KARELIA-AMMATTIKORKEAKOULU
Teknologiaosaamisen johtamisen koulutusohjelma

Ylempi ammattikorkeakoulututkinto

Kari Halonen

IDENTITEETINHALLINNAN JA HENKILÖYDINTIETOJEN KEHITTÄMINEN

Opinnäytetyö
Huhtikuu 2015

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Huhtikuu 2015** **Teknologiaosaamisen johtaminen YAMK** Tikkarinne 9 80220 JOENSUU (013) 260 600

Tekijä
Kari Halonen

Nimeke
Identiteetinhallinnan ja henkilöydintietojen kehittäminen

Toimeksiantaja
Yritys

Tiivistelmä

Tutkimuksen tarkoituksena on havaita ja raportoida mahdollisia puutteita ja virheitä ulkoisten palveluntuottajien henkilöydintietojen käsittelyssä. Tutkimuksen tuloksena tuotetaan konkreettisia prosessien korjaustoimenpiteitä ja toiminnan jatkokehittämissuunnitelma.

Tutkimuksessa keskitytään ulkoisten asiantuntijoiden käyttöoikeuksien elinkaaren hallintaan ja tässä työssä käsiteltävän henkilöydintiedon laatuun. Tutkimus osoittaa tarpeen henkilöydintietojen laadun ja käyttöoikeuksien käsittelyn kehittämiseen. Työn aikana on kehitetty Privileged Access Rights -hallintajärjestelmän prosessia. Uusina tuotteina on noussut tarve jatkotutkimukselle Privileged Access Management (PAM) -järjestelmän liiketoimintatarpeista yrityksen toimintaympäristössä.

Tutkimuksen tulosten perusteella voidaan osoittaa selkeä tarve jatkokehittää ulkoisten työntekijöiden henkilöydintietojen hallintaa sekä koko yrityksen tasolla identiteetin ja pääsyn hallintaa.

Kieli	Sivuja 82
Suomi	Liitteet 12
	Liitesivuja 31

Asiasanat

identiteetinhallinta, henkilöydintieto, pääkäyttäjäoikeudet

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
April 2015
Degree Programme in Technology
Competence Management

Tikkarinne 9
80220 JOENSUU
FINLAND

Author (s)
Kari Halonen

Title
Development of Person Master Data and Identity Management

Commissioned by
Yritys

Abstract

The purpose of this work was to find and report possible deviations and errors in user's personal identity and access management processes. As the result of the investigation, concrete development plans will be created as well as recommendations to develop person master data management, identity governance and management.

This study focuses on how to develop personal identity and access management at corporate level. Special target group is external employees and consultants. During this work the Privileged Access Rights process has been further developed. There is need for further research on Privilege Access Management tool.

Based on the results of the research there is a clear need to continue to develop external users Master Data Management and corporate level Identity and Access Management.

Language

Finnish

Pages 82

Appendices 12

Pages of Appendices 31

Keywords

identity management, personal master data, privileged access management

Sisältö

Liitteet

Esipuhe

Tutkimusraportti on kirjoitettu yhteiskuntapalveluita tuottavan yrityksen tietoturvajohdon toimeksiannosta. Tutkimuksessa on keskitytty yrityksen tietoteknisten peruspalveluiden käyttäjien identiteetinhallinnan nykytilaan. Raportissa esitetään tutkimuksen aikana esille nousevia käyttäjäidentiteettien hallintaan liittyviä kehityskohteita. Erityisenä kiinnostuksen kohteena ovat vuokratyöntekijöiden, ulkoisten resurssien, konsulttien ja partnereiden käyttäjäidentiteettien elinkaaren hallinta. Tutkimuksen tuloksia voidaan käyttää yrityksen identiteetinhallinnan toimintojen kehittämisen tukena.

Tutkimuksen aikana on kehitetty, ja tulosten avulla tullaan kehittämään sisäisten prosessien toiminnallisuuksia, käytäntöjä ja ohjeistuksia tietoturvallisempaan ja toimintoja tehostavaan suuntaan. Työ tarjoaa identiteettien hallinnan toteuttamisen perustaksi uusia toimintamalleja ja työkaluja. Tutkimus, haastattelut ja raportti on toteutettu vuosien 2014 ja 2015 aikana.

Esitän kiitokseni yrityksen turvallisuusjohtajalle mahdollisuudesta työskennellä kiinnostavan ja haastavan aiheen parissa. Samalla kiitän työn valmistelussa ja apuna toimineita kollegoita sekä asiantuntijoita. Lopuksi haluan kertoa erityiskiitokset Siljalle ja Otolle tuesta opinnäytetyön kirjoittamisessa.

Joensuu, Huhtikuu 2015

Kari Halonen

Käsitteet ja lyhenteet

CMDB, Configuration Management Data Base, konfiguraatiotietokanta
CRM, Customer Relationship Management, asiakkuudenhallinta
ERP, Enterprise Resource Planning, toiminnanohjausjärjestelmä
IAM, Identity and Access Management, identiteettien ja pääsyn hallinta
IdaaS, Identity as a Service, identiteetin hallinta palveluna
IdM, Identity Management, identiteetin hallinta
ITSM, IT Service Management, IT-palvelun hallinta
MD, Master Data - ydintieto, esimerkiksi asiakas-, henkilöstö- tai toimittajatietoja
MDM, Master Data Management, henkilöydintiedon hallintaprosessi
PAR, Privileged Access Rights, etuoikeutetut käyttöoikeudet
RBAC, Role-Based Access Control, rooliperusteinen käyttöoikeusmalli

1 Johdanto

Ammattitaito ja oman työn arvostus nousevat esille käytettäessä työtehtävään suunniteltuja, toimivia ja turvallisia työvälineitä. Oikea-aikaiset käyttöoikeudet ja tehtävään sopivat käyttövaltuudet ovat sopivien IT-työkalujen lisäksi osa työntekijän työkalupakkia. Käyttöoikeuksien tilaaminen ja hallinnointi ovat osa yrityksen käyttöoikeuksien hallintaprosessia. Esimiehen onnistuminen resurssien osaamisenjohtamisessa on osaltaan kytketty yrityksen käyttöoikeusprosessien toimivuuteen. Oikea-aikainen ja tehtävän mukainen käyttöoikeus ovat käyttöoikeuden käsittelyprosessin ydinvaatimuksia.

Työtehtävien suorittamiseen kuulumattoman luottamuksellisen tiedon vuotaminen yrityksen ulkopuolelle, tai työtehtäviin kuulumattoman tiedon käsittely voi tuottaa yrityksen liiketoiminnoille vakavia ongelmia. Edellisen työtehtävän käyttöoikeudet voivat periytyä uuteen työtehtävään tai toisen liiketoiminnan palvelukseen siirtyneelle työntekijälle tai konsultille. Tehtävän vaihdoksessa työntekijä ei pääse irti edellisistä vastuista tai tehtävistä ja näin uuden tehtävän tehokas haltuun ottaminen viivästyy. Tarpeettoman laajat käyttövaltuudet voivat avata pääsyn tietoon, johon henkilöllä ei työroolinsa vuoksi tulisi pääsyä olla. Käyttöoikeuksien laaja kertymä yhdelle työntekijälle voi aiheuttaa organisaation kannalta vaarallisen työyhdistelmän. Käyttöoikeuksien ajantasainen seuranta ja raportointi pienentävät riskejä vaarallisten työyhdistelmien syntymiseen ja liiketoimintatiedon vuotamiseen asiaan kuulumattomien henkilöiden saataville.

Henkilöresurssien käytön ohjaaminen ja käyttöoikeushallinta voidaan nähdä myös muutosjohtamisen näkökulmasta. Onnistuminen muutoksen johtamisessa vaatii tuekseen käytössä olevien työkalujen ja resurssien saumatonta yhteistyötä. Resurssien oikea-aikaista käyttöön saattamista voidaan tukea toimintojen sekä prosessien kehittämisellä ja järjestelmien välisten rutiinitehtävien automatisoinnilla.

Käyttöoikeuden tilaajilla ja ylläpitäjillä on tärkeä rooli liiketoimintakriittisten tietojen suojaamisessa. Käyttöoikeuksien hallinta ohjaa konkreettisesti tekemistä ja on mitä suurimmassa määrin työn ja prosessien johtamisen apuväline. Käyttöoikeuden elinkaarimallin tutkiminen ja kehitystyö tukevat osaamisen johtamista yrityksen tasolla.

1.1 Tehtävänanto

Edellisessä luvussa esitettyjen havaintojen ja käytännön toiminnasta tehtyjen oletamusten perusteella yrityksen turvallisuusjohtaja antoi tehtäväksi selvittää tutkimuksellisin menetelmin käyttöoikeuksien hallintaprosessin todelliset ongelmakohdat. Työn tavoite on tutkimuksellisin menetelmin havainnoida identiteetinhallinnan elinkaaren ongelmia, sekä arvioida ja raportoida mahdollisia kehityskohteita. Tässä raportissa esitellään kehityspolku identiteetinhallinnan työvälineille ja kehitysehdotuksia käytössä oleviin prosesseihin.

Turvallisuusjohtaja nosti esille kiinnostuksen ulkoisten palveluntuottajien eli konsulttien käytössä olevien käyttäjätunnusten elinkaaren hallinnassa havaittuihin ongelmiin ja niiden ongelmien ratkaisemiseen. Tutkimuksessa kerätään käyttöoikeuksien tilaajilta kehitysideoita ja toiveita käyttöoikeusprosessin laadun ja toiminnan tehostamiseksi.

1.2 Kehittämistehtävä

Kehittämistehtävän tavoitteena on yrityksen henkilöydintietojen ja identiteetinhallinnan kehittäminen. Kehittämistehtävän syötteenä ja tukena käytin työkaluina

haastatteluita ja prosessien läpimenoaikojen havainnointia. Työn tuloksena annan suosituksia kehittämistoimenpiteiksi.

Tutkimuskysymyksien avulla pyrin tunnistamaan käyttöoikeuksia tilaavien käyttäjien havaintoja ja odotuksia identiteetin hallintaprosessin toiminnasta ja käyttäjätunnus tilauksien läpäisyajoista. Annetun tehtävän ja kohderyhmän perusteella määrittelin seuraavat tutkimuskysymykset.

1. Millaisia odotuksia käyttöoikeuden tilaajilla on tilausprosessiin?

Tavoitteena on kerätä tilaajan havaintoja, käsityksiä ja odotuksia käyttöoikeuden tilausprosessista. Pyrin havaitsemaan haastateltavan käsityksiä käyttöoikeusprosessin kokonaisuudesta. Haastattelukysymyksistä johdetun keskustelun avulla kerään tunnuksen tilaajan käsityksiä ja odotuksia identiteetinhallinnan yksityiskohtaisiin toimintoihin.

2. Millaisia odotuksia prosessin käyttäjillä on käyttöoikeusprosessin läpimenoaikoihin?

Tilaaja-asiakkaan odotukset tilauksen läpimenoajalle vaihtelevat käyttötapauksen mukaan. Tavoitteena on tunnistaa käyttäjätunnuksien tilaajien näkemyksiä ja odotuksia käytettävien resurssien oikea-aikaiseen osaamisen johtamiseen. Resurssien oikea-aikaisen käytettävyyden takaamiseksi on syytä käsittää tilaajan vaatimukset uuden käyttöoikeuden tilaukseen, käyttöoikeuden muutokseen tai tunnuksen sulkemisen läpimenoajoille.

3. Kuinka tilaaja haluaa kehittää käyttöoikeuden elinkaaren hallintaprosessia?

Tässä havainnoidaan tilaajan toiveita tutkittavaan prosessiin. Tavoitteena on saada tilaajakäyttäjien kehitysideoita ja toiveita prosessin toiminnan kehittämiseksi. Haastattelukysymysten avulla syvennän ymmärrystäni haastateltavien näkemyksistä ja toiveista tavoiteltuun identiteetin hallintaprosessiin.

1.3 Tehtävän rajaus

Tutkimuksessa käsiteltävä alue rajataan yrityksen henkilökunnan ja ulkoisessa palvelussuhteessa tai sopimussuhteessa olevien luonnollisten henkilöiden käyttöoikeuksien- ja identiteetin elinkaaren hallinnan tutkimukseen, sekä toiminnan kehittämissuunnitelman luomiseen. Tutkimusosassa keskityn yrityksen esimiesten ja IT-asiantuntijoiden kokemuksiin identiteetinhallinnan prosesseista. Yksi tutkimushaara tulee käsittelemään palvelimien laajennettujen käyttövaltuuksien Privileged Access Rights -prosessia (PAR). PAR-prosessin toiminnan tutkimisen yhdistäminen tähän tutkimukseen on perusteltua, koska ulkoisten palveluntuottajien käyttövaltuuksiin lisätään hyvin usein laajennettuja käyttöoikeuksia.

Yrityksen asiakkaiden identiteetinhallinta ja liiketoimintasovellusten käyttöoikeushallinta on järjestetty liiketoiminnoissa, ja se on sovellusten System Managereiden vastuulla. Liiketoimintasovellusten käyttäjätunnusten, sekä asiakkaiden tunnusten käsittely rajataan tämän tutkimuksen ulkopuolelle. Työssä nousi esille tapahtumien läpimenoaikojen rekisteröinti myös ulkoistuskumppanin toiminnanohjausjärjestelmässä. Ulkoistuskumppanin liiketoimintasyiden ja muiden asiakkaiden tietosuojan vuoksi on läpimenoaikojen analysointi ulkoistuskumppanin toiminnanohjausjärjestelmästä rajattu pois tästä tutkimuksesta.

1.4 Opinnäytetyön rakenne

Toimeksiantajan toivomuksesta kuvaan tutkimuksen tilaajaa ja toimintaympäristöä niin yleisellä tasolla kuin se tässä yhteydessä on toimivaa. Tämä lähestymistapa käy hyvin esille luvussa kaksi, jossa esittelen tilaajan lyhyesti. Samassa luvussa esittelen tilaajalle aiemmin tehtyjä tätä aihetta sivuavia tutkimuksia.

Kolmannen luvun olen varannut tutkimuksen teoreettisen taustan ja tietopohjan esittelyyn. Tilaaja hyödyntää IT-palvelutuotannossaan vahvasti ITIL-mallia, joten on

luonnollista kuvata tätä maailmaa myös muutamalla sanalla. Nostan esille myös identiteetinhallintaan ja tietoturvaan liittyviä perustermejä. Teoriaosuuden loppuun kokoan lyhyen katsauksen käytetyistä käyttöoikeusvaltuusmalleista.

Neljänteen lukuun olen koonnut tarjolla olevien tutkimusmenetelmien kirjoa. Luvussa kuvaan perusteluita valitsemaani päätutkimusmenetelmään ja muihin tutkimuksessa käyttämiini työkaluihin. Viidennessä luvussa kuvaan haastatteluista saamiani havaintoja. Kuudennessa luvussa paneudun tutkimuksessa havaittuihin prosessien läpimenoaikoihin. Luvussa seitsemän tuon esille muutamia mielenkiintoisia seikkoja, jotka nousivat esille tutkimuksen aikana.

Lukuun kahdeksan olen kerännyt johtopäätöksiä tutkimuksesta. Esittelen lyhyen tähtäimen kehityskohteita, joita on toteutettu työn edetessä. Otan tässä esityksessä kantaa myös pitkän aikavälin kehityskohteisiin. Lopuksi esittelen tämän tutkimuksen tuloksena syntyneet ajatukset kiinnostavista jatkotutkimus- ja kehityskohteista.

2 Toimeksiantajan esittely

Tutkimuksen tilaajana toimii yhdyskuntapalveluita tuottava yhtiö. Henkilökuntaa yrityksen palveluksessa 31.12.2014 tilinpäätöstietojen mukaan oli noin 9000. Yrityksen päämarkkina-alueita ovat Pohjoismaat ja Venäjä.

Yhtiön IT-palveluita johdetaan ja ohjataan keskitetysti. Yrityksen IT-toiminnot jakautuvat hallintoon ja IT-palveluiden ohjaus- ja suunnittelutoimintoihin. Liiketoimintojen omilla IT-yksiköillä on vahva osaaminen ja vastuu divisioonien omien liiketoimintasovellusten hallinnoinnissa ja identiteetinhallinnassa.

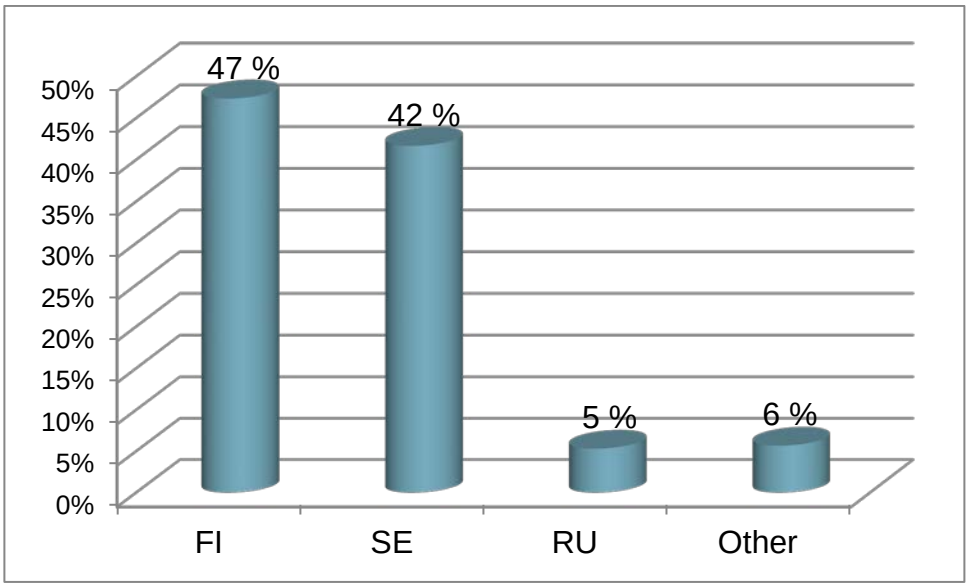
Toiminnan kohdistuminen ydinliiketoiminnan osaamiseen on lisännyt ulkoistuspalveluiden, partnereiden ja konsulttien käyttöä. Käyttäjätunnuksista 36 % on partnereiden ja konsulttistatuksella olevien henkilöiden käytössä (taulukko 1).

Taulukko 1. Käyttäjätunnusten jakauma, sisältäen loppukäyttäjä- ja pääkäyttäjätunnukset (CMDB 2014).

Tyyppi	Prosentti
Työntekijä	61 %
Konsultti	36 %
Yhteiskäyttö	2 %
Other	1 %
Total	100 %

Yrityksen sisäisten ohjeiden mukaan kaikilla ulkoisilla palveluntuottajilla tulee olla yrityksen liiketoiminnan esimiesroolissa (manageri) toimiva henkilö. Manageriroolin vastuulla on esimerkiksi varmistua, että työntekijän käyttöoikeudet ovat käytettävissä, ja huolehtia käyttöoikeuksien sulkemisesta oikea-aikaisesti. Tässä yhteydessä managerin tehtävät eivät kaikissa tapauksissa pidä sisällään työnjohdollisia vastuita. Esille on noussut tapauksia, joissa managerin rooli on annettu yksikön hallinnollisen työntekijän suoritettavaksi. Toisaalta (Haastateltava 6 2014) toteaa. "Teknisissä ympäristöissä managerin tulee antaa työlupa tehtävälle ohjelmointimuutokselle". Tällaisissa tapauksissa managerin valvontavastuu nousee erittäin merkittävään rooliin. Managerin roolissa olevien henkilöiden määrä on tutkimusta tehtäessä noin 500 henkilöä. Samaan aikaan konsulttistatuksella olevia aktiivisia käyttäjätunnuksia on noin 4000 kpl.

Konsultin roolissa toimivat henkilöt ovat jakautuneet maantieteellisesti ja läpi liiketoimintojen seuraavasti. CMDB-raportista poimittujen tietojen mukaan (kuvio 1) mukaan Suomessa ja Ruotsissa on palkattu eniten konsultteja, Venäjällä ja muissa kohteissa konsulttien käyttö on vähäisempää.



Kuvio 1. Konsulttitunnusten jakautuminen maittain (CMDB 2015).

Konsulttitunnusten jakautuminen maantieteellisesti Suomi-Ruotsi akselille voi omalta osaltaan kuvata liiketoimintojen kehittämistyön keskittyvän Pohjoismaihin.

Tässä esityksessä konsulteilla tai ulkoisilla työntekijöillä tarkoitetaan erillissopimuksella työskenteleviä palveluntuottajia, asiantuntijoita, konsultteja, partnereita, väliaikaista työvoimaa. Kielitoimiston sanakirjan mukaan liikkeenjohdon konsultti on liikeyritysten taloudelliseen ja tekniseen kehittelyyn ja neuvontaan erikoistunut henkilö. Toimitussuhteessa olevat henkilöt ovat tyypillisesti ulkoisia työntekijöitä, jotka eivät ole työsopimussuhteessa yritykseen. Palvelussuhteessa olevilla henkilöillä tarkoitetaan yritykseen työsopimussuhteessa olevia henkilöitä. Tähän joukkoon voidaan käyttöoikeushallinnan yhteydessä rinnastaa myös johtajasopimuksella olevat henkilöt.

Toimeksiantajalle on tehty vuonna 2006 esiselvitys yrityksen työntekijöiden ja partnereiden identiteetinhallinnasta. Tämä selvitys antaa hyvän läpileikkauksen identiteetinhallinnan tuolloisesta tilanteesta.

Esiselvityksessä on havaittu, että käytössä ei ole keskitettyä näkymää identiteetti- ja pääsyoikeustietoon. Tämä sama seikka nousi esille myös tässä tutkimuksessa. Identiteetin- ja pääsynhallintajärjestelmään, joka hallinnoisi keskitetysti työntekijäin

ja konsulttien pääsyoikeuksia, ei ole katsottu tarpeelliseksi investoida. Havaintojeni mukaan yksittäisiä identiteetin- ja käyttöoikeushallinnan prosesseja on kuitenkin kehitetty (Kunnas 2006).

Kunnaksen esiselvityksessä mainitaan, että muutamat tunnistetut sovellukset käyttävät tunnistamisessa roolipohjaisia tai käyttäjäryhmiin perustuvia käyttöoikeuden hallintatapoja. Tämä huomio roolipohjaisten käyttöoikeuksien vähäisestä käytöstä pitää paikkansa tänäkin päivänä. Roolipohjainen käyttöoikeuksien hallinta on hyvin harvinaista yrityksen käytössä olevissa liiketoimintasovelluksissa. Roolipohjaisen käyttöoikeushallinnan rakentaminen koskemaan yrityksen käyttöoikeustoimintoja ja kaikille sovelluksille on haastava tehtävä. Roolipohjaisen käyttöoikeushallinnan rakentaminen vaatii syventävää tutkimustyötä käyttöönoton tueksi.

Esiselvityksestä nousi esille identiteetinhallinnan puutteita ja havaintoja käyttöoikeuksien auditoinnin haasteellisuudesta. Kunnas ehdottaa tutkimuksessaan toimenpiteitä olemassa olevien käyttöoikeuksien keskitettyyn raportointiin. Keskitetyn identiteettien hallintatyökalun puuttuessa on hyvin vaikea kerätä ja raportoida yksittäisen käyttäjän käyttöoikeuksia liiketoimintasovelluksiin. Kattavan käyttöoikeusraportoinnin puute on nähtävissä edelleen.

Kunnaksen tutkimuksessa nostetaan esille ongelma, joka on relevantti myös tänä päivänä. Liiketoimintasovelluksiin on voinut jäädä avoimeksi käyttäjätunnuksia henkilöille, jotka ovat jo poistuneet työntekijävahvuudesta. Ongelman voi aiheuttaa keskitetyn henkilöydintietojärjestelmän puute ja automatisoidun de-provisioinnin puuttuminen henkilöydintiedon ja hakemistopalvelun, sekä liiketoimintasovelluksien väliltä.

Kunnas on nostanut esille myös manuaalisen työn määrän. Tämä sama ilmiö nousi omassa tutkimuksessani esille käyttäjätunnusten käsittelyssä. Automaattista käyttöoikeuden provisiointia on pyritty laajentamaan. Kuitenkin käyttöoikeuksien käsittelyyn on jäänyt edelleen manuaalisia työvaiheita, niin käyttöoikeuksien perustamiseen, muutostilanteiden hallintaan kuin varsinkin käyttöoikeuksien päättämiseen. Toiminnan tehostamisen ja operatiivisten kustannusten vähentämiseksi manuaalisen työn vähentämisen suunnitteluun tulee kiinnittää huomiota.

Kunnaksen tutkimuksessa on erityisen ansiokasta järjestelmällinen paneutuminen toimintaprosessien kehittämiseen. Esiselvityksessä hän on suositellut kaikkien käyttäjätunnusten identiteettien hallinnan keskittämistä HR-järjestelmässä suoritettavaksi. Lisäksi hän on suositellut käyttöoikeushallinnan vastuun hajauttamista liiketoimintayksiköille. Tällä hetkellä peruskäyttöoikeuden implementointivastuu on Service Deskillä ja liiketoimintasovellusten osalta liiketoimintojen System Managereilla. Käyttöoikeuden hyväksyminen liiketoimintasovelluksiin saadaan liiketoimintayksiköltä.

3 Teoreettinen tausta

Tietoperusta muodostaa analyysin ja kehittämistyön perustan. Kehittämistyöhön liittyvät oleelliset käsitteet kootaan yhteen ja samalla käsitteiden väliset kytkennät määritellään loogiseksi kokonaisuudeksi. (Ojasalo et al. 2009, 25). Edellisen ajatuksen yhdistäminen raporttiin oli kokemukseni mukaan haastavaa ja samalla antoisaa. Tähän työhön olen poiminut teoreettiseksi taustaksi IT-palvelutuotannon hyviä käytäntöjä ja identiteetinhallintaa liittyviä perusteorioita. Käytän soveltuvilta osilta tukena ITIL- ja CobIT-palvelumalleja, ISO 27002 -menettelyohjeita sekä ISF Best Practises -mallia. Käsittelen lisäksi myös identiteetinhallintaa sivuavia teoreettisia käyttöoikeusmalleja sekä identiteetinhallintaan liittyviä teorioita.

3.1 ITIL-näkökulma

Information Technology Infrastructure Library (ITIL) on IT-palveluiden hallintaan ja johtamiseen käytettävä dokumenttikokoelma. ITIL:n kehityksestä vastaa The IT Service Management Forum (itSMF) -käyttäjäyhdistys. Malli on laajalti käytetty IT-palveluntuotannon prosessien yhdenmukaistamisessa. ITIL-malli tukee IT-palveluiden elinkaariajattelua ja palveluiden jatkuvaa kehittämistä. ITIL Access Management kuuluu palvelutuotannon (Service Operation) osa-alueelle.

ITIL-näkemyksen mukaan Access Management tarjoaa sallituille käyttäjille mahdollisuuden käyttää sovittuja palveluita. Samalla kontrolloidaan järjestelmien käyttöä sekä estetään valtuuttamattomien käyttäjien pääsy tietojärjestelmiin, palveluihin, tietoihin tai laitteisiin. Pääsyoikeudenhallinta auttaa suojaamaan esimerkiksi tietojen luottamuksellisuutta, oikeellisuutta ja saavutettavuutta. Nämä termit tunnistetaan englanninkielellä Confidentiality, Integrity ja Availability (CIA). Pääsyoikeudenhallinta (Access Management) tunnistetaan myös termeillä oikeuksienhallinta (Rights Management) tai Identiteetinhallinta (Identity Management). (Hanna et al. 2007, 3).

University of Oxfordin näkemyksen mukaan (Usica 2013, 3), ITIL-prosesseista muutosten hallintaprosessi (change management) on avainasemassa pääsynhallinnan näkökulmasta. Muutosten hallintaprosessin kannalta kaikki pyynnöt käyttöoikeuteen voidaan nähdä muutoksena olemassa olevaan tilanteeseen. Palvelupyynnöt voidaan toteuttaa standardimuutoksina tai erillisinä palvelupyyntöinä olettaen, että pyyntö on hyväksytty palvelutason hallinnassa (service level management).

Palvelutason hallintaprosessin avulla tuotetaan palvelutasosopimus käytettäville palveluille. Palvelutasonkuvaus sisältää yleensä selvityksen siitä kenelle tarkasteltava palvelu on tarkoitettu, sekä millaisia mahdollisia kustannuksia palvelusta muodostuu ja millainen palvelutaso palvelun käyttäjäryhmille voidaan taata. Käyttäjäryhminä voidaan nähdä eritasoiset palveluiden käyttäjät. ITIL-mallissa konfiguraation hallinnan (configuration management) ja pääsyoikeuksien hallinnan välillä

on vahva sidos. Konfiguraation hallintaa käytetään tallettamaan kuvaus pääsyoikeuden yksityiskohdista. (Usica 2013, 3).

Taylorin ja Nissenin toimittaman ITIL-oppaan mukaan, ja aiemmin toteaman ITIL-mallin mukaan, pääsynhallinta on osa palvelutuotantoa. Pääsynhallintaprosessin avulla tuotetaan käyttöoikeus haluttuihin palveluihin tai palveluryhmille. Toisin sanoen pääsynhallinta mahdollistaa palvelukuvauksessa (Service Cataloque) kuvattujen palveluiden käyttämisen. Samalla pääsynhallinta toteuttaa tietoturva- ja saatavuushallinnan (Security and Availability Management) vaatimukset. (Taylor et al. 2007, 104).

3.2 COBIT

Control Objectives for Information and related Technology (CobIT) on nimensä mukaisesti kontrolli ja viitekehys, jonka avulla rakennetaan kontrolleja IT-palvelutoiminnan varmistamiseksi. CobIT-viitekehyksessä korostuu erityisen selvästi kytkentä liiketoiminnan tarpeisiin.

CobIT-mallin kehittäjän toimii maailmanlaajuinen ISACA-yhteisö. Yhteisön juuret ulottuvat vuoteen 1969. Tuolloin Systems Audit and Control Association nimellä perustettu yhteisö on laajentunut yli 115000 jäsenyhteisön maailman laajuiseksi IT-alan vaikuttajien yhteenliittymäksi. ISACA-yhteisö on kehittänyt maailmanlaajuisesti käytettyjä IT-alan hyviä käytäntöjä ja toimintamalleja tietojenkäsittelytoimintojen tueksi.

ISACAn kehittämä CobIT-viitekehys ottaa kantaa identiteetin- ja pääsyoikeudenhallintaan Deliver and Support luvun osassa DS5 Ensure System Security. (CobIT 4.1, 118). CobIT-viitekehyksen näkökulmasta identiteetinhallinnalla (Identity Management) varmistetaan järjestelmän sisäisten, ulkoisten ja väliaikaisten käyttäjien yksilöllinen tunnistaminen käytettäviin liiketoimintajärjestelmiin, IT-ympäristöön,

järjestelmien toimintaan, kehitykseen ja ylläpitotehtäviin. Mallin mukaan käyttäjät on tunnistettava sovitun autentikointimekanismin avulla. Pääsyoikeuden hallinnassa varmistutaan, että käyttäjän oikeudet järjestelmiin ja tietoon vastaavat dokumentoituja liiketoimintavaatimuksia. Työtehtävien vaatimusten on oltava sovitettu käyttäjien oikeuksiin. (CobIT 4.1). Tämä ajatus voidaan nähdä myös vaatimuksena pienimmän käyttöoikeuden toteuttamiseen (Guttman et al. 1995).

CobIT ottaa kantaa myös käyttöoikeuden hakemiseen. Mallin suosituksen mukaan käyttöoikeuden hakeminen käyttäjälle tapahtuu työnjohdon toimesta. Käyttöoikeuden hyväksyntä tulee saada järjestelmän omistajalta tai hänen valtuuttamalta taholta. Lopuksi turvallisuudesta vastaava henkilö aktivoi käyttöoikeuden. (CobIT 4.1, 118).

Tämän työn kannalta on hyvä huomata, että CobIT suosittelee käyttämään henkilöiden identiteetin ja pääsyoikeuksien hallintaan keskusrekisteriä (central repository) (CobIT 4.1,118). Tässä keskusrekisterissä säilytetään sisäisten, ulkoisten ja väliaikaisten käyttäjien identiteettejä keskitetyssä henkilötietovarastossa.

3.3 ISF

Information Security Forum (ISF) on informaatioteknologian alueella toimivien yritysten ja yhteisöjen yhteenliittymä. ISF:n tavoitteena on kehittää IT-alan parhaita käytäntöjä ja toimintamalleja. ISF on perustettu vuonna 1989. ISF:n tavoitteena on suorittaa tutkimustoimintaa ja ratkaista keskeisiä kysymyksiä tietoturvan ja riskienhallinnan alueilla. Yhdistys kehittää parhaita käytäntöjä, prosesseja ja ratkaisuja niin, että ne vastaavat yhdistyksen jäsenistön tarpeita. (ISF 2014).

ISF:n näkemyksen mukaan identiteetin ja pääsyoikeuden hallinnan periaate on tuottaa tehokkaasti ja johdonmukaisesti käyttäjän tunnistaminen (identification), todentaminen (authentication) ja pääsyn hallinta (access control) koko organisaati-

ossa. ISF:n mukaan käyttöoikeushallinnan tavoitteena on rajoittaa verkkoon pääsy vain valtuutetuille käyttäjille, ja varmistaa käyttäjätietojen eheys (integrity) (Chaplin et al. 2013, 113).

Arvioni mukaan ISF:n kirjaamat hyvät käytännöt ovat linjassa ISO/IEC 27000 tietoturvallisuusstandardien kanssa. ISF:n ajatukset ovat syntyneet jäsenyritysten näkemyksistä hyviksi käytännöiksi. Tässä tarkasteltavana oleva yritys on jäsenenä Infomation Security Forum järjestössä. Yritys käyttää muiden IT-alan hyvien käytäntöjen muun muassa ISF:n julkaisemia käytäntöjä tietoturvatyönsä kehityksen tukena.

3.4 ISO/IEC 27000

Standardisarja ISO/IEC 27000, Information technology Security techniques Information security management systems Overview and vocabulary koostuu useista tietoturvallisuutta käsittelevistä standardeista. Standardi ISO/IEC 27000 sisältää tietoturvallisuuden hallintajärjestelmän kuvauksen ja standardisarjan esittelyn yleisellä tasolla. (Suomen standardisoimisliitto SFS 2014, 12). Tutkimusaineistoa kootessani havaitsin, että tietoturvallisuuden standardisarjan ISO/IEC 27000 menettelyohje SFS ISO/IEC 27002 on käyttökelpoinen tämän tutkimuksen tietopohjana.

ISO/IEC 27001, Information technology Security techniques Information security management system Requirements standardissa kuvataan vaatimuksia tietoturvallisuuden hallintajärjestelmälle. Tietoturvallisuuden hallintakeinojen menettelyohje SFS ISO/IEC 27002 perustuu ISO/IEC 27001 vaatimusmäärittelyyn. Menettelyohjeessa tarkastellaan 14:ää tietoturvallisuuden pääkohtaa ja näiden 35:a pääturvallisuusluokkaa, joihin on kehitetty 114 turvallisuuden hallintakeinoa. (Suomen Standardisoimisliitto 2014, 12). Standardissa ISO/IEC 27005 esitellään tietoturvariskien hallintaa koskevia ohjeistuksia. Tässä standardissa käsitellään riskien arviointia, käsittelyä, hyväksyntää, viestintää, seurantaa ja katselmointia. (Suomen standardi-

soimisliitto SFS 2014, 10). Tämän tutkimuksen kannalta kiinnostavia suosituksia ovat muun muassa työsuhteen aikana toteuttavat käyttöoikeuskäsittelyyn liittyvät kontrollit. Työtehtävän muutokseen tai päättämiseen ohjaavat toimenpiteet sekä pääsyoikeuksien hallinta kokonaisuudessaan.

Organisaation ulkopuolisen työntekijän työsuhteen päättyessä on mahdollista, että ulkopuolinen osapuoli suorittaa työsuhteen päättämisprosessin. Menettelyohjeen mukaan päättämistoiminto suoritetaan yrityksen ja ulkopuolisen palveluntuottajan välisen sopimuksen mukaisesti. (Suomen standardisoimisliitto SFS 2014, 38). Tämän ajatuksen mukaan käyttöoikeuden päättäminen voidaan sopimuksella ulkoistaa partnerin toteutettavaksi.

Pääsynhallinnan osalta menettelyohje antaa ohjeita liiketoiminnallisiin vaatimuksiin, pääsyoikeuksien hallintaan, käyttäjien vastuisiin, sekä järjestelmien ja sovellusten pääsyn hallintaan. Käyttövaltuusperiaatteesta on kerrottu myöhemmin lisää luvussa "Pienimmän käyttövaltuuden periaate".

Käyttövaltuuksia käsiteltäessä SFS ISO/IEC 27002 menettelyohje kehottaa ottamaan huomioon asianmukaisen lainsäädännön vaatimukset (Suomen standardisoimisliitto SFS 2014, 52). Henkilötietolain yhteysvaatimuksen perusteella sopimuksen päättyessä henkilötiedot on poistettava järjestelmästä. (Henkilötietolaki 1999/523). Tämä vaatimus on otettava huomioon henkilön identiteetin ja henkilöydintiedon käsittelyssä ja varsinkin sopimussuhteen päättyessä. Teknisen seurannan ja jäljitettävyyden vuoksi henkilön käyttäjätunnuksesta jää merkintöjä erilaisiin teknisiin lokeihin tai päiväkirjoihin vielä työsuhteen päättymisen jälkeenkin. Käyttäjätunnuksen ja identiteettitietojen välisen yhteyden katkettua, on henkilön kiistattoman identiteetin tunnistaminen vaikeaa.

Standardin näkemyksen mukaan ylläpito-oikeuksia on hallittava muodollisella hallintaprosessilla, joka perustuu yrityksen käytäntöihin. Pääsyoikeuksia tulee uudelleen arvioida säännöllisin aikavälein ja työsuhteen muutosten jälkeen. Sisäisten organisaatiomuutosten tai tehtävien vaihdon jälkeen oikeudet on katselmoitava ja

myönnettävä uudelleen. Ylläpito-oikeuksien käyttövaltuuksien kohdalla katselmointi ja käyttöoikeuden tarkastus on suoritettava useammin kuin normaaleille päivittäisessä käytössä oleville käyttöoikeuksille. Katselmuksia varten ylläpito-oikeuksien käyttäjätileihin kohdistuvat muutokset on talletettava. (Suomen standardisoimisliitto SFS 2014, 58–60). Havaintojeni mukaan konsulttitunnusten ja pääkäyttäjäoikeuksien katselmointi suoritetaan säännöllisin väliajoin managerien toimesta. Muutoksien tallettaminen ei havaintojeni mukaan ole toiminnassa.

3.5 Henkilötietolaki

Henkilötietolain 8. §:ssä kuvataan henkilötietojen käsittelyn yleisiä edellytyksiä. Laissa mahdollistetaan henkilötietojen kerääminen rekisteriin muun muassa perustuen seuraavaan mainintaan. "Henkilötietoja saa käsitellä ainoastaan, jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun näihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan (yhteysvaatimus)." (Henkilötietolaki 1999/523). Edellisen perusteella voidaan myös tulkita, että rekisterin pitäjä on velvollinen poistamaan rekisteröidyn tiedot sopimuksen päättyessä.

Rekisterinpitäjän on osoitettava käyttötarve henkilötietojen rekisteröintiin. Samalla rekisterinpitäjän on osoitettava, että rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn. Tiedonantovelvollisuuden perusteella rekisteröidyllä on oikeus tarkastaa tietonsa. Samainen tiedon suojaamispykälä vaati suojaamaan välitettävän tiedon ja varmistumaan vastaanottajan oikeellisuudesta. (Henkilötietolaki 1999/523).

3.6 Arkkitehtuuri

Valtiovarainministeriön julkaiseman kokonaisarkkitehtuurin hallintamallin mukaan kokonaisarkkitehtuurilla tarkoitetaan systemaattista ja rakenteista kuvausta toimintakokonaisuudesta ja kokonaisuuteen kuuluvien osien välisestä suhteesta. Kokonaisarkkitehtuurin avulla kuvataan organisaation toimintaprosessien, tietojen ja järjestelmien toiminnankokonaisuus. Kokonaisarkkitehtuurin avulla muodostetaan yhdenmukainen näkemys organisaation toimintaympäristöstä toiminnan kehittämiseksi ja muutosten hallinnan tueksi. Kokonaisarkkitehtuurin kuvaamisella edistetään tietojärjestelmien yhteen toimivuutta, ja varmistetaan tiedon käytettävyys organisaation palvelutoiminnassa. (Valtiovarainministeriö 2013, 7).

Lidenin näkemyksen mukaan kokonaisarkkitehtuuri on strategisen johtamisen väline, joka on kehitetty organisaatioiden tueksi jäsentämään IT-toimintaa hallittaviksi ja ymmärrettäviksi kokonaisuuksiksi. Kokonaisarkkitehtuurimallin tavoitteena on yhtenäistää toiminnan kehittämistä. Malli pyrkii kuvaamaan, kuinka eri elementit liittyvät toisiinsa. Näitä elementtejä ovat ihmiset, prosessit, järjestelmät ja liiketoimintayksiköt. Identiteetinhallinta nähdään kokonaisarkkitehtuurin näkökulmassa johtamiskysymyksenä, eikä niinkään teknisenä haasteena. (Liden 2012, 39).

Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) on julkaissut kokonaisarkkitehtuurin suunnittelumenetelmän JHS 179. Menetelmässä kuvataan toiminnan, prosessien, palvelujen, tietojen, tietojärjestelmien ja niiden tuottamien palvelujen muodostaman kokonaisuuden rakenne. Kokonaisarkkitehtuurin tavoitteena on muodostaa kokonaisvaltainen lähestymistapa organisaation toimintaan, prosessien hallinnointiin ja kehittämiseen (JHS179 2012, 9).

Valtiovarainministeriön julkaiseman KA-hallintamalli ohjeen mukaan kokonaisarkkitehtuuri tarjoaa organisaation johdolle tilannekuvan organisaation toiminnasta ja toimintaa tuottavista rakenteista. Malli auttaa samalla ymmärtämään paremmin kehitystavoitteiden vaikutuksia toimintaan ja rakenteisiin. Kokonaisarkkitehtuurimallin avulla voidaan perustella toiminnan kehittämiseksi tarvittavien resurssien han-

kintaa. Mallin avulla voidaan varmistua kehittämistyölle asetettujen tavoitteiden laadukkuudesta. Samalla voidaan varmistua, ettei toiminnassa synny perustelemattomia päällekkäisiä menetelmiä ja toimintoja. (Valtiovarainministeriö 2013, 8). Kokonaisarkkitehtuuri jaetaan neljään osa-alueeseen, jotka ovat liiketoiminta-arkkitehtuuri (business architecture), tietoarkkitehtuuri (information architecture), järjestelmäarkkitehtuuri (system architecture) ja teknologia-arkkitehtuuri (IT architecture).

Liiketoiminta-arkkitehtuurimallissa (business architecture) kuvataan ydinliiketoiminnan organisaatioiden rakenne, tavoitteet ja liiketoimintaprosessit. Prosessinäkökulmasta identiteetinhallinta liittyy vahvasti liiketoiminta-arkkitehtuuriin. Palvelun hyötynäkökulmasta tarkasteltuna liiketoimintaprosesseilla on tarpeita saada identiteettejä ja käyttöoikeuksia henkilöille, jotka käyttävät ydinliiketoiminnan käytössä olevia järjestelmiä. Toiminnan ja tehtävien muuttuessa tarpeettomat oikeudet poistetaan pienimmän käyttöoikeuden (least privilege) periaatteiden mukaisesti. (Liden 2012, 40; Suomen standardisoimisliitto SFS 2014, 38).

Tietoarkkitehtuurissa (information architecture) kuvataan tietovirtoja ja käytettäviä tietovarastoja, sekä organisaation käyttämien tietojen merkityksiä liiketoiminnalle. Tietojen yksikäsitteinen ymmärtäminen, toiminta ja yhdenmukaisuus tuottavat johtamisen näkökulmasta tehokasta ja virheetöntä toimintaa. (Liden 2012, 40).

Tietoarkkitehtuurin kannalta on tärkeää tunnistaa kunkin tiedon ns. autoratiivinen lähde. Tällä tarkoitetaan tiedon attribuuttien perussijaintia, josta tiedot siirretään muiden järjestelmien käytettäväksi. Tietojen ylläpitotoimenpiteet toteutetaan vain tähän autoratiiviseen lähteeseen. Todennäköisesti yrityksessä on useita autoratiivisia lähteitä. Kuitenkin jokin näistä lähteistä on valittava identiteetinhallinnan kannalta perusrekisteriksi. Tämän rekisterin välityksellä organisaatioon tuotetaan uudet identiteetit (Liden 2012, 40–42).

Järjestelmäarkkitehtuurissa (system architecture) kuvataan yrityksen käyttämän järjestelmä- tai sovelluspaletti, vastuut, vastuuvapautukset sekä järjestelmien väliset liittymät. Järjestelmäarkkitehtuurin avulla osoitetaan, kuinka käytössä olevat

järjestelmät tukevat yrityksen ydinliiketoiminnan tavoitteita. Keskitetyn identiteetinhallinnan kannalta järjestelmäarkkitehtuuri ottaa kantaa mihin järjestelmiin keskitetty identiteetti halutaan tai voidaan provisioida.

Teknologia-arkkitehtuuri (IT architecture) tuottaa organisaatiolle nimensä mukaisesti tekniset ratkaisut, joilla tuetaan muiden arkkitehtuuriosa-alueiden toimintoja ja tavoitteita. Mallissa kuvataan yrityksen käytössä olevat standardit, teknologialinjaukset ja käytettävät työkalut. Identiteetinhallinnan kannalta teknologia-arkkitehtuurin ominta kenttää on kuvata järjestelmät, joilla identiteetinhallinta ja järjestelmien väliset käytettävissä olevat tekniset rajapinnat toteutetaan. (Liden 2012, 40., 44).

3.7 Tiedon laatu

Päätöksen teko perustuu oikea-aikaiseen ja oikeaan tietoon. Tiedon laadulla on merkittävä rooli oikeiden ja oikea-aikaisten päätösten tekemisessä. Identiteettien käsittelyssä käyttäjän tunniste- ja sopimustietojen laadulla ja oikeellisuudella on suuri merkitys päätöksenteon pohjana. Identiteetti- tai sopimustiedon heikko laatu lisää operatiivisia kustannuksia. Väärän tiedon korjailuun, sekä oikean tiedon etsintään kulutetaan tiedon käsittelijöiden työaikaa ja energiaa.

Tiedon laatua on kuvattu muun muassa seuraavilla termeillä; tarkkuus (accuracy), ajantasaisuus (timeliness), täydellisyys (completeness) ja luotettavuus (consistency) (Haug et al. 2011, 6). Tarkkuudella voidaan tässä yhteydessä käsittää henkilöydintiedon attribuuttien yksilöiviä ominaisuuksia. Ajantasaisuudella pyritään kuvaamaan oikea-aikaista tietoa käyttöoikeuksista tai tiedon omistajuuksista. Täydellisyys termillä voidaan tavoitella esimerkiksi henkilöydintiedossa täydellistä osoitetietoa. Luotettavuutta voidaan tarkastella tietojen tarkastusvelvollisuuden kautta.

3.8 Identiteetinhallinta

Identiteetinhallinnan eräs tavoite on tilanne, jossa valtuutetuille henkilöille taataan oikea-aikainen pääsy tavoiteltuun tietoon tai resursseihin, käyttäjäkokemuksen ollessa miellyttävä. (Kasanen 2010). Tietotekniikassa digitaalinen identiteetti on kokoelma attribuutteja, jotka kuvaavat objektia tai tarkasteltavaa kohdetta. Objektit voivat tässä yhteydessä olla vaikkapa henkilöitä. Näiden attribuutteina tunnistetaan nimi, käyttäjätunnus ja käyttöoikeus. Identiteetinhallinta toimii kokoavana prosessina, jonka avulla ohjataan identiteetin käsittelyä eri prosessien ja järjestelmien välillä. Toimintaa sopimuksilla, toimintakäytännöillä ja tietojärjestelmillä ohjaavaa arkkitehtuuria Liden kutsuu identiteetinhallinta-arkkitehtuuriksi. (Liden 2012, 11).

Arvidssonin ja Lidenin mukaan käyttäjäobjektin sähköinen identiteetti rakennetaan erilaisien attribuuttien avulla, jossa attribuutit toimivat identiteetin pienimpinä rakenneyksikköinä. Tässä yhteydessä henkilön ydinattribuuttien esimerkkeinä ovat etu- ja sukunimi, sähköpostiosoite, puhelinnumero ja käyttäjätunnus. Käyttäjän identiteetin ydinattribuuteissa on mukana myös yksilöiviä tunnisteita. Näiden tunnisteiden avulla henkilöt pystytään erottamaan toisistaan. Käyttäjätunnus, suomalainen henkilötunnus tai työntekijänumero on useimmiten riittävän erottavia tunnisteita. Identiteetinhallinnan kannalta on tärkeää, että yksilöivä tunniste on yksiselitteisesti tietyn käyttäjän attribuutti. (Liden 2012, 12., Arvidsson 2014, 21). Tutkittavan yrityksen tapauksessa on huomattava, että konsultille ei saada työntekijänumeroa yrityksen henkilöstönhallintajärjestelmästä. Konsultin yksilöivä tunnus identiteetinhallintajärjestelmälle on tuotettava siis jonkin muun tiedon pohjalta.

3.9 Identiteetin ja käyttöoikeuden hallinta

Kokemukseni mukaan identiteetin ja käyttöoikeuksien hallinnassa kohdataan päivittäin haasteita käytettävyyden, joustavuuden ja tietoturvan alueilla. Käyttöoikeuden käsittelyprosessin, joka sisältää tilaamisen, arvioinnin, hyväksymisen ja toteuttamisen kohdejärjestelmiin, on tuettava liiketoimintoja joustavasti ja turvallisesti. Oikea-aikainen ja riittävillä käyttöoikeuksilla varustettu käyttöoikeus tukee liiketoimintojen tarpeita saada työhön varattu resurssi tehokkaasti käyttöön.

Järjestelmien käyttäjillä ja asiakkailla on tarpeita käyttää toimintoja mistä ja milloin vain. Käyttäjien lisääntyneet vaatimukset asettavat identiteetinhallinalle itsepalveluvaatimuksia ja automaattisia oikeuden välittämistarpeita (federointi) muihin järjestelmiin. Toimintaa valvovat viranomaiset tai käytössä olevat standardit voivat asettaa vaatimuksia tarkastella käyttäjien suorittamia toimenpiteitä. (ISO/IEC 27002 2005, 56). Oikea-aikaisella ja tehtävän mukaisella käyttöoikeudella on merkitystä resurssien tehokkaassa hyödyntämisessä. Tietoturvan ja riskienhallinnan näkökulmasta katsottuna on tunnuksen nopealla sulkemisella työ- tai palvelusuhteen päättyessä erityistä merkitystä liiketoimintojen informaation suojaamisessa.

Käyttäjien identiteettien ja käyttöoikeuksien hallintaan on kehitetty järjestelmiä, jotka tunnetaan yleisesti nimellä Identity and Access Management (IAM). Identiteetin ja käyttöoikeuden hallintaa käytetään tyypillisesti käyttäjätunnusten luomiseen, käyttöoikeuksien muutoksiin, käyttöoikeuksien raportointiin ja käyttöoikeuden lopettamiseen. (Cser et al. 2012, 3).

Cserin näkemyksen mukaan identiteetin ja käyttöoikeuden hallintaa voidaan toteuttaa seuraavilla tavoilla. 1. manuaalinen käyttöoikeuksien hallinta, 2. toteutetaan itse tarjolla olevilla työvälineillä, 3. omissa tiloissa sijaitsevilla kaupallisilla tuotteilla, tai 4. hankitaan palveluntuottajalta jaettuna palveluna Identity and access management as a service (Idaas) periaatteella. (Cser et al. 2012, 2).

Manuaalisen käyttöoikeuksienhallinnan työllistävä vaikutus on syytä huomioida valmisteltaessa IAM-projektin liiketoimintamallia. Tarkasteltavassa yrityksessä

käyttöoikeuksien perustamisia ja päättämisiä suoritettiin vuoden 2014 aikana 3311 kappaletta (CMDB 2015). Forresterin arvion mukaan help desk puhelun hinta vaihtelee 9 ja 10 dollarin välillä (Cser et al. 2012, 4). Laskennallisena ITSD-tapahtuman hintana voidaan käyttää 10 euroa. Edellä esitetyllä käyttäjätunnusavausten tapahtumamäärillä IT Service Desk -työn hinta uusien tunnuksien avauksille olisi 33.000 euroa. Tässä laskelmassa ei ole huomioitu esimiehen ja työntekijän tunnuksen tilaukseen kuluttamaa aikaa. Manuaalisen prosessin tehokkuus vaihtelee IT-henkilökunnan työkuorman mukaan. Manuaalisen toiminnan yhtenä haittana on havaittu myös alttius virheisiin. Lyhyellä tähtäimellä organisaatio säästää rahaa välttämällä investointeja. Forresterin tutkimus suosittelee ottamaan käyttöön käyttöoikeuksien automatisoinnin yli 1000:n käyttäjän ympäristöissä (Cser et al. 2012).

Oman tai vuokratun henkilökunnan avulla toteutettu IAM-ratkaisu on ohjelmoitavissa tarkasti vastaamaan yrityksen erityistarpeita. Itse rakennetussa ja ylläpidetyssä tuotteessa on varauduttava ylläpitoon varattujen resurssien käytöstä aiheutuviin jatkuviin kustannuksiin. (Cser et al. 2012, 7). Valmiiden kaupallisten tuotteiden sijoittaminen omiin tiloihin ja omalle laitealustalle aiheuttavat yritykselle Forresterin näkemyksen mukaan 15–50 dollarin kustannukset per käyttäjätunnus. Tässä mallissa lisenssi- ja ylläpitokustannukset ovat tarkasti budjetoitavissa. Automatisoinnin avulla ylläpidon ja IT Service Desk toiminnan työvoimakustannukset saadaan pysymään maltillisina. Luonnollisesti tässä sitoudutaan toimittajaosapuoleen ja tuotteen ylläpitoihin ja elinkaareen. (Cser et al. 2012, 7).

Identity as a Service (IdaaS) mallin etuina voidaan nähdä tehokas kustannusvastaavuus. Tilaaja maksaa todellisesta käytöstä. Käyttöoikeuden hinta on verrannollinen hallittaviin käyttäjämääriin. Työvoimakustannukset ja laiteinvestoinnit ovat siirretty palveluntuottajan vastattavaksi. Mallista on hyvä huomata, että toiminnallisuudet ovat juuri sitä, mitä toimittaja on luvannut toimittaa. Samoin järjestelmän muuttaminen vastaamaan yrityksen omia tarpeita voi olla hyvin vaikeaa tai mahdotonta. (Cser et al. 2012, 8). IdaaS-mallissa näen mielenkiintoisia mahdollisuuksia suurten asiakasmassojen identiteettien hallintaan.

Arvioitaessa kaupallisia tuotteita itse ylläpidettyihin ohjelmistoihin, voidaan vertailussa aloittaa ylläpitokustannuksista, tapahtumamääristä ja tarvittavista lisensseistä. IAM-tuotteissa hallinnoitavien käyttöoikeusroolien lisenssihinnat voivat vaihdella merkittävästi. Lisenssi- ja käyttöoikeusmääriä tarkastellessa on hyvä tunnistaa identiteettimäärien käsittelytarve. Taloudellisesta näkökulmasta katsottuna on eri asia käsitellä järjestelmässä yrityksen omaa henkilökuntaa ja ulkoisia palveluntuottajia, kuin ottaa mukaan myös asiakkaiden identiteettien käsittely. Riskien hallinnan ja tietoturvan kannalta tarkasteltuna on hyvä hallita IdaaS-palvelun mahdolliset tietoturvariskit. Käyttäjien identiteettien tallettaminen ja käsittely palvelumallissa voi olla yrityksen liiketoiminnoille mahdotonta tiedon kriittisyyden tai toimintaa valvovien viranomaisten asettamien rajoitusten vuoksi.

3.10 Ydintieto

Julkisen hallinnon suositusten (JHS179 2012) mukaan "Master Dataksi eli ydintiedoksi luokitellaan tieto, jota käytetään useassa käyttökohteessa samanlaisena ja jota useampi prosessi tai toiminto tarvitsee tai hyödyntää. Ydintieto on pysyväisluonteista tietoa, joka kuvaa tietokokonaisuuksia. Ydintiedosta tulisi olla yhtenäinen käsitys koko organisaatiossa ja samalla se on avaintietoa organisaation toiminnalle. Ydintietoa on yleisesti asiakas-, tuote-, henkilöstö-, materiaali- ja toimittajatieto." (JHS179 2012, 9).

Julkisen hallinnon suositukset kuvaavat Master Data Management (MDM) toiminnon seuraavasti. "MDM on toiminto ja prosessi joka hallinnoi, korjaa ja ylläpitää toiminnan edellyttämää Master Dataa eli ydintietoa. Sen tehtävänä on huolehtia riittävästä ydintiedon laadusta, jotta raportointi ja seuranta voidaan pitää luotettavana ja yksikäsitteisenä." (JHS179 2012, 10). Henkilöydintiedon hallintaan käytetään yleisesti MDM-hallintomallia. Arvidssonin mukaan MDM voidaan käsitteellistää kokoelmaksi prosesseja, hallintomalleja, toimintoja, standardeja ja työkaluja.

Näiden avulla hallinnoidaan ja määritellään organisaation staattista ydintietoa yksiselitteisesti. Tyypillisesti ydintieto ei ole muuttuvaa tapahtumatietoa. (Arvidsson 2014, 18–22).

Ydintiedon lähteessä pidetään yllä keskitetysti tietoja henkilön tunnistamiseen, työsuhteeseen ja sopimuksen kestoon liittyviä attribuutteja. Yrityksen henkilöydintieto standardissa määritellään ymmärrettävästi henkilöydintieto entiteetin attribuutit. Henkilötietojen tapauksessa ydintietojen dominanttilähteen omistajalla on vastuu ja valta henkilöydintietojen ylläpidon järjestelyihin ja käsittelyyn. Järjestelmän suunnittelussa ja prosessien kehittämisessä on lähdettävä liikkeelle huomiosta, että olemassa oleva liiketoiminnallinen tilanne tulee muuttumaan. Liiketoimintarakenne voi muuttua, yrityksiä ostetaan, toimintayksiköitä yhdistetään ja liiketoimintoja myydään. Näihin jatkuviin muutoksiin järjestelmien on taivuttava tiedon laadun heikentymättä. (Päijänen 2014, 12).

Ydintiedon käsittelyssä voidaan käyttää periaatetta "kirjoita kerran käytä monesti". Saman tiedon tallettaminen useaan paikaan lisää myös virheen mahdollisuuksia ja työajan hukkaa. Henkilöydintiedon laatupoikkeamat voivat myös lisätä yrityksen kokemia tietoturvariskejä. Puutteelliset tai väärät tiedot aiheuttavat helposti ongelmia esimerkiksi ohjelmistolisenssien hallintaan. Kuten Gröbner ja Frenken ovat artikkelissaan todenneet, virheet henkilö ydintiedoissa lisäävät viivettä ongelmien ratkaisussa, lisäävät virheiden mahdollisuutta ja tuottavat ylimääräisiä kuluja käyttöoikeuksien käsittelyyn. (Gröbner et al. 2013).

Arvidssonin mukaan henkilötietojen laatumittarit on syytä tunnistaa. Laatumittareina voidaan käyttää vaikkapa tiedon ajantasaisuutta, oikea-aikaisuutta ja oikeellisuutta. Sitä saat mitä mittaat lausahdukseen perustuen, ydintiedon tunnistamisen ja tiedon laadun mittaamisen avulla käsiteltävän ydintiedon laatutaso saadaan nousemaan. Henkilötietojen tulee olla ajantasaista ja samalla tasolla eri järjestelmissä. Tietoja julkaistaan järjestelmiin sovitusti ja ylläpitoprosessin tulee olla näkyvillä prosessissa toimiville. Ydintietojen tulee olla jatkuvassa ylläpidossa koko elinkaarensa ajan. (Arvidsson 2014).

Haug et al. ovat tutkimuksessaan todenneet seuraavaa. Liiketoimintaprosessien keskeisiä käsitteitä ovat asiakas, pääsyoikeus, sopimus, sopimuksen kesto, tuote ja sijainti. Muun muassa näitä käsitteitä voidaan tunnistaa henkilöydintiedon rooleissa. Henkilöydintieto määritellään tiedoksi, jossa talletetaan toiminnalle ominaisia harvoin muutettavia perustietoja. Tyypillisesti henkilöydintieto talletetaan vain kerran yhteen tietojärjestelmään ja muut järjestelmät voivat käyttää näitä tietoja. (Haug et al. 2011, 169).

Master Data Management käsite pitää sisällään välineet ja prosessit, joiden avulla vähennetään saman tiedon uudelleen tallentamista. Identiteetin attribuuteille määritellään yhteinen tietojärjestelmä, josta identiteettitietoa siirretään muihin järjestelmiin. Tätä tietolähdettä kutsutaan autoratiiviseksi lähteeksi. Näitä autoratiivisia lähteitä voi olla useampia, mutta jokin järjestelmistä on syytä asettaa perusrekisteriksi. Tämän perusrekisterin tehtävänä on tuottaa uudet identiteetit muiden tietojärjestelmien käyttöön. Etuna keskitetyllä perusrekisterillä on, että identiteettejä pidetään yllä vain yhdessä paikassa. Näin toimien vältetään saman tiedon päällekkäistä ja toistuvaa käsittelyä. Identiteetin päättäminen perusrekisteristä käynnistää käyttöoikeuksien poistamisen samalla myös muista järjestelmistä. (Liden 2012, 42).

Shah, Manathara ja Hoeppen mukaan MDM-järjestelmän arkkitehtuuriratkaisua voidaan lähestyä erilaisista näkökulmista ja tarpeista. MDM-ratkaisu voidaan rakentaa konsolidoimalla ydintietoa eri lähteistä yhteen tietokantaan. IT-alusta voi olla mikä tahansa käyttöön parhaiten sopiva alusta. Tässä tarkoituksessa voi toimia tähän tehtävään tarkoitettu SQL-kanta, yrityksen ITSM-järjestelmä, tai vaikkapa olemassa oleva HR-järjestelmä. Keskitetyssä mallissa tietoa syntyy yhdessä dominantissa järjestelmässä, joka voi toimia globaalina toiminnanohjausjärjestelmänä tai HR-järjestelmänä. Järjestelmässä ydintiedot suodatetaan sekä jaellaan muille IT-järjestelmille. (Shah et al. 2012, 11).

Rekisteri dataviittaus toteutuksessa ydintiedot on hajautettu erillisiin tietojärjestelmiin. (Shah et al. 2012, 11). Kuten teoriaosassa aiemmin on huomioitu, hajautetussa mallissa ongelmaksi voi muodostua tiedon oikea-aikainen ja luotettava yllä-

pitäminen (Haug et al. 2011, 169). Lisäksi moneen paikaan talletetun ydintiedon ylläpito voi aiheuttaa ylimääräisiä kustannuksia.

Rinnakkaisessa transaktiomallissa syntyy perustietoa, jonka laatu on vaihtelevaa. Tämä tieto välitetään MDM-järjestelmään, jossa tieto siistitään liiketoimintatarpeiden ja tietojärjestelmien vaatimusten mukaiseksi. Keskitetyssä MDM-mallissa ydintiedon puhdistaminen ylimääräisestä tiedosta ja tiedon oikeellisuuden varmistaminen (validiointi) suoritetaan MDM-järjestelmässä. Malli ei ole reaaliaikainen, joten esille voi nousta ongelmia ja viiveitä tietojen vahvistamisessa ja siistimisessä. (Shah et al. 2012, 11).

Hybridimallissa ydintietoa luodaan useissa eri lähteissä. Tietoa suodatetaan ja siistitään keskitetysti tarpeita vastaavaksi. Ydintieto talletetaan keskitettyyn kohteeseen ja toimitetaan yhdestä lähteestä eri IT-järjestelmien käyttöön. (Shah et al. 2012, 11). Tutkittavassa yrityksessä on käytössä henkilöydintietojen tallennuksessa hybridimalli. Henkilökunnan tietoja talletetaan yrityksen HR-järjestelmässä ja konsulttien tiedot löytyvät keskitetysti yrityksen AD-järjestelmästä.

3.11 Riskialttiit työyhdistelmät ja pienimmän käyttöoikeuden periaate

Saltzer ja Schroeder ovat esitelleet perustutkimuksessaan "The Protection of Information in Computer Systems" (Saltzer et al. 1975) muun muassa käyttöoikeuksien erottamisen (engl. separation of privilege) ja pienimmän käyttöoikeuden (engl. least privilege) periaatteet. (Saltzer et al. 1975, e., f).

Tutkijat olivat lähestyneet separation of privilege termiä konkreettisesti tietojen suojaamisen suojausmekanismilla. Käyttöoikeuksien erottamisen perusperiaate esiteltiin suojattavan kohteen avaamiseen kahdella fyysisellä avaimella. Suojausavaimet ovat kahden henkilön hallussa. Menettelystä on luotu kontrolli, jossa vaikuttava

toimenpide aktivoidaan kahden toimijan yhteisellä päätöksellä. (Saltzer et al. 1975, e).

Kahden avaimen perusperiaatetta on kehitelty edelleen työtehtävien eriyttämiseen. Tehtävien eriyttämisen perusperiaate tunnistetaan separation of duties tai segregation of duties -merkityksillä. Riskialttiit tehtävät pyritään jakamaan toiminnassa usealle työntekijälle. Riskialttiiden toimintojen jaon tavoitteena on estää vaarallisten työyhdistelmien syntyminen. Tästä käy esimerkkinä laskun hyväksyminen ja maksattaminen yrityksen tilitä kahden henkilön suorittamana työnä.

Pääsyoikeuksien hallinnassa käytetty least privilege -ajatusmalli, on yleisesti tunnustettu tietoturvaperiaate. Tutkijat Guttman ja Boback esittelivät periaatteen tavoitteena tarjota tietojärjestelmien käyttäjille vain ja ainoastaan heidän työssään tarvitsemansa oikeudet. "Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties." (Guttman et al. 1995).

Tietoturvallisuuden hallintakeinojen menettelyohjeissa (standardi SFS ISO/IEC 27002) kehotetaan pääsynhallintasääntöjä määriteltäessä oletusarvoisesti estämään kaiken mitä ei erikseen ole sallittu. "Kaikki on kiellettyä, ellei sitä erikseen sallita", "Everything is generally forbidden unless expressly permitted." (Suomen standardisoimisliitto SFS 2014, 52–53).

Pienimmän käyttöoikeuden politiikalla pyritään ennaltaehkäisemään vahinkoja tai haittavaikutusten laajuutta. Työntekijälle annetaan vain hänen kyseisessä tehtävässä tarvitsemat oikeudet ei enempää. Samalla on varmistuttava, että työntekijällä on tehtävistä suoriutumiseen riittävät valtuudet. (Saltzer et al. 1975).

Edellä kuvattua pääsynhallinnan perusperiaatetta on noussut haastamaan ihmiskeskeinen tietoturvan lähestymistapa People Centric Security (PCS). Tutkijoiden Ant ja Scholtz 2014 esittämän näkemyksen mukaan käyttöoikeuksia laajentamalla lisätään työntekijöiden vastuuta. Tavoitteena ihmiskeskeisessä lähestymistavassa ovat työtehtävien joustavuus ja identiteettihallinnon sopeuttaminen. (Ant et al. 2014).

Tällä hetkellä yrityksen tietoturvapolitiikka on rakennettu pienimmän käyttöoikeuden toteutusvaatimusten mukaiseksi. Tietoturvapolitiikan muutosajatukseen en ota tässä tutkimuksessa kantaa. Kuitenkin käytettävissä politiikoissa ja kontrolleissa on tarkoituksellisia poikkeamia. Otetaan esimerkkinä tästä vaikkapa palvelinten ylläpitotehtäviin tarkoitetut laajennetut pääkäyttäjäoikeudet (PAR). Työasemien Local Admin Rights (LAR) oikeuskäsittelyllä annetaan käyttäjälle perusteltuja liiketoimintatarpeita varten pääkäyttövaltuudet ja ohitetaan pienimmän käyttöoikeuden periaate.

3.12 Privileged Access Management (PAM)

Palvelinympäristössä laajennetuilla käyttöoikeuksilla suoritetaan tyypillisesti ohjelmistojen asennuksia, muutoksia ja ylläpitotöitä kohdejärjestelmään. Paikalliset pääkäyttäjäoikeudet mahdollistavat kohdejärjestelmän täydellisen hallinnan. Osaavan pääkäyttäjän käsissä pääkäyttäjäoikeudet kuuluvat ylläpitäjän luonnolliseen työkalupakkiin. Kuitenkin on tilanteita jolloin pääkäyttäjän oikeuksia halutaan järjestelmän omistajan toimesta hallita ja valvoa tehtyjä toimenpiteitä.

Laajennettujen käyttöoikeuksien hallintajärjestelmää kutsutaan englanninkielisellä nimellä Privileged Access Management (PAM) tai Privileged Identity Management (PIM). Käytän tässä yhteydessä lyhennettä PAM. PAM-järjestelmän perusominaisuuksina voidaan tunnistaa pääkäyttäjäoikeuksien hallinnointi, pääkäyttäjätunnuksien avulla tehtyjen tapahtumien rekisteröinti ja tapahtumien todennettavuus. On hyvä huomata, että pääkäyttäjätasoisilla oikeuksilla voidaan päästä suoraan liiketoimintakriittisiin tietoihin.

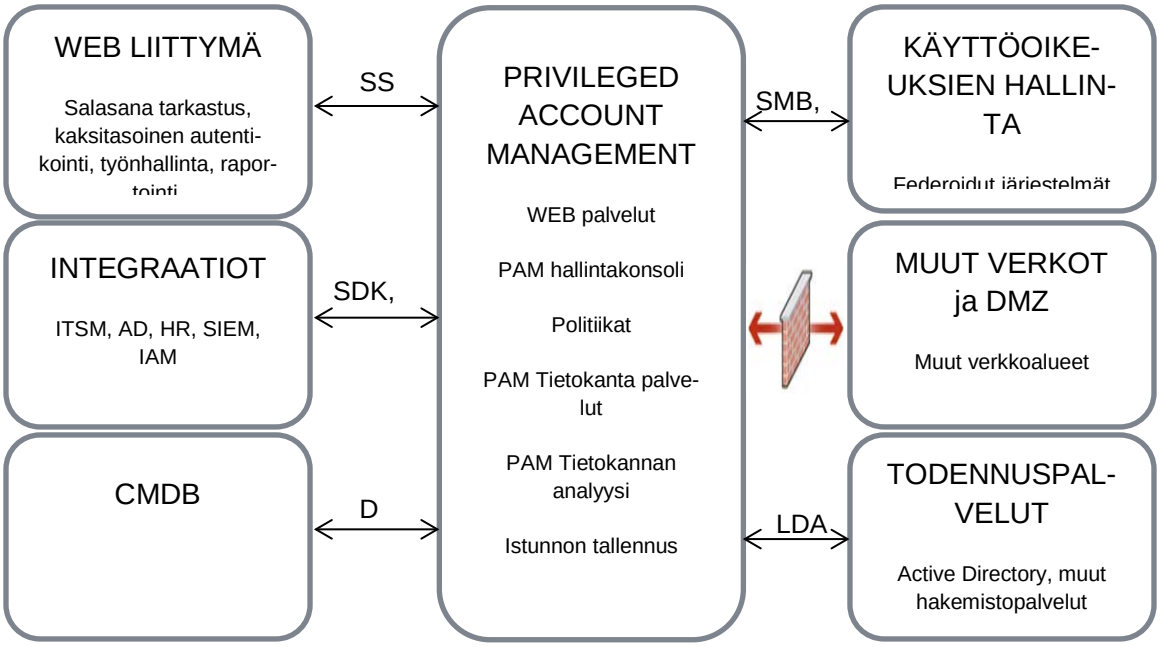
Riskien hallinta, toiminnan ulkoinen auditoija tai toimintaa valvova viranomainen kiinnittää huomiotaan yrityksen pääkäyttäjäoikeuksien valvontaan. Joissakin tapauksissa vain henkilökohtaiset pääkäyttäjäoikeudet ovat sallittuja, mutta tapahtumien talletus jää järjestelmän oman tapahtumarekisteröinnin varaan. Pääkäyttäjäoi-

keuksilla on mahdollista tyhjentää tapahtumatiedostot, joten kontrolli on näennäinen.

PAM-järjestelmä antaa mahdollisuuden hallinnoida pääkäyttäjäoikeuksia keskitetysti. Oikeuksien hallinta tapahtuu erillisessä palvelussa, joka ei päästä laitteen ylläpitotehtäviä suorittavaa henkilöä kirjautumaan suoraan kohdelaitteelle. Tässä käyttötapauksessa PAM-järjestelmä voidaan nähdä välitinpalvelimen roolissa.

Käyttötapauksista tavallisin lienee tapahtumien tallennus. Kohdelaitteella suoritetut tapahtumat voidaan tallettaa lokiriveinä tai vaikkapa kuvaruututapahtumien videotallennuksina erilliseen palvelimeen. Tällöin historiallisten tapahtumien seuranta onnistuu, vaikka kohdelaitteen tapahtumalokit olisi tarkoituksellisesti ylikirjoitettu.

Kuviossa 2 on esitelty PAM-toiminnallisuuksia arkkitehtuuritasolla.



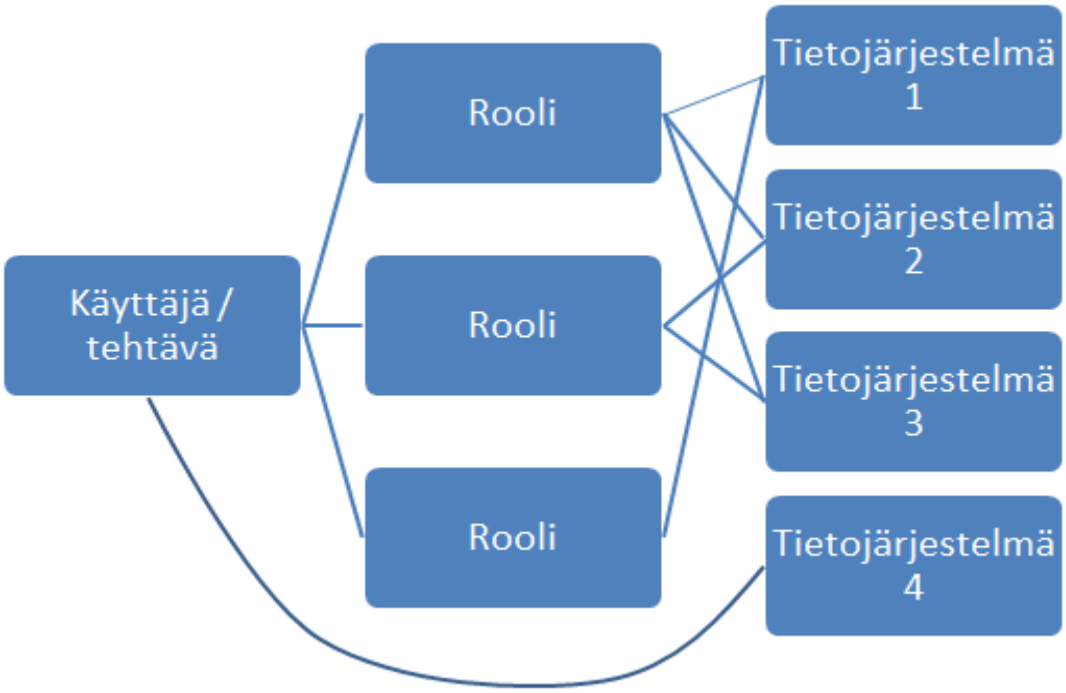
Kuvio 2. Privileged Account Management -arkkitehtuuri.

3.13 Role Based Access Control (RBAC)

Rooliperusteisen käyttöoikeusmallin Role Based Access Control (RBAC) teorian ja perustan julkaisivat NIST-tutkijat Ferrairo ja Kuhn vuonna 1992. Mallia on laajennettu useasti ja standardiksi RBAC-käyttöoikeusmallia esittelivät tutkijat Sandhu, Ferraiolo ja Kuhn jo vuonna 2000. Standardiksi RBAC-käyttöoikeusmalli julkaistiin vuonna 2004. (O'Connor et al. 2010).

Roolipohjainen käyttöoikeusteoria lähestyy käyttöoikeuksien hallintaa työtehtävien ryhmittelyyn perustuvan näkökulman kautta. Liiketoiminnoilla ja sen yksiköillä on kullakin omat tehtävänsä ja osaamisalueensa. Näiden olettamusten avulla voidaan muokata käyttöoikeuksista kutakin työtehtävää parhaiten palvelevat oletusroolit ja käyttöoikeusmallit. Työntekijät liitetään näihin rooleihin omien osaamisalueidensa mukaisesti. Tässä mallissa nousee korostetusti esille työntekijän oikeus informaatioon tai tehtävän suorittamiseen. Rooliperustainen malli on joustava ja mallin avulla voidaan hyvällä suunnittelulla ehkäistä vaarallisten työyhdistelmien syntymistä. Ravi Sandhun ja työryhmän julkaiseman tutkimuksen mukaan rooli voidaan nähdä toisaalta kokoelmana käyttäjiä ja toisaalta kokoelmana käyttöoikeuksia. Käyttöoikeusroolin avulla kytketään nämä kokoelmat toisiinsa. (Sandhu et al. 1995, 5).

Kuviossa 3 esittelen roolipohjaisen käyttöoikeusmallin perusideoita. Yhdellä käyttäjällä voi olla erilaisia työrooleja ja näillä rooleilla työtehtävien vaatimusten mukaisia oikeuksia eri liiketoimintasovelluksiin tai tietojärjestelmiin. Lisäksi käyttäjällä voi olla suoria rooliperustaisen järjestelmän ulkopuolisia oikeuksia suoraan haluttuihin tietojärjestelmiin. Tällä mahdollistetaan poikkeamamenettely järjestelmiin joiden käytössä roolipohjaisuus ei toimi tai ei ole järkevää toteuttaa.



Kuvio 3. Roolipohjainen käyttöoikeusmalli. Mukailee koulutusmateriaalia. Sparta Henkilöydintieto, roolitieto ja sähköinen identiteettitieto. (Sparta 2014) ja (Sandhu et al. 1995, 18).

Eräänä ongelmana voi olla tiedonomistajien ja tuottajien sitouttaminen roolipohjaiseen ajatteluun. Siirtymisvaiheessa roolipohjaiseen malliin suunnittelun ja mallin valmistelutyön määrä on suuri. Tätä kautta RBAC-mallin käyttöönotto ja perustaminen yrityksen käyttöön voidaan nähdä työläänä. On normaalia, että organisaatioiden tiedon omistaminen on hajautunut. Tiedonomistajien velvollisuudet voivat olla epämääräisiä tai hallintomallissa määriteltyjä vastuita ei ole jalkautettu aina käytännön toimintaan saakka. Tiedon omistajuuden ollessa epäselvä on käyttöoikeusroolien luominen työlästä. Rooliperusteisessa käyttöoikeuskäsittelyn määrittelyssä (RBAC) on roolimassasta pyrittävä seulomaan perusroolit tai niin sanotut tehtävien suorittamisen arkkiroolit.

Rooliperustaisen käyttöoikeuksien hallinnan perusteiden mukaisesti, osa työntekijän käyttöoikeuksista voidaan perustaa jo työntekijän rekrytoinnin yhteydessä. Työntekijä tulee kuulumaan valittuun liiketoiminta-alueeseen, osastoon ja työryhmään. Hän sijoittuu maantieteelliseen tai vaikkapa kielialueen mukaiseen ryhmään.

Ryhmille voidaan tarvittaessa luoda ennakkoon valittuja ominaisuuksia ja pääsyoikeuksia haluttuihin tietovarastoihin tai niiden osiin. Samalla voidaan tarjota oletusarvoisesti työntekijän perusroolin mukaisia sovelluksia tai näkymiä yrityksen yhteisiin palveluihin sekä liiketoimintasovelluksiin. Asiantuntijuuden perusteella työntekijälle voidaan roolipohjaisen ajattelun mukaan tuottaa oletusarvoiset oikeudet samoilla perusteilla, kuten hänen kollegoilleenkin on tuotettu. Näistä perusasetuksista muodostuu roolipohjaisen käyttöoikeuden hallinnan peruskivi. Kerran suunniteltu käyttöoikeusmalli voidaan monistaa seuraaville työntekijöille helposti ja tehokkaasti. Roolipohjaisen käyttöoikeusmallin hyödyntäminen helpottaa ja nopeuttaa linjaesimiehen toimintaa uuden henkilön rekrytointitilanteessa ja käyttöoikeuksien muutos- ja päättämistilanteissa.

Rooliperustaisen käyttöoikeuskäsittelyn etuina ovat tutkimuksessaan O'Connor ja Loomis kuvanneet joustavuuden, läpinäkyvyyden ja kehittyneen käyttöoikeuksien provisioinnin. Rooliperustaisesta käyttöoikeuskäsittelyn hyötyjinä he esittävät liiketoimintajohdon, henkilöstöhallinnon ja IT-hallinnon. (O'Conor et al. 2010, 12). Nähdäkseni rooleihin perustuva käyttöoikeuksien hallinta tuo mukanaan holistisen näkymän käyttöoikeuksiin. Käyttöoikeuksien keskitetty raportointimahdollisuus aina sovellustasolle saakka auttaa ehkäisemään vaarallisten työyhdistelmien syntymistä.

3.14 Valittu teoria

Tutkimuksen otsikon mukaisesti keskityn yrityksen henkilöydintietojen ja identiteetinhallinnan toimintaan. Valitsen analyysin tueksi identiteetin ja pääsynhallinnan näkökulman (Identity and Access Management). Identiteetin ja pääsynhallintajärjestelmä tukee käyttäjätunnusten luomista, käyttöoikeuksien muutoksia, käyttöoikeuksien raportointia ja käyttöoikeuden lopettamista. (Cser et al. 2012, 3). Mielestäni IAM-tietoperusta tukee hyvin asetettua tutkimustehtävää.

4 Tutkimusmenetelmät

Kehittämistyön lähestymistapana tai menetelmänä on mahdollista käyttää tapaustutkimusta tai toimintatutkimusta. Seuraavassa perustelen tutkimuksellisen lähestymistavan valintaa eri näkökulmista tarkasteltuna. Mika Metsämuuronen on todennut seuraavaa. "Koska tutkittavat ilmiöt ovat joskus hankalasti hahmotettavissa, saattaa tietomme ja ymmärryksemme ulkopuolelle jäädä jotain mitä emme pysty tavoittamaan" (Metsämuuronen 2009, 217). Tällä ajatuksella varustettu tutkija antaa ikään kuin etukäteen anteeksi itselleen sen, että kaikkia ilmiöitä ei välttämättä tässä tutkimuksessa havaittu tai huomattu etsiä. Kvantitatiivinen tutkimus perustuu vahvasti positivismiin tai postpositivismiin. Tutkija pyrkii ajattelemaan, että totta on se, mitä voidaan konkreettisesti tavoittaa. (Metsämuuronen 2009, 220). Kokemukseni mukaan haastattelujen analysoinnin ja tarkentavien kysymysten avulla tieto tutkittavasta aiheesta tai ongelmasta luonnollisesti lisääntyy.

Konstruktivismissa todellisuus on eri henkilöiden suhteellinen kokemus todellisuudesta. Tietoa todellisuudesta voidaan saada tutkijan ja tutkittavan ollessa toisiinsa interaktiivisesti yhteydessä (Metsämuuronen 2009, 218). Ajatuksen voi konkretisoida haastattelu- tai kyselytutkimuksen suorittamiseksi. Kvalitatiivisen tutkimuksen metodologia eli oppi tiedon hankinnan menetelmistä perustuu konstruktivismiin. Kvalitatiivisen tutkimuksen tiedonhankintavälineinä käytetään tyypillisesti haastatteluita.

Lähestyn tutkimusotteen valintaa metodologisten pohdintojen kautta. Tavoitteeni on kerätä tietoa toiminnassa havaituista ongelmista prosessin auditoinnin, läpimenoaikojen mittauksen ja haastattelujen avulla. Valitut työvälineet antavat näkymän tutkittavaan kohteeseen. Kvantitatiivisia menetelmiä käyttämällä voin mitata ja todistaa prosessin läpimenoaikoja ja näin tavoittaa näkymän prosessin pullonkauloihin. Numeeriset mallit eivät kuitenkaan kykene täysin yksiselitteisesti ratkaisemaan varsinaista tutkimusongelmaa, joka liittyi käyttöoikeuksien elinkaaren jat-

kumiseen työsuhteen päätyttyä. Pohdiskelun tuloksena valitsen tutkimuksen päämetodologiaksi kvalitatiivisen tutkimusotteen.

4.1 Kvalitatiivisen tutkimuksen strategia

Laadullisen tutkimuksen tiedonhankinnassa käytetään erilaisia toimintamalleja. Tapaustutkimuksella pyritään kokoamaan tietoja tutkittavasta aiheesta monipuolisesti. Tavoitteena on ymmärtää ilmiötä syvällisesti. Tapaustutkimukset toimivat usein ponnahduslautana toiminnan kehittämiseen. Tehtävänannossa esiintyi vaatimus kehittää toimintaa tai tuottaa kehitysideoita.

Fenomenologinen tutkimus on oppi ilmiöistä. Tässä tutkimusalueessa tutkimusaineistoon tutustutaan avoimesti pyrkien kokonaisnäkemykseen. Näkemyksestä muodostetaan yleinen merkitysrakenne, jonka avulla ongelma pyritään analysoimaan ja ratkaisemaan. Etnografisen tutkimuksen välineitä voidaan käyttää erityisesti ihmisten ja ilmiöiden tarkkailuun ja ymmärtämiseen. Analyysissä pyritään tuomaan julki inhimillisen käyttäytymisen merkityksiä. Aineistopohjaisessa teoriassa (grounded theory) pureudutaan käytössä olevaan tutkimusmateriaaliin, jonka pohjalta luodaan tutkimuksen teoria. Aikaisempia teorioita ei tässä tutkimusmenetelmässä välttämättä käytetä, vaan tavoitteena on uuden teorian luominen.

Toimintatutkimuksessa osallistutaan tutkittavan ilmiön toimintaan tai prosessiin. Tavoitteena on ratkaista käytännön tilanteita, ongelmia, muuttaa sosiaalisia käytäntöjä tai vaikkapa tarjota uusia näkökulmia työskentelyyn. Diskurssianalyysi ja narratologia tutkivat tekstiä, puhetta, kielen käyttöä, kertomuksia ja tarinoita. Tämä tutkimussuunta ei vastaa tällä kerralla asetettuihin tavoitteisiin.

Ihmisten käsityksiä asioista ja ilmiöistä tutkitaan fenomenografisella tutkimuksella. Tässä yhteydessä tämän tutkimusmenetelmän ongelmana on tutkittavien käsitysksien muuttuminen riippuen kysymysten näkökulmasta kohteena olevaan tutkimus-

ongelmaan. (Metsämuuronen 2009, 222–242). Käsittääkseni tässä menetelmässä tulosten yleistettävyys on haasteellista, ja tämän tutkimuksen tarkoituksena on päästä kiinni yleistettäviin ja pragmaattisiin tuloksiin.

Edellisten pohdintojen perusteella tutkimusstrategioista osallistuva toimintatutkimus tukee hyvin tehtävänannossa määriteltyjä tavoitteita. Valitsen tutkimusstrategiaksi kvalitatiivisen osallistuvan toimintatutkimuksen.

Tutkimusmetodeina käytän avainhenkilöiden haastatteluita, identiteetinhallinnan prosessien tukimusta ja käytännön toiminnan havainnointia. Tulosten analysoinnin suoritan haastatteluaineiston sisältöanalyysin avulla (Ojasalo et al. 2009, 124). Oletuksenani on, että ulkoisten työntekijöiden elinkaaren hallinnassa on epävarmuutta, ja yrityksen IT-hallinnon asettamat tietoturvavaatimukset vähimmän käyttöoikeuden vaatimuksesta eivät täyty. Työssä havainnoidaan myös muiden vastaavan kokoisten yritysten käyttämiä identiteettien hallintamalleja ja parhaita toimintamalleja (best practises). Tässä työssä tehtävien tutkimusten ja haastatteluiden pohjalta luodaan käsitys yrityksen käyttäjätunnusten ja käyttöoikeuksien elinkaaren tapahtumista.

4.2 Haastattelut

Valitsin haastatteluihin kaksikymmentä yrityksen, ulkoistuskumppanin ja samalla alalla toimivien yritysten palveluksessa työskentelevää johtaja-, esimies- tai asiantuntijarooleissa olevaa henkilöä. Henkilöhaastattelut valmistelin ennakkoon vapaamuotoisiksi keskustelutilaisuuksiksi. Haastattelutilanteissa ohjasin keskustelua aihealueittain käsittelemään havaittuja ongelmia ja mahdollisia kehittämiskohteita. Tavoitteeni oli löytää kommentteja ja ideoita identiteetin ja käyttöoikeuden hallinnan prosessien ongelmakohtiin, henkilöydintiedon lähteisiin, käyttöoikeustyyppeihin, käyttötapauksiin ja toivottuihin prosessien läpimenoaikoihin. Tavoitteeni va-

paamuotoisissa haastatteluissa oli välttää haastateltavan vastauksia mahdollisesti ohjaavaa kysymys ja vastaus haastattelumallia.

Lisäksi kävin vapaamuotoisia keskusteluja kollegayritysten edustajien kanssa benchmark-hengessä. Aiheena keskusteluissa olivat ulkoisten työntekijöiden henkilöydintiedon hallinta ja IAM-hankkeet. Tavoitteenani oli havainnoida muiden saman kokoluokan yritysten toimintamalleja sekä kokemuksia IAM-käyttöönotoista. Näitä keskusteluita kävin eri yhteyksissä talvella 2014. Kahdenkeskisiin keskusteluihin osallistui viiden yrityksen edustajia Suomesta ja Ruotsista.

4.3 Prosessien mittaaminen

Tunnuksen perustamiseen käytetyn ajan havaitseminen ja mittaaminen on yksi perusedellytys tunnuksen perustamistapahtuman tehokkuuden ja toiminnan ymmärtämiseksi. Samalla voidaan tarkastellaan Service Level Agreement (SLA) vaatimustenmukaisuuden toteutumista. Vanha viisaus "sitä saat mitä mittaat" auttaa kokemukseni mukaan toteuttamaan tilaajan tahtotilan seurattavissa prosesseissa.

Haastatteluiden ja prosessien havainnoinnin tukena poimin tapahtumamääriä käyttäjätunnustilaus- ja PAR-prosessin tapahtumista. Varmistaakseni haastateltavien antamien lausuntojen paikkansapitävyyttä tarkastelin käyttäjätunnustilausten ja PAR-avauspyyntöjen läpimenoaikoja. Läpimenoaikojen poimintaa suoritin yrityksen IT Service Management Data Warehouse raporttigeneraattorin avulla. Tapahtumamäärien havainnointiin käytin toiminnanohjausjärjestelmästä saatuja raportteja. Tarkasteltavat aineistot on poimittu pääasiassa aikavälillä 1.6.2014–31.12.2014, jos ei erikseen muuta mainita.

4.4 Toiminnan havainnointi

Osallistuvan toimintatutkimuksen työkalupakkiin sopii erinomaisesti prosessien ja tapahtumien omakohtainen ja kokemusperäinen havainnointi. Tässä menetelmässä tutkijalla on mahdollisuus osallistua itse prosessin toimintoihin ja kokea henkilökohtaisesti prosessin toiminnallisuus. Metodin hyvänä puolena on tutkijan ja luonnollisesti haastateltavien läheinen kosketus prosessin toimintaan.

Läheinen kokemus prosessiin voi toisaalta luoda tilanteen, jossa prosessin ongelmat ovat muuttuneet ominaisuuksiksi. Riskinä on, että ominaisuuksia ei osata nähdä ongelmina. Tätä huomiota voi tukea haastateltavan kommentti PAR-oikeuskäsittelyprosessin läpimenoajoista. "Jengi ei kuitenkaan ole valittanut PAR:ien läpimenosta. Onko jengi tottunut siihen että PAR on hidas. Joko ovat kyllääntyneet tai ovat tyytyväisiä. Ehkäpä pahimmat valittajat ovat löytäneet automaattisen tavan re-aktivoida PAR:it." (Haastateltava 5 2014). Kommentista voidaan tunnistaa epäily, että käytännössä prosesseja voidaan käyttää vastoin alkuperäisiä prosessin tarkoitusta tai tavoitteita.

5 Haastattelututkimus

Tavoitteenani oli kerätä käyttäjäkokemuksia henkilöiltä, jotka käsittelevät ulkoisten työntekijöiden, kuten konsulttien käyttöoikeuksia tai identiteetin hallintaprosessia. Haastatteluilla pyrin tavoittamaan käyttäjien prosessiin kohdistuvia odotuksia. Haastatteluissa sain esille mielenkiintoisia ja kehittäviä ajatuksia identiteetinhallinnan prosessien kehittämiseksi.

Haastatteluiden tukena käytin haastattelukysymyksiä, joiden perusteella jatkoimme haastateltavan kanssa vapaata keskustelua. On myönnettävä, että tiukasti samoissa kysymyksissä pysyttelevä haastattelu kaikille haastateltaville olisi ollut haastat-

telijalle helpompi menettelymalli. Vastausten jatkokäsittely ja analysointi olisi ollut yksinkertaisempaa kysymys ja vastaus menetelmän avulla. Monipuoliseksi kertynyt haastatteluaineisto antoi laajan näkymän tutkittavaan aiheeseen. Haastatteluissa käyttämäni kysymykset on kuvattu liitteessä 9.

Tilaajan toivomuksesta olen anonymisoinut lähteenä käytettyjen henkilöiden nimet ja tehtävänimikkeet. Samoin yrityksen tunnistetiedot, alkuperäisissä raporteista ja kuvakaappauksissa nähtävillä olevat käyttäjätunnustiedot tai liiketoimintaan viittaavat tiedot on sanitoitu tunnistamattomuusvaatimuksen vuoksi.

Haastateltavien mielipiteet perustuivat heidän kollegoiltaan saamiinsa tietoihin ja omakohtaisiin kokemuksiinsa. On huomattava, että haastattelussa saadut tulokset ovat henkilöiden subjektiivisia näkemyksiä, jotka perustuvat muodostuneeseen näkemykseen ja haastateltavan asenteesta syntyviin mielipiteisiin. Haastattelujen tulokset eivät välttämättä perustu mitattuun toistettavaan ja todistettavaan tietoon.

Haastateltavien vastaukset kirjasin tekstinkäsittelyohjelmalla tekstidokumenteiksi. Työstin haastatteluaineistot käyttäen haastattelujen luokitteluun teemoittelu ja tyypittelymenetelmää (Silius. 2008). Haastattelujen sisällöt jaoin käsiteltävän asian mittaisiin lauseisiin tai kokonaisuutta palveleviin osiin. Lauseista poimin samankaltaisuuksia ja tyyppejä, jotka kuvasivat yhtä asiaa tai asiakokonaisuutta. Teemoittelun tuloksena syntyneen materiaalin siirsin taulukkolaskentaohjelmaan havaitsemieni kokonaisuuksien tai tyyppien mukaan.

Tyyppeinä käytin kuvaavia termejä. Esimerkkeinä termeistä; toiminta, omistaja, ongelma, riski, kehitys, master data. Tässä yhteydessä esimerkiksi "master data" teeman alle keräsin lausuntoja, joissa otettiin kantaa henkilöydintiedon tallentamiseen. Teemoittelun avulla sain kerättyä haastateltavien yhteisiä näkemyksiä ja näin sain rekisteröityä kannanottoja tutkimuksen kysymyksien tueksi.

Siliuksen mukaan teemoittelussa pyritään pelkistämään haastatteluja ja tekstistä pyritään hakemaan koodituksen tai indeksoinnin avulla kokonaisuuksia. Käytännön ongelmien ratkaisemisessa teemoittelun on havaittu olevan toimiva ratkaisu. (Silius 2008, 4). Kokemukseni mukaan teemoittelun avulla sain rakennettua aihepiirin mu-

kaisia kokonaisuuksia. Ja kuten aiemmin totesin, teemoittelun avulla pystyin havaitsemaan ja hakemaan haastatteluaineistosta yhdistäviä tekijöitä.

5.1 Haastatteluiden satoa

Haastatteluissa pyrin hakemaan käyttöoikeuden tilaajien odotuksia tilausprosessiin, käyttöoikeuden toimittamisen oikea-aikaisuuteen ja identiteettien hallintaan. Haastatteluissa erottuivat omiksi kokonaisuuksiksi ulkoisten työntekijöiden henkilöydintiedon hallinta, sekä läpimenoaikojen ennustamattomuus normaalin käyttöoikeuden ja PAR-oikeuden tilauksessa. Esille nousi myös havaintoja konsulttien käyttöoikeuksien elinkaaren hallinnassa.

Haastatteluissa käydyissä keskusteluissa tuotiin esille myös koulutuksen ja viestinnän merkitys tiedon ja asenteiden muokkaajana. Kehitysidea konsulttitunnuksen aktiivisuuden sitomisesta sopimuksen kestoaikaan nousi esille useissa haastatteluissa.

5.2 Tunnustilauksen läpimenoaikojen ennustamattomuus

Käyttäjätunnustilauksen ja varsinkin PAR-oikeuden tilausprosessien läpimenoajat olivat useiden haastateltavien mielestä pitkiä. Erityisen harmilliseksi haastateltavat kokivat käyttäjätunnusprosessien läpimenoaikojen voimakkaan vaihtelun. Haastateltavien odotusarvot prosessin läpimenoajoille kuvaavat mainiosti nykytilannetta. "Käyttäjätunnuksen läpimenoaika vaihtelee paljon. Voi heitellä laidasta laitaan." Tämän haastateltavan toiveena oli, "Jos edes kolmessa päivässä tunnuksen voisi saada, niin olisi hyvä." (Haastateltava 5 2014).

Käyttöoikeuden tilaus- ja toimitusprosessin keston ennustamattomuus aiheuttaa työnjohdolle houkutuksen jättää tunnus aktiiviseksi. Haastatteluista kävi ilmi, että tunnuksia on jätetty tarkoituksella aktiiviseksi. Tärkein syy tunnuksen aktiiviseksi jättämiseen oli haastateltavien mielestä käyttäjätunnuksen ja pääkäyttäjäoikeuden aktivoinnin ajallinen kesto ja tunnuksen toimitusprosessin läpimenoaikojen vaihtelevuus. Haastateltava perusteli tunnuksen avoimeksi jättämistä, "Tunnuksia pidetään auki kaiken varalta, koska tunnuksen avaaminen on hidasta ja incident [häiriö] tilanteessa apua tarvitaan nopeasti." (Haastateltava 13 2015).

5.3 PAR-tilaus

Pääkäyttäjäoikeusprosessin läpimenoajat eivät haastateltavien mielestä olleet tyydyttävällä tasolla. Kuten seuraavassa haastattelun lainauksessa todetaan, "Miten paljon nyt maksetaan PAR-oikeuden odottelusta." Haastateltava on valmis rakennuttamaan prosessiin lisää automaatiota, joka on luettavissa seuraavasta ajatuksesta. "PAR läpimenoajan ennustamattomuus on riittävä syy automaation lisäämiselle." (Haastateltava 4 2014)

Useimpien haastateltavien mielestä PAR-tilauksen läpimenoaika ei vastannut System Managereiden odotuksia. Odotusarvo oikeuspyynnön kestolle käy hyvin ilmi seuraavasta kommentista. "PAR-oikeuden liittäminen tunnukseen ideaali tilanteessa yhdessä työpäivässä." sekä "Valtaosa parreista on käytössä seuraavana päivänä." (Haastateltava 4 2014) Kuitenkin sama haastateltava toteaa, "Läpi talon turhautuminen prosessin hitauteen." Edellisistä kommenteista voidaan havaita frustraatiota ja kyllääntymistä prosessin läpimenoaikojen vaihteluun ja hidasteluun.

Ulkoistuskumppanin edustajan kanssa käydyissä keskusteluissa nousi esille, että ulkoistuskumppanin agentit eivät olleet kaikissa tapauksissa kirjanneet tapahtumia asiakkaan CMDB-järjestelmään. Tapahtumien kirjaamattomuus näkyy tilaajalle

tilatun oikeuden puutteena. Tämän havainnon perusteella päätin kerätä lisätodisteita PAR-prosessin läpimenoajoista muista lähteistä. Palaan näihin tuloksiin myöhemmin.

5.4 Henkilöydintiedon hallinta

Useimmat haastateltavat kiinnittivät huomionsa ulkoisten työntekijöiden henkilöiden ydintiedon käsittelyyn. Yrityksen asiakkaiden master datan eli henkilöydintiedon todettiin sijaitsevan yrityksen asiakastietojärjestelmissä (CRM). Työntekijöiden osalta master data tiedot on talletettu henkilöstön hallintajärjestelmään (HR).

Havaintojen mukaan yritysten väliset toimeksiantosopimukset pitävät harvoin sisällään varsinaisten työntekijöiden identiteettitietoja. Haastatteluissa tuotiin esille muun muassa seuraavaa. "Sopimussuhteessa olevien henkilöiden osalta sopimustietoja on talletettu moniin kohteisiin." "Ei ole keskitettyä näkymää sopimussuhteessa olevien työntekijöiden sopimusten omistajuuteen tai kestoon." (Haastateltava 8 2014). Näistä kommenteista voidaan havaita puutteita ulkoisten työntekijöiden henkilöydintietojen hallinnassa.

Identiteetinhallinnan kannalta erottava tekijä yrityksen varsinaisiin työntekijöihin on, että heitä ei ole rekisteröity yrityksen HR-järjestelmään. "Konsulttien sopimukset jäävät oletusarvoisesti liiketoiminnan ja konsultin palkanneen henkilön tiedoksi. Sopimuksen tekohetkellä on harvoin tiedossa työhön konkreettisesti osallistuvien henkilöiden tietoja." (Haastateltava 7 2014). "Sopimustietokanta puuttuu, mistään ei kumuloidu sopimuksen tai käyttäjätunnuksen kestoja." (Haastateltava 1 2014). "Tiedot löytyvät omasta sopimuksesta, jos olen itse palkannut konsultin." (Haastateltava 4. 2014).

Käyttöoikeuksien käsittelyn osalta todettiin seuraavaa. "Esimiehen tai yrityksen managerin velvollisuus on ilmoittaa työsuhteen päättämisestä. HR-järjestelmä tuo

sen edun, että työsuhteen päättyessä tunnus voidaan sulkea automaattisesti. Jos poislähtevän työntekijän tunnarit jäävät roikkumaan, niin on mahdollista, että käyttäjä pääsee tunnuksillaan kiinni [yrityksen tietojärjestelmiin] etäkäyttöyhteyden kautta." (Haastateltava 7 2014). Edellä olevasta kommentista voidaan tunnistaa esimiehen tai managerin vastuu tunnuksen sulkemiseen työsuhteen päättymisessä. Työsuhteen päättäminen katkaisee automaattisesti käyttöoikeudet vain henkilökuntaan kuuluvalta henkilöltä. Konsultin tunnuksien etäkäyttömahdollisuus jatkuu, jos esimies tai manageri ei tilaa tunnuksen sulkemista.

Tähän samaan ongelmaan on kiinnittänyt huomiotaan myös yrityksen käyttämä ulkoinen tilintarkastusyhtiö. Tilintarkastusraportissaan "Corporate IT Service management letter 2013" tilintarkastus on antanut korjausehdotuksia ja suosituksia käyttäjäoikeuksien käsittelyyn. Raportissa kuvataan muun muassa huomioita ja riskejä konsulttien AD-käyttäjätunnusten sulkemismenettelyissä. Tilintarkastusraportissa suositellaan kehittämään ja automatisoimaan muutoksenhallinnan prosesseja ja toimintamalleja. Raportissa annetaan muun muassa suositus poistaa turhat ja käyttämättömät tunnukset välittömästi käyttötarpeen päätyttyä.

5.5 Käyttäjätunnuksen elinkaari

Oletukseni ulkoisten työntekijöiden käyttäjätunnuksen elinkaaren hallintaan liittyviin epävarmuuksiin ovat haastattelujen analyysissä paljastuneet todelliseksi. Näyttää vahvasti siltä, että yrityksen tietoturvapolitiikan vaatimus vähimmän käyttöoikeuden vaatimuksesta ei kaikissa käyttötapauksissa täyty. Ulkoisten palveluntuottajien palvelusopimuksien päättyminen ei käynnistä automaattista konsulttien käyttäjätunnuksen sulkemista. Esimiesohjeiden mukaan työsopimuksen päätyttyä vastuu tunnuksen sulkemisen tilaamisesta on yrityksen managerilla.

Haastatteluiden perusteella voidaan olettaa, että konsulttien tunnuksia voi jäädä tahattomasti avoimeksi. Joissakin tapauksissa haastateltavat kertoivat ongelmana olevan, että sopimuskumppanit eivät ilmoita konsultin työsopimuksen purkautumisesta. "Konsultin työsuhteen päättyessä ei välttämättä ilmoiteta mihinkään." (Haastateltava 5 2014). Haastatteluissa nousi esille seuraava toteamus olemassa olevasta tilanteesta, "Konsulttitunnuksia suljetaan harvoin heti välittömästi [työn päättymisen jälkeen]." (Haastateltava 5 2014). Palvelusopimuksessa olevista puutteista kumpuava ongelma nousee esille seuraavassa kommentissa, "Poislähtevistä konsulteista saadaan harvoin tietoa." (Haastateltava 4 2014). Kehitystoiveena tämän ongelman poistamiseksi esitettiin teknistä kontrollia, "Voisiko konsultin tunnuksen [päätymisen] kytkeä sopimuksen elinkaareen." (Haastateltava 4 2014).

Kuten haastateltava seuraavassa kehitysideanaan esittää, "Tunnus automaattisesti disabloidaan, jos tunnusta ei ole käytetty viiteen viikkoon. Jos tunnus disabloidaan, niin enabloimisen on oltava nopea ja tapahduttava soitolla tai automaattitoiminnalla." (Haastateltava 9 2014). Vaikka haastateltava suosittelee asentamaan automaattilukituksen käyttämättömälle tunnukselle, niin on huomattava, että tunnusten automaattinen lukitus lyhyissä työsuhteissa voi olla resurssien käytettävyyden kannalta haastavaa. Kuten haastateltava toteaa on käyttämättömien tunnusten automaattinen lukitseminen ja samalla tunnuksen nopea palautus mahdollisuus eräs tapa kontrolloida ulkoisten työntekijöiden tunnusten käyttöä.

Tunnuksen sulkemattomuus voi aiheuttaa tilanteen, jossa irtisanotun konsultin käyttäjätunnus on aktiivisena yrityksen järjestelmiin. Tätä kautta ex-konsultilla on käyttöoikeuksien mukainen suora pääsyoikeus liiketoimintasovelluksiin tai vaikkapa avoimena olevan projektin suunnittelutietoihin. Tämä on selkeä tietoturvariski, joka on pyrittävä poistamaan järkevillä ja toimivilla kontrolleilla. Aktiivisena olevat käyttämättömät tunnukset aiheuttavat oikeutettua huolta haastateltavissa. Konsulttitunnusten sulkemattomuus työvelvollisuuden päätyttyä on selkeästi riski ja Akilleen kantapää yrityksen käyttöoikeuksien hallinnassa.

5.6 Havaintoja identiteetin hallinnasta

Havaintojeni mukaan yrityksen hallussa oleviin identiteetteihin liittyy erilaisia näkökulmia. Yrityksen hallinnollinen IT (CIT) tarkastelee henkilöidentiteettiä liiketoiminta-arkkitehtuurin kannalta. Henkilöstöhallinto katsoo identiteettejä pääasiassa varsinaisen työntekijän identiteetin ja henkilön tunnistamisen näkökulmasta. IT-palveluyksikkö tunnistaa käyttäjän teknisenä objektina ja identiteetinhallinnan teknologia-arkkitehtuurin näkökulmasta. Liiketoimintojen sovellustenomistajat taas katsovat henkilöiden identiteettejä liiketoiminnan sovellusten käyttöoikeuksien näkökulmasta.

Käyttöoikeuden tilausprosessin käynnistäminen, käyttöoikeuden muutokset ja päättämisen tilaaminen ovat linjajohdon vastuulla. Työnjohdollisesta näkökulmasta prosessien ongelmien tunnistaminen ja prosessin automatisoinnin oletetaan antavan lisäarvoa käyttöoikeushallinnan toimintoihin. Haastatteluissa nousi esille huomioita ulkoisen tarkastuksen antamista huomautuksista konsulttitunnusten käsittelyssä. Seuraava kommentti kokoaa useiden haastateltavien huomiot auditoinnin palautteista. "Audit [ulkoinen toiminnan tarkastelu] rokottaa joka vuosi konsulttitunnuksien hallinnasta." (Haastateltava 9 2014). Yrityksen käyttämä ulkoinen tilintarkastus on kiinnittänyt huomionsa konsultointisopimusten päättymisen yhteydessä epämääräiseksi ajaksi avoimeksi jääviin käyttäjätunnuksiin. Auditoijataho on kirjannut tämän toiminnan tutkimusraporttiin poikkeamaksi hyviin käytäntöihin ja on antanut kehotuksen korjata toimintatapoja tai prosesseja.

Konsulttien identiteettien hallinnan osalta on nähtävissä, että ulkoisten työntekijöiden henkilöydintietojen hallinta on jäänyt paikallisten työnjohtajien oman aktiivisuuden ja ammattitaidon varaan. Esimerkiksi manageri- tai esimiestietojen paikkansa pitävyyteen ei voi kaikissa tapauksissa luottaa. Konsulttien henkilöydintietoja käsitelleessä keskustelussa sain esille muutaman henkilöydintietojen ylläpitoa kuvaavan kommentin. "Tällä hetkellä tällaista konsultti Master Dataa ei ole." (Haastateltava 7 2014).

Haastateltava kertoi konsulttien identiteetin tallettamisesta HR-järjestelmään seuraavaa. "We do register some consultants in HR system today but that is when you have a specific need e.g. acting as a manager for employees." Joidenkin esimiesasemassa toimivien konsulttien tietoja on viety HR-järjestelmään. (Haastateltava 14 2015). Tästä lausunnosta voidaan nähdä, että HR-järjestelmässä on valmius tallettaa konsulttien henkilöydintietoja.

HR-järjestelmässä on käytössä erilaisia syötettävän tiedon laatuun liittyviä varmistuksia. Seuraavassa kommentissa kerrotaan HR-järjestelmän tietojen laatukontrolleista. "The principle regarding employment is that you have to have a valid contract, a valid manager and proper contact information. There are also a lot of processes to follow up the data quality of the registered data." (Haastateltava 14 2015). Tietojen syöttämisen yhteydessä varmistetaan seuraavat tiedot; sopimus-, manageri- ja yhteystiedot on syötettävä järjestelmään työntekijän tietoja perustettaessa. Tietojen syöttämisen yhteydessä syötettävän tiedon laatua valvotaan prosessin eri vaiheissa.

Työsuhteen päättyessä suoritetaan automaattisia de-provisiointi toimenpiteitä. "When employment ends certain action will also be executed e.g. sending the status terminated to IT systems in an automated fashion. This automation I guess is what you strive for related to the consultants." (Haastateltava 14 2015). Tämän perusteella voin olettaa, että konsulttien identiteetinhallinta toimisi teknisenä suorituksena HR-järjestelmässä. Jos tekninen toteutus onnistuisikin, niin prosessin kannalta tilanne ei ole niin yksinkertainen, kuten seuraavasta kommentista voin päätellä. "I guess if the process is defined how things should be handled a tool like HR-system could possibly help but would in our case be a new scope of usage." (Haastateltava 14 2015). Kommentin mukaan konsulttien käyttöoikeuksien siirtäminen käsiteltäväksi HR-järjestelmään olisi HR-toiminnoille uusi aluevaltaus. Tämän saman huomion vahvisti myös HR-yksikön prosessivastaava haastattelussaan. Myös hänen mukaansa HR-järjestelmällä on valmius käsitellä konsulttien identiteettejä. Hänen kertomansa mukaan tällä hetkellä muutamien konsulttien identiteetit on talletettu HR-järjestelmään.

Ulkoisen työntekijän käyttäjätunnuksen käyttöoikeuden jatkaminen tapahtuu automaattisesti kuuden kuukauden välein. Päätös käyttöoikeuden jatkamisesta on konsultin managerilla. Kuten aiemmista kommenteista on voitu havaita tunnuksia voidaan pitää aktiivisena tilanteita varten, joissa konsultin palveluksia tarvitaan nopeasti. Tähän toimintaan lienee osaltaan johtanut käsitys käyttäjätunnuksien tilausprosessin hitaudesta. Tunnuksien auki pitäminen ilman toimittajan ja asiakkaan välistä sopimusta ja työvelvoitetta ei ole hyvien tietoturvakäytäntöjen mukaista toimintaa. Sopimuksettomassa tilassa olevien ulkoisten työntekijöiden rekisteröinnissä yhtiön järjestelmiin, voidaan nähdä vastakkainasettelu myös henkilötietolain henkeä vastaan (Henkilötietolaki 1999/523).

5.7 Tiedon laatu

Tällä hetkellä ei ole käytössä kattavaa käyttöoikeuksien raportointia. Käyttöoikeusnäkymien puuttuminen on johtanut tilanteeseen, jossa vaarallisten työyhdistelmien hallinta pyritään toteuttamaan sovellustasolla. Sama ongelma toistuu myös asiakirja-arkistojen kohdalla. Tutkiessani jaettujen hakemistojen omistajuuksia, hämmästyin orpojen hakemistorakenteiden suuresta (23000) määrästä. Tästä on seurauksena, että hakemiston käyttöoikeuden saamisessa IT-henkilökunnan on tehtävä manuaalista selvitystyötä omistajuuden ratkaisemiseksi. Sillä aikaa tiedon tarvitsija käy tyhjäkäynnillä ja odottaa käyttöoikeuksia tarvitsemaansa tietoon. Tämä on konkreettinen esimerkki ydintiedon laatupoikkeamasta. Tiedon omistajuuden puuttuessa aineiston käyttöoikeuden selvittelyyn kuluu manuaalisena selvittelytyönä aikaa ja resursseja. Selvitystyön aikana tieto ei ole käytettävissä tiedon tarvitsijalle.

Vastuussa olevan managerin ja työntekijän välillä oleva kytkentä voi kadota. Syyksi tähän paljastui automaation puuttuminen identiteetinhallinnassa. Konsultin työtehtävien muuttuessa tai palkkaavan liiketoiminnan vaihtuessa managerin tieto ei vaihdu automaattisesti. Tilanteessa, jossa managerilla on kymmeniä konsultteja

hallinnollisina alaisinaan, on riskinä että manageri ei tiedosta konsulttien työtehtävien vaihtumista tai päättymistä. Osittain tämän hallinnollisen esimiesroolin tuloksena konsulttien tunnuksia voidaan pitää yllä tarpeettomasti.

Haastatteluissa nousi esille eräs mielenkiintoinen relaatio manageritiedon ja konsulttitunnuksen välille. Haastateltavan 4 mukaan "Murhe on siinä että, kun konsultin manageri poistuu, niin meillä ei ole mitään tapaa kontrolloida konsulttitunnuksen poistamista. Kontrollimekanismi yrityksen palveluksesta poistuneen managerin ja konsulttitunnuksen väliltä puuttuu. Riskinä on että tunnus jää auki pitkäksi ajaksi". Tämä kommentti tukee myös tiedon laadussa olevia poikkeamia. Teknisten kontrollien ja automaation puute aiheuttavat edellä kuvattuja ongelmia henkilöydintiedon laatuun.

Konsultin palkkaavalla henkilöllä on luonnollisesti paras tieto konsultin työsopimuksen kestoajasta, kuten seuraavasta kommentista voidaan päätellä. "Ainoastaan konsultin palkkaaja tietää milloin konsultti aloittaa työn tekemisen ja kuinka kauan hän on työssä ja milloin tunnus on tarpeen poistaa." (Haastateltava 9 2014). Esimiesten käytössä ei ole keskitettyä konsulttien henkilöydintietokantaa. Tästä johtuen esimiehet tai managerit ovat järjestäneet sopimushallinnan ja vuokratyöntekijöiden identiteetinhallinnan parhaaksi katsomallaan tavalla. Esimiesten suorittama ydintiedon hallinta omissa paikallisissa järjestelmissään tuottaa samaa tietoa käsitteleviä tietovarastoja eripuolille organisaatiota.

Haastatteluissa nousi esille toive sopimuksen sulkemispäivämäärän tallettamisesta esimerkiksi tunnuksen tilauksen yhteydessä. "Tunnuksen sulkemispäivämäärä olisi uusi ominaisuus, jonka toiminta on määriteltävä, rakennettava ja implementoitava. Tavoitteena on, että konsulttitunnus disabloidaan sopimuksen päättymispäivänä." (Haastateltava 2 2014). "Koska sopimustietokanta puuttuu, niin mistään ei kumuloidu sopimuksien tai käyttäjätunnuksen kestoja." (Haastateltava 1 2014). Haastateltava 4 totesi seuraavaa. "Usein tiedetään sopimuksen päättymispäivä.", "Konsulttitunnuksia suljetaan harvoin heti välittömästi työn päätyttyä." ja "Konsulttisopimuksia ei kirjata keskitetysti mihinkään." Lisäksi haastateltava esitti seuraavan toi-

vomuksen, "Konsulttisopimuksessa on oltava sopimuksen aikaikkuna ja sopimuksella on oltava selkeä omistajuus." (Haastateltava 4 2014).

Edellä havaituista kommentista voidaan päätellä, että sopimuksen päättymispäivän tietoja ei kirjata tai sopimuksen päättymispäivää ei käytetä käyttöoikeuden automaattisen päättämisen tukena. Havaintojeni mukaan ITSM-lomakkeella on tunnusta tilatessa mahdollista syöttää tunnuksen päättymispäivä (termination date). Tämän ominaisuuden avulla tunnus on teknisesti mahdollista sulkea automaattisesti sopimuksen päättymispäivänä.

5.8 Haastatteluiden lopuksi

Ojasalo et al. mukaan haastattelun tulosten analysointia voidaan suorittaa haastatteluaineiston teemoittelun ja sisältöanalyysin avulla. Haastattelujen analysoinnin tavoitteena on määritellä mitä toimintoja ja tavoitteita yrityksessä pidetään prosessin toiminnan kannalta tärkeinä menestystekijöinä. (Ojasalo et al. 2009, 124). Haastatteluiden analysoinnin ja teemoittelun avulla pystyin nostamaan esille ongelmakohtia, selkeitä kehityskohteita ja haastateltavien yhteisiä toiveita prosessien tuotosten kehittämiseksi. Teemoittelutekniikan avulla yksinkertaistin ja selkeytin haastattelumateriaalia. Sain nostettua haastatteluista näkyviin tutkimusongelmien kannalta olennaisia aiheita. Kokemukseni mukaan haastateltavat osallistuivat innokkaasti haastatteluihin. Havaintojen perusteella he kokivat omalla panoksellaan kehittävänsä yrityksen käytössä olevia prosesseja. Haastateltavien panos työssä saatuihin tuloksiin on ollut merkittävä.

5.9 Vertailututkimus

Karjalaisen esityksen mukaan "Mitä benchmarking on". Benchmarking-arviointi sisältää vertailua ja kiinnostusta muiden suoriutumiseen kiinnostuksen kohteena olevassa toiminnossa (Karjalainen 2002). Vertailevaa tutkimusmetodia tai benchmarking-arvioinnin perustaa käytin keskusteluissa samalla alalla toimivien tai samansuuruisten yritysten edustajien kanssa.

Tutkimuksellisena välineenä käytin epävirallista elävää keskustelua. Keskusteluita en nauhoittanut tai tallentanut elektroniseen muotoon. Käytyjen autenttisten keskustelujen avulla sain koottua yleisnäkymää ja käsitystä muiden alalla toimivien yritysten identiteetinhallinnan metodeista ja käytännön toteutuksista. Sain hyvän yleiskuvan keskusteluissa mukana olleiden henkilöiden lausunnoista eri yritysten toimintatavoista, IAM-toiminnoista ja henkilöidentiteettien hallintapolitiikoista.

5.10 Toimittajaesittelyt

Tutkimusaiheen perustietojen kokoamisvaiheessa kutsuin yritykseen vierailulle identiteetin hallintatuotteita edustavia ja suunnittelupalveluita tarjoavia yrityksiä. Esitykset antoivat hyvän näkymän identiteettihallinnan nykytilanteesta ja toiminnan kehittämisen suunnista yleisellä tasolla. Oman näkemyksensä identiteetinhallintaan ja IAM-palveluihin ovat tämän selvitystyön tueksi käyneet esittämässä RSA, Propentus, Panorama, Nixu ja HP.

5.11 Kyselytutkimus

Tutkimuksen alussa valmistelin laajaa esimieskäyttäjille suunnattua kyselytutkimusta Webropol-työkalulla. Haastatteluissa esille nousseiden huomioiden ja saamani palautteen perusteella, päätin jättää laajan kyselytutkimuksen tässä yhteydessä toteuttamatta. Perustelen päätöstäni sillä, että kahdenkymmenen asiantuntijan ja esimiestasoisen henkilön haastattelut ovat tuoneet esille tutkimusalueen ydinongelmat. Päätökseni laajan kyselytutkimuksen peruuttamisesta osoittautui myöhemmin oikeaksi päätökseksi. Ydinhenkilöille suunnatuilla haastatteluilla ja pienemmällä otoksella sain haastatelluilta hyvin kattavan näkemyksen varsinaisten tutkimusongelmien löytämiseksi.

6 Tapausmäärät ja läpimenoajat

Tässä luvussa tarkastelen prosessien näkökulmasta kerättyjä ja mitattuja tapahtumamääriä ja läpimenoaikoja. Haastateltavien mielestä tarkasteltavassa prosessissa on hitautta. Päätin vahvistaa haastattelujen antamia vaikutelmia havainnoimalla todellisia tapahtumamääriä ja prosessien läpimenoaikoja.

Tapausmäärien ja läpimenoaikojen tutkimuksessa käytin apuna yrityksen ERP- ja CMDB-järjestelmiin kirjattuja tapahtumia. Työtilausten läpimenoaikojen tutkimuksessa tapahtumien aloitus ja päättymishetkien analysoinnin avulla pyrin saamaan esille prosessin todellisia suoritusaikoja. ERP-järjestelmän tuottamien raporttien avulla selvitin käyttäjä- ja tapausmääriä.

Työkaluina prosessin tapausmäärien ja läpimenoaikojen seurantaan ja mittaamiseen käytin IT Service Management Data Warehouse (liite 1) raporttigeneraattoria

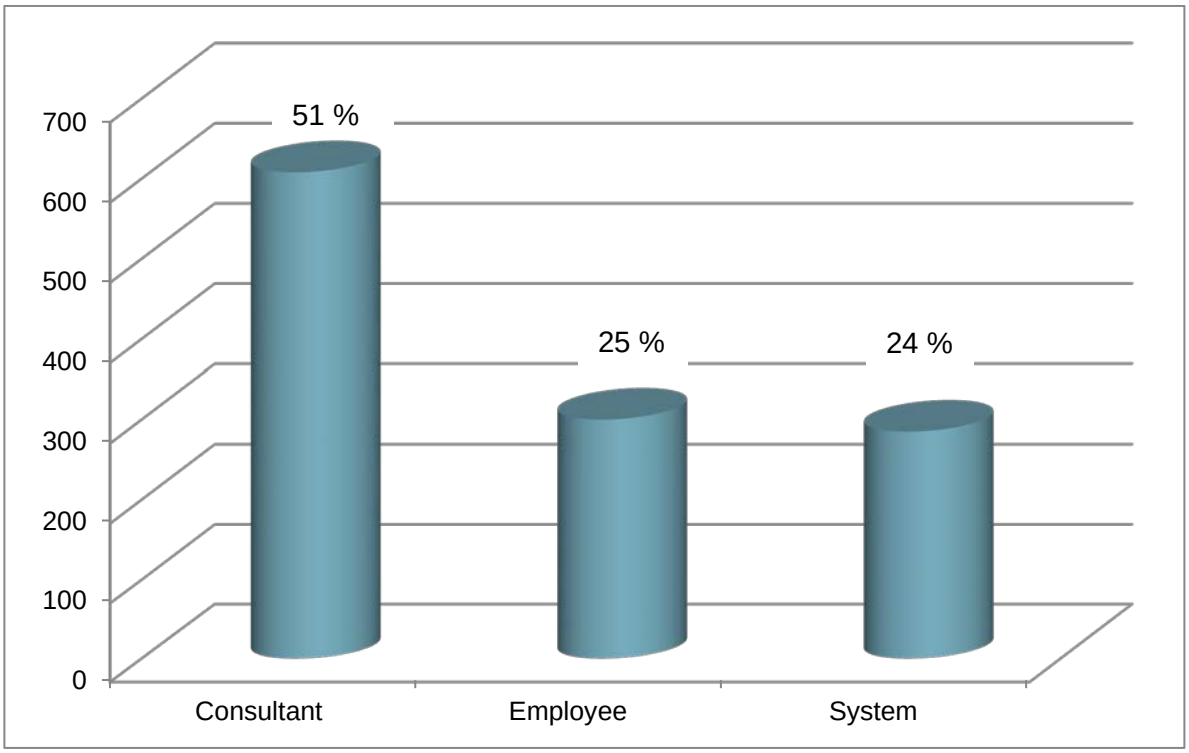
ja kuukausittain CMDB-järjestelmästä tuotettavia käyttäjä-, työasema- ja PAR-raportteja. Nämä raportit ovat saatavilla yrityksen intranetissä. Raporttien tietojen esittelymuodon muokkaamiseen käytin Excel, PowerPoint ja OneNote 2010 ohjelmia.

6.1 Ulkoistuskumppanin PAR-tunnukset

Yrityksen käyttäjätunnusraporttia tutkiessani havaitsin, että ulkoistuskumppanin käytössä olevia pääkäyttäjätunnuksia ei ole kirjattu yrityksen CMDB-tietokantaan palvelimen lisätietoihin. Nämä pääkäyttäjätunnukset ovat haettavissa yrityksen AD-järjestelmästä. Yrityksen AD:sta keräämieni tietojen mukaan ulkoistuskumppanin käytössä on lähes 1400 Consultant tyyppistä käyttäjätunnusta. Näistä tunnuksista noin 960 oli tarkoitettu ulkoistuskumppanin suorittamiin palvelimien pääkäyttäjätehtäviin.

Ulkoistuskumppanin pääkäyttäjätunnuksien rekisteröimättömyys CMDB-järjestelmän PAR-tietoihin vääristää poimittavia PAR-raportteja. Käyttöoikeushallinnan ja seurannan kannalta on huomattava, että ulkoistuskumppanin pääkäyttäjäoikeudet ovat raportoitavissa vain yrityksen AD-järjestelmästä. Palvelimien pääkäyttöön tarkoitetut PAR-tunnukset upotetaan tyypillisesti palvelimen local security ryhmiin. Näiden sisältö avautuu porautumalla AD:n kautta ryhmän aliryhmiin sijoitettuihin käyttäjätunnuksiin. Tämä raportointitapa on kankea ja vaivalloinen järjestelmistä vastuussa oleville system managereille.

Mielestäni ulkoistuskumppanin identiteettitietojen tallettaminen ainoastaan AD:hen, piilottaa todellisuudessa ulkoistuskumppanin pääkäyttäjät system managereilta. Järjestelmästä vastuussa olevat henkilöt eivät voi helposti saada nähtävilleen kenellä ulkoistuskumppanin henkilökunnasta on pääkäyttäjätasoiset käyttöoikeudet vastuullaan olevaan palvelimeen ja sitä kautta tietojärjestelmän tietoihin.



Kuvio 4. PAR-oikeuksien jakauma käyttäjätyypeittäin. (CMDB 2014).

Kuvion perusteella pääkäyttäjäoikeuksia on konsulttien käytössä 51 % ja työntekijöiden käytössä 25 % kaikista luovutetuista pääkäyttäjäoikeuksista.

Näiden havaintojen pohjalta halusin selvittää olemassa olevien henkilöydintietojen oikeellisuutta. Erityisenä tarkastelun kohteena ovat käyttäjätunnuksen esimiestieto ja sopimuksen päättymispäivä. Tarkastelun perusteella 4 %:lle konsulttityypin pääkäyttäjätunnuksille ei ole merkitty yrityksen esimies- tai manageritietoa. Tarkemmassa tarkastelussa nousi esille, että yrityksen manageritieto puuttuu säännöllisesti ulkoistuskumppanin käytössä olevilta käyttäjätunnuksista.

Käyttäjätunnusobjektien aloituspäivämäärä, käyttäjätunnuksen muutospäivä, viimeinen kirjautumispäivä ja tunnuksen automaattinen vanhenemispäivämäärä oli rekisteröity 99 %:ssa tapauksista. Konsultointisopimusten päättymispäiviä ei ollut rekisteröity käytössä olevaan koontiraporttiin. Ulkoistuskumppanin pääkäyttäjätyöhön käyttämiä tunnuksia oli kirjattu yrityksen CMDB-järjestelmään kaikkiaan neljä kappaletta. Todellisuudessa ulkoistuskumppanin työntekijöitä on monikertainen

määrä. Tutkimuksen perusteella voidaan havaita, että ulkoistuskumppanin käytössä olevien tunnusten tiedon laatu ei ole samalla tasolla kuin muiden ulkoisten työntekijöiden tietojen laatu.

6.2 Aktiiviset tunnukset

Pyrin varmistamaan haastatteluissa esille noussutta havaintoa käyttämättömien tunnusten jättämistä avoimeksi. Konsulttien käytössä olleista tunnuksista on ollut käyttämättömänä viimeisen kolmen kuukauden aikana 35 %. Prosenttiluku muodostuu konsulttien normaalitunnuksista 29 % ja pääkäyttäjätunnuksista 6 %. Työntekijöiden tunnuksista käyttämättä on ollut 6 % (Taulukko 2).

Taulukko 2. Tunnusta ei ole käytetty viimeiseen kolmeen kuukauteen (CMDB 2014).

Luokka	Prosenttia tunnuksista
Työntekijä	6 %
Konsultti	35 %
Yhteiskäyttö	47 %
Other	67 %

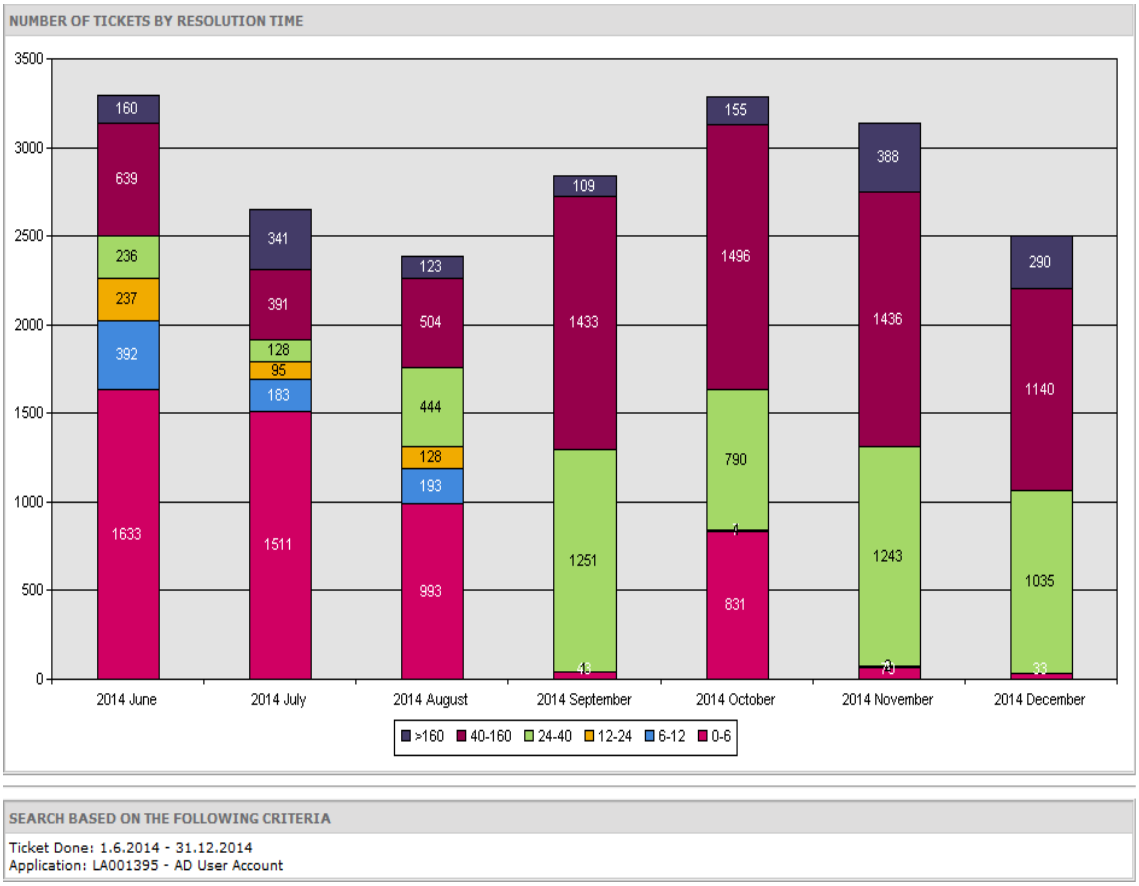
Edellä esitetty taulukko tukee haastatteluissa esille noussutta väitettä tunnusten avoimena pitämiseen. Konsulttien henkilökohtaisia tunnuksia ja yhteiskäyttöisiä tunnuksia on pidetty aktiivisina ilman todellista jatkuvaa käyttötarvetta.

6.3 Käyttöoikeuden hallintaprosessi

Tässä tutkimuksessa kiinnostuksen kohteena olevat konsulttien tai partnereiden käyttöoikeuden tilaaminen, muutos ja päättäminen tapahtuvat saman prosessin avulla, kuin varsinaisen työntekijänkin käyttöoikeuden tilaaminen. Käyttöoikeuden hallintaprosessi (Access Management) on esitelty tarkalla tasolla liitteessä 2 Käyttäjätunnuksen tilausprosessista (AD User Account) poimitun raportin perusteella pyyntöjä oli seuranta-aikana (1.6.–31.12.2014) tehty 20089 kappaletta (kuva 1). Tavoitteeni oli havaita käyttäjätunnuksien tilauksien määriä ja pyyntöjen todellisia läpäisyaikoja. Olin hyvin epäileväinen saamaani tulokseen perustuen tapahtumien suureen määrään.

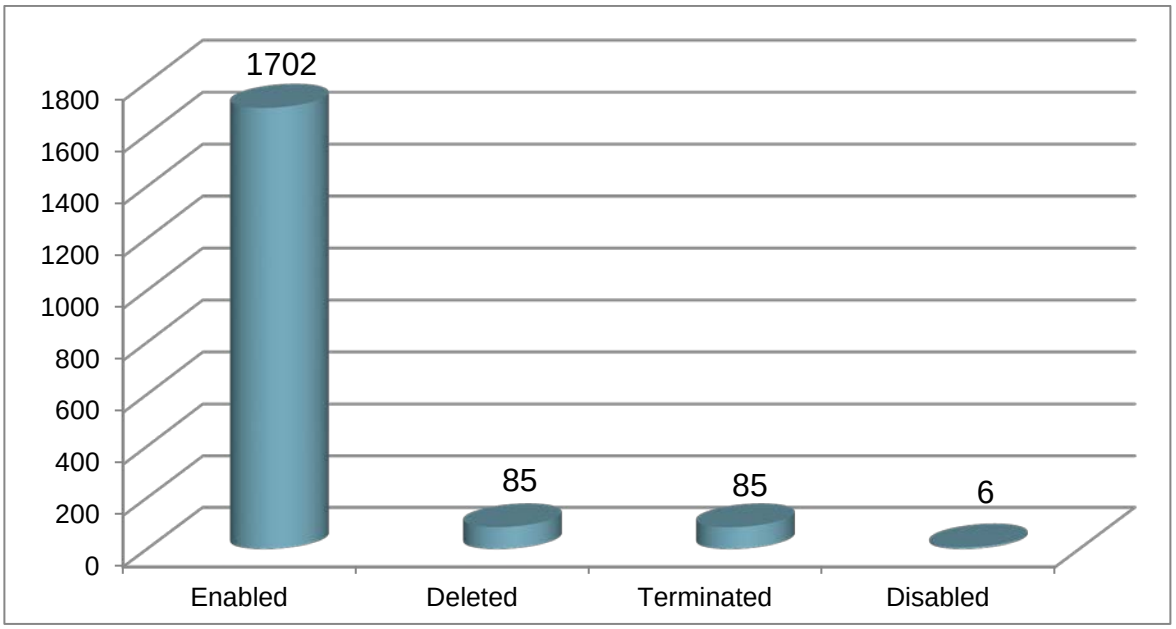
Kuva 1. AD User Account jonossa käsiteltyjä tapahtumia 1.6.–31.12.2014 välisenä aikana. (CMDB 2015).

Kuvassa esitetty tapahtumien keskimääräinen läpäisyaika 59,9 tuntia on kalenteriaikana noin seitsemän ja puoli työpäivää. Lähestyin läpäisyaikojen tarkastelua edelleen kuvion 5 avulla. Tässä esitetään AD User Account työjonoon liittyvien toimenpiteiden vaihteluvälejä. Merkille pantavaa on pitkien toimitusaikojen suuri määrä. Otetaan esimerkkinä vaikkapa joulukuu 2014 jolloin 290 työpyyntöä oli kestänyt yli 160 tuntia. Tämä tarkoittaa yli 20:tä työpäivää. Samansuuntainen näkymä on havaittavissa myös marraskuussa, jolloin 388 työpyyntöä oli viettänyt jonossa yli kaksikymmentä työpäivää. Tämäkään tarkastelukulma ei paljasta yksittäisen käyttäjätunnuksen käsittelyyn kuluvaa aikaa. Näkymä antaa kuitenkin osviittaa haastatteluissa esille tulleille huomioille ennustamattomista käsittelyajoista.



Kuvio 5. Käyttäjätunnukseen liittyvien tehtävien käsittely- ja läpimenoaikoja ajalla 06 – 12 / 2014. (CMDB 2015).

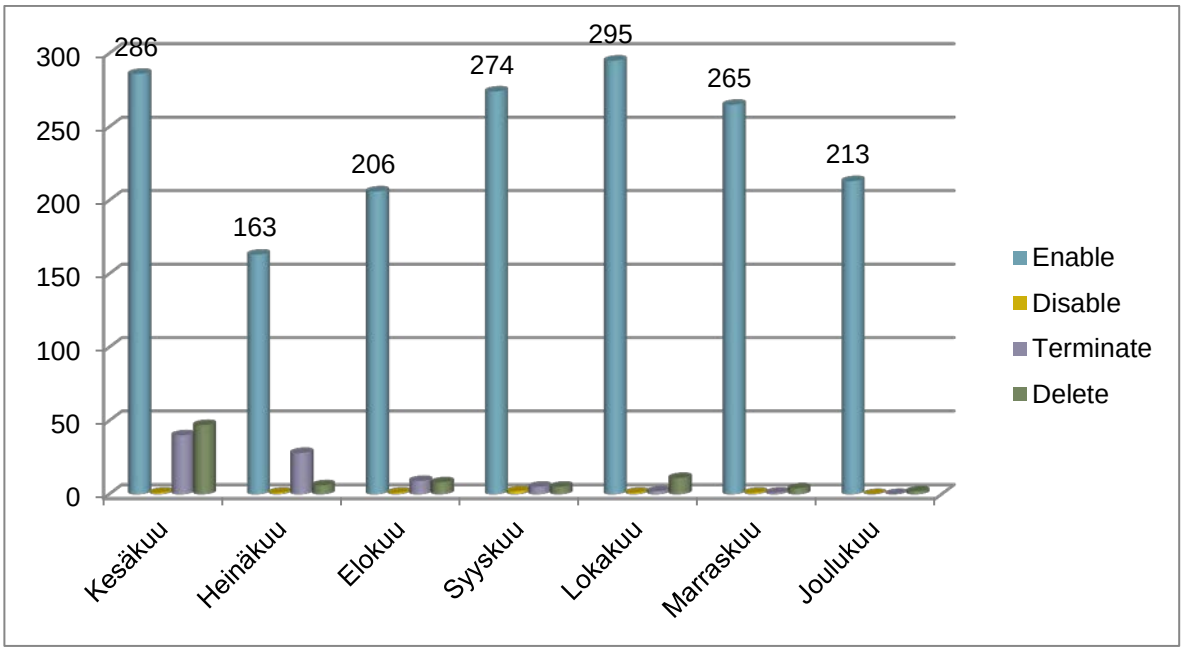
Uusien käyttäjätunnuksien avausmäärät saadaan luotettavasti esille kuukausittain julkaistavista CMDB-raporteista (All_UserIDs_2015-01-01). Vuoden 2014 kesäkuun ja joulukuun 2014 väliseltä ajalta raportista poimittujen tapausmäärien mukaan tunnuksia oli perustettu kaikkiaan 1702 (taulukko 2). Kuviossa 6 esitetään uusien perustettujen käyttäjätunnusten käsittelymääriä. Kuviossa esitellään luotujen (enabled), lukittuun tilaan siirrettyjen (disabled), terminoitujen (terminated) ja tuhottujen (deleted) käyttäjätunnusten tapahtumamäärät kesäkuusta joulukuuhun 2014.



Kuvio 6. Käyttäjätunnusten käsittelymäärät ajalla 06 – 12 2014. (CMDB 2015).

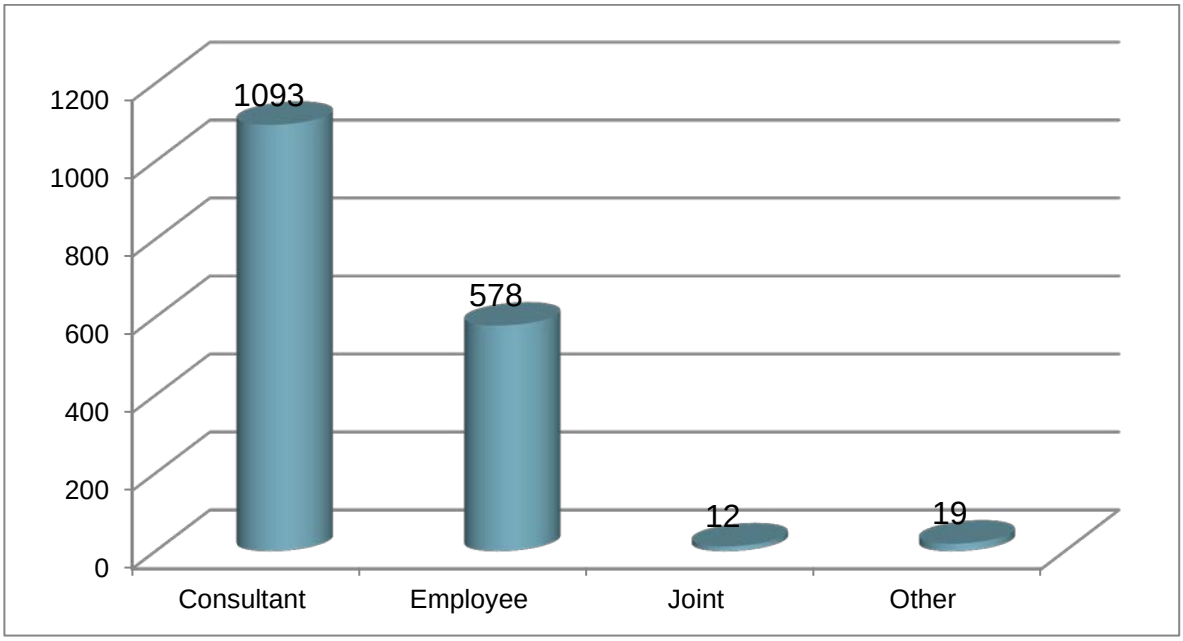
Tässä yhteydessä enabled tila ilmoittaa uusien luotujen käyttäjätunnusten määrän. Disabled tilassa tunnus on asetettu lukittuun tilaan joko IT Service Desk agentin toimenpiteillä tai yleisimmin kirjoittamalla salasana väärin. IT Service Desk agentti voi aktivoida tunnuksen merkitsemällä käyttäjän AD-tiedoissa tunnuksen aktiiviseksi. Terminated tilassa aiemmin disabloitu käyttäjätunnus on siirretty AD:n Disabled OU rakenteeseen odottamaan lopullista tuhoamista. Tunnuksen palauttaminen aktiiviseksi enabled tilaan vaatii IT Service Desk agentin manuaalisia toimenpiteitä. Tunnuksen tuhoamisessa (Deleted) käyttäjätunnus poistetaan kokonaan ja lopullisesti AD:stä. Samalla tunnuksen kotihakemisto poistetaan yrityksen tietojärjestelmästä. (Haastateltava 3 2015).

Kuvio 7 esittää kuukausittaiset käyttäjätunnuksiin liittyvät tapahtumamäärät. Käyttäjätunnuksia on kuukausittain perustettu keskimäärin 243 kappaletta.



Kuvio 7. Kuukausittainen käyttäjätunnuskäsittelyn jakauma. (CMDB 2015).

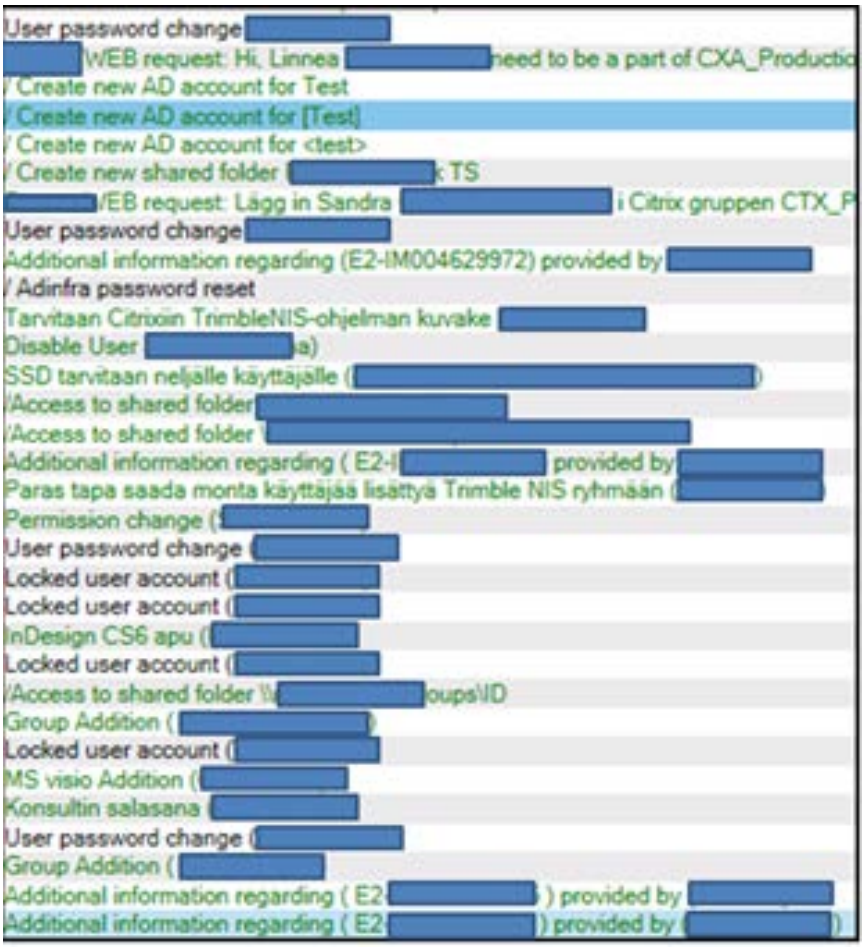
Päätin tarkastella tarkastelujaksolla (06 – 12 / 2014) suoritettuja käyttäjätunnuksien avaamisia käyttäjätunnustyypeittäin. Kuviossa 8 voidaan havaita, että uusia tunnuksia on avattu yhteensä 1702 kappaletta. Konsulttitunnuksia on 1093 kappaletta ja työntekijätunnuksia 578 kappaletta. Muita tunnuksia oli avattu yhteensä 31 kappaletta.



Kuvio 8. Uusien tunnuksien avausmäärät ajalla 06 – 12 / 2014. (CMDB 2015).

Avausprosessin läpimenoajan mittaaminen osoittautui haastavaksi tehtäväksi. Keskusteluissa nousi esille seuraava kommentti. "Työjonossa AD User Account käsitellään myös muita käyttäjätunnuksiin liittyviä töitä" (Haastateltava 3 2015). Tämän lausuman mukaan käyttöoikeustilaukseen käytettävän tarkan ajan selville saaminen on hyvin vaikeaa. Pyysin tämän väitteen tueksi vielä asiantuntijalausunnon prosessihallinnosta. Saamani vastauksen mukaan "AD User Account -applikaatiolle kirjataan kaikki tiketit, jotka ko. palveluun liittyvät. Suurin osa on muita kuin uusien avauspyyntöjä. Edelleenkään emme saa heiltä [ulkoistuspartneri] oikeita tikettien valmistumisajankohtia, joten mikään tilasto meillä ei pidä paikkaansa ulkoistuskumppanin tikettien osalta." (Haastateltava 8 2015).

Edellä olevien lausumien tueksi poimin hetkellisen näkymän yrityksen AD User Account työjonoon (kuva 2). Kuvassa esiintyvistä työpyyntöjen otsikoista voidaan päätellä jonossa käsiteltävän laajasti käyttöoikeuksiin ja myös muihin käyttäjien tarpeisiin liittyviä työtehtäviä. Haastateltavalta 8 saamieni tietojen mukaan, tällä hetkellä yrityksellä ei ole mahdollisuutta luotettavasti mitata käyttäjätunnusten avausaikojen SLA-tasoa käytössä olevilla välineillä. Kriittinen suhtautuminen tutkimuksessa saatuihin tuloksiin, tuotti myös uutta taustatietoa ulkoistuskumppanin palvelutoimintojen mittaamisesta ja SLA:n arvioinnin luotettavuudesta.



Kuva 2. Hetkellinen näkymä AD User Account työjonoon. (CMDB 2015).

Käyttäjätunnusten avausaikojen mittaaminen ja todistaminen ei onnistu käytössä olevilla mittareilla. Haastatteluissa mainittu käyttäjätunnusten avausaikojen vaihtelu jää käytössä olevilla välineillä todistamatta.

6.4 Pääkäyttäjäoikeusprosessin läpimenoajat

Pääkäyttäjäprosessin läpimenoaikojen tarkastelua varten keräsin yrityksen ERP-järjestelmästä PAR-tilausten läpimenoaikoja ennen ja jälkeen PAR-prosessiin suoritettuja muutoksia. PAR-prosessissa käsitellään vain pääkäyttäjäoikeuksiin liittyviä työpyyntöjä. Tästä syystä PAR-prosessin osalta saadut mittaustulokset kuvaavat

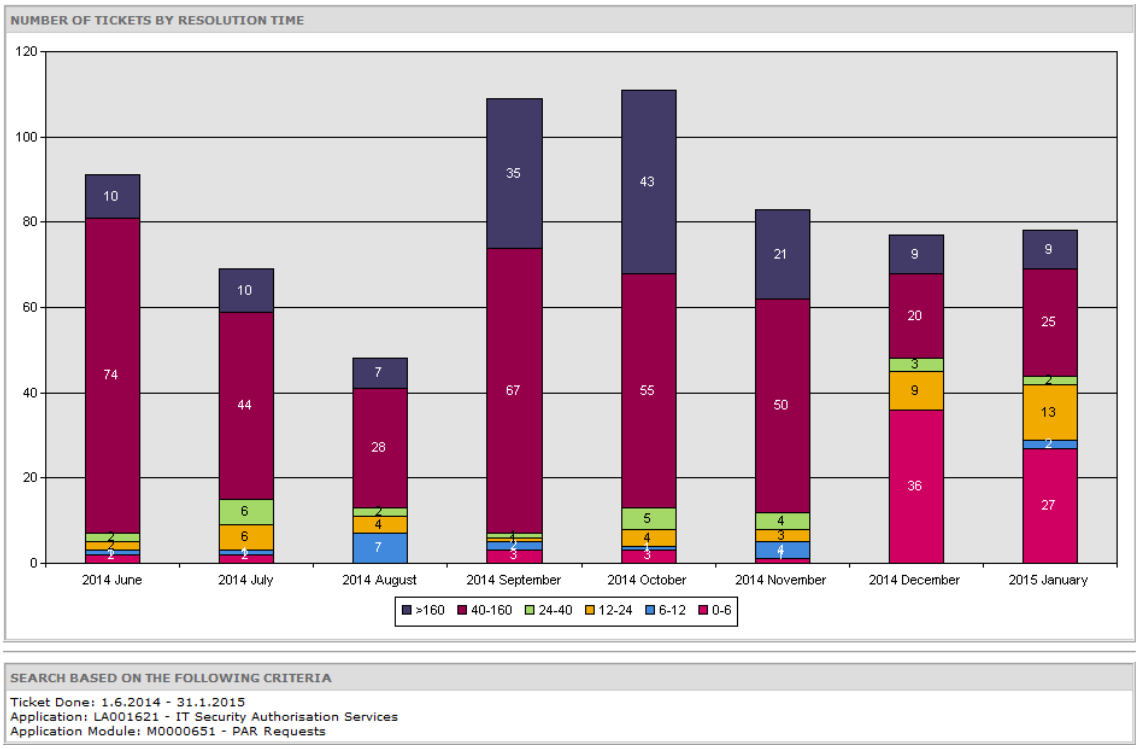
realistisesti tapahtumien todellisia läpimenoaikoja. Seuraavassa taulukossa on esitetty PAR-prosessin prosentuaalisesti jakautuneita läpimenoaikoja seitsemän kuukauden mittausjaksolta (taulukko 3). Huomattavaa on, että PAR-prosessin muutos tapahtui joulukuun alussa. Konkreettiset muutokset prosessin nopeutumiseen olivat nähtävissä jo kuukauden seurantajakson jälkeen.

Taulukko 3. PAR-prosessin läpäisyaikoja (CMDB 2015).

Hr	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
0- 24	5 %	13 %	23 %	6 %	7 %	10 %	58 %	54 %
24->160	95 %	87 %	77 %	94 %	93 %	90 %	42 %	46 %

Mittaustulosten perusteella prosessin läpimenoajat nopeutuivat joulukuussa merkittävästi. Joulu- ja tammikuussa tehdyistä pyynnöistä yli 50 % on ratkaistu ja toimitettu asiakkaalle alle 24 tunnin läpimenoajalla. Tässä on huomattava, että muutoksen jälkeinen otos kattaa tätä kirjoitettaessa kahden kuukauden seurannan. PAR-prosessin läpimenoaikaa tullaan jatkossa seuraamaan kuukausittain.

Kuvio 9 esittää PAR-prosessin läpimenoaikoja hieman tarkemmalla tasolla ennen ja jälkeen PAR-prosessiin suoritettuja korjaustoimenpiteitä. Myös tämän kuvion perusteella voidaan havaita joulukuun sekä tammikuun aikana avattujen tapahtumapyyntöjen läpäisyaikojen nopeutuneen merkittävästi. Kuvion mukaan tehdyistä avauspyynnöistä keskimäärin 58 % voitiin toteuttaa saman vuorokauden kuluessa. Ennen muutosta alle vuorokaudessa suoritettujen työpyyntöjen keskiarvoinen määrä verrattuna koko tapahtumamäärään oli noin 11 %.

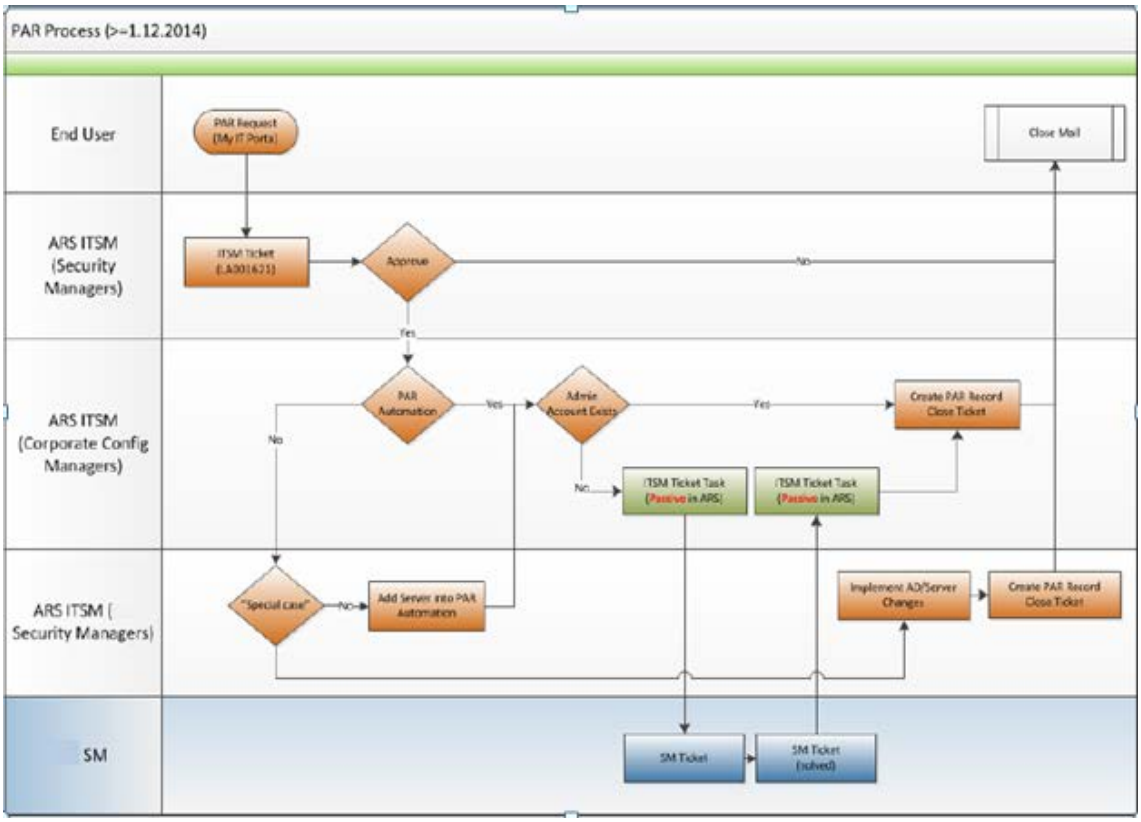


Kuvio 9, PAR-prosessin läpimenoaikoja (CMDB 2015).

PAR-prosessin läpimenoaikojen esityksestä nousi esille keskustelussa ulkoistuskumppanin Service Desk Managerin kanssa virheen mahdollisuus. Tapauksen läpimeno ajan mittaaminen päättyy, kun ulkoistuskumppanin agentti päättää tapahtuman yrityksen CMDB-järjestelmään. Jos agentti viivyttelee työn päättämisessä, myös mitattava aika pitenee. Tästä kirjausvirheestä on voinut aiheutua ero todellisen käyttöoikeustilanteen ja mitattujen tapahtumien välille. PAR-oikeuden tilaajan kannalta työ tulee valmiiksi, kun ulkoistuskumppanin agentti merkitsee työn valmistuneeksi asiakkaan toiminnanohjausjärjestelmään.

Palvelimen ollessa PAR-automaation piirissä, hyväksytty PAR-pyyntö käsitellään kokonaisuudessaan yrityksen sisäisessä toiminnanohjausjärjestelmässä. Aikaisemmin työpyyntö välitettiin manuaalisesti ulkoistuskumppanin toiminnanohjausjärjestelmään käsiteltäväksi. Uudessa toimintatavassa yrityksen sisäinen työryhmä käsittelee käyttöoikeuspyynnön ERP-järjestelmän välityksellä lisättäväksi AD-hakemistojärjestelmään. Työryhmä suorittaa käyttöoikeuden provisioinnin manuaalisesti ERP-järjestelmään. Muutos välitetään ERP-järjestelmästä automaattisesti

kerran vuorokaudessa suoritettavalla päivityksellä AD-järjestelmään kohdepalvelimen local admin ryhmään. Uudistettu PAR-prosessi otettiin käyttöön 1.12.2014 (kaavio 1).



Kaavio 1. 1.12.2014 käyttöön otettu PAR-prosessi. (Haastateltava 8 2014)

Prosessimuutoksen ja uuden palveluaikalupauksen perusteella työpäivän aikana ennen klo 14:sta toimeenpantavaksi lähetetty PAR-pyyntö on käytettävissä seuraavana työpäivänä. Kello 14:sta jälkeen toteutettavaksi toimitettu työpyyntö aktivoidaan seuraavan vuorokauden automaattisessa käsittelyssä.

7 Havaintoja

Edellisistä tutkimuksista ja niiden tuloksista nostan esille seuraavia havaintoja:

- Käyttäjätunnuksien avauksia suoritettiin puolen vuoden aikana 1702 kappaletta

- Näistä avauksista konsulttitunnuksia oli 1093, työntekijä 578 ja muita tunnuksia 31

- Käyttäjätunnuksien tilausten läpimenoaikoja ei voida mitata luotettavasti

- Muutokset käyttäjätunnuksiin suoritetaan manuaalisena työnä

- Vastuu käyttäjätunnuksien avaamis- ja sulkemistilauksesta on yrityksen manage-reilla

- Keskitettyä henkilöydintietojen hallintaratkaisua ei ole

- Käyttöoikeuksien keskitettyä raportointijärjestelmää ei ole

- Konsulttien henkilöydintietojen laatu AD:ssä vaihtelee

- Ulkoistuskumppanin PAR-käyttäjien tiedot ovat vain AD:ssä

Identiteetin omistajuus ei ollut kaikkien haastateltavien mielestä täysin selvä. Joi-denkin haastateltavien käsityksen mukaan identiteetin omistaa yrityksen tietohallin-to. Eräiden mielestä identiteetin omistajuus on liiketoiminnoilla. Kaikilla haastatelta-villa oli kuitenkin selkeä käsitys identiteetinhallinnan hyötyjistä. Liiketoimintayksiköt hyötyvät oikea-aikaisesta käyttäjätunnuksesta ja työtehtävässä tarvittavilla oikeuk-silla varustetuista käyttöoikeuksista.

Useissa haastatteluissa nousi esille konsulttitunnuksen henkilöydintietovarasto puute. Henkilöstöhallinnon järjestelmässä pidetään yllä yrityksen varsinaisten työn-tekijöiden identiteettiä. Sopimuksien hallintajärjestelmä keskittyy sopimuksen do-kumentaation tallentamiseen ja rekisteröintiin. Järjestelmässä ei pidetä yllä ulkois-ten työntekijöiden tietoja. Konsulttien henkilöydintietojen sijoittamisella keskitettyyn

tietovarastoon pyritään mahdollistamaan henkilöydintietojen laadun paraneminen. Yrityksen henkilöstöhallinnon järjestelmä kykenee teknisesti tallettamaan niin työntekijöiden kuin konsulttienkin henkilöydintiedot. Menettelytavan muutoksessa on kysymys sisäisestä tahdosta, prosessien uudelleen määrittelystä, taloudellisesta panoksesta ja työkalujen hienosäädöistä.

Ulkoistuskumppanin PAR-tunnusten rekisteröinti ja seuranta on mahdollista yrityksen AD-järjestelmän avulla. CMDB-tiedoissa ulkoistuskumppanin PAR-tunnuksia palvelimille ei ole esitelty. Tämä PAR-käyttäjätietojen rekisteröintipuute vaikeuttaa käyttöoikeuksien tarkastelua ja raportointia.

Henkilötietolain virheettömyysvaatimuksen perusteella voidaan tulkita, että henkilörekisterin pitäjä ei voi tallettaa vanhentuneita tietoja rekistereissään. Sopimuksen päättymisen jälkeen rekisterin pitäjällä on velvollisuus poistaa sopimuksettomien käyttäjien henkilötiedot rekistereistään (Henkilötietolaki 1999/523). Tämän periaatteen toteuttamiseksi työn suosituksien avulla tuotetuille prosessin ja toimintojen kehittämisajatuksille on vahvoja perusteita.

Yrityksen toimiessa myös Venäjällä, on otettava huomioon Venäjän lainsäädännön vaatimukset muun muassa yrityksen venäläisten työntekijöiden ja konsulttien henkilötietojen säilytykseen. Vuoden 2016 syyskuun alussa voimaan tulevat Venäjän tietosuoja lainsäädännön vaikutukset yrityksen tapaan käsitellä yrityksen henkilötietoja. Tällöin ne on otettava tarkasteltuun ennen lainsäädännön muutoksia. Venäjällä 1.9.2016 voimaan tulevassa tietosuojalaissa määrätään seuraavasti. "The data operators are obliged to ensure recording, systemisation, accumulation, storage, clarification (update, change) and extraction of personal data of citizens of the Russian Federation with the use of databases located in the territory of the Russian Federation when collecting this personal data in any manner, including via the Internet, except for the cases specified in Items 2, 3, 4, 8 of Paragraph 1 of Article 6 of this Federal Law." (Rumyantsev 2014, 18). Kirjoitetun lain hengen mukaan dataoperaattoreiden tulee varmistua, että Venäjän federaation kansalaisten (citizens of the Russian federation) henkilötietojen käsittelyssä käytettävät järjestelmät

on sijoitettu Venäjän federaation alueelle. Tämä laki koskee myös internetin kautta tarjottavia palveluita.

Tällä hetkellä yrityksessä käytettävien venäläisten työntekijöiden käyttäjätunnusten AD-rekisteröinnit on talletettu myös Venäjälle. AD:n ylläpidon ja tietojen rekisteröinnin kannalta tulevan lain kirjain olisi jo täytetty. Uuden lain vaatimukset on otettava huomioon suunniteltaessa ja muodostettaessa venäläisten työntekijöiden ja konsulttien henkilöydintietojen hallintaan käytettävää Master Data Management järjestelmää.

Roscomnadzor on Venäjän federaation liikenneministeriöitä vastaava viranomainen. Federal Service for Supervision of Communications and Mass Media Roscomnadzor valvoo mediaa, viestintää, informaatioteknologiaa ja telekommunikaatiota sekä jakaa paikallisia radiotaajuuksia. Roscomnadzor toimii Venäjän henkilötietolain valvovana viranomaisena, joka tuottaa tarvittaessa lain soveltamisohjeet. Lakiasiaintoimisto Castren & Snellman lakiasiantuntijan mielestä tätä tutkimusraporttia kirjoitettaessa paras strategia on odottaa Roscomnadzorin tuottamia lain tulkintaohjeita. (Rumyantsev 2014, 39).

8 Johtopäätökset ja suositukset

Väliaikaisten työntekijöiden henkilöydintietojen hallinnan on oltava vähintään samalla tasolla, kuin on varsinaisen henkilökunnan henkilöydintiedon hallinnointi. Tiukalla käsittelypolitiikalla voidaan tarkoituksella tai tahtomatta aiheuttaa konflikti tietoturva- tai käyttöoikeuspolitiikan, eri järjestelmien käytettävyyden ja IT:n välillä. Kehitystoiminnan tavoitteena ei suinkaan ole, että IT pyrkii paikkaamaan hankalaksi suunniteltuja prosesseja. Pikemminkin järjestelmien toimivuus ja notkeus on tuotettava kontrolloidulla automaatiolla. Kontrolloivana henkilönä käyttäjätunnusten

valvonnassa toimii luonnollisesti henkilön palkannut esimies. Vaihtoehtona on siirtää sopimuksellisesti konsulttitunnusten käsittely palveluita tuottavan organisaation vastuulle. Tällöin ulkoistuskumppanin esimiehellä on oltava tarvittavat työkalut ja riittävät valtuudet ulkoisten tunnusten hallinnointiin yrityksen järjestelmissä. Näihin muutoksiin voidaan suunnata seuraavilla toimenpiteillä.

8.1 Kehitystoimenpiteet

Laajempina kehitystoimenpiteinä suosittelen aloitettavaksi henkilöydintietojen hallinnan kehittämisen yhdistämällä henkilöydintiedot henkilöhallinnon järjestelmään. Suosittelen aloitettavaksi identiteetin ja pääsynhallintajärjestelmän (IAM) hankinnan valmistelun.

1 Henkilöydintietojen siivous käyttämättömistä tunnuksista ja yrityksen manageritietojen liittäminen käytössä oleviin tunnuksiin
2 Ulkoisten työntekijöiden henkilöydintiedot siirretään käsiteltäväksi henkilöstöhallinnon järjestelmään
3 Yrityksen laajuisen PAM-järjestelmän käyttöönottaminen
4 IAM-järjestelmän suunnittelu ja käyttöönotto

8.2 Henkilöydintietojen siivous

Ydintiedon laatukysymykset ovat nousseet esille keskusteluissa toimittajien kanssa. IAM-konsulttipalveluita tarjoavat yritykset ovat esityksissään tähdentäneet henkilöydintiedon siivoamista ennen IAM-projektin aloittamista. Tämän siivoustyön arvo tulee nousemaan esille projektin myöhemmissä vaiheissa. Henkilöydintiedon

ajantasaistamisella saavutetaan merkittävä etu suunniteltaessa ja rakennettaessa integrointirajapintoja autoratiivisen tietovaraston ja tietojärjestelmien välille. Ensisijaisesti integroitavia kohteita ovat henkilöydintietojen autoratiivinen lähde, hakemistopalvelu AD, toiminnanohjausjärjestelmä ja mahdollinen tuleva IAM-järjestelmä. Lisäksi liiketoimintapäätöksellä määriteltyjä sovelluksia voidaan käsitellä erillisinä provisiointi- ja federointikohteina.

Henkilöydintietojen siivoaminen ja ajantasaistaminen on ensimmäinen askel yrityksen kokonaisvaltaisessa identiteettien hallintaprojektissa. Ydintietojen siivoaminen ja täydentäminen tulee toteuttaa AD:ssa talletettaviin tunnuksiin. Tavoitteena on korjata henkilöydintiedot niin, että tunnuksien omistajuuden (manageri) tiedot ovat ajan tasalla. Ulkoistuskumppanin tunnuksissa manageritietona voidaan käyttää yrityksen hyväksymää palveluntuottajan edustajaa.

8.3 Henkilöydintiedon kehittäminen

Tietoarkkitehtuurin näkökulmasta henkilöydintiedon perusrekisteri tukee vahvasti tiedon yksikäsitteisestä ymmärtämistä ja ajatusta tiedon ainutkertaisuudesta. Identiteettien hajautettu hallinta ei edellä olevien havaintojen perusteella nykyisellään vastaa informaatioarkkitehtuurin vaatimuksia. Havaintojeni ja haastattelujen perusteella on nähtävissä, että yrityksen henkilöydintiedot on sijoitettu työntekijöiden osalta henkilöstön hallintojärjestelmään. Konsulttien osalta tiedot on talletettu hakemistopalveluun sekä yrityksen ITSM-järjestelmään. Teoriaosassa mainittu hybridimalli kuvaa yrityksen tämän hetkistä ydintiedon tallettamisen arkkitehtuuria. Henkilöydintietoa on talletettu ja käsitellään useissa eri järjestelmissä.

Tutkimusosassa tehty havainto ulkoistuskumppanin pääkäyttäjätunnusten näkymättömyydestä yrityksen CMDB-järjestelmässä on esimerkki puutteellisesta ydintiedosta. Käyttöoikeushallinnan avoimuus ei ole mielestäni tällä hetkellä ulkoistuskumppanin pääkäyttäjäroolissa olevien henkilöiden kohdalta hyvien IT-käytäntöjen

mukaista. Riskien hallinnan kannalta avoin käyttöoikeuksien raportointimahdollisuus kaikkiin käytössä oleviin käyttöoikeuksiin lisää System Managereiden, sisäisen riskienhallinnan ja ulkoisten auditoijien luottamusta toimivaan käyttöoikeushallintaan.

Ulkoisten käyttäjien henkilöydintietojen hallinnan suunnittelussa on käsitettävä, että HR-yksikkö ei tee työtään mahdollista IAM-järjestelmää varten. Arkkitehtuurin ja integraatiotoiminnallisuuksien kannalta sopimussuhteessa olevien työntekijöiden tiedot on syytä tallettaa ja ylläpitää ulkopuolisina henkilöinä yhteen järjestelmään. Palveluntuottajasta tulisi tallettaa yrityksen henkilöydintietostandardin vaatimusten mukaiset tiedot. Näin menetellen henkilöydintietojen laatu voidaan taata paremmin. Nykyinen henkilötietojärjestelmä voi toimia yrityksen keskitettynä henkilöydintietojen lähteenä.

Suosituksenani on muodostaa ulkoisten ja sisäisten työntekijöiden identiteeteille henkilöydintiedon hallintaan koko yrityksen laajuinen yhteinen henkilöydintietojen perusrekisteri. Tämän rekisterin avulla pyritään varmistamaan tiedon laatu ja henkilöydintietojen oikeellisuus. Yrityksen henkilöydintieto standardiin (liite 4) on lisättävä ulkoisten työntekijöiden palvelusopimuksen aloitus- ja päättymispäivämäärä. Tätä lisätietoa voidaan myöhemmin käyttää tunnuksen automaattiseen deprovisiointiin.

8.4 PAM-järjestelmän käyttöönotto

Syksyn 2014 aikana yrityksen liiketoiminnassa esille nousi tarve kehittää pääkäyttäjäoikeuksilla suoritettavien tehtävien seuranta- ja valvontamenetelmiä. Tästä johtuen aloitettiin uuden PAM-järjestelmän käyttöönoton valmistelu. PAM-selvitystyölle on varattu yrityksen projektimallin mukaiset resurssit. Tässä on huomattava, että ensimmäisen vaiheen tavoite on rakentaa PAM-ympäristö liiketoimintaa valvovan viranomaisen vaatimuksesta. Päätös järjestelmän myöhemmästä laajentamisesta

koko yrityksen käyttöön, tehdään liiketoiminnan suorittamasta koeajosta saatujen kokemusten perusteella keväällä 2015.

8.5 Identity and Access Management (IAM)

Identiteettien hallinnan kehittämiseksi on yrityksessä aloitettava keskustelu Identity Access Management (IAM) järjestelmän tarpeesta yrityksen CIO-toimiston, liiketoiminta-arkkitehdin, tietoturvan ja liiketoimintojen välillä. Valmistautuminen IAM-projektiin on syytä suorittaa huolella. IAM-järjestelmien suunnittelua konsultoivien toimittajien kanssa käydyissä keskusteluissa saadun tiedon mukaan, normaalisti IAM-järjestelmän määrittelyyn ja implementointiprojektiin käytetään aikaa yleensä yli vuosi. Tästä näkökulmasta katsoen liiketoimintatarpeen kartoittaminen ja budjettivarauksen suunnittelu on syytä aloittaa hyvissä ajoin ennen suunniteltua IAM-järjestelmäprojektia.

Keskusteluissa IAM-järjestelmän tarpeesta yritykselle on noussut esille tarpeita automatisointiin käyttäjätunnuksien provisioinnissa ja de-provisioinnissa. Automatisoitavia kohteita ovat tyypillisesti käyttäjätunnusten ja oikeuksien hakeminen, salasanojen nollaaminen ja tunnusten aktivoiminen itsepalveluna. Kehitystoiveita on tullut esille myös käyttöoikeuksien raportointiin ja seurantaan liittyvien kysymysten ja vaatimusten ratkaisemisessa.

8.6 Jatkotutkimuksia

Tutkimuksen kuluessa tunnistettiin uusia kehityskohteita, joiden tutkimisen ja kehittämisen avulla voitaisiin todennäköisesti kehittää yrityksen toimintoja. AD-

hakemistopalvelun todettiin sisältävän merkittävän määrän omistajattomia rakenteita. Omistajuuksien tunnistaminen ja merkitseminen näihin rakenteisiin tulee nopeuttamaan muutoshallintaa ja kehittää oleellisesti hakemistopalveluiden tietoturvaa. Tämä kehitystyö tuottaa omistajuudet omistajattomille hakemistoille.

8.6.1 Rooliperustainen käyttöoikeusmäärittely

Yritys käyttää osittain rooliperusteisia käyttöoikeuksien määrittelyä. Rooliperustaista käyttöoikeusmäärittelyä ei kuitenkaan ole toteutettu läpi organisaation. Rooliperustaisen käyttöoikeusmäärittelyn tutkimustyön tuloksena voidaan yritykselle rakentaa standardi perusrooleista. Käyttöoikeuksien rooliperustainen määrittely tukee mahdollisuuksia käyttöoikeuksien provisiointiin aina liiketoimintasovelluksiin saakka. Rooliperustainen käyttöoikeusmäärittely lisää mahdollisuuksia käyttäjätunnuksien käsittelyn automaatioon. Liiketoiminnoille automaatiosta voidaan nähdä syntyvän lisähyötyä tunnuskäsittelyn nopeutumisen ja virheiden vähenemisen myötä.

8.6.2 Identity as a Service (IdaaS)

Identiteetin hallintajärjestelmien kehitys mahdollistaa myös palvelumallin käyttöön. IdaaS-malli tuottaa mahdollisuuden hankkia identiteetinhallinta palveluna. Tämän alueen mahdollisuudet on syytä kartoittaa erillisellä tutkimuksella. Tutkimuksessa on tarkasteltava samalla yrityksen työntekijöiden, ulkoisten vuokratyöntekijöiden ja yrityksen asiakkaiden identiteettien ja palveluiden hallintaa. Tähän kokonaisuuteen kuuluvat luonnollisesti pilvipalveluiden käyttöoikeuksien federointi-palvelut (kirjautuminen yhdellä tunnuksella eri palveluihin) ja identiteettien hallintapalvelut raportointeineen.

8.7 Tutkimuksen arviointi

Tutkimuksen laatu perustuu moniin seikkoihin. Laadun varmistamiseksi on tutkimuksen tarkoitus, tutkimustehtävät ja valitut menetelmät esitettävä loogisesti tutkimussuunnitelmassa. Aineistonkeruun tueksi valittuja metodeja harkitsin tarkoin. Tässä tutkimuksessa metodeiksi valitsin haastattelut ja prosessien läpimenoaikojen havainnoinnin mittausten avulla. Näkemykseni mukaan prosessien mittaamisen perusteella tuotettu raportointi varmisti haastattelututkimuksen tuloksia. Valittuja menetelmiä voin hyödyntää jo suoritettujen korjaustoimenpiteiden vaikutusten seurantaan.

Teorioiden yhdistäminen tutkimusaiheeseen oli tutkimuksen alkumetreillä haastavaa. Tutkimuksen kuluessa totesin teorioita ja lähdemateriaaleja olevan tarjolla riittävästi. Lähdeaineiston siirtyminen kirjastoista ja painetusta materiaalista digitaaliseen muotoon on nopeuttanut merkittävästi lähdemateriaalien etsimistä. Näkemyksiä, mielipiteitä ja käsiteltävien kohteiden erilaisia painotuksia on tarjolla runsaasti. Tästä syystä tarjolla olevaa materiaalia on syytä arvioida kriittisesti.

Materiaaleja etsiessäni havaitsin, että uusimmat ja mielenkiintoiset tutkimukset tai tieteelliset raportit on usein sijoitettu maksullisiin palveluihin. Hyvänä esimerkkinä ovat vaikkapa Gartner ja Forrester -tutkimuslaitosten kaupalliset aineistot. Kaupallisten materiaalin ansioksi voi laskea ammattimaisen lähestymistavan käsiteltävään aiheeseen. Tutkimuksen tekijän on hyvä varautua tutkimusbudjetin suunnittelussa myös materiaalihankinnan kuluihin.

Tutkimukseen suoritetussa haastatteluosuudessa koen onnistuneeni keräämään haastateltavilta ydintietoja havaituista ongelmista. Haastatellessani sain kirjattua ylös näkemyksiä ja ajattelua ohjaavia mielipiteitä. Hyvänä esimerkkinä toimii vaikkapa identiteetinhallinta tutkimuksen sivutuotteena syntynyt PAR-prosessin uudistamistarve. Työn aikana keräämieni tietojen ja kokemukseni perusteella ongelmallisen PAR-prosessin toiminnan kehittäminen suoritettiin syksyn 2014 aikana. Tä-

män kehitystyön mahdollisti konkreettisessa toiminnassa piilevien ongelmien tunnistaminen ja perusteltu raportointi. Tietojen etsimisessä perustelutyön pohjaksi tutkitut teoriat, suoritetut haastattelut ja kerättyjen tietojen analysointi tukivat erinomaisesti prosessien ja uusien menetelmien suunnittelua ja kehittämistä.

Tämän työn kuluessa käytin hyväkseni tutkimuksellisia menetelmiä ja järjestelmällistä tietojen keräämistä. Keräsin tietoa useista tietolähteistä yrityksen toiminnan kehittämiseen. Tutkimuksen kuluessa huomioin reaalimaailman muutokset ja ympäristön muuttuvat vaatimukset. Havainnoin toiminnallisia puutteita ja tietoturvariskejä. Havaintojen perusteella tehtävät korjausesitykset tarvitsevat resursseja, eivätkä välttämättä toteudu tutkimuksessa esitettyjen metodien mukaisesti.

Vertaisryhmäkeskusteluista tehtyjen havaintojen perusteella tutkimuksen tuloksia voidaan hyödyntää myös laajemmassa kontekstissa. Toimeksiantajan kannalta tutkimukselle konsulttitunnusten käyttöoikeuksien elinkaaren käsittelyn kehittämiselle on ollut tilaus. Kokonaiskuvan selvittäminen, kehitysehdotukset ja suositukset tuottavat lisäarvoa tutkimuksen tilaajalle.

Työn kuluessa yrityksessä on herätty todelliseen tarpeeseen kehittää identiteetinhallintaa. Tämän työn kuluessa yritys ryhtyi aktiivisesti kehittämään pääkäyttäjäoikeuksilla tehtävän työn seurantaa ja raportointia. Tästä tilanteesta kehittämistyöstä on hyvä hetki jatkaa eteenpäin. Raportissa esitettyjen havaintojen avulla on mahdollista jatkaa varsinaiseen identiteettienhallinta järjestelmän kehittämiseen ja käyttöönottoon.

Lähteet

Ant, A., Scholtz, T. 2014. Take a People-Centric Approach to Simplify Identity and Access Management. Stamford: Gartner.

Arvidsson, J. 2014. Sparta Consulting Oy. 2 Sparta Sähköisen identiteetin ja henkilöydintiedon koulutusmateriaali. Jyväskylä: Sparta Consulting Oy.

Chaplin, M., Rycroft, S., ISF Members. 2013. The Standard of Good Practice for Information Security. London: Information Security Forum Limited.

Chief Architect, Development Manager. 2013. Green belt project presentation. PAR Access Management. Espoo: Yrityksen intranet.

CobIT 4.1. 2007. CobIT 4.1. Framework Control Objectives Management Guidelinse Maturity Models. The IT Governance Institute. Rolling Meadows: ITGI.

Cser, A., 2012. Use Commercial IAM Solutions To Achieve More Than 100% ROI Over Manual Processes. Forrester. www.forrester.com. (Viitattu 25.2.2015).

CMDB. 2014. ITSM Data Warehouse. Espoo: Yrityksen intranet.

Ernst & Young. 2013. Identity and access management. Beyond compliance. EYGM Limited.

Green, T. (editor). 2010. CISSP Exam guide fifth edition. New York: McGraw Hill.

Gröbner, M. & Frenken, Chr. 2013. Three steps to managing Master Data. Munich: Roland Berger Strategy Consultants Holding GmbH. http://www.rolandberger.com/expertise/functional_issues/information_management/2013-02-11-rbsc-news-Three_steps_for_managing_master_data.html. (Viitattu 4.11.2014).

Guday, T. 2012. Käyttöoikeushallintaprosessin kehittäminen Vantaan kaupungin organisaatiossa: tapaustutkimus. Opinnäytetyö. Espoo: Laurea ammattikorkeakoulu. http://www.theseus.fi/bitstream/handle/10024/53356/Guday_Tewodros.pdf?sequence=1. (Viitattu 24.8.2014).

Guttman, B., Roback, E.A. 1995. An Introduction to Computer Security: The NIST handbook. Washington: U.S. Department of Commerce. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf. (Viitattu 15.11.2014).

Hanna, A., Macfarlane, I., Rance, S. 2007. A Dictionary of IT Service Management. Terms, Acronyms and Abbreviations ITIL V3 edition. Wokingham: itSMF Ltd.

Harris, S. 2010. CISSP Exam Guide Fifth Edition. New York: McGrawHill.

Haug, A., Zachariassen, F., van Liempd, D. 2011. The costs of poor data quality. Journal of Industry Engineering and Management. OmniaScience. http://www.jiem.org/index.php/jiem/article/view/232. (Viitattu 12.11.2014).

Henkilötietolaki. 1999/523.

Hu, V., Schnitzer, A., Sandlin, K. 2013. NIST Special Publication 800-162 Attribute Based Access Control Definition and Considerations. U.S. Department of Commerce http://csrc.nist.gov/projects/abac/july2013_workshop/july2013_abac_workshop_abac-sp.pdf. (Viitattu 16.11.2014).

ISACA. 2014. About ISACA. http://www.isaca.org/about-isaca/Pages/default.aspx. (Viitattu 30.12.2014).

ISF. 2014. About Us. https://www.securityforum.org/membership/. (Viitattu 30.12.2014).

ISO/IEC 27002. 2005. International Standard. Information technology- Security techniques- Code of practice for information security management. Geneva: ISO/IEC 2005.

Iverson, B., Gaehtgens, F., Krapes, S. 2015. Critical Capabilities for Identity Governance and Administration. Stamford: Gartner.

JHS 179 ICT-palvelujen kehittäminen. Kokonaisarkkitehtuurin kehittäminen. 2012. Julkisen hallinnon tietohallinnon neuvottelukunta. http://www.jhs-suositukset.fi/suomi/jhs179. (Viitattu 22.11.2014).

Karjalainen, A. 2002. Mitä Benchmarking arviointi on? Oulun Yliopisto. http://www.oulu.fi/w5w/benchmarking/bm.RTF. (Viitattu 13.1.2015).

Kasanen, H. 2010. Keskitetty identiteetinhallinta. Referenssiarkkitehtuuri. Secproof Oy. http://www.slideshare.net/hannuk/idmreferenssiarkkitehtuuri. (Viitattu 18.10.2015).

Kielitoimisto. 2014. Kotimaisten kielten keskus ja Kielikone Oy. http://www.kielitoimistonsanakirja.fi/. (Viitattu 7.1.2015).

Kunnas, J. 2006. Yritys Enterprise Identity Management for Employees and Partners. Pre-Study. K2 Data Solutions Oy. Espoo: Yrityksen intranet.

Linden, M. 2012. Identiteetin- ja pääsynhallinta luentomoniste. http://www.cs.tut.fi/~linden/iam-pruju.pdf. (Viitattu 13.10.2014).

Metsämuuronen, J. 2012. Tutkimuksen tekemisen perusteet ihmistieteissä. Helsinki: International Methelp Oy.

National Institute of Standards and Technology. 2014. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. U.S. Department of Commerce http://dx.doi.org/10.6028/NIST.SP.800-162. (Viitattu 1.11.2014).

National Institute of Standards and Technology. 2013. Security and Privacy Controls for Federal Information Systems and Organizations. U.S. Department of Commerce http://dx.doi.org/10.6028/NIST.SP.800-53r4. (Viitattu 2.11.2014).

National Institute of Standards and Technology. 2014. Attribute Based Access Control (ABAC) overview. U.S. Department of Commerce http://csrc.nist.gov/projects/abac/. (Viitattu 1.11.2014).

Oberhofer, M., Dreibelbis, A. 2008. An introduction to the Master Data Management Reference Architecture. IBM. http://www.ibm.com/developerworks/data/library/techarticle/dm-0804oberhofer/#resources. (Viitattu 21.10.2014).

O'Connor, A. & Loomis, R. 2010. 2010 Economic Analysis of Role-Based Access Control. Final Report. Gaithersburg: National Institute of Standards and Technology. http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf. (Viitattu 15.11.2014).

Ojasalo, K., Moilanen, T., Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOYpro Oy.

Oracle. 2015. PeopleSoft Supplier Relationship Management. http://www.oracle.com/us/products/applications/peoplesoft-enterprise/053337.html. (Viitattu 9.2.2015).

Päijänen, J. 2014. Sparta Consulting Oy. Sparta Henkilöydintiedon prosessit ja hallintamalli koulutusmateriaali. Jyväskylä: Sparta Consulting Oy.

Rumyantsev, S. 2014. New Russian data processing requirements. Helsinki: Castren & Snellman.

Sandhu, R., Coyne, E., Feinstein, H., Youman, C. 1995. Role-Based Access Control Models. National Institute of Standards and Technology. http://csrc.nist.gov/rbac/sandhu96.pdf.

Saltzer, J., Schroeder, M. 1971. The Protection of Information in Computer Systems. http://www.cs.virginia.edu/~evans/cs551/saltzer/. (Viitattu 15.11.2014).

Shah J., Manathara M., Hoeppe A. 2012. Process-Driven Master Data Management For Dummies. Hoboken: Software AG.

Suomen Standardisoimisliitto SFS ry. 2014. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Information Technology. Security techniques. Code of practice for Information security controls. Helsinki: Suomen Standardisoimisliitto SFS ry.

Taylor, S. & Nissen, C. F. 2007. Passing your ITIL Foundation Exam. Norwich: The Stationery Office.

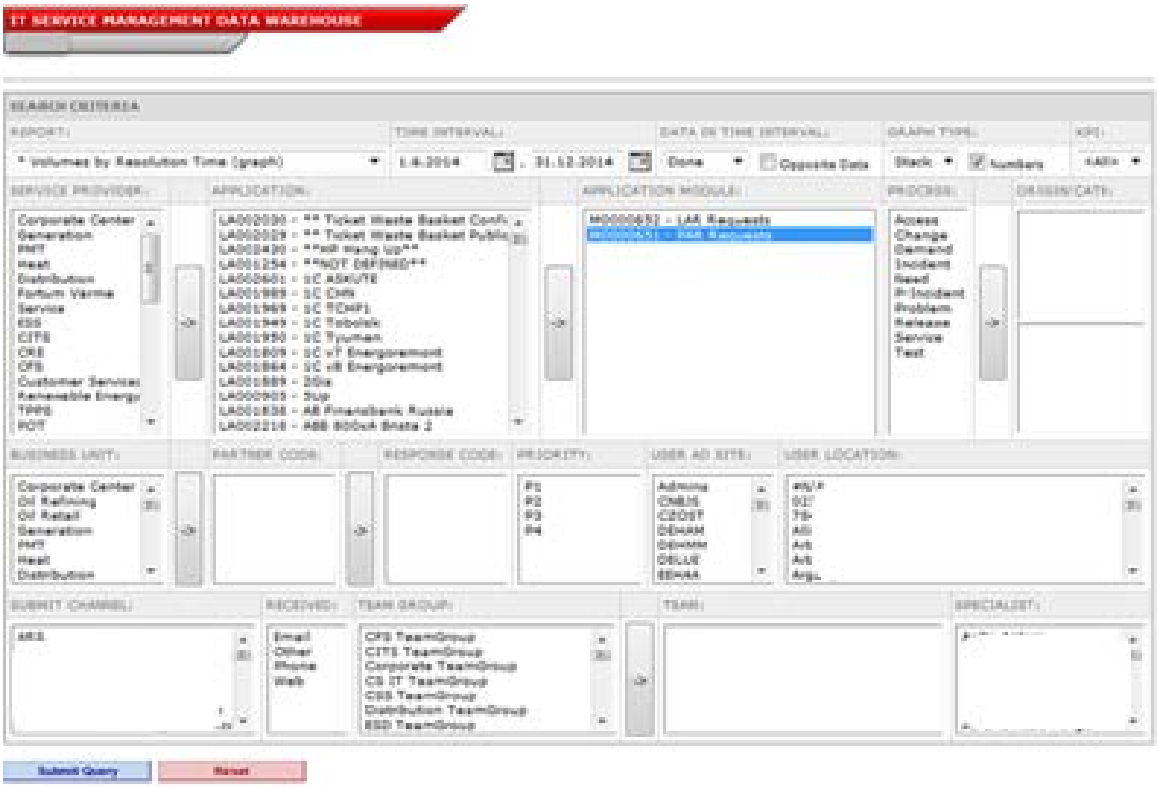
Silius, K. 2008. Teemoittelu ja Tyypittely. Tampereen Teknillinen Yliopisto. Tampere: http://matriisi.ee.tut.fi/hmopetus/hmjatkoopintosemma/2008/Silius_teemoittelu-tyypittely_141108.pdf. (Viitattu 3.11.2014).

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV- Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. http://www.fsd.uta.fi/menetelmaopetus/. (Viitattu 4.11.2014).

Ucisa. ITIL- A guide to access management. University of Oxford. Oxford. https://www.ucisa.ac.uk/~/media/Files/members/activities/ITIL/service_operation/access_management/ITIL_a%20guide%20to%20access%20management%20pdf.ashx. (Viitattu 15.12.2014).

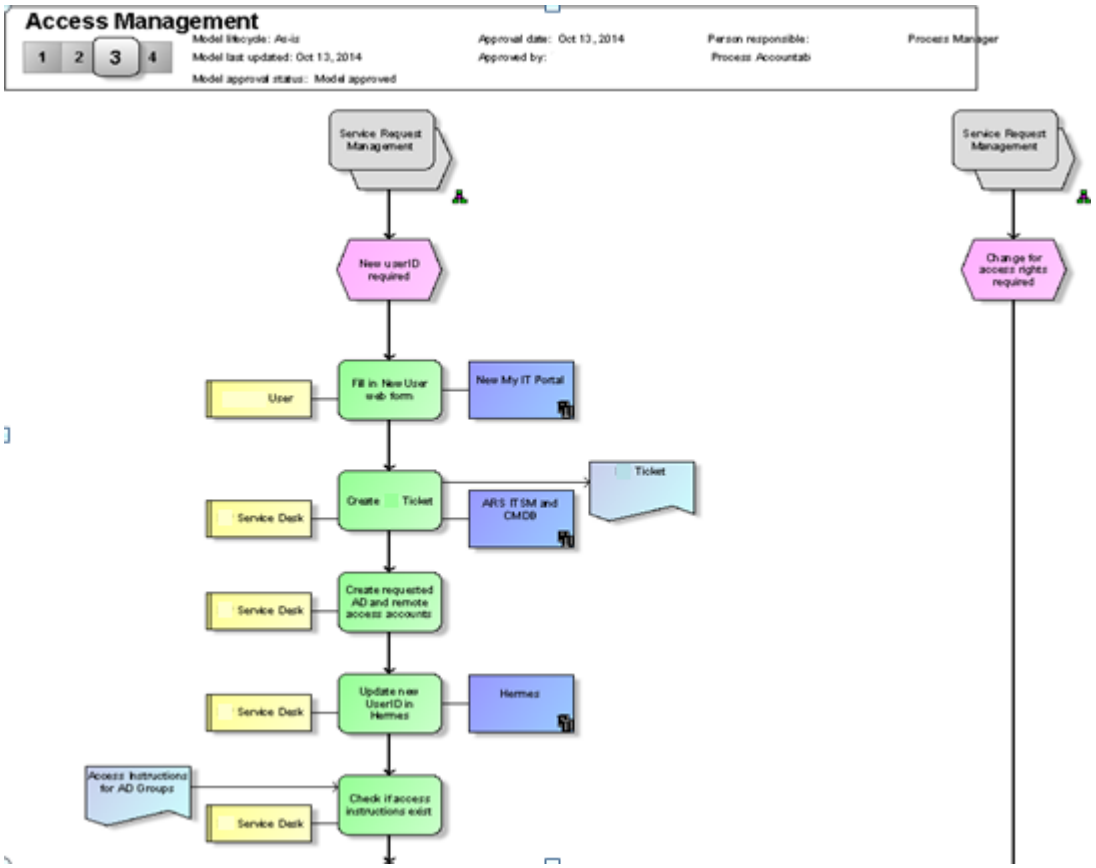
Valtiovarainministeriö. 2013. Kunnan kokonaisarkkitehtuurin hallintamallin kehittäminen. https://www.kuntarakenne.fi/kao-wiki/fi/tietoa-sivustosta/ Kunnankokonaisarkkitehtuurinhallintamallinkehittaminen20131230.pdf. (Viitattu 4.10.2014).

Raporttigeneraattorin asetukset



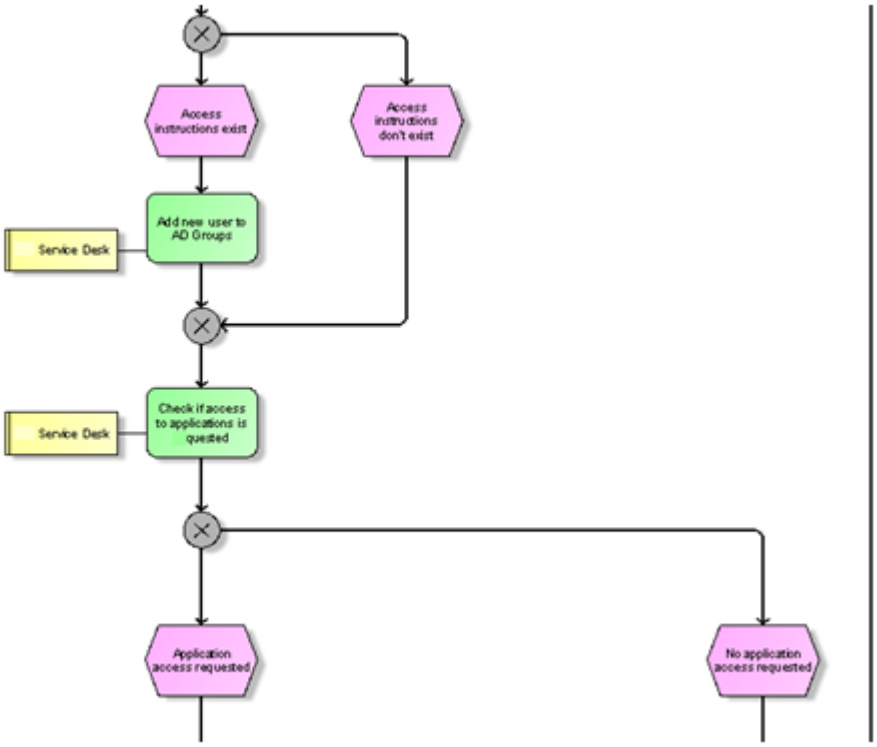
Kuva 3. CMDB-järjestelmän raporttigeneraattorin asetukset PAR-prosessin läpimenoaikojen mittausjärjestelyssä.

Käyttöoikeuden hallintaprosessi



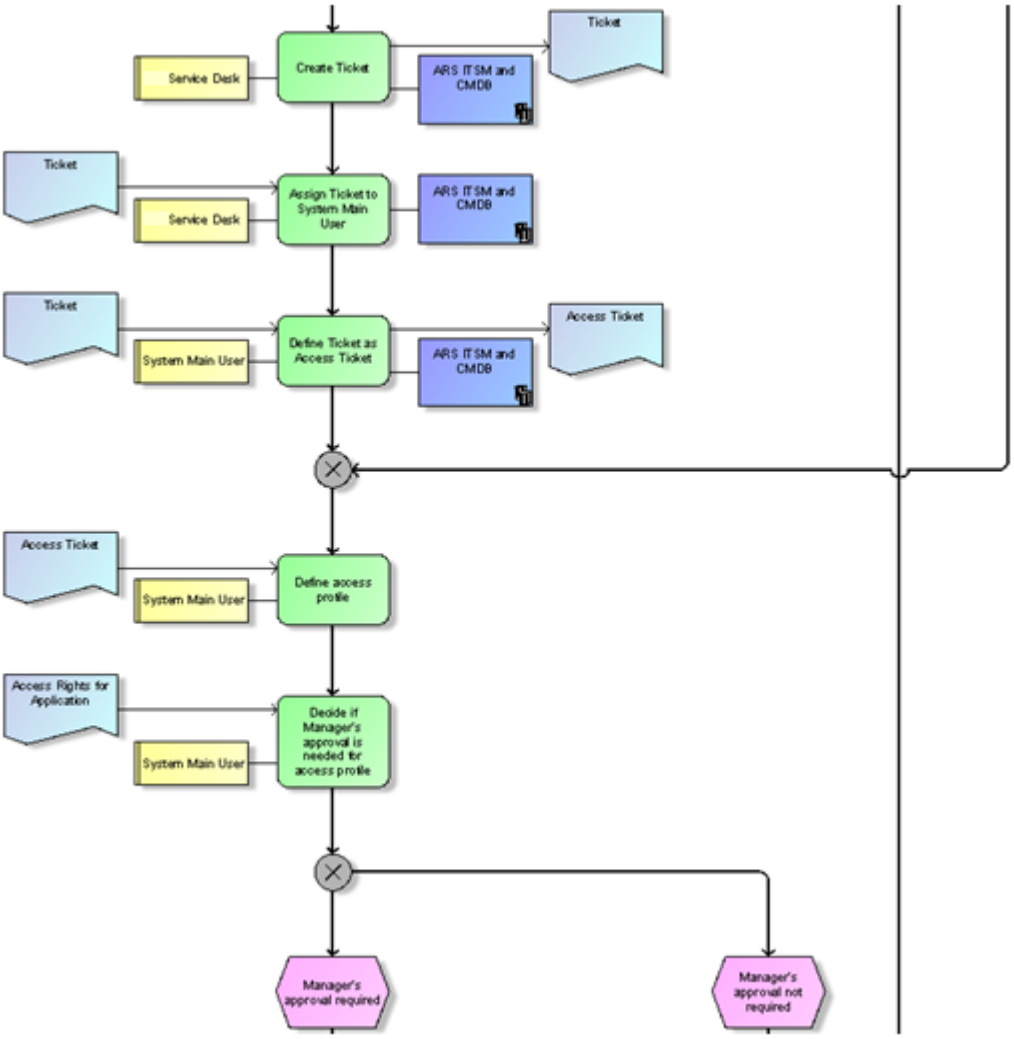
Kaavio 2. Käyttöoikeuden hallinta prosessikaavio, sivu 1.

Käyttöoikeuden hallintaprosessi (access management process).



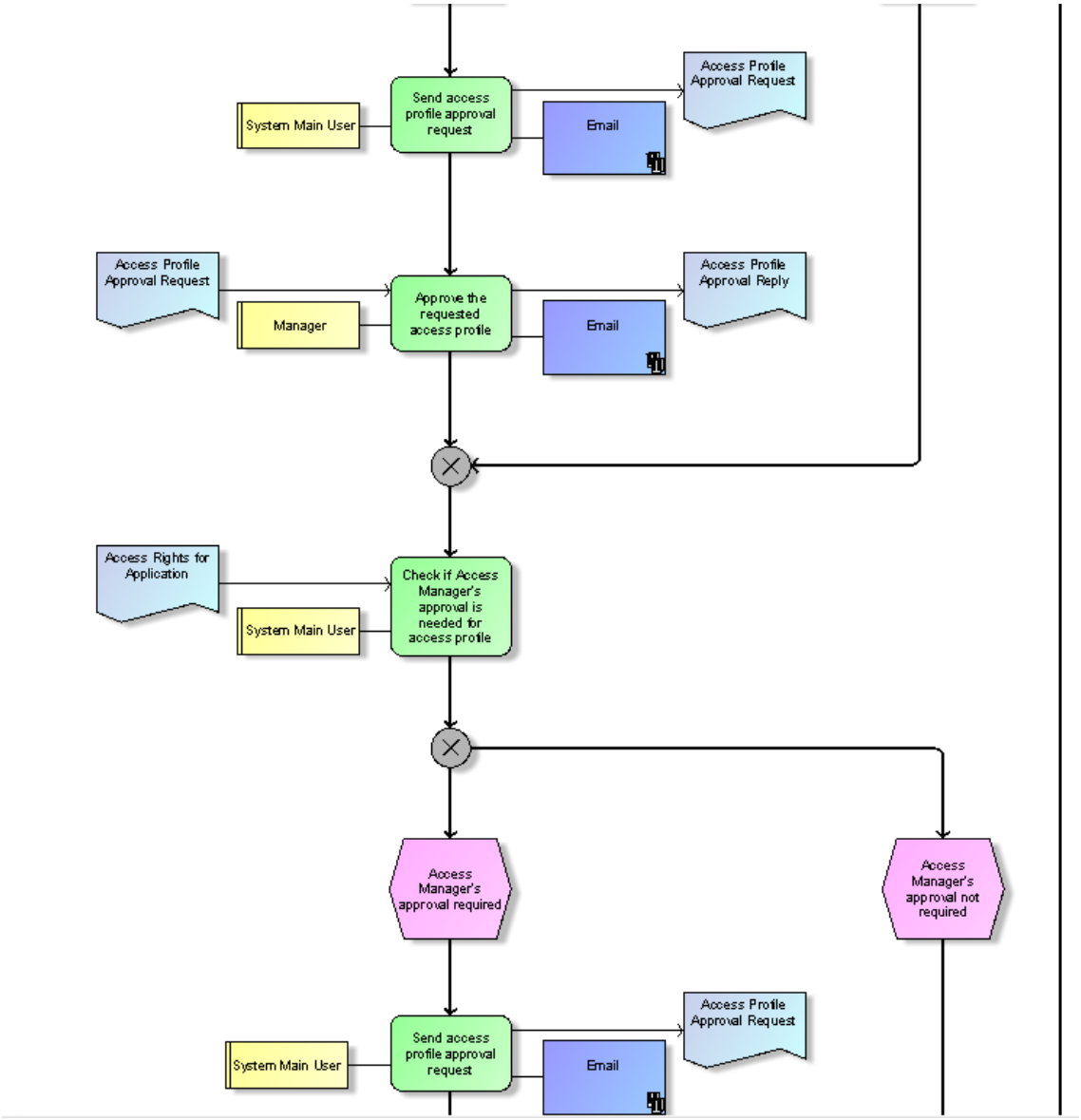
Kaavio 3. Käyttöoikeuden hallinta prosessikaavio, sivu 2.

Käyttöoikeuden hallintaprosessi (access management process).



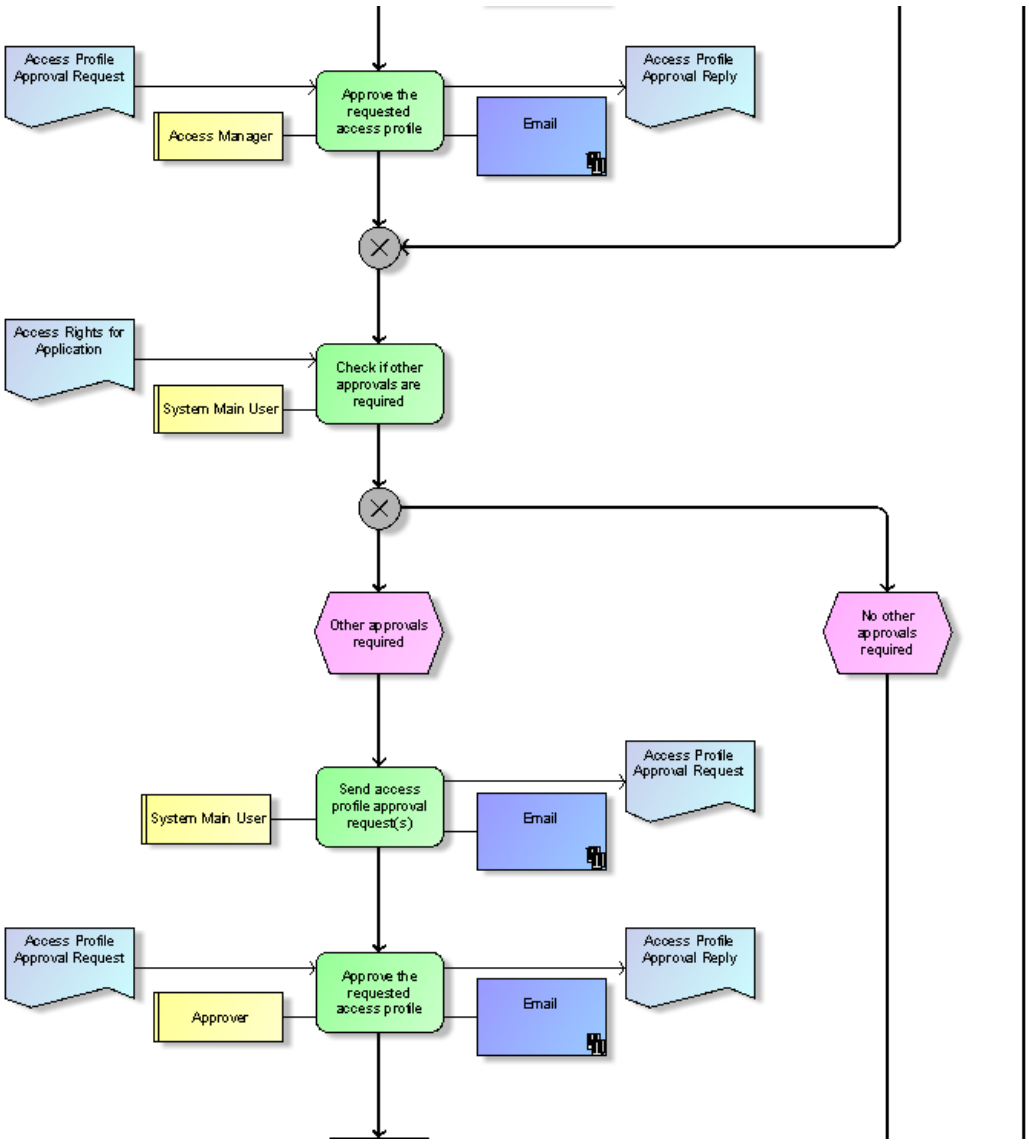
Kaavio 4. Käyttöoikeuden hallinta prosessikaavio, sivu 3.

Käyttöoikeuden hallintaprosessi (access management process).



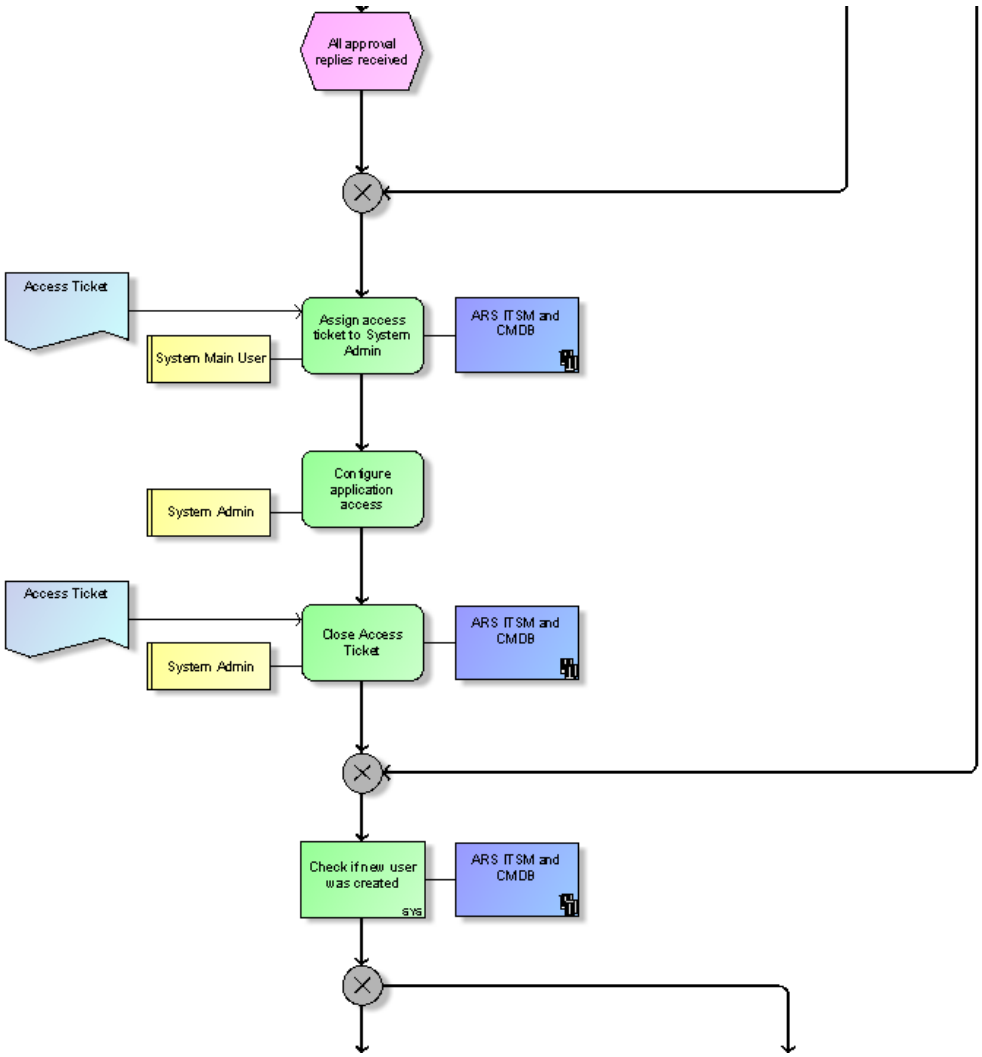
Kaavio 5. Käyttöoikeuden hallinta prosessikaavio, sivu 3.

Käyttöoikeuden hallintaprosessi (access management process).



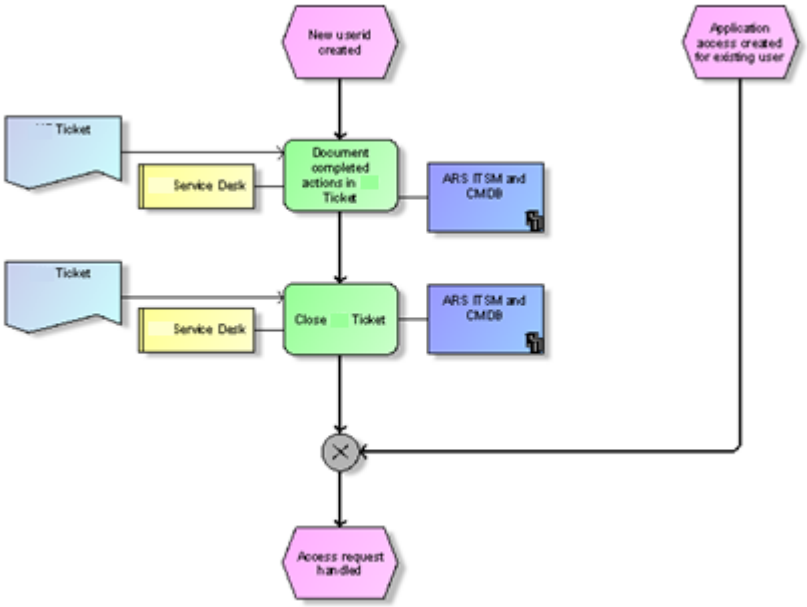
Kaavio 6. Käyttöoikeuden hallinta prosessikaavio, sivu 4.

Käyttöoikeuden hallintaprosessi (access management process).



Kaavio 7. Käyttöoikeuden hallinta prosessikaavio, sivu 5.

Käyttöoikeuden hallintaprosessi (access management process).



Kaavio 8. Käyttöoikeuden hallinta prosessikaavio, sivu 6.

Security aspects for Non-Corporate employees email usage

- Non-Corporate employees working for company must use company e-mail if any of the following conditions are met;
  - The non-Corporate employee is communicating with company customers by e-mail.
  - The non-Corporate employee's own e-mail is of public character (e.g. hot-mail, gmail, yahoo) and not dedicated for the non-Corporate employee's company.
- If none of the above conditions are met the consultant's company manager decides whether the non-Corporate employee shall use own e-mail or company e-mail.
- Important considerations when making the decision to use company email or not can be;
  - type of information that will be managed (e.g. sensitive information such as procurement documents, personal information, agreements etc. can increase the appropriateness to use company e-mail).
  - length of contract and position in company organization (e.g. non-Corporate employees with long term contract can increase the appropriateness to use company e-mail).

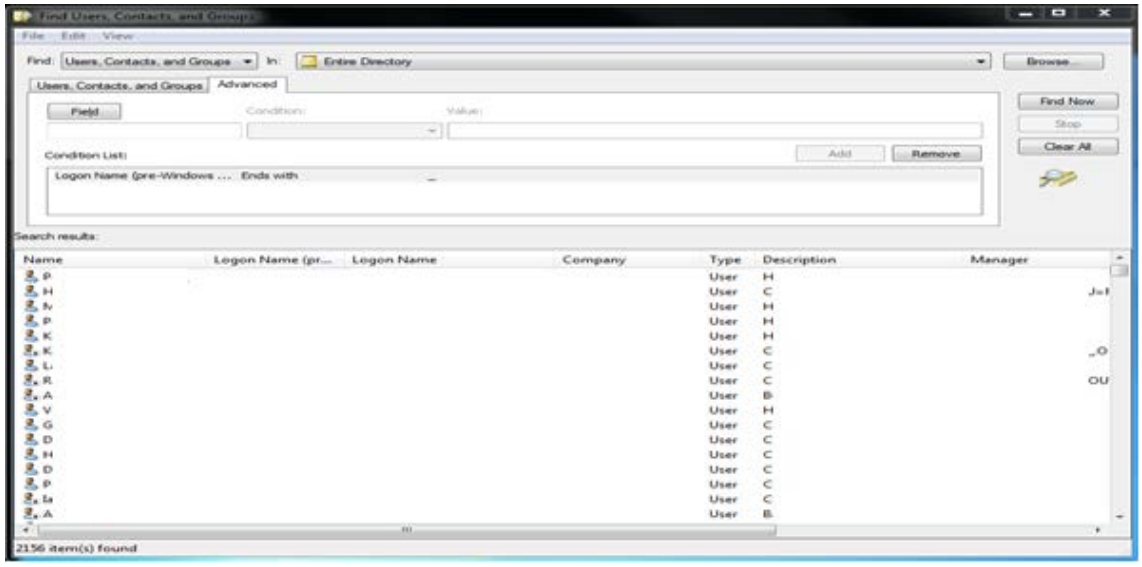
Note! If the non-Corporate employee uses his/her own company e-mail and is acting on behalf of company, the messages must clearly state that the non-Corporate employee is acting on behalf of company.

Henkilöydintieto standardi

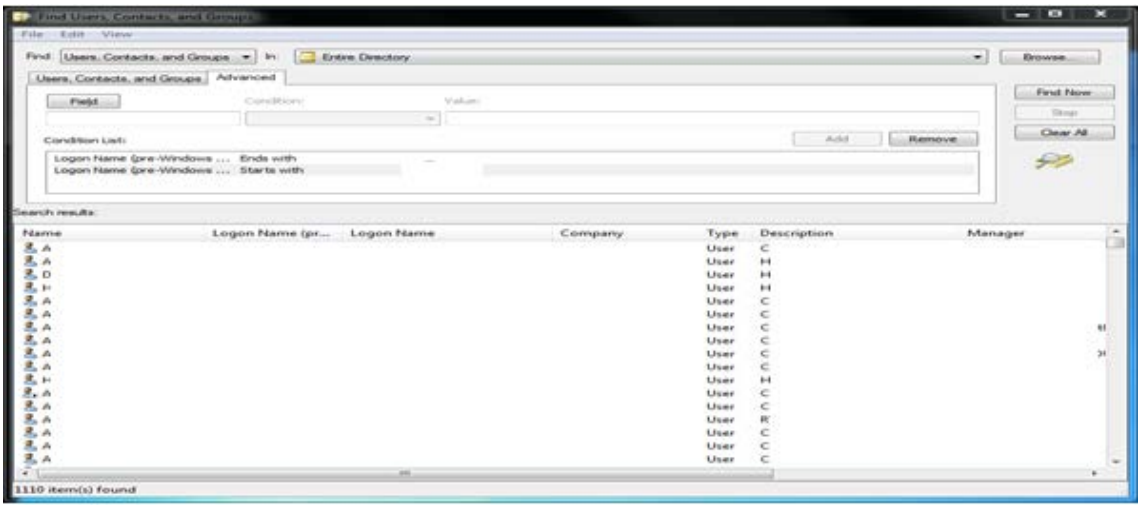
Information	Common HR MD for all Employees	Master system	Classification
First name	X	HR	Public
Last name	X	HR	Public
Employee number	X	HR	Public
User id	X	Active Directory (AD)	Public
Superior ID	X	HR	Public
Mobile phone number	X	Comppany Phone book	Public
Business Phone number	X	Comppany Phone book	Public
Company	X	HR	Public
Business unit	X	CMDB	Public
Division	X	HR	Public
Department	X	HR	Public
Respons code	X	CMDB	Public
Location code / Site Key	X	HR	Public
EmployeeType	X	HR	Public
HR status	X	HR	Public
RegularTemporary	X	HR	Public
Mother Tonque / preferred communication language	X	HR (proposal)	Public
Partner Code	X	CMDB	Public

AD Finder poiminta

2156 käyttäjällä on PAR-oikeus (login tunnus päättyy alaviivaan _)



Ulkoistuskumppanin PAR tunnukset 1110 kpl (xhpnnnnnnn_)



Ilmoitus käyttöoikeuden vanhenemisesta

From:
To:
Cc:
Subject: User Account for Rxxxxxxxx Kxxxxx (xxxxxxxx) Will Expire on 4.6.2014
Sent: ma 5.5.2014 4:08

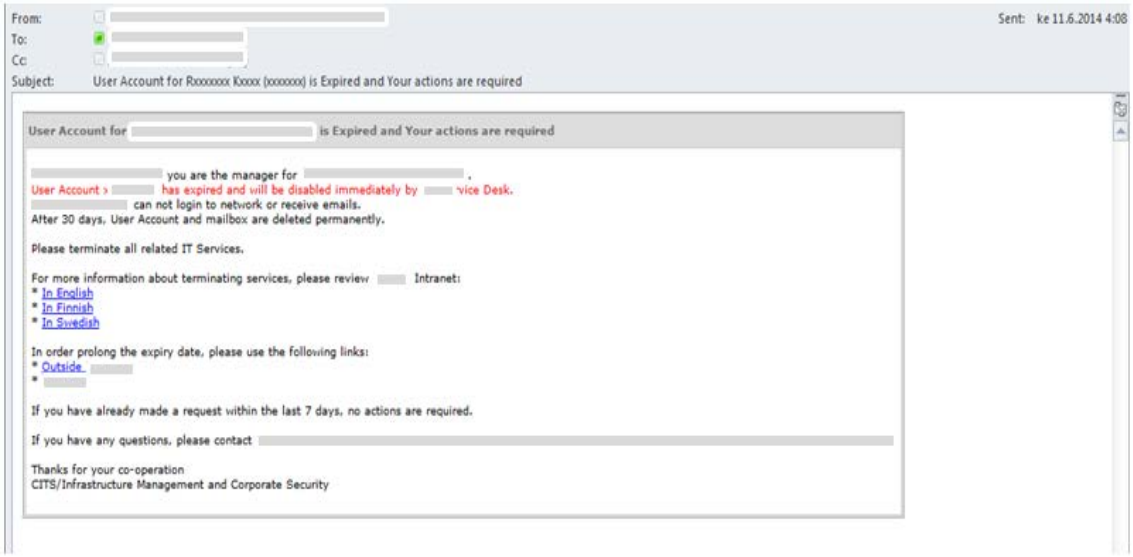
User Account for [redacted] Will Expire on 4.6.2014

[redacted] in order to prolong the expiry date or to terminate the User Account, please use the New My IT Portal - Subordinates

Please note that User Account cannot be used after it has expired, but Costs related to the User Account will continue to be invoiced until all the related services have been terminated.
For more information about terminating services, please review [redacted]
http://[redacted] /en/Services/it_and_telecom_services/it_and_telecom_services.htm

If you have already made a request within the last 7 days, no actions are required.

Thanks for your co-operation
CITS/Infrastructure Management and Corporate Security



From:
To:
Cc:
Subject: User Account for Rxxxxxxxx Kxxxx (xxxxxxx) is Expired and Your actions are required
Sent: ke 11.6.2014 4:08

User Account for [redacted] is Expired and Your actions are required

[redacted] you are the manager for [redacted] .
User Account > [redacted] has expired and will be disabled immediately by [redacted] vice Desk.
[redacted] can not login to network or receive emails.
After 30 days, User Account and mailbox are deleted permanently.

Please terminate all related IT Services.

For more information about terminating services, please review [redacted] Intranet:
* In English
* In Finnish
* In Swedish

In order prolong the expiry date, please use the following links:
* Outside [redacted]
* [redacted]

If you have already made a request within the last 7 days, no actions are required.

If you have any questions, please contact [redacted]

Thanks for your co-operation
CITS/Infrastructure Management and Corporate Security

IAM-liiketoimintavaatimukset

Identiteetinhallinta koostuu kokonaisuudesta, jonka osajoukkoja ovat ohjeistot, menetelmät, prosessit, henkilöydintieto ja käytettävät työvälineet. Näitä ovat muun muassa toiminnanohjausjärjestelmä Enterprise Resource Planning (ERP) ja konfiguraationhallintajärjestelmä (CMDB), MDM- tai HR-järjestelmä, hakemistopalvelu (AD) ja IAM-järjestelmä. Erillisen IAM-järjestelmän lisäarvoa tutkittaessa ja perusteltaessa hankintapäätöksiä, on hyvä tunnistaa IAM-järjestelmän tuoma lisäarvo yritykselle.

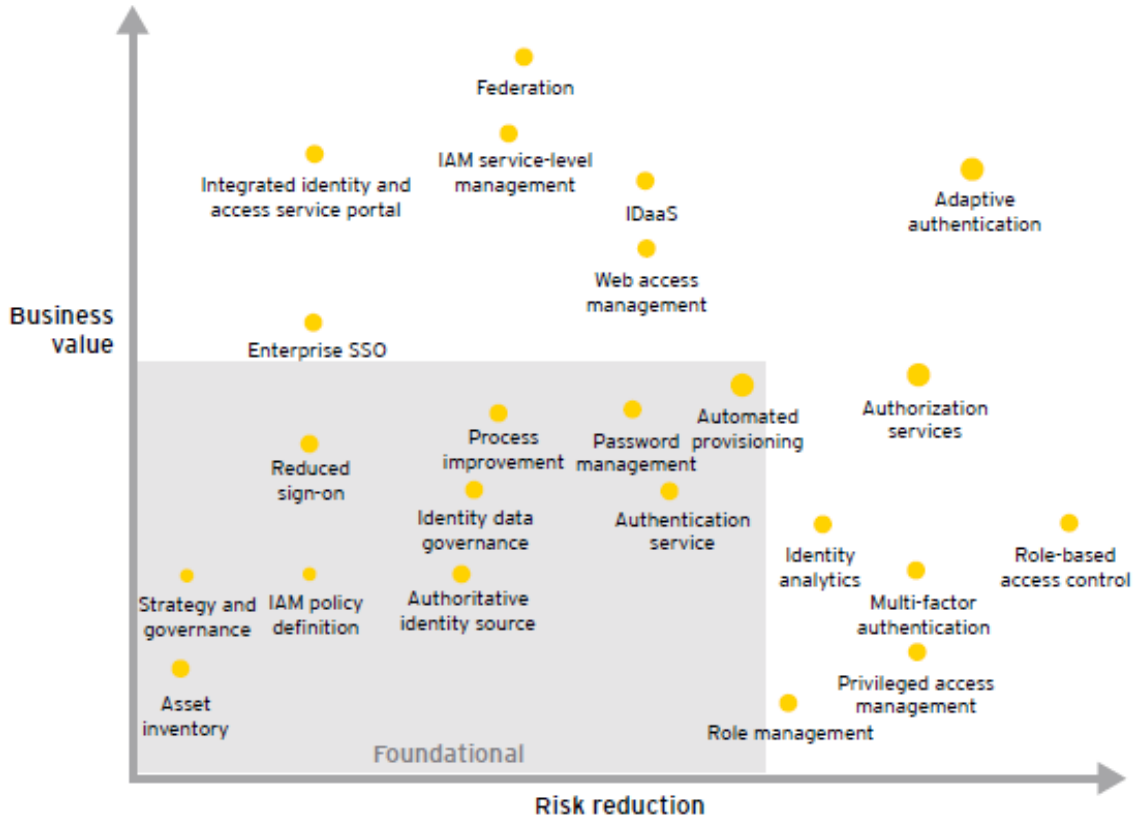
Riskienhallinnan näkökulmasta IAM-järjestelmän tuottama mahdollisuus analysoida ja raportoida olemassa olevia käyttöoikeuksia tai vaarallisia työyhdistelmiä rajoittuu luonnollisesti järjestelmien provisiointiasteen mukaiseksi. Automaattisen provisioinnin piirissä olevien järjestelmien käyttöoikeusraportointi voidaan toteuttaa IAM-järjestelmän avulla. Manuaalisen provisioinnin piirissä olevien järjestelmien käyttöoikeusraportointi on järjestettävä edelleen suoraan sovelluksen työvälineillä. Identiteettien ja tunnuksien keskitetty hallinta voidaan nähdä riskien hallinnan ja tietoturvallisuuden kannalta kehittyneinä kontrolleina ja varsinkin seurantamahdollisuuksina verrattuna nykyiseen tilanteeseen. Tällä hetkellä keskitettyä raportointia ei ole tarjolla.

Ernst & Young tutkimuslaitoksen esityksen mukaan IAM-järjestelmän ominaisuuksia voidaan kuvata riskien pienentämisen ja liiketoiminnan arvon mukaan. Heidän näkemyksen mukaan rooliperusteinen käyttöoikeuskontrolli vähentää riskejä liiketoiminnalle merkittävästi. Samalla on huomattavat, että malli ei kuitenkaan tuota merkittävää taloudellista lisäarvoa liiketoiminnalle. (Ernst & Young 2013, 16). O'Conorin mukaan rooliperustainen käyttöoikeusmallin hyötyjinä on liiketoiminta-johto, henkilöstöhallinto ja IT-hallinto. (O'Conor et al. 2010, 12).

Hyvin suunniteltu ja toteutettu roolipohjainen käyttöoikeusmallin tukee linjajohtoa ja liiketoimintojen vastuuhenkilöitä käyttöoikeuksien tilauksissa ja muutostilanteissa. Tätä kautta pohdin liiketoiminnan saamaa lisäarvoa rooliperusteisesta käyttöoikeusmallista. Mielestäni saavutettu arvo on suhteellisesti korkeampi kuin kuvassa on esitetty. Perustelen näkemystäni roolipohjaisen käyttöoikeuskäsittelyn avulla automaation lisäämisellä. Automaattinen provisiointi nopeuttaa sovellustasolla käyttöoikeuksien aktivointia. Hyvin suunniteltu roolipohjaisten käyttöoikeuksien automaattisen provisioinnin voidaan nähdä vähentävän liiketoimintojen IT-asiantuntijoiden tekemää käsityötä. Automatisoinnin lisääminen avulla käyttöön palkatut resursseille voidaan provisioida tarvittavat käyttöoikeudet esimiehen ja hyväksymisketjun toimenpiteillä. Automaation lisääminen voidaan toteuttaa selkeillä työrooleihin perustuvilla käyttöoikeuksilla.

Ernst & Youngin esityksen perusteella (kuva 4) IAM-peruspakettiin voidaan nähdä kuuluvan omaisuudenhallintatuote (asset inventory). Käsittelen tätä tuotetta sovellus- ja lisenssihallintaa tukevana moduulina. Tarkasteltavassa tapauksessa asset inventory ei tuo suoraan lisäarvoa yritykselle. Yrityksen käytössä on erillinen ohjelmistolisenssien hallintaohjelmisto sekä varsinainen yrityksen IT-omaisuuden hallintaan tarkoitettu tietokanta (CMDB). Tässä näkökulmassa Ernst & Youngin esitystä on syytä tarkastella analyyttisesti ja arvioida esitystä yrityksen omista näkökohdista.

Kirjautuminen eri järjestelmiin samalla käyttäjätunnuksella ja salasanalla (Federation) on esityksessä nostettu korkeimmalle liiketoiminnalle lisäarvoa tuottavana yksittäisenä komponenttina. Federoinnin liiketoiminta-arvostuksen nosto noinkin ylös tässä yhteydessä voi kummastuttaa. Toisaalta voin perustella korkeaa sijoitusta sillä, että liiketoiminnalle on helppo osoittaa lisäarvoa IAM-tuotteesta, jonka avulla onnistuu kertakirjautuminen moniin paljon käytettyihin järjestelmiin. Rooliperustainen käyttöoikeushallinta ja kertakirjautuminen ovat liiketoimintatapauksia, joiden avulla IAM-järjestelmän hankintaa voidaan perustella liiketoiminnan päättäjille.



Kuva 4. Ernst & Youngin esitys IAM komponenttien vaikutuksista liiketoiminnan arvoon ja riskien pienentämiseen.

Yrityksen henkilötiedot voidaan kuvata henkilöydintietojen standardimallin avulla (liite 4). Standardimalli on päivitettävä ja hyväksytettävä vastaamaan myös ulkoisten työntekijöiden henkilöydintiedon käsittelyn tarpeita. Tässä tapauksessa konkreettisena lisäyksenä standardiin voin suositella sopimuksen aloitus- ja päättymispäivän lisäämistä. Tämän lisäyksen avulla voidaan seurata sopimuksen päättymispäivää ja suorittaa tarvittaessa automaattisesti käyttöoikeuden päättäminen sopimuksen päättyessä. Identiteetinhallinnan teknisen konseptin vaatimusmäärittely on syytä aloittaa tässä yhteydessä. Teknisen konseptin kuvauksessa otetaan kantaa yrityksen kokonaisarkkitehtuurimallin osa-alueiden antamien ohjeiden mukaan tekniseen toteutukseen, käytettäviin tietovarastoihin ja identiteetinhallinnan apuna

käytettäviin työkaluihin. Ennen IAM-projektia on syytä tunnistaa käytettävien henkilöydintietojen autoratiivinen lähde ja tutustua tiedon laatuun. IAM-järjestelmän automatisoitujen toimintojen kannalta henkilöydintiedonlaatu on merkittävässä roolissa. Tietoentititeettien merkityksen ja merkintätavan on säilyttävä samana läpi koko tietovaraston. Esimerkkinä vaikkapa postitoimipaikan merkintä. Ihmisen ymmärrys käsittää Helsinki, Hesa ja Hki merkinnät samaa tarkoittavana paikkakuntana. Tietojärjestelmän kannalta näillä esitystavoilla on eri merkitys. Tietojen laadun varmistamiseksi on tässä vaiheessa syytä aloittaa henkilöydintietojen siivous ja yhdenmukaistaminen. Tähän työhön on varattava resursseja ja aikaa riittävästi.

IAM-palvelun suunnittelussa on otettava huomioon muuttuneiden liiketoimintatarpeiden asettamat vaatimukset. Tämän päivän työssä tiedon käyttäjän tarpeet päästä tietoon aina ja kaikkialla sekä pilvipalveluiden käyttöönotto aiheuttavat tiedon suojaamiselle uusia vaatimuksia. Liiketoimintojen vaatimukset ajasta ja paikasta riippumattomaan tiedon käyttämiseen ja samaan aikaan vaatimukset omien laitteiden käyttämiselle työn tekemisessä asettavat identiteettien hallintaan omat haasteensa.

IAM-projektin myyntityö on hyvä aloittaa visiolla tai ajatuksella, jonka avulla kuvataan projektin hyödyt liiketoiminnoille. Visio IAM-työn aloittamiselle ja ajatuksen myyntiin voidaan kuvata vaikkapa seuraavilla ajatuksilla ja tavoitteilla.

- Kulujen vähentäminen

- Nopeuden lisääminen

- Läpinäkyvä raportointi

- Tietoturva-tason kehittäminen

Näitä iskulauseita on syytä avata erillisessä esityksessä.

Operatiivisten kulujen vähentäminen voidaan perustella tapahtuvan itsepalvelun lisäämisellä ja tilausten läpimenoaikojen nopeutumisella. Tästä voidaan johtaa automaation lisäämisen vähentävän palvelupyyntöjen määrää IT Service Deskille ja

yksiköiden IT-henkilöstölle. Samalla käyttöoikeushallinnan tehostaessa toimintaa, asiakastyytyväisyyden voi olettaa nousevan nopeampien vasteaikojen myötä. Olettamuksena on, että oikein suunnitellun ja määritellyn käyttöoikeuden tilauksen, hyväksymisen ja käyttöönoton kautta käyttäjätunnusprosessissa tehtyjen virheiden määrä vähenee. Automaation avulla käsityön määrä liiketoimintasovellusten käyttöoikeusylläpidossa voidaan saada vähenemään.

IAM-järjestelmän sisältämien raportointi ja tapahtumien kirjausominaisuuksien avulla käyttöoikeuksiin kohdistuviin muutostapahtumiin on mahdollista saada todellista seurantaa ja todisteita tehdyistä muutoksista. IAM-järjestelmän selkeänä etuna muutosseurantaan on, että oikeuden pyytämisestä jää rekisterimerkintä. Käyttöoikeuden pyyntö ja hyväksyntä voidaan todentaa myöhemmin. Käyttäjätunnusten automaattinen provisiointi liiketoimintasovelluksissa, mahdollistaa nopean käyttöoikeuksien käyttöön ottamisen. Yrityksen intranetin keskustelusta poimittu kommentti, jossa kerrottiin, "Kesätyöntekijä sai tunnukset vasta viikon odottelun jälkeen" (Intranet. 2015)., voidaan automaation lisäämisen avulla jättää historiaan.

Ajantasaiset näkymät käyttöoikeuksiin on mahdollista IAM- järjestelmän tilannekuvanäkymien avulla. Järjestelmistä on saatavilla helposti ja nopeasti auditointia tukevaa raportointia sekä vaarallisten työyhdistelmien riskiraportit System Managereiden, riskien hallinnan ja tilintarkastajien tarpeita varten. Luonnollisesti raportoinnin ulottaminen sovellustasolle vaatii vahvaa panostuista käyttöoikeushallinnan kehittämiseen myös liiketoimintasovellusten omistajien ja System Managereiden toimesta. Tietoturvatason kohottaminen voidaan todistaa ainakin tunnuksen käytön päättämisprosessissa ja käyttäjätunnuksen de-provisioinnissa liiketoimintajärjestelmistä. Käyttöoikeuden päättäminen kaikista alijärjestelmistä yhden järjestelmän kautta yhdellä toimenpiteellä on vahva tietoturvatason kohottamiseen johtava toimenpide.

IAM-projektin käynnistäminen

IAM-projekti lähtee liikkeelle identiteetin omistajan ja liiketoimintojen yhteisellä päätöksellä. Projektin omistajuus on luonnollisesti yrityksen Chief Information Officer (CIO) johtajan alaisuudessa. Liiketoimintojen voidaan nähdä hyötyvän eniten identiteetin turvallisesta ja tehokkaasta hallinnasta, rahoitus projektille on saatava liiketoiminnoilta. Liiketoimintojen edustus on välttämätöntä olla mukana projektin johtoryhmässä ja suunnittelussa. HR:llä on vahva rooli henkilöydintiedonhallinnassa, joten heidän edustus on luonnollisesti mukana suunnittelutyössä. IT:n rooli ei ole vähäisin vaan IT on mukana vahvasti toteutuksen järjestelyissä ja tuotteiden implementoinnissa.

IAM-kehitystyössä on päätettävä tullaanko järjestelmää käyttämään koko yrityksen tarpeisiin. Tällä tarkoitan myös yrityksen asiakkaiden identiteetin ja pääsyhallintaa käsiteltäisiin samassa IAM-järjestelmässä. Vai rajoitetaanko IAM-järjestelmän käyttö esimerkiksi varsinaisten ja vuokratyöntekijöiden identiteettien ja pääsyoikeuksien hallintaan.

Seuraavassa on muutamia yleisiä IAM-järjestelmän tarjouspyynnön valmistelussa huomioon otettavia liiketoimintavaatimuksia. Näitä määrityksiä voidaan käyttää Request for Proposal (RFP) vaiheen valmistelussa. Yrityksen käyttöoikeushallinnan tulee käsitellä 10000 työntekijätunnusta ja 5000 ulkoista palveluiden tuottajaa. Järjestelmänvalinnassa on varauduttava käsittelemään itsepalveluportaalin avulla noin 200000:nen asiakkaan käyttäjäoikeuksia.

Kuten teoriaosassa järjestelmäarkkitehtuurista kuvattiin, arkkitehtuurimallissa otetaan kantaa mihin järjestelmiin keskitetty identiteetti voidaan provisioida. Lidenin mukaan todellisessa elämässä ei ole mahdollista tuottaa identiteetin provisiointia kaikille yrityksen tietojärjestelmille. (Liden 2012, 44). Lidenin esittämään väitteeseen on helppo yhtyä. Tätä kirjoitettaessa yrityksen CMDB-järjestelmään on talletettu tiedot 1010:stä erillisestä aktiivisesta sovelluksesta (CMDB 25.1.2015).

Valistunut olettamukseni on, että suurin osa käytössä olevista sovelluksista ei käytä käyttäjän autentikointia. Käytössä olevien järjestelmien valmiuksia käyttöoikeuden käsittelyyn saatikka provisioinnin hyödyntämiseen on vaikea arvioida ilman tarkempaa tutkimusta järjestelmien toiminnallisuuksista. Heinon mukaan IAM-projektissa provisioinnin suunnittelu kannattaa aloittaa alle viidestä tietojärjestelmästä. Heino perustelee näkemystään liiketoiminnan tehokkuusvaatimuksella. Jos käyttäjätunnuskäsittelyn provisiointiin käytetty aika on pitkä ja tätä kautta kustannukset provisioinnille nousevat korkeiksi suhteessa saavutettuun hyötyyn. Toinen näkökulman on käyttäjätunnusvaihtelun määrä vuositasolla. Jos vaihtelu ei ole merkittävä, on manuaalinen provisiointi edelleen erittäin suositeltava vaihtoehto (Heino 2015).

Käyttöoikeuden tilaaminen, hyväksyminen, käyttöoikeuden lisääminen (provisiointi), muuttaminen sekä tunnuksen sulkeminen (de-provisiointi) tulee olla hallittavissa itsepalveluportaalin kautta. Integraatiorajapinnat on toteutettava projektissa seuraaviin järjestelmiin: AD (Exchange, SharePoint), ERP-, HR- ja Service Desk-järjestelmä.

Pääkäyttäjätunnusten käsittelyyn valmistellaan erillistä PAM-tuotetta. IAM-tuotteen ja tulevan PAM-järjestelmän välinen integrointi ja provisiointi toiminnot on pystyttävä toteuttamaan käyttöönotossa. Lisäksi järjestelmän on tuettava lokien ja hälytysten välittämistä yrityksen SIEM-järjestelmään. Käyttöoikeuksien ajantasainen valvonta ja raportointi on toteutettava tilannekuvatyyppisellä käyttöliittymällä. Käyttöoikeuksien- ja tapahtumienraportointi tapahtuu tilaajan vapaassa käytössä olevan raporttigeneraattorin avulla.

Käyttöönottoprojektissa on varattava riittävä resursointi niin tilaajan, kuin toimittajan asiantuntijoista. Tyypillisesti käyttöönotto alkaa projektin asetus ja määrittelyvaiheella. Tässä yhteydessä projektin omistaja määrittelee projektin johtoryhmän ja projektipäällikön. Hyvin usein muistutetaan yrityksen johdon sitouttamisesta projekteihin, tässä yhteydessä johdon tuki on erityisen tärkeää, koska projektin tuottamilla muutoksilla on merkittäviä vaikutuksia liiketoimintojen riskien hallintaan.

Projektin märittelyvaiheessa luodaan yksityiskohtainen projektisuunnitelma. Tässä yhteydessä on syytä rakentaa myös testaus- ja viestintäsuunnitelmat sekä viimeistellä vaatimuslista projektin tuotoksille. Ratkaisun arkkitehtuurimalli, järjestelmä arkkitehtuuri ja yksityiskohtaiset suunnittelumallit tuotetaan tässä vaiheessa. Suunnitelmien hyväksynnän jälkeen suoritetaan järjestelmän asentaminen. Tähän vaiheeseen pääsemiseen käytetään aikaan kaksi kuukautta.

Päijäsen mukaan IAM-järjestelmän tuotantoon siirtäminen on syytä toteuttaa suunnitelluissa vaiheissa. Testiympäristön avulla voidaan havaita olemassa olevan henkilöydintiedon toimivuutta ja tiedon laatua. Testauksella tuotetaan arvokasta tietoa ja kokemusta provisioinnin toiminnasta valittuihin kohdejärjestelmiin. Ensimmäisinä IAM-järjestelmän provisiointikohteina on suositeltavaa koeponnistaa ensimmäisenä vaikkapa yhteydet AD- ja Email-järjestelmiin. Ennalta määriteltyjen ja hyväksyttyjen testikierrosten jälkeen järjestelmät voidaan liittää kokonaisuuteen. (Päijänen 2014).

Järjestelmän varsinaisessa implementoinnissa ja tietojen analyysivaiheessa käytettävissä olevat identiteetit ladataan autoratiivisista lähteistä. Tämän hetken tilanteessa autoratiivisia lähteitä olisivat hybridimallin mukaisesti HR- ja AD-järjestelmät. Tietojen sanitointi, esimerkkinä orpojen identiteettien korjaaminen suoritetaan asiakkaan toimesta. Järjestelmän asentamiseen ja tietojen analyysivaiheeseen on varattava kuukauden työpanos.

Mallintamisvaiheessa työnkulkuprosessi rakennetaan järjestelmään. Roolien hallinta ja mallintaminen suoritetaan standarditapausten perusteella. Tässä vaiheessa ei oteta kantaa kaikkien sovellusten käyttämiin rooleihin, vaan keskitytään standardiroolitukseen. Rooli voi vastata kysymykseen onko identiteetillä käyttöoikeutta internetiin, intranetiin tai vaikkapa sähköpostiin. Hienojakoisemmat sovelluskohtaisten roolien suunnittelu ja rakentaminen on suoritettava ensin valmiiksi sovellustasolla. Tämän työn jälkeen sovelluksen rooleja voidaan käyttää IAM-järjestelmän provisioinnissa. Tämän työn kokonaiskestoaika ei saa ylittää kahta viikkoa.

Toimivan käyttöympäristön luomisen jälkeen keskitytään konfigurointiin ennalta valittujen provisiointikohteiden osalta. Ensimmäisinä luonnollisina konfigurointikohteina ovat yrityksen hakemistopalvelu eli AD, HR-järjestelmä ja toiminnanohjausympäristö (ITSM). Tässä oletuksena on, että IAM-järjestelmässä on valmiit rajapinnat kohdejärjestelmiin. Jos rajapintoja joudutaan ohjelmoimaan, niin projektiin on varattava lisäaikaa näiden määritysten ja ohjelmointimuutosten toteuttamiseksi. Käyttöönoton valmisteluun ja automaattisen provisioinnin asetusten hienosäätöön, ennalta RFP:ssä määriteltyjen kohteiden osalta oletetaan kuluvan aikaa kaksi kuukautta.

Toiminnallisessa testaamisessa tavoitteena on koestaa asennuksen provisiointi ja de-provisioinnin toimivuus testiympäristöihin ja testiympäristöistä oikealla tuotannosta siirretyllä materiaalilla. Ennen testauksen hyväksymistä on oltava suoritettuna raportointi, hallintanäkymät ja hälytysten koeajot. Koulutus käyttöhenkilökunnalle, tilaajan edustajille ja service deskille suoritetaan testikannalla. Tuotantoon implementointi suoritetaan asiakkaan hyväksymän testivaiheen jälkeen. Koeajoon, konfiguroinnin säätämiseen, koulutukseen ja tuotantoon siirtymiseen oletetaan kuluvan aikaa noin kuukausi. Projektin tehtäviin kuuluu luonnollisesti järjestelmän dokumentointi, jota suoritetaan järjestelmän kehittyessä. Loppudokumenttiin kootaan yhteen tiedot tuotantoon siirretystä järjestelmästä.

Todellisen IAM-tarjouksen mukaan käyttöönottoprojektin hyvin objektiivinen läpimenoaika on viisi kuukautta. Saadussa IAM-tarjouksessa on huomioitu työntekijöiden ja ulkoisten työntekijöiden tunnusten käsittely sekä provisiointien rakentaminen viiteen yrityksen käytössä olevaan järjestelemään. Nähdäkseni järjestelmän esisuunnitteluun, rahoituskeskusteluihin ja sisäisiin hyväksymismenettelyihin on syytä varata kalenteriaikaa merkittävästi enemmän. IT-järjestelmien hankintaan, toimitukseen ja asennuksiin on lisäksi varattava aikaa noin kaksi kuukautta. Kokonaisuudessaan oletan projektin vievän kalenteriaikaa noin vuoden.

Hinnoittelu

Tämän työn yhteydessä pyysin tarjouksen IAM-toimittajalta ylläkuvatun RFP:n perusteella. Luottamuksellisuuden vuoksi en esittele toimittajaa tai tuotetta yksityiskohtaisesti. Tässä tarkastelussa oleva IAM-tuote on menestynyt tutkimuksen mukaan maailmanlaajuisesti viiden toimittajan kärkikaartiin (Iverson et al. 2015). Tarjotun tuotteen markkinaosuus globaalista IAM-markkinasta on merkittävä.

Tuotteen hankintahinnan lisäksi on huomioitava tuotteen asennus ja projektikulut. Sisäisiä kuluja syntyy oman henkilökunnan ajankäytöstä projektin ohjausryhmän ja projektiryhmän kokouksiin. Yrityksen oman henkilökunnan resursseja ja aikaa on varattava työhön, jota ovat ainakin henkilöydintietojen siivoaminen, suunnittelu, liiketoimintojen näkemysten kartoitus, sisäinen markkinointi, viestintä, esimieskoulutus jne.

Saadun tarjouksen mukaan asiakkaan projektimanagerin tulisi varata työaikaa implementointiprojektiin 6,5 päivää. Arvio asiakaan projektipäällikön ajan käytöstä on mielestäni kovin objektiivinen. Näkemykseni mukaan projektipäällikön työmäärä nousee merkittävästi suuremmaksi, kuin tässä esitetty. Alustavaan määrittelytyöhön ja siivoamistyön valmisteluun, sekä johtamiseen on varatta riittävästi aikaa ja resursseja myös eri liiketoiminnoista. Näkemykseni mukaan yrityksen sisällä tehtävään työhön kuluu kaikilta projektiin osallistuvilta helposti satoja työtunteja.

Kuten aiemmin totesin, manageriroolissa toimii noin 500 henkilöä. Olettaen että kaikille managerin roolissa oleville henkilöille tarjotaan tunnin koulutus muuttuneista prosesseista on helposti noin 500 tuntia käytetty. Jos managerin laskennallinen tuntipalkka sivukuluineen on 50 euroa koulutukseen käyttävän työajan laskennallinen hinta olisi 25.000 euroa. Tehostamalla muutoksen viestintää voidaan näitä luokkahuonekoulutuksia vähentää merkittäväsi. Muista projekteista saamani kokemuksen perusteella yrityksen viestinnän ja markkinoinnin ammattilaisten ammattitaitoa on hyvä käyttää hyväksi myös sisäisessä muutoksen johtamisessa. Viesti muutoksesta saadaan välitettyä kohderyhmälle ammattimaisesti ja tehokkaasti.

Haastateltavat

Haastateltava 1. Yrityksen tukipalvelut. Haastattelu 7.10.2014.

Haastateltava 2. Yrityksen IT-palvelut. Haastattelu 27.5.2014.

Haastateltava 3. Yrityksen IT-palvelut. Haastattelu 27.1.2015.

Haastateltava 4. Yrityksen tukipalvelut. Haastattelu 16.10.2014.

Haastateltava 5. Liiketoiminta. Haastattelu 17.10.2014.

Haastateltava 6. Liiketoiminta. Haastattelu 20.10.2014.

Haastateltava 7. Yrityksen IT-palvelut. Haastattelu 16.10.2014.

Haastateltava 8. Yrityksen IT-palvelut. Haastattelu 7.10.2014. 01/2015.

Haastateltava 9. Yrityksen IT-palvelut. Haastattelu 22.10.2014.

Haastateltava 10. Yrityksen tukipalvelut. Haastattelu 02/2014.

Haastateltava 11. Ulkoistuskumppanin palvelutoiminta. Haastattelu 31.10.2014.

Haastateltava 12. Liiketoiminta. Haastattelu 13.2.2015.

Haastateltava 13. Liiketoiminta. Haastattelu 4.2.2015.

Haastateltava 14. Yrityksen tukipalvelut. Haastattelu. 11.2.2015.

Tutkimus- ja haastattelukysymykset

Tutkimuskysymys 1. Millaisia odotuksia käyttöoikeuden tilaajilla on tilausprosessiin?

- Millaisia käyttö- ja pääsyoikeuksia tilaat uudelle konsultille?
- Oletko tilannut konsulteille käyttöoikeuden, etäkäyttöoikeuden, internetkäyttöoikeuden, extranet-oikeuden, remote desktop -oikeuden, PAR-oikeuden, LAREDO-oikeuden?
- Voitko näyttää missä ovat tilauksessa tarvitsemasi ohjeistot?
- Jos järjestelmä mahdollistaisi ulkoisen ylläpidon tunnuksien avaamiselle, niin voisiko mielestäsi käyttäjätunnuksen tilaamisesta ja ylläpidosta vastata alihankkija?
- Millaisia odotuksia sinulla on käyttöoikeuksien tilaukseen?

Tutkimuskysymys 2. Millaisia odotuksia prosessin käyttäjillä on käyttöoikeusprosessin läpimenoaikoihin?

- Mikä on mielestäsi hyväksyttävä toimitusaika peruskäyttöoikeuden tuottamiseksi: tunteja, työpäiviä, enemmän kuin työviikko (viisi työpäivää tilauksesta)? Jotain muuta, mitä?
- Vaaditteko konsulteilta NDA-sopimuksen allekirjoittamista ennen sopimuksen hyväksymistä?
- Missä tilanteessa tarvitsette konsulteille henkilökohtaista taustatarkastusta?
- Mistä tilaatte taustatarkastuksen?

- Millaista koulutusta tarjoatte konsultille työn aloituksessa suoritettavassa työnohjauksessa? Tarkkaile erityisesti vastausta tietoturvakoulutuksesta.
- Millaisia lisäpalveluita tarvitset konsulttien käyttäjätunnuksen ja käyttöoikeuksien hallintaan?

Tutkimuskysymys 3. Kuinka tilaaja haluaa kehittää käyttöoikeuden elinkaaren hallintaprosessia?

Käyttöoikeuden avaaminen ja sulkeminen.

- Saatko tarvittavat oikeudet haluttuihin järjestelmiin yhdellä tilauksella?
- Millaisia muutoksia haluat tehdä käyttöoikeuden tilausohjeistoon?
- Onko konsulteille jäänyt aktiivisia käyttöoikeuksia työsuhteen päättymisen jälkeen?
- Saatko ilmoituksen konsultin työsuhteen päättymisestä konsultilta itseltään, konsultin työnantajalta vai et mistään?
- Kuka on vastuussa konsultin käyttöoikeuden päättämisestä?

Käyttöoikeuden muutokset ja uudistaminen. Konsultin käyttäjätunnus uudistetaan normaalisti kuuden kuukauden välein. Ilmoitusviestit ovat esillä liitteessä 6.

- Kuinka usein konsulttitunnuksen käyttöoikeuden uudistaminen on mielestäsi syytä suorittaa?
- Perustele esittämäsi toimintatapa?

Taulukot

Tässä liitteessä on kuvattu toimintaohjeet raportissa esiteltyjen taulukoiden tuottamiseksi.

Taulukko 1. Käyttäjätunnusten jakauma, sisältäen loppukäyttäjä- ja pääkäyttäjätunnukset taulukon tiedot poimin raportista "All_UserIDs_2015-01-01". Tulokseen pääsin hakemalla tiedoista ADStatus=Enabled. Poimin aputaulukkoon "Käyttäjätunnukset AccountType pvm" UserAccount ja AccountType -sarakkeet. Näiden tietojen avulla loin Pivot-taulukon, jossa ryhmittelin tulokset AccountType-kentän mukaan sekä laskin ilmentymien käyttäjätunnusmäärät ja esiintymien prosenttiosuudet.

Taulukko 2. Tässä esitellyt käyttäjätunnusten käsittelyyn liittyvien tapahtumien perustiedot ovat saatavissa raportilta "All_UserIDs_2015-01-01". Käsittelin raportin kenttiä ADStatus ja ADObjeCreated erillisessä työtilassa, jossa poimin lopulta alla esitetyt arvot. Näiden lähtötietojen avulla tein graafiset esitykset (kuvio 6 ja 7).

AD-tunnuskäsittelyn määrät.

	Enable	Disable	Terminate	Delete	
Kesäkuu	286	1	40	47	374
Heinäkuu	163	1	28	6	198
Elokuu	206	1	9	8	224
Syyskuu	274	2	5	5	286
Lokakuu	295	1	2	11	309
Marraskuu	265	1	1	4	271
Joulukuu	213	0	0	2	215
Yhteensä	1702	7	85	83	1877

Deleted	85
Disabled	6
Enabled	1702

Terminated	85
	1878

Taulukko 3, "Tunnusta ei ole käytetty viimeiseen kolmeen kuukauteen" esitellään yli kolme kuukautta käyttämättä olleet käyttäjätunnukset. Tämä tieto saadaan poimittua kuukausittain julkaistavasta All_UserIDs_vvvv-kk-pv Excel-raportista yrityksen CMDB-tilastoarkistosta. Taulukkoon on poimittu aktiiviset käyttäjätunnukset , näistä on poimittu Domain Not Ok ilmoituksella olevat rivit. Domain Not Ok merkintä asetetaan automaattisesti AD:ssä käyttäjätunnuksiin, jotka ovat olleet käyttämättöminä yli kolme kuukautta. Tämän tiedon perusteella jaoin Account Typen mukaan työntekijöiden, konsulttien ja yhteiskäyttötunnusten esiintymät taulukkoon. Tuloksissa laskin yhteen konsulttitunnuksen ja konsultin pääkäyttäjätunnukset.

Taulukko 4, "PAR-prosessin läpäisyaikoja (CMDB 7.1.2015)." taulukkoon on poimittu PAR-prosessin läpimenoaikoja. Perustiedot poimin IT Service Management Data Warehouse työkalun raportin "Volumes by Resolution Time (graph)". ITSM-kuvion tiedoista laskin läpimenoajat 0–24 tuntia sekä 24–160 tuntia omiin ryhmiinsä ja perustin saaduista tuloksista taulukkonäkymän Word-tekstinkäsittelyohjelman työkaluilla.

Kuviot

Tässä liitteessä on kuvattu toimintaohjeet raportissa esiteltyjen kuvioiden tuottamiseksi.

Kuvio 1. Konsulttitunnusten jakautuminen maittain. Konsulttitunnusten jakautuminen maittain tiedot poimin raportista "All_UserIDs_2015-01-01". Taulukon ADSiteID-sarake sisältää käyttäjätunnuksen käyttäjän kotimaan ja paikkakunnan, esimerkiksi muodossa FIESP tai SESTO. ADSiteID-sarakkeen maatietojen avulla poimin tunnusten maakohtaiset esiintymät.

Kuvio 2. Privileged Account Management -arkkitehtuuri kuvio on toteutettu PowerPoint-työkalulla.

Kuvio 3. Roolipohjainen käyttöoikeusmalli, mukaillen koulutusmateriaalia. Valmistin kuvion SharePoint-työkalulla.

Kuvio 4. PAR-oikeuksien jakauma käyttäjätyypeittäin. (CMDB-raportit).

Aktiivisten käyttäjätunnusten ja palvelinten tiedot on tuotu käyttäjätunnustiedoista (All_UserIDs_2015-01-01) ja palvelinten PAR-käyttöoikeustaulukosta (Servers_PAR_2014-01-01). Palvelimien PAR-taulukosta poimittuihin tietoihin (UserAccount, AdminAccount, AccountType ja Server) yhdistin All UserIDs tiedoista käyttäjätunnuksen tyypin (UserType). Tämän tyypin yhdistin PAR-listalla olevaan käyttäjätunnukseen Excelin funktiolla: =VLOOKUP($A2;AllUsers!$A$1:$B$13511;2;0).

Koontitaulukon näkymän kokosin Excel Pivot -taulukoinnin avulla. Asetin ReportFilter kentään UserType-tiedon, Row Labels -kenttään poimin AdminAcoount-tiedot ja Values kenttään Count of Server -lukumäärät. Tällä menettelyllä tietojen poiminta voidaan tarvittaessa toistaa tulevissa seurannoissa.

Kuvio 5. "Käyttäjätunnukseen liittyvien tehtävien käsittely- ja läpimenoaikoja ajalla 06 – 12 / 2014" kuviossa esitellyt läpäisyajat poimin IT Service Management Data Warehouse -työkalulla. Tietojen poiminnassa käytin raporttia "Number of tickets by

resolution time (graph)". Poiminnan tein sovellukselle "AD User Account". Kuvaajapylväiden asteikko kuvioissa 4 ja 6 on jaettu kuuteen läpimenoaikaa kuvaavaan alueeseen. Pylväiden läpimenoaikamittaukset on jaettu kuuteen osaan seuraavasti. Alin ryhmä kuvaa prosessin läpimenoaikaa nollasta kuuteen tuntiin, toinen ryhmä kuudesta 12:sta tuntiin (sininen), kolmas ryhmä on 12:sta 24:ään tuntiin (keltainen), neljäs ryhmä 24:stä 40:een tuntiin (vihreä), viides ryhmä 40:stä 160:een tuntiin (tumman punainen) ja viimeinen ryhmä kuvaa prosessin läpimenoaikaa tapauksissa, joissa prosessin kesto on ylittänyt 160 tuntia. Käytössä olleen Data Warehouse työkalun asetukset tälle raportille on kuvattu liitteessä 1.

Kuvio 6. Käyttäjätunnusten käsittelymäärät ajalla 06 – 12 2014. Olen kuvannut tietojen poiminnan kohdassa taulukko 2.
Kuvio 7. Kuukausittainen käyttäjätunnuskäsittelyn jakauma. Tiedot kuvioon poimin taulukosta 2.
Kuvio 8. Kuukausittainen käyttäjätunnuskäsittelyn jakauma. Pohjatietoina kuvion tuloksiin käytin taulukon 2 tuloksia.

Kuvio 9. Uusien tunnuksien avausmäärät ajalla 06 – 12 / 2014, kuvioon pohjatiedot on poimittu raportista "All_UserIDs_2015-01-01". Poimin raportilta aputaulukkoon AD-tunnuksien käsittelymäärät 06 –12 2014 ADObjCreated ja ADObjChanged tapahtumat aikavälillä 2014 06 – 12 . Toin aputaulukkoon ADStatus, ADObjCreated, ADObjChanged, LastKnowLogin, UserAccount ja AccountType sarakkeet. Rivejä aputaulukkoon kertyi 1878. Kuvion perustiedot poimin Pivot-näkymän avulla. Poimin Row Labes -osaan ADStatus ja AccountType kentät sekä Values-osaan UserAccount. Näin sain ratkaistua tapahtumien (enabled, disbled, termintaed ja deleted) määrät. Näistä arvoista poimin konsultti, työntekijä, systeemi ja muut tunnusluokkien avausmäärät (enabled). Kuvio on luotu Excel-työkalun avulla.

Kuvat

Tässä liitteessä on kuvattu toimintaohjeet raportissa esiteltyjen kuvien tuottamiseksi.

Kuva 1. Tunnuksen tilauslomakkeen kuvaruutukopion kuvaruutukauppauksen tein OneNote-ohjelmalla.

Kuva 2. "AD User Account -jonossa käsiteltyjä tapahtumia" kuvaruutukopion kuvaruutukauppauksen tein OneNote-ohjelmalla. Häivytin kuvasta käyttäjäidentiteettiin viittaavat tiedot SharePoint-ohjelmalla.

Kuva 3. "Hetkellinen näkymä AD User Account -työjonoon." AD User Account -näkymän poimin ERP-ohjelman näkymästä. ITSM - Search ITSM tickets - Assignment Key Application: LA001395 AD USer Account - Search. Työpyynnön otsikot esitellään Title-kentässä. Tästä tilanteesta on poimittu kuvaruutukopio OneNote-ohjelman avulla SharePoint-ohjelmaan, jossa tein arkaluontoisten tietojen häivyttämisen. Tuloksena on näkymästä otettu OneNote-kuvaruutukaappaus.

Kuva 4. Ernst & Youngin esitys IAM komponenttien vaikutuksista liiketoiminnan arvoon ja riskien pienentämiseen.