämä antoi sopivasti etäisyyttä jo tutuksi tulleeseen aiheeseen. Myöhemminkin analyysivaiheen edetessä pidin muutamia pidempiä taukoja silloin, kun tuntui, ettei ajatus- ja kirjoitustyö sujunut enää niin vaivattomasti.

Jo tutkimuksen alkuvaiheen haastatteluissa kävi ilmi, että suunnittelemani sähköpostikyselyn toteuttaminen käyttäjätunnusten hakijoille olisi tässä vaiheessa tutkimuksen kannalta hyödytön. Nopeasta järjestelmän käyttöönottoaikataulusta johtuen tietojärjestelmän käyttöön liittyvät ongelmat todennäköisesti veisivät huomion itse prosessin tarkastelusta. Pidän kuitenkin tärkeänä, että prosessia edelleen kehitettäessä myöhemmässä vaiheessa prosessiin osallistujia kuunnellaan ja kerätään heiltä kokemuksia ja kehitysehdotuksia. Sähköpostikyselyä tämän toteutustapana kannattaa harkita.

## 6 Tutkimustulokset

Käyttäjätunnusten hallinnan prosessin mallintaminen osoitti useita kehityskohteita. Mitään suurta yksittäistä virhettä ei tutkimuksessa tullut esille. Esiin nousi useita pieniä asioita, joiden korjaaminen helpottaa ja selkeyttää prosessin kulkua. Erittelen seuraavassa luvussa tutkimuksessa esiin nousseita kehityskohteita sekä käyttäjätunnusten hakijan että prosessinomistajan näkökulmasta. Täysin selkeää kahtiajakoa ei kuitenkaan voi tai ole syytäkään tehdä, koska kyse on kuitenkin kokonaisuudesta enemmän kuin yksittäisistä osatekijöistä. Katsoin myös tarpeelliseksi mainita muutamalla sanalla henkilöstöhallinnon ja tietohallinnon yhteistyöstä käyttäjätunnusten hallinnan prosessin kehittämisessä. Viimeiseen lukuun olen koonnut tutkimustuloksiin pohjautuvat jatkokehitysehdotukset.

### 6.1 Käyttäjätunnusten hakijan näkökulma

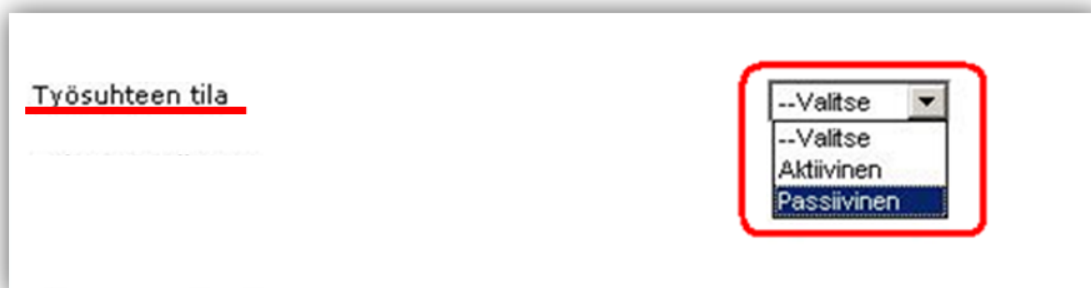
Jo ennen tutkimuksen tekemistä oli selvää, että uuden IdM-järjestelmän käyttöönottoaikataulu oli ollut tiukka. Esimiesten koulutus uuteen järjestelmään ja siihen liittyviin toimintatapojen muutoksiin vaatii jatkossa lisää panostusta, jotta järjestelmän mahdollistamat hyödyt



saadaan kokonaisuudessaan käyttöön. Ajantasaista ohjeistusta ei tällä hetkellä ole saatavilla yrityksen intranetissä, mutta jatkossa on tarkoitus tehdä selkeät kuvalliset ohjeet esimiesten työtä helpottamaan. Tämä oli jo suunnitelmassa ennen tutkimusta, mutta tutkimuksen parannusehdotusten toteutuksen jälkeen ohjeista saadaan selkeämpi ja ymmärrettävämpi kokonaisuus. Vanhat viittaukset tunnustilauslomakkeelle poistetaan esimiesten intranet-ohjeista, jotta väärinkäsityksiltä vältytään. Vanha tilauslomake ei enää ole toiminnassa. Intranetin ohjeiden päivityksen jälkeen varmistetaan tiedon perille meneminen vielä sähköpostilmoituksella esimiehille, johon liitetään saatteeksi maininta siitä, mikä käyttäjätunnusten hallinnan prosessissa on muuttunut. (Niemi 2014.)

Prosessiin kuuluu tällä hetkellä sähköpostitse tehtäviä ilmoituksia, jotka olisivat korvattavissa järjestelmän automaattisesti lähettämällä viesteillä. Tällä hetkellä prosessi toimii siten, että esimiehen luodessa uuden henkilön HR-järjestelmään, hän jättää Työsuhteen tila -valinnan passiiviseksi ja laittaa sähköpostiviestin HR-osastolle, josta käsin tiedot aktivoidaan. Aktiivinen/passiivinen -valinta tarkoittaa järjestelmässä IdM-järjestelmään lähtevää viestiä, ei henkilön työsuhteen tilaa (Kuva 1). (Niemi 2014.) Muuttamalla kentän selitettä todellisuutta kuvaavammaksi, esimerkiksi tietojen siirto IdM:ään ja ohjeistamalla esimiehet valitsemaan tilan aktiiviseksi, tieto uudesta henkilöstä menisi suoraan eteenpäin, eikä erillistä sähköpostia tarvitsisi lähettää.

Myös työsuhteen päättymistilanteessa erillisiltä viesteiltä vältytään, mikäli prosessia muutetaan siten, että esimies ei muuta Työsuhteen tila - valintaa passiiviseksi. Kun työsuhteen päättymispäivä on syötetty, järjestelmä nostaa työsuhteen virhelistalle kyseisen päättymispäivän jälkeen. Henkilön verkkotunnus ja sähköposti sulkeutuvat automaattisesti ja tietohallinto tekee manuaalisesti loput tarvittavat lopetustoimenpiteet, kuten esimerkiksi puhelin- ja intranet-oikeuksien poistot. (Niemi 2014.) Tämä muutos prosessin kulkuun helpottaisi esimiehiä tunnustenhakuprosessissa ja näin myös välttyttäisi unohduksilta ja inhimillisiltä erehdyksiltä.



Kuva 1: Ruutukaappaus HR-järjestelmästä

## 6.2 Käyttäjätunnusten hallinnan prosessin omistajan näkökulma

Tällä hetkellä työntekijän tai ammatinharjoittajan nimenmuutostilanteeseen liittyy paljon manuaalista työtä. Käyttäjätunnuksen muutoksen uudelle nimelle tekee IdM-järjestelmän toimittaja manuaalisesti. Jatkossa tätä tullaan kehittämään automaation suuntaan. Kun HR-järjestelmään muutetaan henkilön nimitietoja, järjestelmän ylläpitäjä ei saa tästä automaattista ilmoitusta vaan esimiehen tulee muistaa tästä informoida erikseen. HR-järjestelmän toiminnallisuutta voisi muuttaa siten, että nimitietojen muutos lähettäisi automaattisen viestin eteenpäin. Ainakin tämän muutoksen mahdollisuutta kannattaa selvittää. (Niemi 2014.)

Tällä hetkellä järjestelmän ylläpitäjälle tulevat sekä hyväksyntäviestit että hyväksynnän jälkeiset toimenpideviestit samaan sähköpostiosoitteeseen. Selvyyden vuoksi olisi hyvä, jos nämä viestit ohjautuisivat erillisiin sähköpostilaatikoihin. Näin puhtaasti ilmoitukselliset ja arkistoitavat viestit olisivat omassa postilaatikossa ja toimenpiteitä vaativat viestit omassaan. (Niemi 2014.)

Tämän hetken käytännön mukaan ammatinharjoittajien kohdalla ilmoitus käyttöoikeuksien käsittelystä ohjautuu takaisin tietohallintoon. Ilmoituskäytännön toteutusta olisi hyvä miettiä uudestaan, koska tietohallintoon ohjautuvien viestien tulisi olla merkityksellisiä saajan kannalta, eikä ilmoituksia itse tehdystä työstä. Ammatinharjoittajien kohdalla kyseiset ilmoitusviestit voisi ohjata esimerkiksi yksikön päällikölle. (Niemi 2014.)

## 6.3 Henkilöstö- ja tietohallinnon yhteistyö

Käyttäjätunnusten hallinnan prosessissa tietohallinnon ja henkilöstöhallinnon tehtävät risteävät monessa kohtaa. Prosessin sujuvuuden kannalta on tärkeää, että näiden tahojen yhteistyö sujuu ja prosessia kehitetään ottaen huomioon molempien osapuolten näkökulmat. Tässä opinnäytetyössä henkilöstöhallinnon roolin tarkastelu rajattiin tutkimuksen ulkopuolelle ja keskityttiin tarkastelemaan prosessia tietohallinnon ja tunnusten hakijan näkökulmista. Muutama tärkeä asia kuitenkin nousi henkilöstö- ja tietohallinnon yhteistyöstä esille, jotka on syytä tässä mainita.

Käyttäjätunnusten hallinnan prosessin kannalta on tärkeää, että henkilöstöhallinnon prosessin kulku on järjestetty uuden työsuhteen alkaessa siten, että perus- ja työsuhtetiedot viedään tietojärjestelmään ennen todellista työsuhteen alkamispäivää. Näin provisiointityöt voidaan suorittaa jo ennen työsuhteen alkua ja käyttäjätunnukset ovat käyttövalmiina työntekijän aloittaessa työsuhteen. Useiden määräaikaisten työsuhteiden ketjuissa on tärkeää, että henkilöstöhallinnon prosessi toimii siten, että tiedot ovat reaaliaikaisesti tietojärjestelmässä. Työsuhteen jatkaminen suullisesti ja ns. muodollisuuksien hoitaminen vasta myöhemmin on

merkittävä riski jatkuvuuden kannalta. Se tulee tiedostaa ja huomioida prosessien kehitystyössä. (Niemi 2014.)

## 7 Yhteenveto ja johtopäätökset

Tutkimuksen lähtökohtana oli etsiä Yritys X:n käyttäjätunnusten hallinnan prosessista kehityskohteita. Taustalla oli nopealla aikataululla käyttöön otettu IdM-järjestelmä ja tarve karsia käyttäjätunnusten hallinnan prosessista vanhentuneita ja turhiksi käyneitä toimintatapoja. Tutkimuksessa tarkasteltiin erilaisia mahdollisuuksia hyödyntää uuden järjestelmän tarjoamia toimintoja prosessin automatisoinnissa ja karsia turhaa manuaalista tai päällekkäistä työtä. Tutkimus antoi vastauksen alussa esitettyyn tutkimuskysymykseen ” Miten yritys X:n käyttäjätunnusten hallinnan prosessia voidaan kehittää?” ja kehitysehdotukset esitellään luvussa 10.

Tutkimus toteutettiin tapaustutkimuksena kevään 2014 aikana. Tiedonkeruu tapahtui haastatteleamalla Yritys X:n tietohallinnossa käyttäjätunnusten hallinnan prosessin omistajaa ja perehtymällä olemassa olevaan dokumentaatioon käyttöoikeushallinnan prosessista. Kokonaisuuden hahmottamisen vuoksi tutustuin myös yrityksen käytössä olevien IdM- ja HR-järjestelmien toimintaan. Olennainen osa tutkimusta oli käyttäjätunnusten hallinnan prosessin mallinnus pohjautuen haastatteluihin ja olemassa olevaan dokumentaatioon. Prosessia tarkastelemalla pyrittiin löytämään selkeitä kehityskohteita.

Reliabiliteetin vaatimus tutkimusaineiston tarkastettavuudesta toteutuu opinnäytetyössä. Haastatteluja ei tallennettu sellaisenaan, jotta yrityksen liiketoiminnan kannalta kriittiset tiedot turvattaisiin, mutta haastattelujen pohjalta tehdyt muistiinpanot ovat tarkistettavissa. Myös opinnäytetyön aineistona ollut dokumentaatio käyttäjätunnusten hallinnan prosessista ja tietojärjestelmien ohjeistus ovat edelleen olemassa ja tarkistettavissa. Tutkimuksen tekijä oli täysin ulkopuolinen suhteessa tutkimuksen kohteena olleeseen prosessiin, eikä mitään eturistiriitoja ole löydettävissä. Näin ollen voidaan todeta tutkimuksen olleen puolueeton.

Validiteetin kannalta olisi saattanut olla parempi, jos opinnäytetyössä olisi ollut tutkimustuloksia useammista eri lähteistä. Ponemon Instituutti ei ollut aiemmin tuttu tutkimuslaitos, mutta selvitysteni perusteella sen luotettavuutta ei ole syytä epäillä. Jonkun toisen kansainvälisen tutkimuslaitoksen tutkimus olisi saattanut tuoda käytännön tasolla vahvistusta työssä viitattujen tutkimustulosten oikeellisuuteen. Kuitenkin tutkimus vastasi asetettuihin tutkimuskysymyksiin ja selkeitä kehitysehdotuksia oli prosessista löydettävissä. Prosessin mallinnus auttoi hahmottamaan prosessin kulkua paremmin ja löytämään vaihtoehtoisia ja yksinkertaisempia toimintatapoja.

Alun perin suunnitellut esimiesten haastattelut jätin tutkimuksen ulkopuolelle, koska tutkimuksen edetessä totesin haastattelujen tuoman lisäinformaation olevan todennäköisesti merkityksetöntä tutkimuksen lopputuloksen kannalta. Jatkossa, kun uuden käyttäjätunnusten hallinnan prosessin ohjeistus on selkeämpää ja käyttö rutinoidumpaa, esimiehille suunnatulla kyselytutkimuksella voidaan saada valaisevaa lisäinformaatiota ja arvokasta aineistoa prosessin kehitystyöhön.

## 8 Jatkokehitysehdotukset

Ensisijainen tutkimuskysymys tälle tapaustutkimukselle oli: ”Miten yritys X:n tietojärjestelmien käyttäjätunnusten hallinnan prosessia voidaan kehittää?”. Tässä luvussa esittelen tärkeimmät jatkokehitysehdotukset tutkimuksen esiin nostamiin ongelmakohtiin. Tutkimuskysymyksiä olivat myös: ”Voidaanko prosessin olemassa olevia käytäntöjä yksinkertaistaa ja karsia turhia työvaiheita?” ja ”Voidaanko uuden IdM-järjestelmän tarjoamia mahdollisuuksia paremmin hyödyntää käyttäjätunnusten hallinnan prosessissa?”. Näihin kysymyksiin pyrin vastaamaan jatkokehitysehdotusten muodossa.

Tutkimusaineiston analyysin perusteella keskeisimmäksi kehityskohteeksi nousi manuaalisten viestien korvaaminen tietojärjestelmän automaatiikalla. Tämä kehityskohde nousi esiin tarkastellessa prosessia sekä prosessin omistajan että käyttäjätunnusten hakijan näkökulmasta. Tämän asian kuntoon saattaminen yksinkertaistaisi prosessia ja karsisi turhaa työtä. Työsuhteen alkamiseen ja päättymiseen liittyvät manuaaliset ilmoitukset on korvattavissa IdM-järjestelmän automaatiolla. Järjestelmä nostaa päättyneen työsuhteen virhelistalle ja tietohallinto voi poimia tiedon ja tehdä tarvittavat toimenpiteet ilman erillistä ilmoitusta. Riski inhimillisille erehdyksille ja unohduksille pienenee huomattavasti, kun tietojärjestelmä nostaa automaattisesti työpöytä tietohallintoon. Vaikka tutkimuksessa ei mitattukaan prosessin läpimenoaikoja, tietojärjestelmän automaatiikka voi oleellisesti nopeuttaa prosessin kulkua.

Tietohallintoon saapuvien viestien selkiyttäminen on myös tärkeä kehityskohde. Tällä hetkellä työpöydät ja arkistoitavat ilmoitukset saapuvat samaan paikkaan. Arkistoitavat ilmoitusviestit ja varsinaiset työpöydät tulee ohjata eri kohteisiin. Näin vältetään tärkeiden työpöytäviestien hukkumiselta ilmoitusviestien sekaan. Tällä hetkellä ammatinharjoittajien kohdalla ilmoitus käyttäjätunnusten käsittelystä ohjautuu takaisin tietohallintoon. Selvyyden vuoksi nämä viestit tulisi ohjata esimerkiksi yksikön päällikölle.

Nimenmuutostilanteeseen liittyen prosessissa on paljon kehitettävää. Tämän osuuden kehitystyö vaatii kuitenkin IdM-järjestelmän toimittajan ja Yritys X:n yhteistyötä. HR-järjestelmä ei tällä hetkellä ilmoita muuttuneesta nimestä vaan tästä täytyy erikseen ilmoittaa tietohallin-

toon. HR-järjestelmän osalta kannattaa selvittää, voiko asetuksia muuttaa siten, että tieto nousisi automaattisesti IdM-järjestelmään. Vaikka tieto nousisikin automaattisesti, tietohallintokaan ei pysty tällä hetkellä nimenmuutosta toteuttamaan vaan pyyntö lähetetään edelleen IdM-järjestelmän toimittajalle, joka tekee tarvittavat muutokset.

Käyttäjätunnusten hakijan kannalta ohjeistuksen uudistaminen ajantasalle on ensiarvoisen tärkeää. Tällä hetkellä uuden järjestelmän hyödyistä saadaan vain pieni osa käytettyä hyväksi, kun käyttäjien aikaa kuluu järjestelmän toiminnan ihmettelyyn. Epävarmuus uuden tietojärjestelmän käyttäjällä voi pahimmillaan ajaa vanhoihin, tutuiksi ja turvallisiksi koettuihin toimintamalleihin. Asiat pyritään hoitaa puhelimitse tai sähköpostitse, kun uuden järjestelmän käytössä on ongelmia. Viittaukset vanhoihin lomakkeisiin ja ohjeisiin tulee poistaa ja tehdä selkeitä, mielellään kuvakaappauksin havainnollistetut ohjeet.

Jatkossa, käyttäjätunnusten hallinnan prosessia edelleen kehitettäessä, kannattaa käyttäjätunnusten hakijoiden ehdotuksia ja mielipiteitä kuulla esimerkiksi sähköpostikyselyn muodossa. Eri osapuolten yhteistyöllä on suuri merkitys jatkuvassa kehitystyössä kohti toimivaa ja tehokasta prosessia.

## 9 Oman osaamisen arviointi

Opinnäytetyön tekeminen oli monella tapaa opettavainen kokemus. Kirjalliseen lähdeaineistoon perustuva kirjoitustyö oli tuttua, eikä se aiheuttanut mitään ongelmia nytkään. Ohjeistus muotoseikkoihin oli kattavaa ja siksi täyden huomion saivat muut, kokonaisuuden kannalta tärkeät osa-alueet. Ajankäyttö ja aikataulut olivat tärkeitä tutkimustyön koossa pitäviä elementtejä. Normaalisti olisin tarttunut työhön aikataulua sen kummempia suunnittelematta, mutta nyt jälkikäteen voin todeta, että aikataulu ja siinä pysyminen antoivat työskentelylle aivan uudenlaista ryhdikkyyttä. Asetin selkeitä tavoitteita kunkin työvaiheen etenemiselle, mutta jätin myös tarpeeksi pelivaraa aikatauluun, jotta odottamattomat muutokset suunnitelmiin tai tarvitsemani tauot analyysivaiheessa eivät sekoittaneet aikataulua kokonaan. Lähestyvä kesä ja pitkä kesälomakausi olivat vahva porkkana pysyä suunnitellussa aikataulussa, jottei opinnäytetyöprosessi venyisi pitkälle syksyyn.

Prosessin mallintaminen oli mielestäni keskeisessä roolissa kokonaisuuden hahmottamisessa ja auttoi prosessin kehityskohteiden määrittelemisessä. Koska olen vahvasti visuaalinen oppija, tämän työvaiheen merkitys vielä korostui entisestään. Mallinnustyö sujui yllättävän luontevasti siitä huolimatta, että aikaisempi kokemus prosessimallinnuksesta rajoittui yhteen ryhmätyöhön opintoihin liittyen. Tähän vaikutti varmasti myös se, että käytössä oli tuttu, yksinkertainen työkalu, millä mallinnus toteutettiin. Työn jälki olisi ehkä ollut laadukkaampaa, jos

mallinnuksen olisi tehnyt varta vasten siihen suunnitellulla työkalulla, mutta jälkikäteen arvioiden uskon, että tekemäni ratkaisu oli tässä tapauksessa ainoa oikea.

Prosessin omistajan kanssa käydyt keskustelut ja haastattelut nostivat esiin jo ennen analyysivaihetta paljon kehitysehdotuksia ja vuorovaikutus antoikin vielä lisää motivaatiota työn läpiviennin. Tietoisuus siitä, että työllä oli oikeasti merkitystä, oli minulle erityisen tärkeää. Uskon, että opinnäytetyöprosessin läpiviennin onnistumisen ja oman oppimisen kannalta oli tärkeää tiedostaa, mitkä olivat kokonaisuuden kannalta tärkeitä työvaiheita ja keskittyä näihin ja jättää toisarvoiset asiat vähemmälle huomiolle.

## Lähteet

### Kirjalliset lähteet

Andreasson, A. & Koivisto, J. 2013. Tietoturva toteuttamassa. Helsinki: Tietosanoma.

Bertino, E. & Takahashi, K. 2011. Identity Management: Concepts, Technologies and Systems. Norwood: Artech House. Viitattu 20.3.2014. Saatavissa Ebook Library -tietokannassa: <http://laurea.eplib.com/patron/Read.aspx?p=634511>

Coyne, E.J. & Davis J.M. 2008. Role Engineering for Enterprise Security Management. Norwood: Artech House.

Ferraiolo, D.F., Kuhn R.D. & Chandramouli, R. 2007. Role-Based Access Control. 2. painos. Norwood: Artech House.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2004. Tutki ja kirjoita. 10. painos. Jyväskylä: Gummerus Kirjapaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2008. Tutki ja kirjoita. 13.-14. painos. Helsinki: Kustannusosakeyhtiö Tammi.

Jordan, E & Silcock, L. 2006. Strateginen IT-riskien hallinta. Helsinki: Edita Prima.

Kananen, J. 2008. Kvantti. Kvantitatiivinen tutkimus alusta loppuun. Jyväskylä: Jyväskylän yliopistopaino.

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylä: Suomen Yliopistopaino - Juvenes Print.

Kuula, A. 2011. Tutkimusetiikka. Aineistojen hankinta, käyttö ja säilytys. 2. painos. Tampere: Vastapaino.

Sharoni, I., Spaulding, K., Williamson, G. & Yip, D. 2012. Identity Management: A Primer. Viitattu 20.3.2014. Lewisville: MC Press. Saatavissa Ebook Library -tietokannassa: <http://laurea.eplib.com/patron/Read.aspx?p=839198>

Taylor, A., Alexander, D., Finch, A. & Sutton, D. 2013. Information Security Management Principles. Chippenham: CPI Antony Rowe Ltd. Viitattu 20.3.2014. Saatavissa Ebook Library - tietokannassa: <http://laurea.eplib.com/patron/Read.aspx?p=1213992>

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannus-osakeyhtiö Tammi.

Valtiovarainministeriö. 2006. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. Helsinki: Edita Prima.

Sähköiset lähteet

Hiltunen, L. 2009. Validiteetti ja reliabiliteetti. Viitattu 27.4.2014.

[http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius\\_ ja\\_reliabiliteetti.pdf](http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ ja_reliabiliteetti.pdf)

JUHTA - Julkisen hallinnon tietohallinnon neuvottelukunta. 2012. JHS 152 Prosessien kuvaaminen. Viitattu 10.8.2014.

<http://docs.jhs-suositukset.fi/jhs-suositukset/JHS152/JHS152.pdf>

Linden, M. 2012. Identiteetin- ja pääsynhallinta. Luentomoniste. Viitattu 31.3.2014.

<http://www.cs.tut.fi/~linden/iam-pruju.pdf>

Ponemon Institute. 2011. Insecurity of Privileged Users -Global Survey of IT Practitioners. Viitattu 26.4.2014.

<http://h30507.www3.hp.com/hpblogs/attachments/hpblogs/666/62/1/HP%20Privileged%20User%20Study%20FINAL%20December%202011.pdf>

Ponemon Institute. 2012. Future State of IT Security - A Survey of IT Security Executives. Viitattu 7.5.2014.

[http://www.ponemon.org/local/upload/file/Future\\_state\\_of\\_IT\\_Security\\_FINAL%207.pdf](http://www.ponemon.org/local/upload/file/Future_state_of_IT_Security_FINAL%207.pdf)

Ponemon Institute. 2012. The Human Factor in Data Protection. Viitattu 26.4.2014.

[http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt\\_trend-micro\\_ponemon-survey-2012.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf)

Ponemon Institute. 2014. About Us. Viitattu 20.9.2014

<http://www.ponemon.org/about-ponemon>



Tietotekniikan liitto. 2013. Tutkimusraportti - IT-barometri 2013. Viitattu 7.5.2014.  
[http://www.ttlry.fi/sites/ttl.ttlry.mearra.com/files/file-uploads/Tutkimus/IT-barometri/ITBarometri\\_Tutkimusraportti\\_2013\\_julkinen\\_fin.pdf](http://www.ttlry.fi/sites/ttl.ttlry.mearra.com/files/file-uploads/Tutkimus/IT-barometri/ITBarometri_Tutkimusraportti_2013_julkinen_fin.pdf)

Julkaisemattomat lähteet

Niemi, J. 2014. Käyttäjätunnustenhallinnan prosessin omistajan haastattelut 7.4., 14.4., 23.4. ja 15.5.2014. Yritys X. Helsinki.

## Kuvat

Kuva 1: Ruutukaappaus HR-järjestelmästä .....	25
---	----

## Kuviot

Kuvio 1: Vastaajien käyttöoikeuksien ajantasaisuus ja syyt eriteltyinä, mikäli ne eivät ole ajantasaisia (Ponemon Institute 2011, 5).....	13
Kuvio 2: Vastaajat arvioivat väittämien todennäköisyyden omassa yrityksessään (Ponemon Institute 2011, 6). .....	14
Kuvio 3: Tietoturvan kannalta merkittävimmät inhimilliset uhkatekijät vastaajien mielestä (Ponemon Institute 2012a, 14). .....	15
Kuvio 4: Tietoturvan kannalta merkittävien inhimillisten uhkatekijöiden kehitys tulevaisuudessa vastaajien mukaan (Ponemon Institute 2012a, 14). .....	15
Kuvio 5: Vastaajien mielestä organisaation tärkeimmät tietoturvateknologiat uhkia vastaan (Ponemon Institute 2012b, 5).....	16
Kuvio 6: Vastaajien arvio IT:n merkityksestä yrityksen menestykselle tulevaisuudessa (IT-barometri 2013, 21). .....	17
Kuvio 7: Best Practise menetelmien käyttö vastaajien yrityksissä (IT-barometri 2013, 29).18	
Kuvio 8: Roolien mukainen käyttäjähallinta (mukaillen Linden 2012, 31). .....	19

## Liitteet

Liite 1 Käyttäjätunnusten hallinnan prosessikaavio .....	37
--	----

