Haaga-Helia
ammattikorkeakoulu Oy

Sähköisen identiteetinhallinnan ja käyttöoikeuksien tilausprosessin toimintamallin kehittäminen

Miikka Allén

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2017

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Miikka Allén

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Sähköisen identiteetinhallinnan ja käyttöoikeuksien tilausprosessin toimintamallin kehittäminen

Sivu- ja liitesivumäärä
31 + 13

Opinnäytetyön otsikko englanniksi
Operations models for electronic identity management and for the requisition process of acces rights

Tämän opinnäytetyön tarkoituksena on kuvata kaupanalan sähköisen identiteetin ja käyttöoikeuksien hallinta - ja tilausprosessia sekä selvittää miten ja millä tavoin olemassa olevia prosesseja voidaan kehittää enemmän liiketoimintaa tukeviksi.

Opinnäytetyön teoriaosuus sisältää identiteetinhallinnan, sekä käyttöoikeuksien tilausprosessin esittelyn. Teoriaosuudessa käydään läpi prosessin ongelmatilanteita, joihin tarvitaan it-kehitystoimenpiteitä, jotta Yrityksen liiketoimintaa tukevat it-tehtävät on mahdollista suorittaa tehokkaasti ja tulevaisuudessa yksinkertaistetun uuden prosessin mukaisesti. Prosessin tehokkuuden tavoitteena on kehittää yksinkertainen prosessi Yrityksen käyttöoikeushallinnan työvälineeksi, jotta työntekijöille voidaan antaa it-oikeudet eri järjestelmiin nopean prosessin kautta työsuhteen alussa, tai käyttöoikeuksien tarpeen muuttuessa.

Opinnäytetyön tavoitteena on saada aikaan kehitysehdotuksia, millä parantaa kaupanalan yritysten käyttöoikeuksien tilaamisprosessia, sekä saada aikaan säästöjä vähentämällä It-toimittajien ja Yrityksen Tietohallinnon manuaalista työtä.

Keväällä 2018 voimaan astuva uusi EU:n tietosuojalaki antaa myös hallitulle sähköiselle identiteetinhallinnalle kehitystarpeen, jonka vuoksi tämän tutkimuksen tulokset ovat erittäin relevantteja yritykselle ja myös muiden toimialojen toimijoille.

Opinnäytetyön tietoperusta pohjautuu tekijän työkokemuksesta saadusta tietämyksestä, sekä aiheesta löytyvästä kirjallisuudesta ja esimerkkitapauksista. Järjestelmän omat dokumentaatiot ja sen kuvaukset olivat lisämateriaaleja, jotka tukivat mallin kehittämistä. Lisäksi kehittämistyötä varten tietolähteinä käytettiin laajaa kansainvälistä kirjallisuutta.

Opinnäytetyön tulokseksi saatiin aikaan kehitysehdotuksia ja uusi sähköisen identiteetinhallinnan ja käyttöoikeusprosessi -malli. Haastatteluista saatu data ja tutkimuksen kehitysehdotukset ovat tukeneet kehittämistä ja uuden mallin toteuttamista. Opinnäytetyön tuloksena syntynyt malli vastaa myös uuden EU:n tietosuoja-asetuksen asettamiin vaatimuksiin. Malli lisää yrityksille identiteetinhallinnan kustannustehokkuutta ja muuttaa oleellisesti yrityksen operatiivista toimintaa niiltä osin entistä tehokkaammaksi ja toimivammaksi sekä toimittajan että asiakkaan näkökulmasta.

Asiasanat
Käyttöoikeushallinta, IAM, IDM

Sisällys

1 Sanasto

AD	Active Directory. Microsoftin Windows -toimialueen käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä tietokoneista, ja verkon resursseista.
Käyttäjähallinta	Käyttäjäidentiteetti ja käyttäjätilitietojen ylläpitojärjestelmä.
Identiteetti	Kuvaa käyttäjää ja millä käyttäjä voidaan tunnistaa.
IAM	Identity and Access Management. Tarkoittaa tässä asiayhteydessä organisaatioon liittyviä sääntöjä ja toimintoja, jonka avulla varmistetaan järjestelmien asianmukainen käyttö.
IDM	Identity Management. Mahdollistaa käyttäjäidentiteettiin yhdistettyjen käyttöoikeuksien hallinnan ja oikeuksien siirron kohdejärjestelmiin.
Tietosuoja	Data Protection. Perustuslain takaama yksityisyyden suoja.
Tietoturva	Tarkoittaa tässä asiayhteydessä tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitoa.
GDPR	General Data Protection Regulation. Keväällä 2018 voimaan astuva EU:n tietosuoja-asetus.
Provisiointi	Identiteetin ja käyttöoikeustietojen välittäminen kohdejärjestelmiin.
HR	Human resources, eli henkilöstöhallinto.
Helpdesk	Käyttötuki. Neuvontayksikkö, joka palvelee organisaatiota tietoteknisissä ongelmakysymyksissä.
Työrooli	Käyttäjärooli, tai työrooli määritellään työntekijän tarvitsemien käyttöoikeuksien näkökulmasta. Rooli sisältää ominaisuudet ja oikeudet järjestelmiin mitä työntekijä tarvitsee suoriutuakseen työtehtävistään.
SAP	Systeme, Anwendungen und Prudukte. Toiminnanohjausjärjestelmä.
SAP CUA	Central User Administration. Järjestelmän osiossa hallinnoidaan SAP tunnuksia ja käyttöoikeuksia.
SQL	Structured Query Lanquage. IBM:n kehittämä standardisoitu ohjelmoinnin kyselykieli, joka mahdollistaa haut ja kyselyt relaatiotietokannoista.
SOAP	Automatisoitu rajapintojen testityökalu.
PROVISIOINTI	Tarkoittaa tässä asiayhteydessä, että uusi käyttäjä saa käyttöoikeudet automatisoidusti.

2 Johdanto

Tämä opinnäytetyö on osa Haaga-Helian ammattikorkeakoulun Tietojenkäsittelyn koulutusohjelmaa. Aloitin työskentelyn Yrityksen palveluksessa 2012. Käyttöoikeudet ja käyttöoikeusprosessit ovat osa it-ammattilaisen toimenkuvaani, siten tämän aiheen valinta opinnäytetyöksi tuntui luontevalta vahvan työelämäkokemukseni ja osaamiseni näkökulmasta. Tässä opinnäytetyössä käytetään ”Yritys” sanaa luottamuksellisuuden vuoksi, kohdeyrityksen oikean nimen sijasta.

Opinnäytetyön tarkoituksena on selvittää käyttöoikeuksien tilaamisprosessin nykytilan ongelmat ja selvittää siihen liittyviä kehitysmahdollisuuksia. Tämän työn tuloksena syntyy uusi toimintamalli jonka pohjalta yritys voi nopeuttaa henkilöstön käyttöoikeuksien tilaamisprosessia, sekä saada aikaan säästöjä vähentämällä työmäärää It-toimittajan ja Yrityksen Tietohallinnon osalta. Myös keväällä 2018 voimaan astuva uusi EU:n tietosuoja-asetus antaa vaatimuksen yrityksille parantaa henkilötietoihin liittyvää tietosuojaa.

Opinnäytetyön tietoperustana käytettiin omien kokemuksien ja havaintojen lisäksi Yrityksen dokumentaatiota ja aiheen prosessi kuvauksia. Lisämateriaalia saatiin haastatteluista, sekä käyttäjähallinnan, että järjestelmän toimittajan asiantuntijoilta. Myös omat havainnot ja kokemukset antoivat hyvän perustan opinnäytetyölle. Menetelmäkuvauksia varten tietolähteinä käytettiin aiheeseen liittyvää kansainvälistä kirjallisuutta.

2.1 Tavoitteet ja rajaus

Opinnäytetyön tarkoituksena on kuvata Yrityksen käyttöoikeuksien hallinta ja tilausprosessia. Myös identiteetinhallinnalla on olennainen osuus tässä opinnäytetyössä. Opinnäytetyössä pyritään löytämään identiteetinhallinnan prosessin ongelmakohdat ja niiden pohjalta kehittää käyttöoikeuksien tilausprosessia, sekä identiteetinhallintaa uuden tietosuojalain ja tietoturvan peruskäsitteiden mukaisiksi. Käyttöoikeuksien tilaamisprosessi on tarkoitus saada tulevaisuudessa mahdollisimman automatisoiduksi ja sujuvaksi prosessiksi. Sen tarkoituksena on, että työntekijät saavat tilatut käyttöoikeudet sovittujen aikojen puitteissa.

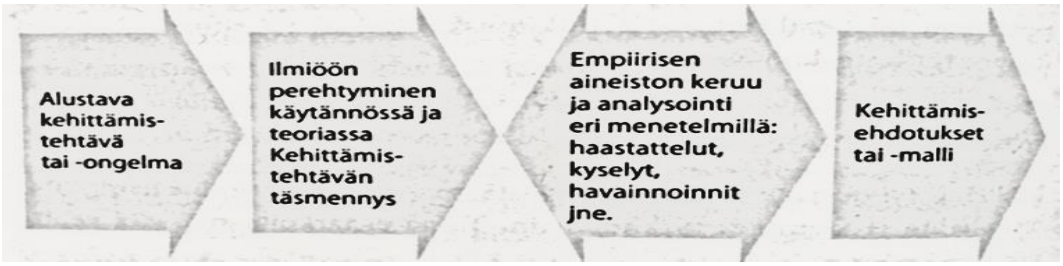
Prosessin kehittämisen on myös tarkoitus vähentää henkilöstöhallinnon, It-toimittajien, sekä Tietohallinnon manuaalista työtä merkittävästi. Opinnäytetyön tavoitteena omalle oppimiselle on saada opinnäytetyön aikana lisätietoa identiteetinhallinnan prosesseista ja niiden tarjoamista mahdollisuuksista huomioiden myös uuden EU:n tietosuoja-asetuksen,

joka astuu voimaan keväällä 2018. Opinnäytetyö on rajattu Yrityksen käyttöoikeuksien tilausprosessiin. Yritys on osa suurta suomalaista monialakonsernia.

2.2 Tutkimusmenetelmä

Tämän opinnäytetyön tutkimusmenetelmäksi on valittu tapaustutkimus. Tapaustutkimus soveltuu hyvin tämän kehittämistyön toteuttamiseen, kun tehtävänä on tuottaa kehittämisehdotuksia ongelmalliseksi havaittuun prosessiin. Tutkimuksen kohde eli tapaus voi olla esimerkiksi yritys tai sen osa, yrityksen tuote, palvelu tai prosessi. (Ojasalo, Moilanen & Ritalahti 2015, 52.) Tapaustutkimuksessa lähdetään tyypillisesti liikkeelle analysoitavasta tai tutkittavasta tapauksesta. Kehittämisen kohteesta kiinnostuneella on usein ilmiöstä jonkinlaista aiempaa tietoa, mikä mahdollistaa alustavan kehittämistehtävän määrittelyn. (Ojasalo, Moilanen & Ritalahti 2015, 54.)

Tapaustutkimuksessa on tyypillistä, että monenlaisia menetelmiä käyttämällä saadaan syvällinen, monipuolinen ja kokonaisvaltainen kuva tutkittavasta tapauksesta. Tapaustutkimusta on mahdollista tehdä niin määrällisin, kuin laadullisinkin menetelmin tai niitä yhdistelemällä. Usein tapaustutkimus liitetään erityisesti laadulliseen tutkimukseen ja menetelmiin, mutta siinä on siis mahdollista hyödyntää myös määrillisiä menetelmiä (esimerkiksi kyselyjä). Aineistot kerätään yleensä luonnollisissa tilanteissa, esimerkiksi tilanteita havainnoimalla tai analysoimalla kirjallisia aineistoja (esimerkiksi yrityksen erilaiset raportit). Haastatteluja käytetään usein tiedonkeruumenetelmänä tapaustutkimuksessa. Tämä johtuu siitä, että tapaustutkimus liittyy tyypillisesti ihmisen toiminnan tutkimiseen eri tilanteissa, jolloin itse toimijat, eli kehitettävän ilmiön asiantuntijat voivat kuvata ja selittää ilmiötä. Asiantuntija voi myös selvittää tilanteeseen johtaneita syitä, joiden todenperäisyyttä voi tutkia muilla menetelmillä (esimerkiksi havainnoimalla todellisia tilanteita). (Ojasalo, Moilanen & Ritalahti 2015, 55.)



Kuvio 1. Tapaustutkimuksen vaiheet (Ojasalo, Moilanen & Ritalahti. 2015, 54)

3 Käyttövaltuushallinnan periaatteet ja lainsäädäntö

Tietojärjestelmässä on oltava luotettava käyttäjähallinta, johon ainoastaan siihen valtuutetuilla henkilöillä on oikeus luoda, lisätä, muuttaa tai poistaa tietojärjestelmään sisältyviä tietoja, kuten asiaryhmitystä. Yleensä tämän hoitaa yrityksen tietohallinto, tai siihen ulkoistettu IT- toimittaja.

Käyttövaltuudet ovat tietojärjestelmien käyttäjille myönnettyjä henkilökohtaisia oikeuksia tietojärjestelmän käyttöön tai tietojen saantiin. Käyttövaltuudet ovat työtehtävien mukaisia ja ne on pidettävä ajan tasalla. Käyttövaltuuksien antaminen, muuttaminen ja poistaminen on dokumentoitava ja niiden hallinnasta on tallennuttava tietojärjestelmään valvontalokitietoa. Tietojärjestelmien käyttäjillä tulee olla henkilökohtainen käyttäjätunnus ja salasana tietojärjestelmiin. Kun tietojärjestelmään kirjaudutaan etäyhteydellä, on edellytettävä luotettavaa tunnistamista. Ulkopuolisten pääsy järjestelmään
estetään normaaleilla käyttöoikeuksien hallintamenetelmillä ja palomuuriratkaisuilla. (Valtiovarainministeriö Vahti 2009.)

3.1 Käyttövaltuushallinnon ongelmat

Vahti on julkisen digitaalisen turvallisuuden johtoryhmän ohjesivusto. Vahti-ohjeiden tarkoitus on toimia työkaluna organisaatioille tietoturvan ylläpitämisessä. Vahtiohje on saatavissa verkko-osoitteesta: https://www.vahtiohje.fi. Vahti-ohjeessa 2006 ongelmat, joiden mukaan nykyään vallitseva tapa hoitaa käyttövaltuushallintoa perustuu epämääräisesti määriteltyihin hallintaprosesseihin ja vastuisiin tehtävistä ja niihin liittyvistä järjestelmistä sekä tiedoista.

Ensisijaisesti vastuussa olevat hallintoyksiköt ovat usein käytännössä delegoineet käyttövaltuushallinnon ja jopa niihin liittyvän omistajanvastuunsa tietohallinto-organisaatioille. Käyttövaltuuksien myöntämistä ei valvota riittävän tarkasti ja työntekijälle saatetaan antaa tiedostamatta liian laajat käyttövaltuudet jotka eivät vastaa työntekijän työroolia. Yrityksen palveluksesta poistuneiden tai toisiin tehtäviin siirtyneiden työntekijöiden vanhat käyttövaltuudet saattavat jäädä epämääräiseksi ajaksi voimaan, kun käyttövaltuuksien hallintaprosessit ovat tältä osin puutteelliset ja kun voimassaolevien valtuuksien pätevyyttä ei valvota eikä tietoja päivitetä hallintajärjestelmiin. Todellisuudessa tämä johtaa tilanteeseen, jossa

erilaiset riskit esim. tietosuojassa ja tietoturvassa altistuvat vakaville väärinkäytöksille kasvavat lopulta merkittäviksi. (Valtiovarainministeriö Vahti 2006.)

Identiteetin ja pääsynhallinta lyhennetään kirjaimin IAM, Identity and Access Management, joka tarkoittaa prosessien, datan tai muun teknologian liittämistä yhteen niin että käyttäjillä on yksi sähköinen identiteetti. IAM tarkoittaa identiteetinhallintaa ja lyhennetään kirjaimin IDM, Identity Management ja pääsynhallintaan AM, Access Management. (Itewiki 2017.)

Keskitetty IAM tai IDM on ratkaisu moniin sellaisiin ongelmiin, jotka aiheutuvat keskitetyn käyttövaltuushallinnan puutteesta. Yleinen ongelma organisaatioissa, joilta puuttuu keskitetty IAM tai IDM toteutus, on esimerkiksi se, että eri järjestelmiin on erilaisia käyttöoikeuksien anomistapoja ja ne joudutaan rakentamaan sekä ylläpitämään useilla eri päällekkäisillä käyttäjähallintajärjestelmillä. Samalla työntekijällä voi olla virheellisesti useita identiteettejä, eivätkä henkilöön liittyvät tiedot, kuten tehtävänimike ja yhteystiedot, ole kaikissa järjestelmissä ajan tasalla. Jos käytönvalvontaa ei pystytä systematisoimaan on käyttäjätietojen päivittäminen ja käyttöoikeuksien muuttaminen hidasta ja kustannustehotonta. Tästä on usein käytännössä seurauksena se, että lopettaneiden työntekijöiden käyttöoikeuksia on edelleen voimassa, mikä muodostaa riskin myös tietoturvalle. (Andreasson & Koivisto 2013, 117 – 118.)

Tehottomuutta havaitaan tyypillisesti yrityksen käydessä systemaattisesti läpi järjestelmiä, tai prosesseja, joissa käsitellään tietoa. Tällöin voidaan havaita ongelmallisia kohtia prosessissa, johon tarvitaan tehostamista. Yleinen ongelma on, että samaa tietoa käsitellään useassa eri paikassa, kun saman asian voisi tehdä yhdessä järjestelmässä. Vähentämällä usean tahon tietojen käsittelyn työtä saadaan prosessiin tehostusta koko liiketoiminnalle ja samalla koko yrityksen liiketoiminta ja tietoturva paranevat. (Tietosuoja-opas – 5.)

3.2 Lainsäädäntö ja organisaation toiminta käyttäjähallinnassa

Laki henkilötietojen käsittelystä (Laki 523/1999) mukaan edellyttää henkilötietojen suojaamista, tietojen tarpeellisuus ja virheettömyysvaatimuksen sekä käyttötarkoitussidonnaisuuden vaatimuksen huomioon ottamista. Lisäksi käsittelyssä tulee ottaa huomioon muutkin henkilötietojen käsittelyä koskevat vaatimukset. Kaikkien edellä mainittujen vaatimusten noudattaminen ja noudattamisen valvonta ja siten suojaamisvelvoitteesta huolehtiminen edellyttää, että eri järjestelmien käyttöoikeudet ovat määritelty ja dokumentoitu asianmukaisesti, jotta niiden valvonta pystytään suorittamaan laadukkaasti. Tämä merkitsee

myös sitä, että käyttäjäoikeudet kokonaisuudessaan on määriteltävä myös henkilötasolla. (Valtiovarainministeriö Vahti 2006, 11 – 12.)

Etenkin suuryrityksien on oleellista määritellä ensimmäiseksi se yksikkö, joka vastaa käyttövaltuushallinnasta eli käytännössä asiaan liittyvien kokonaiskonseptin tekeminen. Vastuuyksikkö on usein esimerkiksi yrityksen tietohallinnossa, koska usein tietohallinnolla on keskeinen rooli käyttövaltuuksien hallinnassa ja valvonnassa. Kuitenkin myös prosessien ja eri organisaatioyksiköiden omistajien vastuu käsiteltävien tietojen ajantasaisuudessa, oikeellisuudessa, käytettävyydessä ja eheydessä on suuri. Juridisen rekisterin pitäjän vastuulla on taas henkilötietojen lainmukainen käsittely, sekä vastuu niiden oikeellisuudesta. (Andreasson & Koivisto 2013, 108.)

Käyttöoikeushallinnassa on huomioitava erilaiset keskeiset päätökset ja määräykset, joita voi ilmetä säännöissä, sopimuksissa, tai ohjeissa. Sääntöjä tulee noudattaa organisaation tietoturvapolitiikan mukaisesti. Käyttöoikeushallintaan liittyviä kysymyksiä käsitellään usein myös hyvän johtamisen ja hallintotavan menettelyissä. Lähimpänä yksittäistä työntekijää koskevat velvollisuudet ovat usein salassapitosäännöissä, sekä käyttäjäoikeuksien tilausprosessissa. (Andreasson & Koivisto 2013, 109.)

3.3 Tietosuoja käyttäjähallinnassa

Identiteetti ja käyttövaltuushallinnan ratkaisuissa on hyvä muistaa sen tarkoitus ja sillä suojattavat oikeudelliset intressit. Käyttöoikeus on usein henkilökohtainen. Oikeus liitetään käytännössä tarkoin määritettyyn henkilöön, jolloin on aina kyse henkilötietojen käsittelystä. Käyttövaltuushallinta on laaja prosessi ja sen kaksi merkittävää vaikutusalaa ovat henkilöllisyyden todentaminen ja sen riittävä taso sekä tavoite, jota käyttövaltuushallinnalla pyritään suojaamaan. Kyse on siis tavoitteesta varjella jonkun yksityisyyttä tai joitakin tietoja, jotka eivät ole tai jotka eivät saa olla yleisesti saatavilla. Nämä tavoitteet ovat hyvinkin erilaisia eri yrityksissä ja erilaisia tietoja käsitellessä. (Andreasson & Koivisto 2013, 119.)

Organisaation tulisi panostaa tietosuojaan saman tasoisesti kuin tietoturvaan, sillä esimerkiksi yrityksen talous ja sen kustannustehokkuus ovat rinnakkain seurattavia operatiivisia toimintoja. Tietosuojassa tulisi pyrkiä tilaan, jossa se on luonnollinen osa yrityksen prosesseja ja jota käsitellään arkipäisenä osana tietoturvaa. Yritysten tulisi miettiä tietosuojavastaavan henkilön roolia. Tietosuojavastaava voi olla yrityksen sisäinen tai ulkoinen vastuuhenkilö, joka vastaa prosessien toimivuudesta ja siitä, että kokonaisuus pysyy eheänä.

Yrityksen tietosuojaan vaikuttavat kuitenkin monet muutkin tahot. Loppukäyttäjät, pääkäyttäjät, sekä prosessien omistajat ovat tärkeässä roolissa tietosuoja-asioissa. Siksi on ehdottoman tärkeää, että tietosuojavastaavalla on kyky huolehtia (koordinoida), että nämä henkilöt toimivat työssään oikein. Tietosuojavastaavaksi ihanteellinen henkilö onkin yhteistyökykyinen ja kannustava valmentaja. (Tietosuoja-opas – 9.)

3.4 GDPR – EU tietosuoja-asetus 2018

GDPR, General Data Protection Regulation, eli uusi EU:n laajuinen tietosuoja-asetus astui voimaan keväällä 2016, jonka siirtymäaikalaki perustuu vielä Suomen henkilötietolakiin (Laki 523/1999). Uusi EU-laki astuu voimaan keväällä 2018. Yrityksillä on nyt mahdollisuus miettiä, kuinka uuden tietosuoja-asetuksen mukaiset velvoitteet tulisi hoitaa.

Organisaatioiden ylimmällä johdolla on kokonaisvastuu tässä asiassa. Ylimmän johdon on sitouduttava ja oltava ajan tasalla tietoturva-asioiden kehitystyöstä. Tämä ei tarkoita pelkkää riskianalyysien ja raporttien seuraamista. Kun henkilötietoja käsitellään, on aina syytä varmistaa mitä tietoja henkilörekistereihin on kerätty, sekä millä prosesseilla ja järjestelmillä henkilötietoja käsitellään ja mikä on henkilötietojen tarkoitusperä. Tältä pohjalta on helppoa lähteä laatimaan tarvittavia rekisteriselosteita, sekä kuvata organisaation toimintaa ja ohjeistusta tietosuojan kannalta. Kuvaus pitää tehdä mahdollisimman kattavasti ottaen huomioon poikkeustilanteet ja niihin varautuminen. Jotta johto saadaan sitoutettua, täytyy myös nämä asiat kuvata myös liiketoimen näkökulmasta.

Nykyisestä identiteetinhallinnan prosessista tulee yrityksen tehdä tilanneanalyysi. Mitä teknologioita käsittelyssä käytetään ja verrata sitä uuden tietosuoja-asetusten vaatimuksiin. Tämän työn jälkeen yrityksen tulee toteuttaa riskikartoitus ja rakennettava siltä pohjalta kehityssuunnitelma, jolla korjataan ilmenneet puutteet ja ristiriidat. Lopputuloksena saadaan tieto siitä mihin henkilötietoja kerätään ja mihin tarkoitukseen sen elinkaarimallin kuvion kaksi mukaisesti. (Kuvio 2, 7)

Kuvio 2. Henkilötietojen elinkaari (Valtiovarainministeriö Vahti 1 2016.)

On oleellista selvittää, kenellä on oikeudet käsitellä henkilötietoja ja missä järjestelmissä tietoja päivitetään ja ylläpidetään. Tähän prosessiin tuo huomattavaa etua toimiva IDM eli Identiteetinhallinta ratkaisu, jolloin auditointi ja valvonta ovat yritykselle helppo toteuttaa. Henkilötietojen elinkaaren hallinnan sujuva prosessikuvaus. (Kuvio 2, 7)

Henkilötietojen turvallisessa käsittelyssä avainasioita ovat dokumentointi ja sitä tukevat prosessit. Ohjeistuksiin ja jatkuvaan koulutukseen, sekä selkeisiin toimintamalleihin tulisi myös panostaa. Yritysten tulisi myös kiinnittää huomiota selkeisiin vastuunjakoihin, eli määrittää vastuut selkeästi henkilöille, jotka ovat sitoutuneita annettuihin vastuualueisiin. Hyvin toteutettuna uusi tietosuoja-asetus voi tarjota myös liiketoimintaetuja sekä kustannussäästöjä. (Propentus 2017.)

EU:n tietosuoja-asetus ”pähkinänkuoressa”. Muistilista yrityksien valmistautumiselle uuteen tietosuojalakiin keväällä 2018. Mitä muutoksia laki tuo? Seuraavien kysymysten avulla voidaan selvittää yrityksen tietosuojauksen tarpeet suhteessa uuteen EU:n tietosuoja-asetukseen.

Oman datan tilan selvitys seuraavien kysymysten avulla:

- Mitä henkilötietoja yrityksen tiedostoissa on ja miksi?
- Onko henkilötietojen käsittely tietosuojalain mukaista?
- Kuka on rekisteri ja ylläpitovastuussa tiedoista?

Yrityksen hallussa olevat henkilötiedot tulevat olla sellaisessa muodossa, että niistä ei saa selville ketä henkilötiedot koskevat. Tietokantojen tulee olla myös suojattuja mahdollisten tietomurtojen varalta. Henkilötietojen määrät tulee minimoida ja tietojen tulee olla ajan tasalla. Yrityksen hallussa olevien tietojen tulee olla välttämättömiä yrityksen toiminnalle sekä ylimääräiset ja virheelliset tiedot tulee poistaa. Tietojen oikeellisuutta tulee ylläpitää jatkuvasti.

Tietojärjestelmien toimintavarmuus tulee olla taattua, jotta jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoituus ovat taattuina. Järjestelmän on pystyttävä palauttamaan menetetyt tiedot nopeasti. Henkilötietoihin kohdistuvat tietoturvaloukkaukset on ilmoitettava viranomaisille 72 tunnin kuluessa. Jos tietoturvaloukkauksesta on todennäköisiä haittavaikutuksia asianomaiselle taholle, on rekisterin ylläpitäjän ilmoitettava asiasta

myös rekisteröidylle taholle. Yrityksen tulee tehostaa sisäistä valvontaa ja ottaa käyttöön menettely, joka sopii yrityksen tietojenkäsittelyn turvallisuuden varmistamiseksi.

Tietosuojavastaava on nimitettävä yrityksiin, joiden toimintaan perustuu rekisteröityjen henkilötietojen järjestelmällinen seuranta ja käsittely. Tietosuojavastaavan tehtävä on kehittää, valvoa ja varmistaa tietosuojan toteutuminen, joka voi olla yrityksen oma työntekijä, tai ulkoistettuna palveluna hankittu. Tietosuojavastaavan tehtävä on verrattavissa pääluottamusmiehen tehtävään. Oleellista on, että uuden EU-tietosuojalain vaatimusten mukaisesti yritykselle voidaan asettaa tietosuoja-asetusten laiminlyönnistä huomautus tai sanktio, joka voi olla enimmillään 20 miljoonaa euroa tai 4% yrityksen vuotuisesta liikevaihdosta.

Siirtymäaika EU:n uudelle tietosuoja-asetukselle on 2018 toukokuulle. Yritysten on viimeistään nyt aika luoda toimintamalli, jolla seurataan yrityksen hallussa olevia henkilötietorekistereitä, ja miten niiden käsittely toteutetaan jatkuvan ja turvallisen vaatimusten mukaisesti. Avuksi kannattaa yrityksen koon ja tarpeiden mukaan ottaa ulkoinen asiaan perehtynyt It-toimittaja, joka konsultoi yritystä nykytilan kartoituksessa ja uuden tietosuojalain sovittamista sujuvasti yrityksen arkipäivään. (Emce, 2016.)

4 Tietoturvallisuus

Tietoturvallisuuden perusperiaate on suojata järjestelmiin liittyviä tietoja, palveluja sekä tietoliikennettä niihin kohdistuvilta riskeiltä erilaisissa olosuhteissa teknisillä sekä hallinnollisilla toimenpiteillä. (Vahti 3, 2007.) Tietoturvallisuus on koko organisaation asia, johon liittyy paljon elementtejä, mutta tärkeimmät asiat liittyvät ihmisten toimintaan ja liiketoimintaprosesseihin. Tietoturvallisuuteen on kiinnitettävä erityistä huomiota aina yrityksen prosesseista, henkilöstöhallinnan tai sidosryhmien kanssa työskentelyyn. Tietoturvan laiminlyönti saattaa aiheuttaa ylimääräisiä sanktioita tai mainehaittoja. Toimiva tietoturva on hyvä kilpailutekijä yrityksen liiketoiminnalle. Tietoturva auttaa tekemään myös asioita oikealla tavalla esimerkiksi muutoksenhallinnassa ja käyttäjäroolien hallinnassa. Hyvin hoidettu tietoturva ehkäisee viivästymisiä toimituksissa, toiminnoissa ja ehkäisee muita ongelmia. Hyvä tietoturva antaa myös yrityksestä luotettavan ja vastuullisen kuvan. (Tietosuoja-opas – 5.)

4.1 Tietoturva käyttäjähallinnassa

Jokaisen organisaation tulee huolehtia käyttöoikeuksien hallinnoinnista sekä siihen liittyen määritellä käyttövaltuushallinnan periaatteet. Jokaisen organisaation käytössä olevan tietojärjestelmän, sovelluksen ja henkilörekisterin osalta tulee määritellä myös ne henkilöt, joilla on oikeus käyttää ko. tietojärjestelmää, tieto siitä mitä käyttöoikeudet sisältävät, sekä milloin käyttöoikeus päättyy. Mitä suurempi organisaatio on kyseessä sitä haastavampaa käyttöoikeuksien hallinta yleensä on. Organisaatiossa tulee olla myös määriteltyinä asiaan liittyvät vastuuhenkilöt ketkä myöntävät käyttöoikeudet järjestelmiin, sekä ketkä vastaavat oikeuksien ajan tasalla pidosta. Työ tai palvelussuhteen päätyttyä käyttöoikeudet tulee poistaa välittömästi. Vastuu käyttövaltuushallinnon periaatteiden määrittelystä on johdolla, jonka asiana on nimetä käytännön toiminnasta vastaavat henkilöt ja määritellä heidän tehtävänsä. Vastuiden määrittely tehdään organisaatiokohtaisesti. Käyttöoikeuksien myöntäminen on kuitenkin aina sidoksissa myös palvelussuhteeseen ja siihen liittyvään tehtävänkuvaukseen. (Valtiovarainministeriö Vahti 2006, 11.)

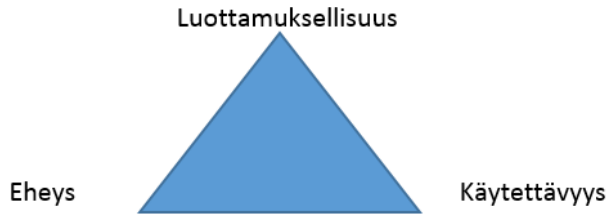
4.2 Tietoturvan käytännön periaatteet

Tietoturvan käytännön perusperiaatteita on kymmenen ja niitä tulee poikkeuksetta hyödyntää toiminnan ja tietojärjestelmien kehittämisessä. Tietoturva käsitetään periaatteessa laajasti: siihen kuuluvat myös keskeiset tietosuojaperiaatteet:

1. Tietoturva ja tietosuoja ovat Suomen lainsäädännön mukaisesti osa organisaation päivittäistä toimintaa ja koskevat koko toimintaa ja henkilöstöä.
2. Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan sitä, että tieto on suojattava monenlaisilta uhilta. Tarkoituksena on varmistaa liiketoiminnan jatkuvuus, minimoida toiminnalliset riskit sekä maksimoida investoinneista ja liiketoiminnasta saatava tuotto.
3. Tietoturvaan liittyvät ongelmat tulee mieluummin ehkäistä ennalta kuin hoitaa jälkikäteen.
4. Tietoturva – ja tietosuoja-asiat pitää huomioida laajasti: ne eivät liity vain tietotekniikkaan.
5. Paperiset asiakirjat, sähköiset tietovarannot, tietojärjestelmät, tietotekniset laitteet, tietoverkot ja niihin liittyvät palvelut on pidettävä asianmukaisesti suojattuina sekä normaali – että poikkeustiloissa.
6. Tietoturvallisuuden saavuttamiseksi pitää toteuttaa sopivia turvajärjestelmiä, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto – ja laitteistotoiminnoista.
7. On varmistettava, että luottamukselliset, arkaluontoiset ja muut salassa pidettävät tiedot kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla ne on saatu.
8. Henkilöstön perehdytys tietoturvaohjeisiin
9. Tietoturvan ohjaus, valvonta ja seuranta pitää organisoida.
10. Tietoturvan laatua tulee valvoa ja kehittää. (Andreasson & Koivisto 2013, 29 – 30.)

4.3 Tietoturvan perustavoitteet

”Tietoturvallisuuden kulmakivet” -kuviossa on esitetty näkemys tärkeimmistä tietoturvan osa-alueista yrityksille. (Kuvio 3, 11)



Kuvio 3. Tietoturvallisuuden kulmakivet, piirretty kuvio. (Miikka Allén, 2017)

Kuvion kolme mukaisesti (Kuvio 3, 11) Vahti-ohje ohjeistaa yrityksen tietoturvan toteuttamista seuraavasti: ”yrityksen tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.” (Valtiovarainministeriö Vahti 2007, 13.)

Vahti 2008 määrittelyn mukaan luottamuksellisuus eli Confidentiality tavoite on:

1) Vaatimusten mukainen tietojen luottamuksellisuuden säilyvyys sekä tietoliikenteeseen ja tietojenkäsittelyyn kohdistuvien oikeuksien toteutuminen.
2) Luottamuksellisuuden tärkeyden ylläpitäminen. (Valtiovarainministeriö Vahti 2008.)

Eheyden eli Integrity tavoitteet:

1) Varmistaa tietojen ja tietojärjestelmien yhteensopivuus, kokonaisvaltaisuus, sekä ajan tasalla olevan tiedon saaminen.
3) Ominaisuus varmistaa, että muutetut tiedot ovat jäljitettävissä tai että niitä ei ole muutettu ilman valtuutusta. (Valtiovarainministeriö Vahti 2008.)

Käytettävyys eli Availability voidaan määritellä seuraavasti: ominaisuus, että järjestelmä, tai palvelu on siihen oikeutetulla taholla saatavissa. Edellä mainitut tiedon suojauksen määritteet ovat saaneet nimensä englanninkielisten alkukirjaimien mukaan CIA eli Confidentiality, Integrity, Availability. (Valtiovarainministeriö Vahti 2008.)

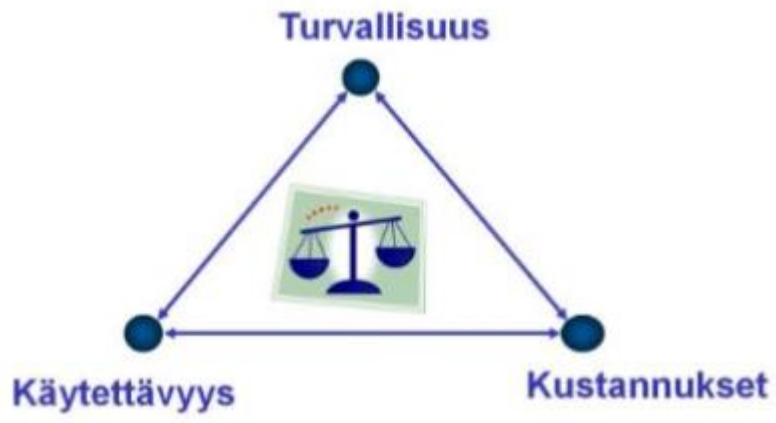
Luottamuksella on tarkoitus turvata tietojärjestelmässä olevat tiedot ja varmistaa että tietoihin pääsevät käsiksi vain niihin valtuutetut tahot. Eheys saavutetaan kun tietojärjestelmän sisältö ei ole ristiriitainen eikä sisällä virheitä. Nopea tietojen saatavuus ja niiden oikeellisuus merkitsevät tietoturvassa hyvää käytettävyyttä. Luottamuksella on tarkoitus turvata tiedon suojaaminen järjestelmissä sen luvattomalta tai vahingoittavalta käytöltä. Luottamuksen tarkoitus on myös turvata tietojärjestelmien tiedot ja laitteet tunnuksilla ja salasanoilla. Salauksen avulla voidaan mahdollistaa parempi luottamus tietojen säilymisessä. Tietojärjestelmässä olevien tietojen eheydestä on aina vastuussa tiedon tuottaja vastuullisella ja ammattitaitoisella toiminnallaan. (Valtiovarainministeriö Vahti 82008.)

Tietojen eheyttä voidaan turvata myös rajoittamalla järjestelmän käyttöoikeuksia sekä suorittamalla säännöllisiä järjestelmän eheystarkastuksia. Hyviin käyttövaltuushallinnan

periaatteisiin kuuluu, että järjestelmiin myönnetään vain tarvittavat käyttöoikeudet. Esimerkiksi kirjoitusoikeudet tulee myöntää vain jos käyttäjän työtehtävät sitä edellyttävät. Eheystarkastukseen voi liittyä esimerkiksi käyttövaltuuksien ja henkilötietojen tarkastaminen. Eheyteen läheisesti liittyvä käsite on myös laatu. Laadun varmistaminen kannattaa jo tehdä huolellisesti määrittelyvaiheessa, koska jälkikäteen laadun parantaminen on erittäin työlästä ja hankalaa. Tiedon eheyden varmistamisessa tulee myös noudattaa samaa toimintamallia. (Valtiovarainministeriö Vahti 2008.)

Käytettävyyttä voidaan parantaa rinnakkaisilla järjestelmillä sekä tehostamalla tietoliikenteen ja järjestelmien suorituskykyä. Myös varmuuskopiointi tulee ottaa huomioon käytettävyyden turvaamisessa. Taloudelliset esteet voivat heikentää käytettävyyden saavuttamista. Rahalla on mahdollista hankkia tehokkaat ja käyttövarmat ratkaisut. Käytettävyyttä voi myös heikentää väärillä tietoturvaratkaisuilla, jotka voivat lisätä kustannuksia. (Turvatieto 2013.)

Edellä kuvatut toiminnot on havainnollistettu kuviossa neljä (Kuvio 4, 13).



Kuvio 4. Turvallisuus, käytettävyys ja kustannukset (Titta Ahlberg, Haaga-Helia)

4.4 Käyttäjä ja työroolit

Työrooli on käyttäjäryhmä, jossa on yksi tai useampia jäseniä. Henkilöllä voi olla yksi tai useampia työrooleja riippuen mihin henkilö tarvitsee toimintavaltuuksia. Työrooleja ei voida eikä pidä kytkeä mekaanisesti henkilöiden työnimikkeisiin tai organisaatiotasoihin. Rooleihin voi liittyä myös sääntöjä, jotka sitovat roolin vain tiettyihin tilanteisiin. Käyttäjiä ei

ole siis järkevä tarkastella yksilötasolla, vaan tulee löytää käyttäjäryhmät tai työroolit, joiden jäsenillä on saman tyyppiset työtehtävät. Näin ollen heillä on samanlaiset tietotarpeet ja toimintavaltuudet, joita kutsutaan työrooliksi. (Valtiovarainministeriö Vahti 2006, 19.)

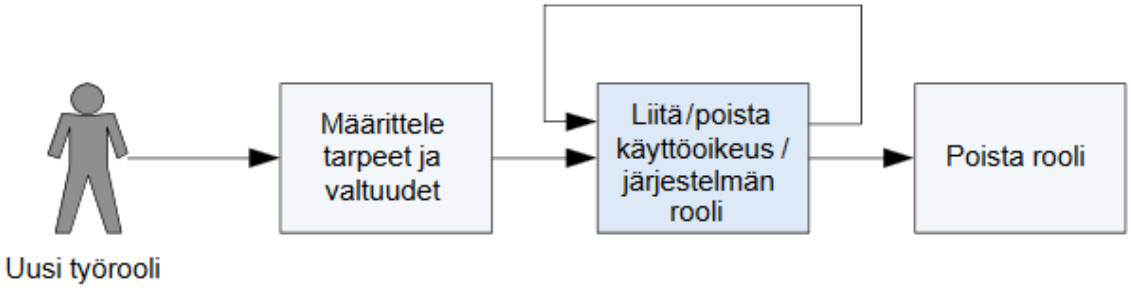
Käyttövaltuuksia määriteltäessä, kun työrooleja kytketään järjestelmän rooleihin, on vastuullista, että työ tehdään kerralla hyvin ja dokumentoidaan käyttäjäroolimatriisiin. (Kuvio 5, 14.) Tämä helpottaa tilanteita, kun jonkun työroolin sisältö muuttuu, tai kun on tarve perustaa uusi työrooli. Vastuullinen käyttäjähallinnasta vastaava henkilö, tai pääkäyttäjä linkittää käyttäjäroolit, tai ylläpidetyt käyttäjäroolit työrooleihin. Työroolille voidaan myöntää useampi käyttäjärooli tarpeen mukaan. Tietoja ylläpidetään matriisissa.

Ohjelmisto- Rooli oikeudet matriisi (oikeudet rooleittain)					
Versio x.x Päivitetty pp.kk.vvvv		Rooli 1	Rooli2	Rooli 3	
ohjelmisto 1		tunnukset ja oikeudet		tunnukset ja oikeudet	
ohjelmisto 2			tunnukset ja oikeudet		
Ohjelmisto 3		tunnukset ja oikeudet			

Kuvio 5. Käyttäjäroolimatriisi esimerkki (Kuntasektori 2013, 14)

Yksittäiselle työntekijälle tehtävät muutokset käyttöoikeuksissa ei aiheuta normaalisti toimenpiteitä käyttövaltuuksien hallinnassa. Työntekijälle tehdään yleensä vain työroolin päivitys. Käytännössä, lisätään tarvittava työrooli, tai poistetaan työrooli, jota henkilö ei tarvitse. Suurissa yrityksissä työrooleja on niin paljon, että ylläpidosta tulee helposti liian raskasta ja aikaa vievää. Jos yrityksellä on käytössä kattava IDM palvelu, niin roolimatriiseja ei välttämättä tarvita.

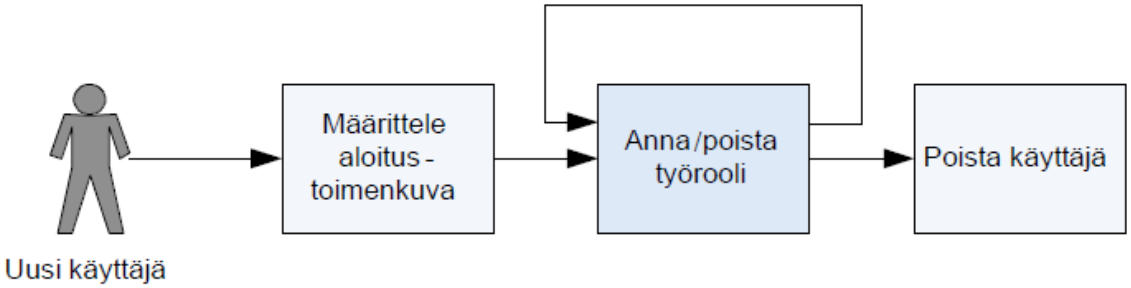
Alla oleva kuva (Kuvio 6, 15) havainnollistaa työntekijän ja työroolien ja niihin liittyvien hallinnoinnin elinkaaria. Edellä kuvattu tapa ylläpitää ja kuvata työrooleja ja niiden sisältöä käyttäjäroolimatriisissa sopii paremmin pieniin toimintaympäristöihin.



Kuvio 6. Työroolin elinkaaren hallinta (Valtiovarainministeriö Vahti 2006)

4.5 Käyttövaltuuksien hallinta ja valvonta

Hyvin hallitussa käyttövaltuushallinnassa käyttövaltuuksien hallinta -ja valvonta prosessit ovat jatkuvan huomion alla. Valvonnassa pidetään huolta, että käyttövaltuushallinnan järjestelmät ja olemassa olevat käyttäjätilit ovat ajan tasalla. (Kuvio 7, 15.)



Kuvio 7. työroolien ja käyttöoikeuksien elinkaari (Valtiovarainministeriö Vahti, 2006)

Valvonnat toteutetaan säännöllisesti käyttäen erilaisia raportoinnin välineitä. Valvonta järjestetään ao. tietojen vastuullisten omistajien toimesta, eli käyttöoikeudet ja työroolit omistavan organisaation toimesta. Säännöllisillä tarkastuksilla seurataan käyttövaltuushallinnassa- ja tiedoissa tapahtuneita muutoksia. Valvonnassa, tai tarkastuksissa havaittuihin epäkohtiin tulee puuttua välittömästi aloittamalla korjaavat toimenpiteet.

Hallintajärjestelmästä tulee saada seuraavat raportit:

- Käyttäjistä ja työrooleista
- Työrooleista ja niihin yhdistetyistä käyttövaltuutuksista
- Käyttäjistä ja heidän järjestelmien käyttövaltuuksistaan
- Käyttäjistä joilla tietynlainen työrooli
- Käyttäjistä joilla tietyn kohteen käyttövaltuus. (Valtiovarainministeriö Vahti 2006, 21.)

Säännölliset vuosittaiset katselmoinnit:

- Onko järjestelmissä käyttäjiä, jotka eivät enää ole yrityksen palveluksessa
- Onko järjestelmissä työrooleja jotka eivät ole enää käytössä
- Onko järjestelmissä kohteita tai käyttöoikeuksia jotka eivät ole enää käytössä
- Onko käyttäjiä joilla vaarallisia työrooli ja käyttövaltuusyhdistelmiä
- Toimivatko hallinnointiprosessit sovitulla tavalla. (Valtiovarainministeriö Vahti 2006, 21.)

5 Identiteetin ja käyttövaltuuksien hallinta

Identiteetin hallinta ja pääsynhallinta ovat tänä päivänä suosittuja teemoja alan seminaareissa. Aiheen käsitteet eivät ole vielä vakiintuneet, vaan englanninkielisistä termeistä on useita eri käännöksiä. Myös englanninkielisessä alan kirjallisuudessa käytetään erilaisia termejä ja lyhenteitä kuvaamaan tätä käyttövaltuushallintaan liittyvää toimintaa. Näistä termeistä yleisimpiä ovat Identity Management (lyhennettynä IM tai IDM) sekä Identity and Access Management (IAM). Etenkään termi Identity Management ei ole täysin vakiintunut. Osassa lähteissä se määritellään henkilöiden identiteetin hallinnaksi, osassa taas pääsynhallinnaksi.

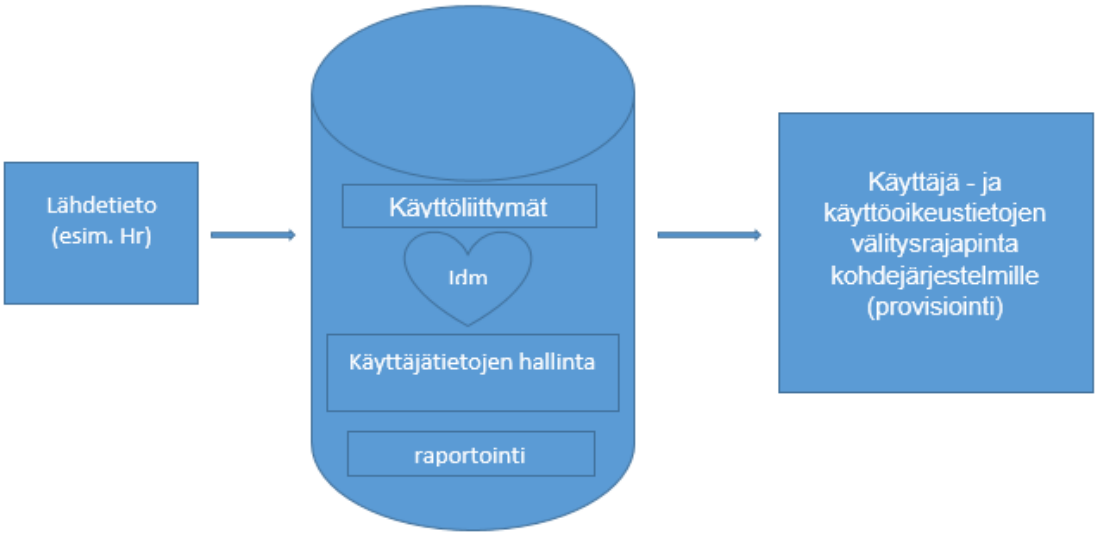
Käyttövaltuushallinnon periaatteet ja hyvät käytännöt -ohjeessa kuvataan selkeästi sitä, mikä käyttäjäidentiteettien ja käyttövaltuuksien hallintajärjestelmä oikeastaan on ja mistä osa-alueista se koostuu. (Kuvio 8, 17.) Tiivistetysti hallintajärjestelmän ytimen muodostaa keskitetty tietovarasto käyttäjistä ja käyttövaltuuksista. Sitä päivittää provisiointijärjestelmä, joka huolehtii siitä, että esimerkiksi uusien käyttäjien, tai muuttuneiden käyttäjäroolien tiedot siirtyvät hallintajärjestelmään ajantasaisesti ja automaattisesti. (Andreasson & Koivisto 2013, 116 – 117.)

Kuvio 8. IDM arkkitehtuuri Yrityksen ympäristöstöstä piirretty. (Miikka Allén 2017)

Tyypillisesti identiteetinhallintaan liittyvät tilanteet liittyvät käyttäjien tunnistamiseen ja käyttäjäoikeuksien hallintaan, Henkilöstöhallinnon-tietojen prosessoitumiseen eri kohdejärjestelmiin, sekä käyttäjän elinkaaren hallintaan esimerkiksi työsuhteen päättyessä, tai työroolin muuttuessa. Monissa organisaatioissa on vielä käyttäjätietojen käsittely hajautettu, joka tarkoittaa vuositasolla suuria kustannuksia, virheiden korjauksia sekä ylimääräisiä työtunteja prosessissa. (Kpmg 2017.)

Hallintajärjestelmän muodostava kuvion yhdeksän mukaisesti: (Kuvio 9, 18.)

- Automaattisen luvitusprosessin eli käyttövaltuuksien haku, hyväksymis- ja luontiprosessin toteuttava osajärjestelmä, johon on liittymät käyttäjätietoja tuottavista lähdetietojärjestelmistä ja jota palvelujärjestelmien käyttäjät ja käyttövaltuuksien hyväksyjät itsepalveluna käyttävät.
- Keskitetty käyttäjä ja käyttövaltuustietovarasto
- Automaattinen käyttövaltuustietojen provisiointijärjestelmä
- Jäljitettävyys – ja raportointitoiminnot. (Valtiovarainministeriö Vahti, 2007, 24.)



Kuvio 9. IDM arkkitehtuurin toiminnalliset osat Yrityksen ympäristöstä piirretty. (Miikka Allén 2017)

Käyttöoikeushallintajärjestelmien tarkoituksena on luonnollisesti yhtenäistää ja selkeyttää tunnuksiin liittyviä toimenpiteitä ja tietoja. Järjestelmillä välitetään esimerkiksi työntekijöiden yhteystietoja, työsuhteen voimassaolotietoja, uusien käyttäjien käyttöoikeushakemuksia sekä käyttöoikeusmuutoksia. Käyttöoikeushallintajärjestelmät tarvitsevat toimiakseen myös muiden järjestelmien apua. Henkilön tullessa työsuhteeseen isoon organisaatioon henkilön työsuhde tulee luoda henkilöstöhallinnan järjestelmään ennen työsuhteen alkua tai heti työsuhteen alkaessa. Yleensä käyttöoikeushallintajärjestelmä saa juuri henkilöstöhallinnon järjestelmästä uuden henkilön tiedot. (Andreasson & Koivisto 2013, 120.)

Keskitetty käyttövaltuushallinta on myös kustannustehokasta. Automatisoimalla käyttövaltuushallinnan tuloksena on merkittäviä säästöjä. Keskitetty käyttövaltuushallinta nopeuttaa luvitusprosesseja huomattavasti ja myös vähentää merkittävästi esimiesten, Helpdeskin ja sovellusvastuuhenkilöiden työmäärää. Tuloksena on myös parempi organisaation tietoturva ja yhtenäisempi ja sujuvampi prosessimalli. (Kuntasektori 2013, 6 – 7.)

6 Käyttövaltuustietojen provisiointi kohdejärjestelmiin

IDM-hallintajärjestelmän provisiointi osa huolehtii uusien ja muuttuneiden käyttäjä- ja käyttövaltuustietojen automaattisesta siirrosta eli provisioinnista kohdejärjestelmiin toisin sanoen yrityksen tai organisaation käytössä oleviin järjestelmiin. Hallintajärjestelmän luvitusprosessien läpi kulkeneet käyttövaltuustapahtumat, uudet käyttäjät, roolit, uudet käyttövaltuudet, käyttövaltuuksien poistot, työsuhteen kesto ym. siirretään automaattisesti kohdejärjestelmien dataksi heti, kun ne ovat syntyneet tai ne ovat ajastettu. Valvonnan kannalta on tietoa siirrettävä myös toiseen suuntaan eli tietojärjestelmästä käyttövaltuuskantaan. Vertaamalla käyttövaltuuskannan ja tietojärjestelmissä olevien valtuustietojen tilannetta, voidaan havaita nopeasti, että yritykset antavat käyttöoikeuksia ohi virallisen prosessin. Tämä tarkoittaa myös sitä, että valtuustietojen provisioinnissa tapahtuu useimmiten teknisiä virheitä eli tiedot jäävät ns. liittymärajapintoihin virheellisinä. (Valtiovarainministeriö Vahti 2006, 26).

Työntekijöille myönnetyt käyttöoikeudet provisioidaan kohdejärjestelmiin manuaalisesti tai automaattisesti IDM:n käyttöliittymän kautta. Automaattisella toiminnalla järjestelmä perustaa tarvittavat oikeudet. Manuaalisella toiminnalla valtuutettu käyttäjä tilaa tai muuttaa työntekijän tarvittavat käyttäjäoikeudet ja työroolit. Identiteetinhallintajärjestelmään voidaan nähdä, millaisia käyttäjäoikeuksia kullakin työntekijällä on hallussa ja kuinka kauan oikeudet ovat voimassa. (Kuntasektori 2013, 55.)

Provisioinnin toiminta yksinkertaistettuna. Uusi työntekijä on palkattu yritykseen. Henkilöstöhallinto lisää tarvittavat tiedot HR-järjestelmäänsä, joka on prosessoitu viemään kaikkien työntekijöiden tiedot järjestelmän tiedostoon päivittäin. Provisiontijärjestelmä valvoo muutoksia mitä tapahtuu tiedostossa ja löytää tiedostosta rivin, jossa on uutta työntekijää koskevat tiedot. Tyypillisesti provisiointijärjestelmällä on joukko sääntöjä ja komentosarjoja, joita käytetään tietojen käsittelyssä. Sääntö voi esimerkiksi ottaa kentän HR-tietueesta ja käyttää sitä selvittämään mitä liiketoiminnallisia rooleja käyttäjällä on. Järjestelmä voidaan myös säätää antamaan käyttöoikeuksia automaattisesti sellaisiin järjestelmiin mihin käyttöoikeuksien myöntämiselle ei tarvita erillisiä valtuutuksia esim. sähköpostin ja toimialuetunnuksen (AD). Tämä logiikka on erilainen jokaisessa organisaatiossa. Provisiointijärjestelmät ovat suunniteltu tehokkaasti muokattaviksi.

Seuraavaksi kun provisiointijärjestelmä on määrittänyt, millainen uusi työntekijän rooli on ja mitä käyttöoikeuksia hänelle on tilattu alkaa tietojen siirtäminen kohdejärjestelmiin. Tämä tapahtuu liittimien (Connectors) avulla, jotka keskustelevat kohdejärjestelmien

kanssa. Liittimet tietävät kuinka lukea, luoda, muokata ja poistaa käyttäjäoikeuksia kohdejärjestelmistä. Näin provisiointijärjestelmä kykenee luoda automaattisesti kaikki käyttäjätilit mitä uusi työntekijä tarvitsee automaattisesti muutamassa sekunnissa.

Liittimet keskustelevat kohdejärjestelmien kanssa käyttämällä kohdejärjestelmien käyttämää protokollaa. Siksi se kommunikoi esim. AD:n kanssa käyttäen ADSI-liittymää, tai muokkaa tietokantaa käyttäen SQL:n avulla. SOAP-protokolla toimii verkkopalveluiden kanssa kommunikoimiseen ja REST:lla taas kommunikoidaan pilvipalvelujen kanssa. Tämä tarkoittaa sitä, että provisiointijärjestelmä on mukautuva. Kohdejärjestelmiin ei tarvitse tehdä muutoksia. Tämä on ratkaiseva ominaisuus provisiointijärjestelmissä, joka tekee niistä yksinkertaisia ja käytännöllisiä työkaluja. On helpompi sopeuttaa yksinkertaisia liittimiä toimimaan kohdejärjestelmien kanssa, kuin alkaa muokata kymmeniä tietojärjestelmiä. (Identity provisioning for dummies 2016.)

7 Käyttöoikeuksien tilausprosessin kehittäminen

Opinnäytetyön aihe on osa yrityksessä vuonna 2013 käyttöön otettua identiteetinhallinnan järjestelmää, joka on osittain automatisoitu. Tämän järjestelmän toimintamalli on kuvattuna kuviossa 10 (Kuvio 10, 23.) Edellisten vuosien aikana opinnäytetyöntekijän oma ammattitaito on kehittynyt järjestelmän toimintaan ja tunnistamaan sen puutteita.

7.1 Kehittämisprojektin toteuttaminen

Opinnäytetyöntekijän vahvan työelämäosaamisen pohjalta syntyi myös malli kehitystyölle, joka aloitettiin elokuussa 2017 osana opinnäytetyön toiminnallista tutkimusta.

Opinnäytetyössä on analysoitu identiteetinhallintaprosessin nykytilaa ja identiteetin ja pääsynhallinnan tarjoamia mahdollisuuksia toteuttaa ne automatisoidusti suoraan järjestelmästä siten, että järjestelmä tuottaa ajantasaiset raportit sekä esimiestasolle että henkilöstöhallinnon käyttöön. Tämän pohjalta opinnäytetyöntekijä on laatinut kehityssuunnitelman, joka vastaa nykyisessä prosessissa havaittuihin puutteisiin. Kehityssuunnitelma hyödyntää myös valmistautumista keväällä 2018 voimaan astuvaan EU:n tietosuojalain asettamiin vaatimuksiin sekä parantaa käyttöoikeuksiin liittyvää tietoturvaa.

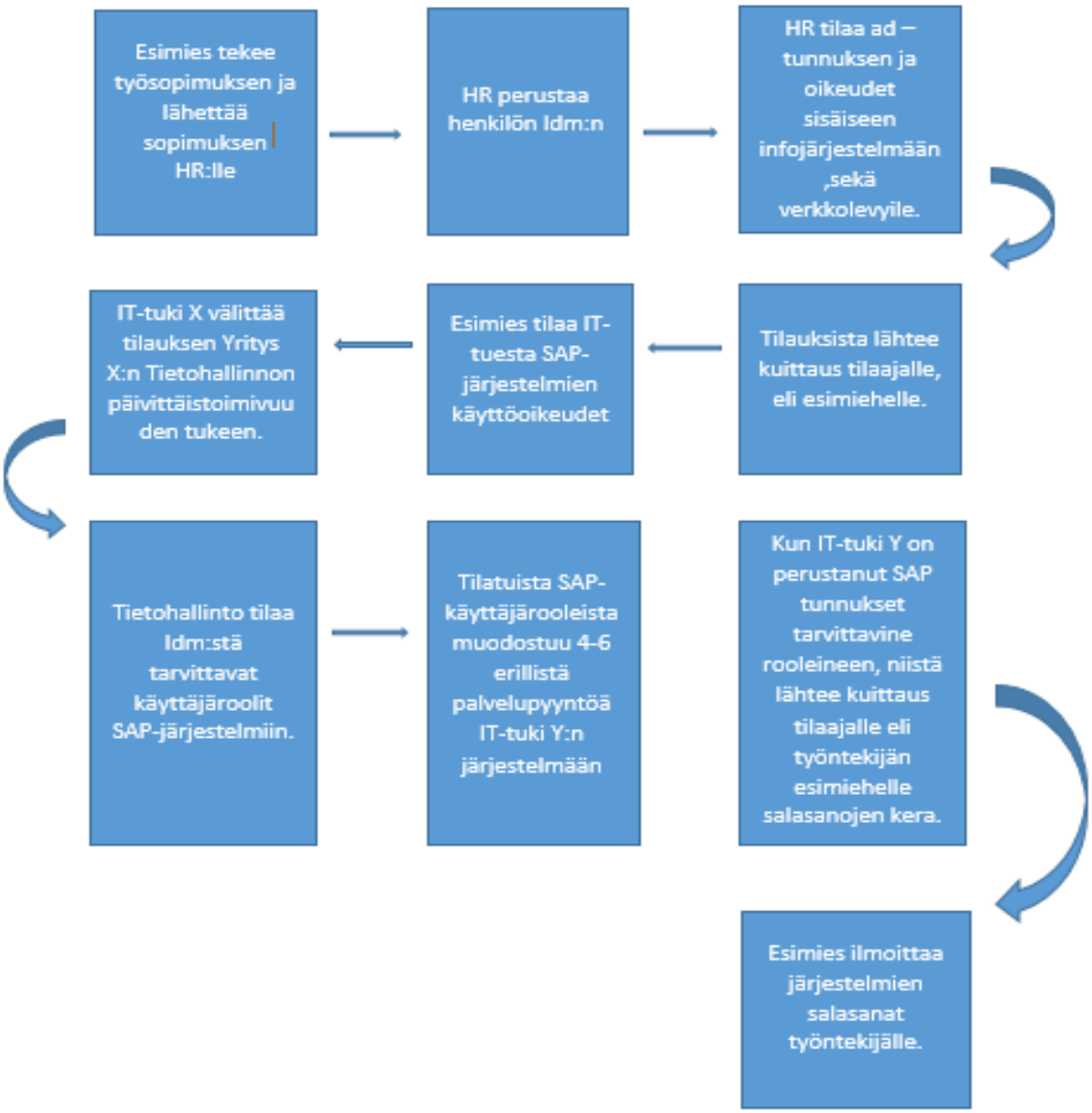
Prosessin nykytilan kuvaukselle ja sen pohjalta opinnäytetyöntekijän laatiman kehityssuunnitelmaan on saanut hyväksyntää ja ammatillista vahvistusta haastattelemalla useita konserniyrityksessä samalla ammatillisella alueella työskenteleviä kollegoita. Opinnäytetyön toiminnallinen tutkimus toteutettiin syyskuussa ja se oli osa kolmen kuukauden pituista opinnäytetyöprojektia. Tutkimuksessa tehtiin kaksi laajaa puhelinhaastattelua haastattelemalla identiteetin ja pääsynhallintaan erikoistuneen yrityksen asiantuntijaa sekä toimitusjohtajaa, jotka vahvistivat opinnäytetyöntekijän ja konserniyrityksen asiantuntijakeskustelujen näkemyksiä siitä, että tässä opinnäytetyössä asiantuntijakeskustelujen ja haastattelujen yhteydessä saadut kommentit tukevat niitä kehittämisideoita, joita opinnäytetyöntekijä on laatinut osaksi identiteetinhallinnan uutta kehityssuunnitelmaa.

Opinnäytetyössä on laadittu kehityssuunnitelma, jossa on tehty edellä mainittujen tietojen analysointi ja niiden perusteella luotu malli, joka on yritykselle kustannustehokkaampi tapa toimia ja hallinnoida käyttöoikeuksien tilausprosessia ja toteuttaa identiteetinhallintaa konserniyrityksessä.

7.2 Konserniyrityksen identiteetin ja käyttöoikeuksien hallinta

Opinnäytetyön tavoitteena on tämän työn tuloksen pohjalta kehittää yrityksen käyttöoikeuksien tilaamisprosessia. Teoriaosuuden pohjalta selvitetään kehitysmahdollisuuksia, joilla mahdollistetaan käyttöoikeuksien tilaamisprosessi mahdollisimman saumattomaksi, sekä kustannustehokkaaksi.

Prosessia hankaloittaa vastuualueiden jakaantuminen ja selkeiden yhtenäisten toiminta-ohjeiden puuttuminen. Tällä hetkellä vastuut ovat jakautuneet yrityksen henkilöstöhallinnolle, tietohallintoyksikölle ja ulkoisille It-toimittajille. Yrityksen tilanne on kuvattu alla olevassa kuviossa käyttöoikeuksien tilaamisprosessin näkökulmasta (Kuvio 10, 23.)



Kuvio 10. Yrityksen käyttöikeuksien tilaamisprosessi piirrettynä. (Miikka Allén, 2017)

Yrityksen käyttöoikeuksien tilaus ja hallintaprosessista tekee haastavaa henkilöstön ja myös toimipisteiden suuri määrä. Henkilöstöä Yrityksen palveluksessa on noin 4000 ja Suomessa noin 80 toimipistettä. Käyttöoikeuksien tilaaminen on tällä hetkellä erittäin pitkä ja hidas prosessi. Asiat valmistuvat eri aikoihin. Esimerkiksi AD-tunnukset toimivat melko pian koska yrityksellä on käytössä näiden tunnusten osalta automaattinen provisiointi IDM-järjestelmässä. Ongelmat kohdistuvat lähinnä SAP-oikeuksien pitkään toimitusaikaan, koska SAP käyttäjäoikeuksilla ei ole automaattiprovisiointia käytössä.

Nykyisessä käyttöoikeuksien tilaamis- ja hallintaprosessissa on havaittuja seuraavanlaisia ongelmia:

- Esimies tilaa SAP-tunnuksia työntekijälle ennen kuin HENKILÖSTÖHALLINTO on ehtinyt perustaa työntekijän IDM:n hallintajärjestelmään. Tästä syntyy palvelupyyntö liian aikaisin ennen kuin HENKILÖSTÖHALLINTO on perustanut uuden työntekijän IDM:n. Tämän takia avoimia palvelupyyntöjä jää odottamaan käsittelyä ja niiden määrä (Liite 4.), sekä tilan seuranta aiheuttaa myös Tietohallinnollle ylimääräistä työtä mm SAP-tunnusten manuaalisen tilaamisen IDM:n kautta. (Liite 2.) Palvelupyynnön elinkaari on myös aivan liian pitkä. Sovittu toimitusaika tunnuksille on neljän työpäivän aikana, joka ei toteudu. Joskus tunnuksien tilausprosessiin saattaa mennä viikkoja.

- Esimies tilaa SAP-oikeuksia sähköpostilla IT-tuki X:n kautta, koska ei ole asiaan suunniteltua järjestelmää, tai lomaketta, joka olisi integroitu Henkilöstöhallinnon järjestelmään. IT-tuki X ei myöskään aina osaa reitittää palvelupyyntöä oikeaan paikkaan. Palvelupyynnön elinkaari pitenee, jos palvelupyyntö poikkeaa väärän paikkaan, missä siihen ei reagoida.

- Yhtenäiset toimintamallit ja ohjeet puuttuvat. Tämä pätee Henkilöstöhallinnon, It-toimittajiin ja Tietohallintoon. Kaikilla näyttää olevan omat toimintamallit prosessissa.

- Päättyneet työsuhteet. Työsuhteen päätösprosessi on hankala, ja se ei toimi aukottomasti. (Liite 3.) Työsuhteen päättämisprosessia ei käytännössä ole. Tieto päättyneestä työsopimuksesta tavoittaa harvoin Henkilöstöhallinnon. Näin ollen IDM:n jää työsuhteen päättäneiden identiteettitiedot ja käyttöoikeudet. Huom. Uusi EU:n tietosuoja-asetus!

- Toimipisteen vaihdoissa tai usealla toimipisteellä työskentelystä ei ole selkeää ohjeistusta esimiehille.

- Esimiesten vaihtuvuus. Esimiestiedot eivät ole IDM:ssä ajantasalla. Työntekijöiden tunnustilausten tiedot ja salasanat menevät väärien henkilöiden s-posteihin.

- SAP-oikeudet poistuvat, ellei järjestelmää käytetä tunnuksilla 90 pv:n aikana. Esim. vanhempainvapaat, pitkät sairauslomat, opintovapaat ym. aiheuttavat hämmennystä oikeuksien puuttumisessa ja johtavat taas pitkään käyttöoikeuksien tilaamisprosessiin. SAP-oikeudet kuitenkin näkyvät IDM:ssä voimassaolevina, joka aiheuttaa tilanteen, että IDM-järjestelmä ei anna tilata uudestaan jo voimassaolevia käyttöoikeuksia. Tämä aiheuttaa manuaalisen SAP tunnuksen luomisen Tietohallinnolle. (Liite 1.)

- Työntekijöiltä saattaa puuttua henkilökohtaiset käyttöoikeudet. On havaittu, että työntekijät tekevät töitä kirjautuneena järjestelmiin muiden henkilöiden käyttäjätunnuksilla. Tämä on järjestelmälisenssien väärinkäyttöä, sekä tietoturvariski.

8 Tulokset

Yrityksen tapauksessa, organisaatiossa, jossa työskentelee n. 4000 työntekijää käyttövaltuudet tulisi sitoa henkilön työsuhdetietoihin ja niissä tapahtuviin muutoksiin. Käytännössä tämä tarkoittaisi sitä, että henkilöstöhallinto eli HR- ja käyttövaltuusprosessit yhdistetään yhdeksi kokonaisuudeksi. HR-järjestelmä tulisi integroida olemassa olevaan identiteetin ja pääsynhallinnan järjestelmään, ja siten liittymän kautta voidaan luoda työntekijöiden tarvitsemat tunnukset ja käyttöoikeudet valittuihin kohdejärjestelmiin automaattisesti. Oikeanlaiset käyttöoikeudet perustuvat HR-järjestelmästä saatuun dataan, jonka perusteella identiteetinhallintajärjestelmä asettaa työntekijöille oikeat käyttäjäroolit. (Itewiki 2017.)
Alla olevassa kuviossa 11 havainnollistettu (Kuvio 11, 26.) prosessin kulku.

Kuvio 11. Käyttöoikeusprosessin kehitysidea piirrettynä. (Miikka Allén 2017)

Järjestelmä tulisi rakentaa niin, että esimies saa tehtyä kaikki toimenpiteet yhdestä paikasta. Myös ohjeistus prosessiin tulee löytyä samasta paikasta missä hallinnoidaan työsuhteita ja käyttöoikeuksia. Ylläpitojärjestelmästä löytyvään ohjeistukseen tulee olla pääsy myös It-toimittajilla sekä kaikilla osapuolilla, jota prosessi koskee. Siksi asianmukainen ohjeistus ja vastuunjako tulee kuvata selkeästi. Järjestelmässä tiedon tulee kulkea molempiin suuntiin. Näin kaikki prosessissa olevat järjestelmät ovat Henkilöstöhallinnon – ja IDM järjestelmien tietojen tasalla.

Työsuhteen päätösprosessi on havaittu ongelmalliseksi. Järjestelmiin on jäänyt paljon työsuhteen päättäneiden henkilöiden tietoja ja käyttäjäoikeuksia. Työsuhteen päätösprosessi

on äärimmäisen tärkeä osa prosessia viitaten keväällä 2018 voimaan astuvaan EU:n uuteen tietosuojalakiin. Esimiehen tulee päättää työsopimus, kun työntekijän työsuhde päättyy, jolloin myös poistopyynnöt käyttöoikeuksiin provisioituvat kohdejärjestelmiin. Jos tämä unohtuu esimieheltä, niin SAP-järjestelmään on automatisoitu ”siivousajo”, joka poistaa käyttöoikeudet järjestelmästä tunnuksilta, joita ei ole käytetty 90:n päivän aikana. Edellä mainitun prosessin jälkeen tapahtumasta tulisi välittyä tieto esimiehelle, joka tarvittaessa päättää työsuhteen. Tässä tilanteessa on erityisen tärkeää, että tieto kulkee molempiin suuntiin järjestelmissä.

Toimipistevaihdoksissa, tai tilanteessa, jossa työntekijä työskentelee useassa toimipisteessä tulisi järjestelmän toimia niin, että uuteen toimipisteeseen käyttöoikeuksia tilattaessa järjestelmä hakee käyttäjän olemassa olevat tiedot järjestelmästä ja kertoo mille toimipisteelle käyttäjällä on jo oikeuksia. Ylläpitojärjestelmässä tulisi olla myös mahdollisuus siirtää käyttöoikeudet toimipisteeltä toiselle, sekä tilata oikeudet uudelle toimipisteelle. Järjestelmä voisi oletusarvoisesti myös tarjota samoja oikeuksia, mitkä työntekijällä on entuudestaan. Järjestelmässä olevien tietojen eheyden varmistamiseksi järjestelmästä tulee olla mahdollisuus tuottaa raportit työntekijöistä ja heidän käyttöoikeuksistaan automaattisesti. Yhtenä toiminnallisuutena tulee olla myös mahdollista tuottaa muistutustoiminto päättyvistä työsuhteista esimiehille ja henkilöstöhallinnolle.

Toimintamalli organisaatiolle, jossa noin 4000 työntekijää. Käyttövaltuudet liitetään henkilön työsuhdetietoihin ja niiden muutoksiin. Tämä tarkoittaa HR-toimintojen ja käyttövaltuusprosessien yhdistämistä yhdeksi kokonaisuudeksi. HR-järjestelmä integroidaan IDM-järjestelmään, joka luo työntekijöille heidän työssään tarvitsemat käyttäjätunnukset ja käyttöoikeudet valittuihin kohdejärjestelmiin automaattisesti. Oikeanlaiset käyttäjäoikeuksien myöntäminen perustuu HR-järjestelmästä saatuun dataan, jonka perusteella IAM-järjestelmä asettaa työntekijälle tilatut roolit. (Itewiki 2017.)

9 Pohdinta

Käyttäjäoikeuksien ja sähköisen identiteetin hallintaprosessi on koettu haastavaksi myös opinnäytetyön kohdeyrityksessä. Keväällä 2018 voimaan astuva uusi EU:n tietosuojalaki antaa ulkoisen vaatimuksen toiminnan kehittämiselle. Opinnäytetyön tavoitteena oli kuvata ja analysoida yrityksen tietosuojan ja tietoturvan parantamismahdollisuuksia sähköisen identiteetin ja käyttäjäoikeuksien osalta. Sähköisen identiteetinhallinnan ja käyttöoikeuksien tilausprosessin toiminnan tehostaminen automatisoimalla järjestelmä tuo myös yritykselle kustannussäästöjä.

Kappaleessa kahdeksan on konserniyrityksen identiteetinhallinta on kuvattu yrityksen tällä hetkellä voimassa oleva prosessi sähköisen identiteetin ja käyttöoikeuksien tilaus- ja hallintaprosessin osalta. Prosessi on koettu monelta osin hankalaksi ja tehottomaksi myös tietosuojan sekä tietoturvallisuuden kannalta. Prosessi aiheuttaa paljon kustannuksia yritykselle sekä manuaalista työtä tietohallinnolle ja henkilöstöhallinnolle. Sovitut ajat käyttöoikeuksien tilaamisessa eivät myöskään toteudu.

Konserniyrityksen identiteetinhallinnan nykytilan pohjalta saatiin aikaan kehitysidea perehtymällä Identiteetin ja pääsynhallinnan ratkaisuihin. Kehitysidea muodostui tutkimalla yrityksen tämän hetkistä tilaa sähköisen identiteetinhallinnan ja käyttöoikeuksien tilausprosessin kannalta.

Opinnäytetyöntekijän oma osaaminen laajeni tämän opinnäytetyön myötä. Uskon että, pystyn hyödyntämään opinnäytetyössäni saamaani oppia myös työelämässä. Toivon myös, että yritykset käyttävät tätä opinnäytetyötä tiiviinä tietopakettina yrityksen tietosuojan ja tietoturvan parantamiseksi identiteettien ja käyttöoikeushallinnan osalta. Tämän opinnäytetyön pohjalta yritys voi saada myös merkittäviä säästöjä ja säästyä tietosuojaan ja tietoturvatarkastuksiin liittyviltä sanktioilta.

Haasteellista opinnäytetyössä oli lähdemateriaalien löytäminen mukaan lukien haastateltavat henkilöt. Aihe on erittäin ajankohtainen ja lopputulos indikoi konserniyritykselle kustannustehokkuutta ja prosessin nopeutumista sekä datan oikeellisuutta verrattuna vanhaan toimintamalliin. Opinnäytetyöntekijä onnistui kuitenkin hyvin kuvaamaan yrityksen käyttöoikeushallinnan nykytilan ja sen vaatimat kehitystarpeet ja jalostamaan siitä edelleen tämän opinnäytetyötutkimuksen tukemana nykyaikainen ja tehokas uusi identiteetinhallinnan malli, joka on sovellettavissa toimialariippumattomasti erikokoisiin yrityksiin. Yrityksen dokumentaatio aiheeseen oli huomattavasti suppeampi mitä ensin oli toivottu.

Haastattelujen avulla on saatu kuitenkin vahvistettua, että opinnäytetyössä kuvatut prosessit olivat yrityksen nykytilan mukaan kuvattu oikein.

Lähteet

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tietosanoma Oy. Helsinki.

Emce 2016. Uusi EU:n tietosuoja-asetus. Luettavissa: https://www.emce.fi/blog/uusi-eun-tietosuoja-asetus-astuu-voimaan-25-5-2018-keta-koskee-mitka-keskeisimmat-muutokset/. Luettu 6.10.2017.

Identiteetinhallinan asiantuntija, puhelinhaastattelu 7.9.2017.

Yrityksen järjestelmäasiantuntija, haastattelu 15.9.2017.

Identity provisioning for dummies 2016 Luettavissa: https://wiki.evolveum.com/display/midPoint/Identity+Provisioning+for+Dummies. Luettu 26.9.2017.

Itewiki It expertise wiki 2017 Luettavissa: https://www.itewiki.fi/opas/kayttajahallinta-iam/#Toteutustapoja-ja-ratkaisumalleja. Luettu 3.10.2017.

Kpmg 2017 Luettavissa: https://home.kpmg.com/fi/fi/home/palvelut/neuvontapalvelut/liikkeenjohdon-konsultointi/digitaalinen-identiteetinhallinta.html. Luettu 15.9.2017.

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri 2013 Luettavissa: http://shop.kunnat.net/download.php?filename=uploads/1747kvh_viitearkkitehtuuri_v1_0.pdf. Luettu 12.9.2017.

Netman 2017 Luettavissa: http://blogi.netman.fi/hubfs/Oppaat/Tietosuoja-opas.pdf. Luettu 10.9.2017.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3-4 painos. Sanoma pro Oy. Helsinki.

Propentus 2017 Luettavissa: https://www.propentus.com/fi/eu-tietosuoja-asetus. Luettu 25.9.2017.

Turvatieto 2013 Luettavissa: https://turvatieto.wordpress.com/2013/05/12/tietoturvallisuuden-peruskasitteita/. Luettu 11.10.2017.

Valtiovarainministeriö Vahti, . 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10229. Luettu 9.8.2017.

Valtiovarainministeriö Vahti, . 2006. Käyttövaltuushallinnon hyvät periaatteet ja käytännöt. Luettavissa: http://www.vm.fi/vm/fi/. Luettu 9.9.2017.

Valtiovaraiministeriö Vahti, .2008. Valtionhallinnon tietoturvasanasto. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229. Luettu 9.10.2017.

Valtiovarainministeriö Vahti, . Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto. Luettavissa: https://www.vahtiohje.fi/web/guest. Luettu 6.9.2017.

Valtiovarainministeriö Vahti, . 2016. Vahti-raportti 1/2016 EU-tietosuojan kokonaisuudistus. Luettavissa: http://vm.fi/documents/10623/2813384/Rousku/a33ac9f4-fb4c-4d68-8e40-c47379fdcc01. Luettu 8.8.2017.

Valtiovarainministeriö Vahti, 2009. Käyttäjähallinta Luettavissa: https://www.vahtiohje.fi/web/guest/kayttajahallinta. Luettu 7.9.2017.

Liitteet

Liite 1. Esimerkki tiketti kohde Yritykseltä

Palvelupyynnön kuvaus:
Meillä on aloittanut osastolla uusi työntekijä Matti Meikäläinen, hänen SAP-tunnukset eivät toimi. SAP-tunnukset tilattu jo kuukausi sitten?

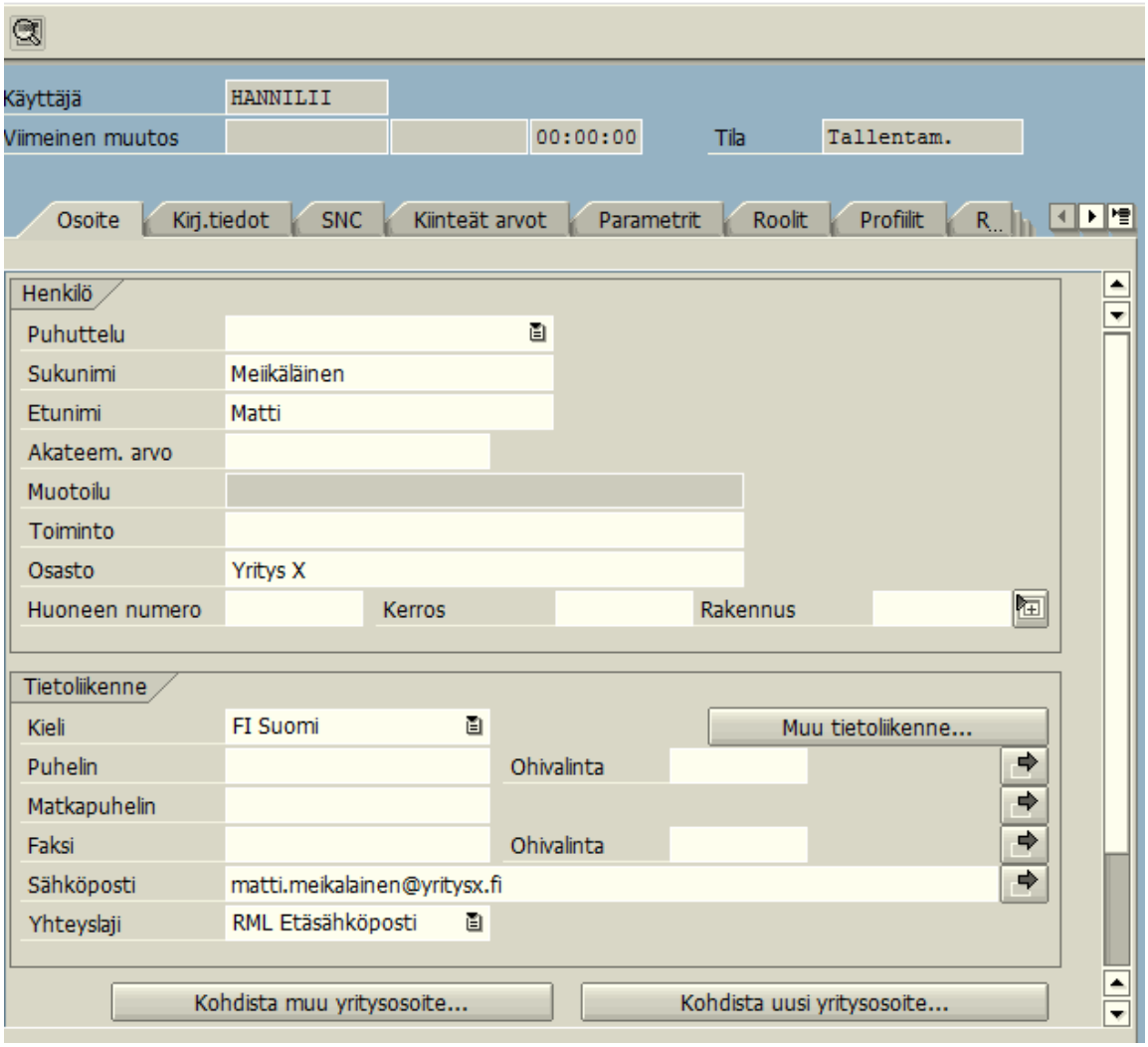
”Tietohallinto huomaa, että toimittajalla paljon jonossa SAP tunnuksia ja toimittaja ei kykene toimittamaan SAP tunnuksia sovitussa ajassa. Tietohallinto tekee tarvittavat SAP tunnukset ja kuittaa SAP tunnuspyynnöt tehdyksi IDM:stä, jolloin työpyynnöt niistä poistuvat myös It-toimittaja Y:n työjonosta.

SAP-tunnusten perustaminen ja siihen liittyvät toimenpiteet ovat aikaa vievää ja työllistää paljon Tietohallintoa. Alla esimerkki miten SAP tunnukset tehdään manuaalisesti järjestelmiin Tietohallinnon toimesta.

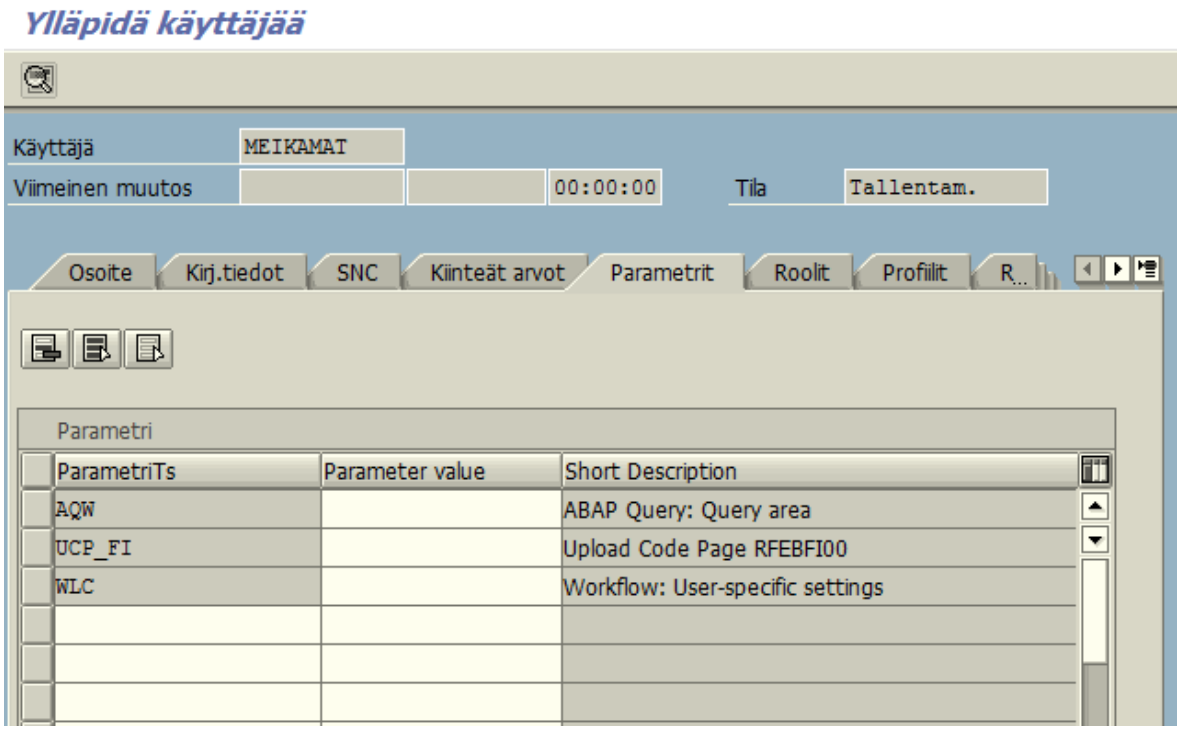
Tunnukset tehdään SAP järjestelmän CUA:ssa (Central User Administration) tapahtumassa SU01

Ensin syötetään käyttäjän tiedot

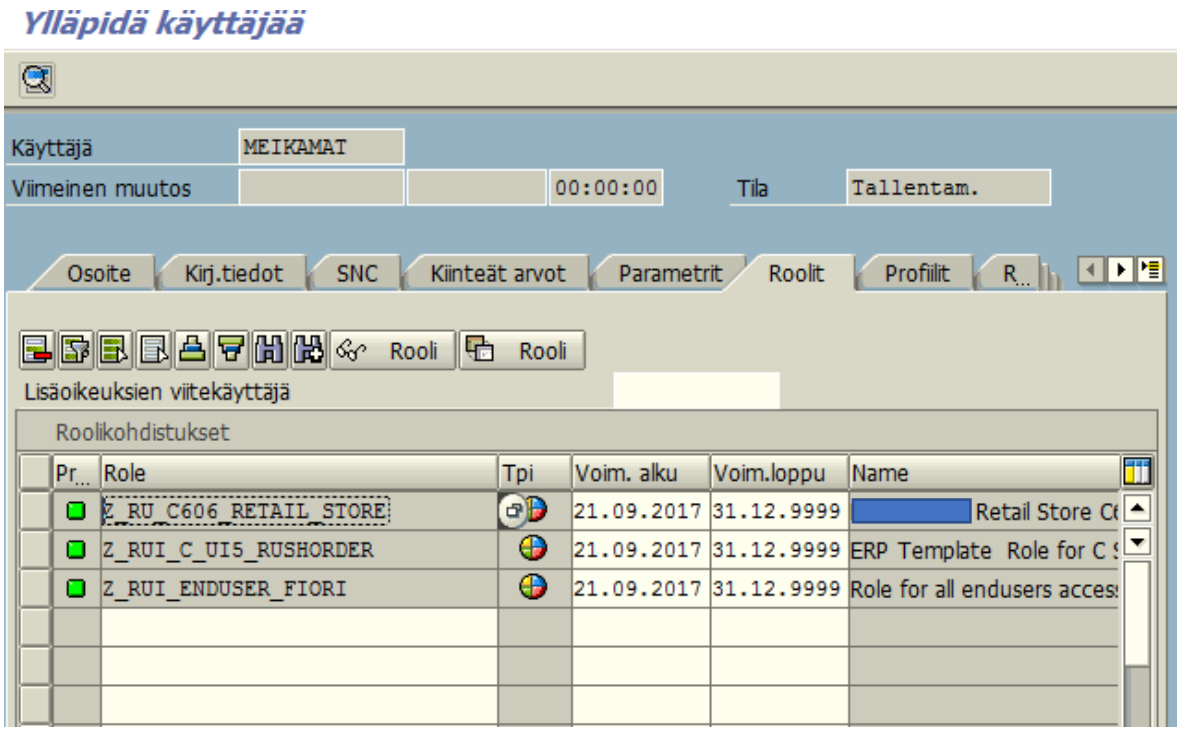
Ylläpidä käyttäjää



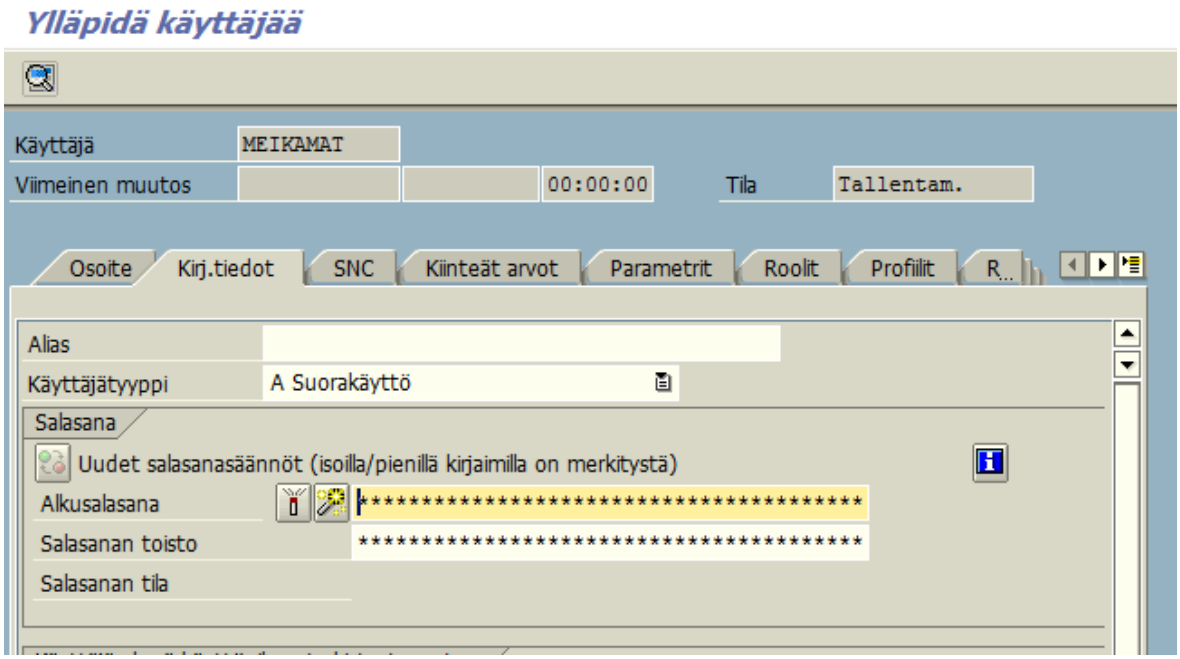
Seuraavaksi ylläpidetään tarvittavat parametrit SAP tunnukselle.



Seuraavaksi käyttäjätunnukselle ylläpidetään esimiehen ilmoittamat ja tilaamat SAP roolit. (työroolit).



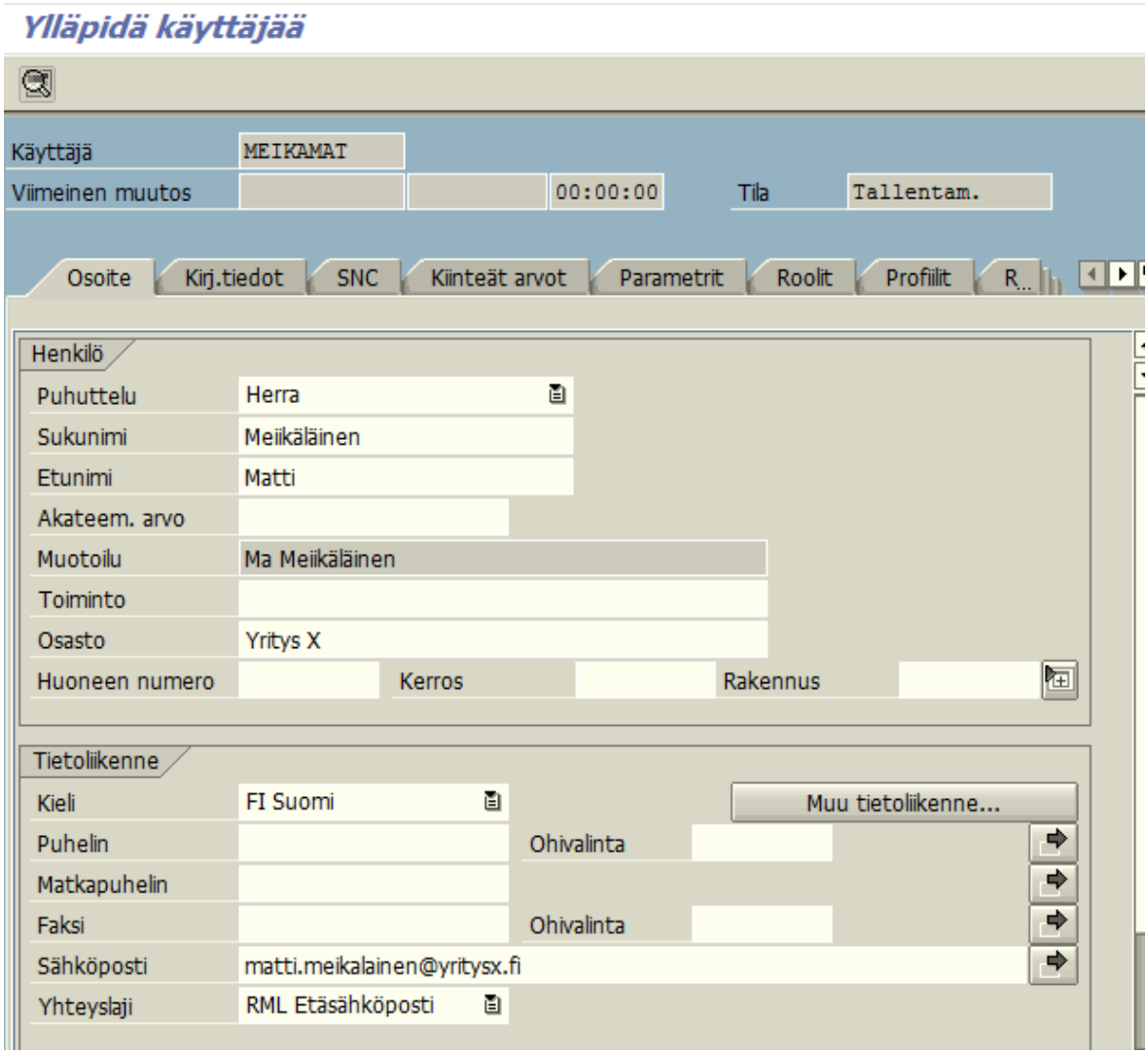
Lopuksi tunnukselle annetaan salasana.



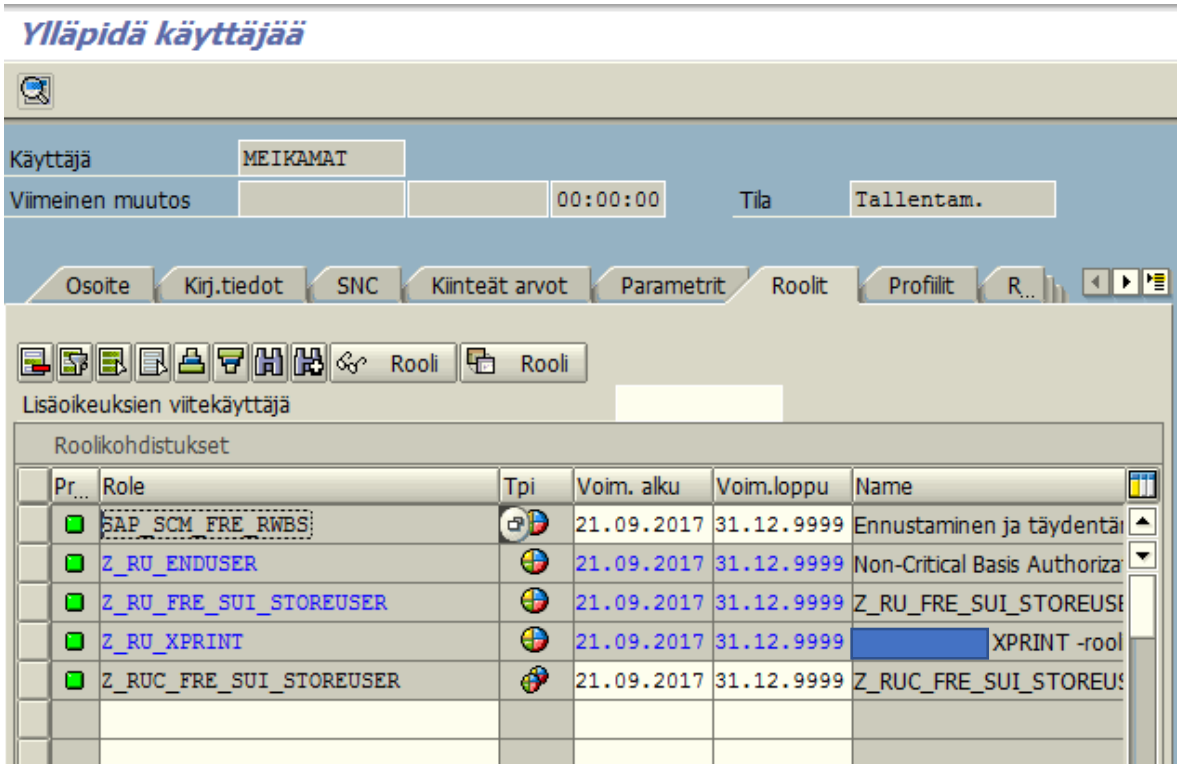
SAP tuotannon tunnus valmis

Yrityksen työntekijöille tehdään aina tunnus myös SAP:n automaattisen täydentämisen järjestelmään. Tunnuksen perustamisessa on hieman eroavaisuuksia verrattuna SAP tuotannon tunnuksen perustamisessa.

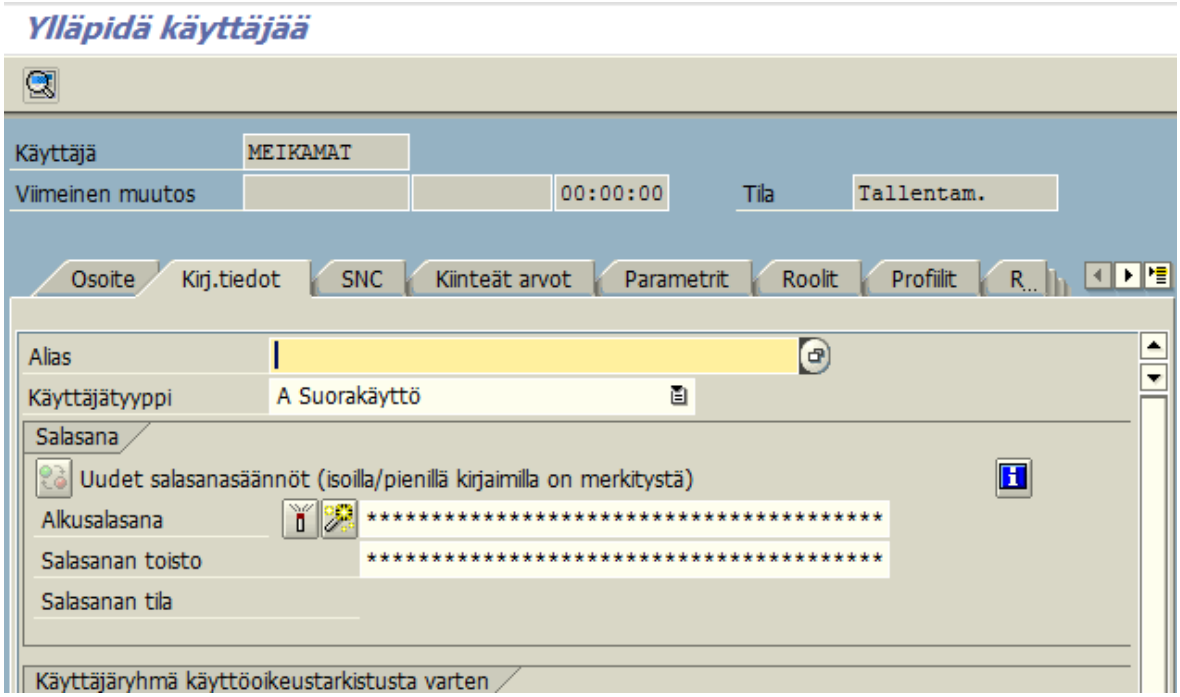
Ensin syötetään käyttäjän tiedot



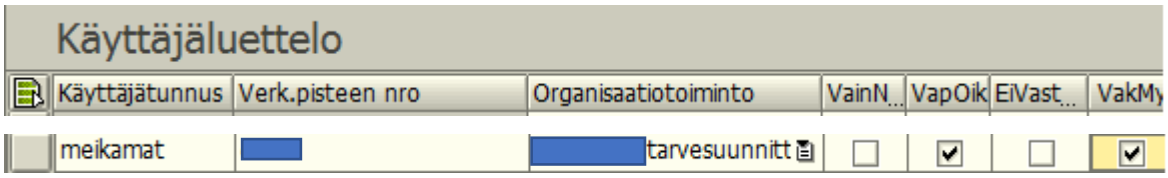
Parametrien ylläpitoa ei tarvita, seuraavaksi ylläpidetään tarvittavat SAP roolit.



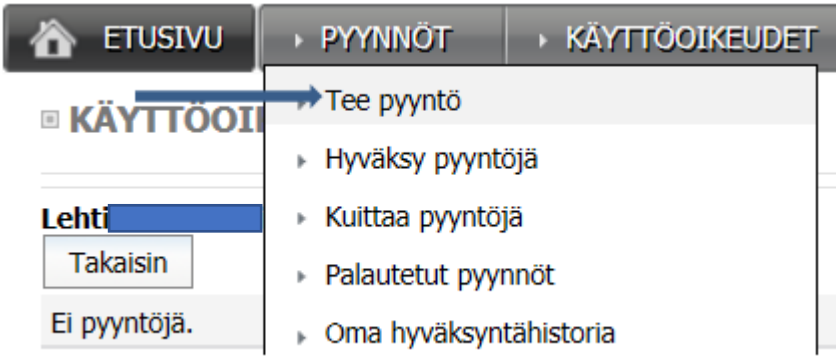
Seuraavaksi annetaan tunnukselle salasana

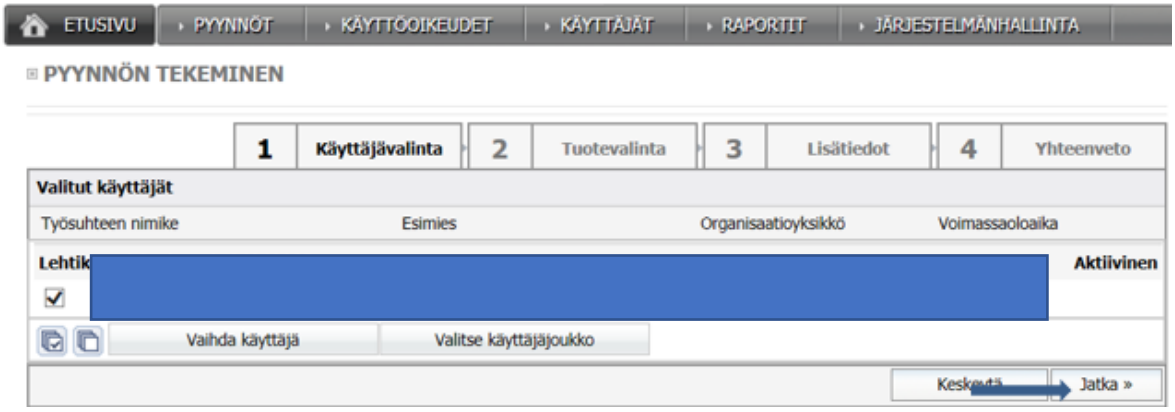


Tunnus pitää lisätä vielä toimipisteen käyttäjäluetteloon, jotta tarvittavat automaattisen täydentämisen oikeudet tulevat voimaan. Tämä osuus tehdään tapahtumassa: /FRE/RWBS/_USER tapahtumassa.


Käyttäjäluettelo
Käyttäjätunnus
Verk.pisteen nro
Organisaatiotoiminto
VainN...
VapOik
EiVast...
VakMy
meikamat
tarvesuunnitt

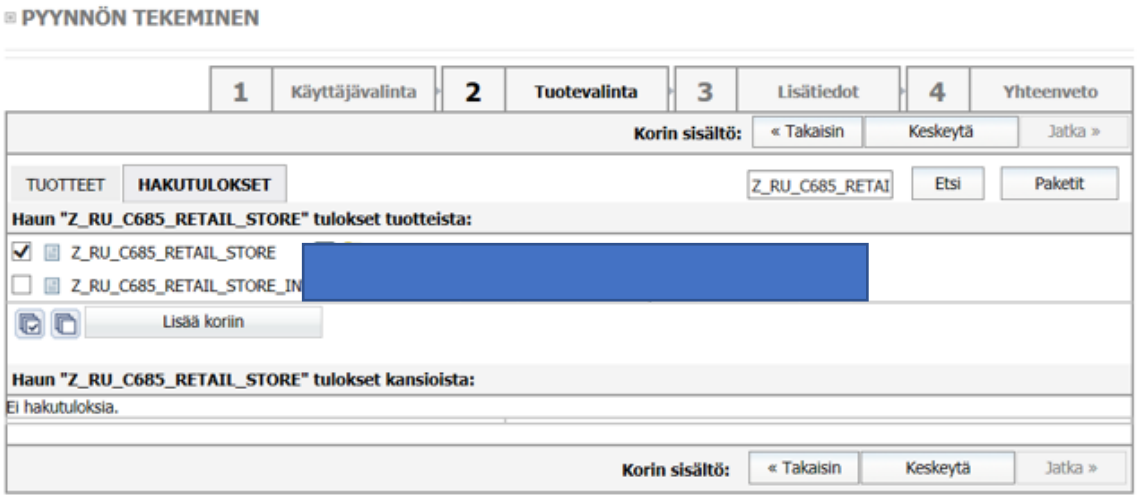
Liite 2. SAP tunnusten manuaalinen tilaaminen IDM-hallintaliittymästä



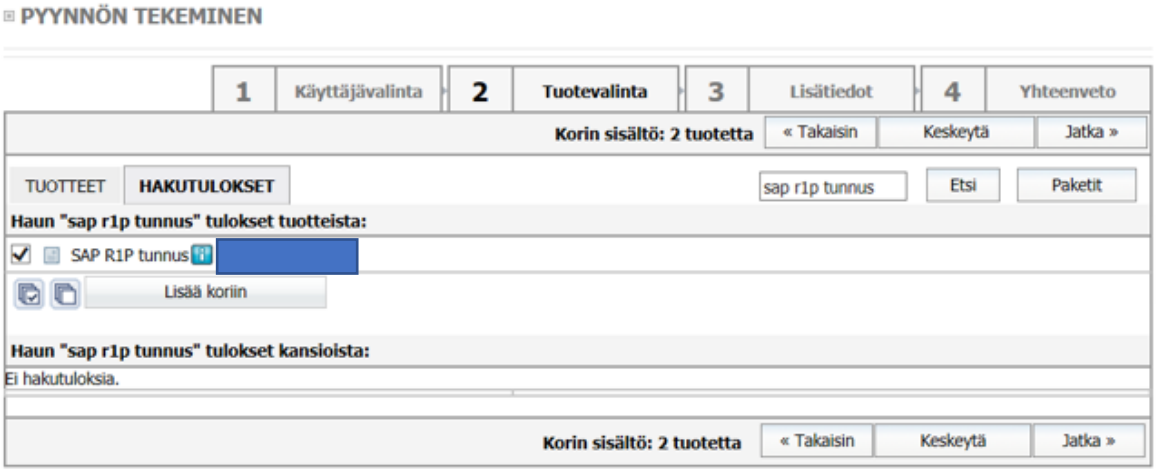


Hae toimipistekohtainen SAP-rooli ja paina ”etsi”.

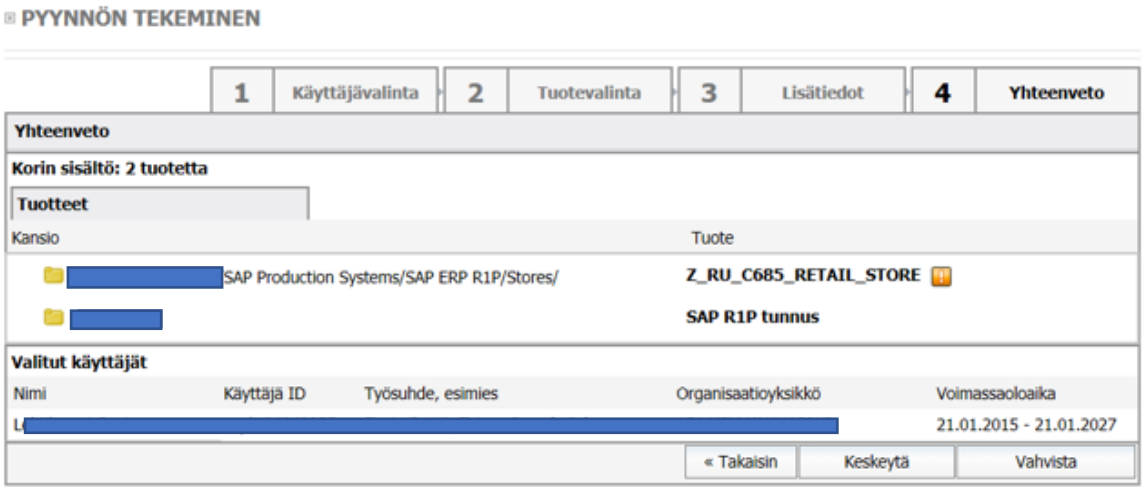
Valitse oikean toimipisteen rooli ja paina lisää koriin painiketta.



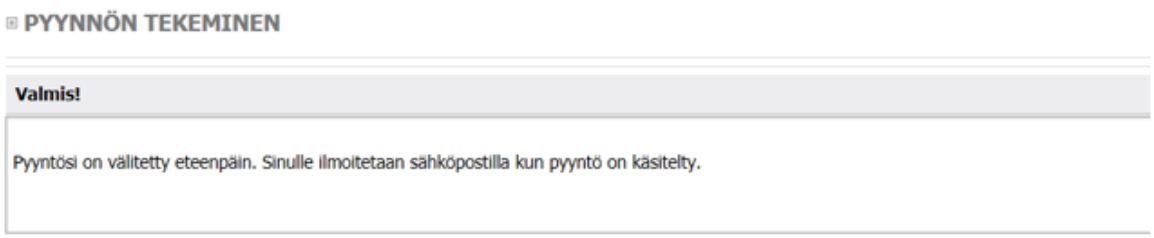
Hae myös SAP tuotannon tunnus. Edellä olevat tilaukset olivat roolit tunnukselle.



Paina jatka painiketta.

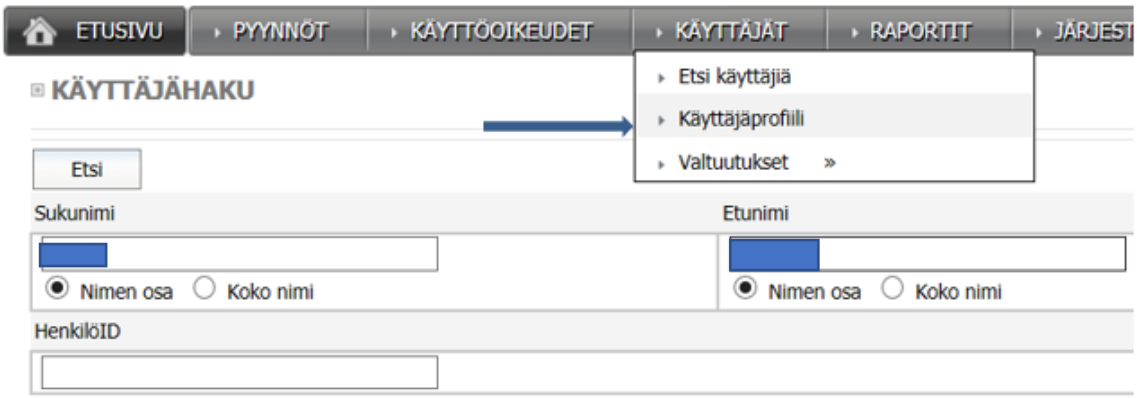


Paina vahvista painiketta. Työpyyntö välittyy It-toimittaja Y:n työjonoon.



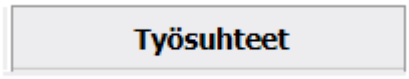
Liite 3. Työntekijän identiteetin ja työroolien poistaminen IDM:stä.

Etsi poistettava henkilö

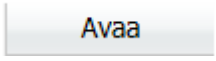


Paina näytä painiketta

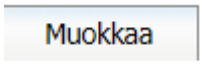
Aktivoi välilehti



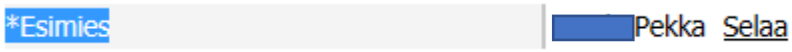
Paina



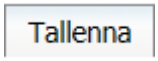
Paina

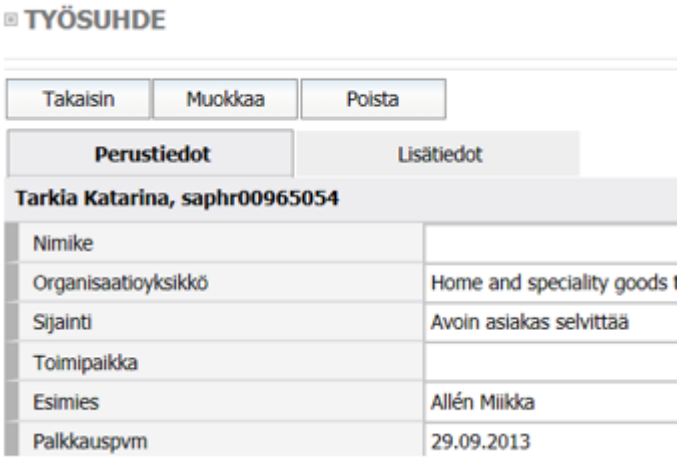


Ota esimiehen nimi talteen ja vaihda esimieheksi itsesi selaa painikkeen takaa.

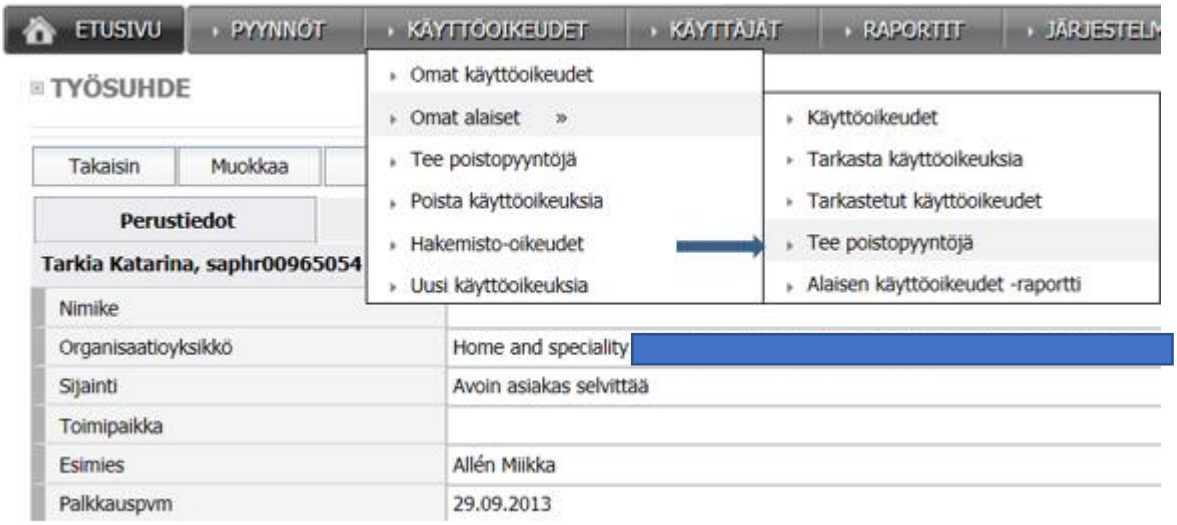


Paina

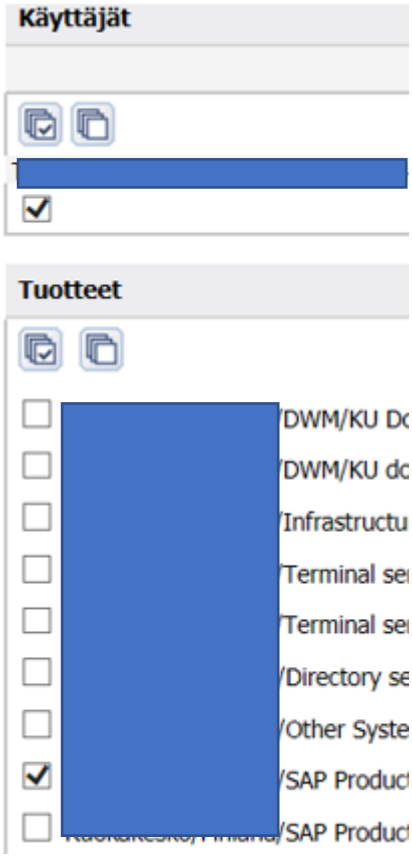




Siirry kohtaan omat alaiset – Tee poistopyyntöjä



Aktivoi henkilön nimi ”ruksilla” ja tee haluamasi henkilön ja käyttöoikeuksien poistopyyntö painamalla painiketta keskeytä käyttöluvat.



Mene takaisin kohtaan etsi käyttäjä.

Toista kohta esimiehen vaihtaminen.

Liite 4. Palvelupyyntöjen lukumääriä

	Joulukuu 2016	Tammikuu 2017	Helmikuu 2017
Sisäinen siirto	12	30	23
Työsuhteen aloittaminen	54	44	32
Työsuhteen päättyminen	71	71	92
Uudelleenpalkkaus	153	39	52
Yhteensä	**290**	**184**	**199**