KARELIA-AMMATTIKORKEAKOULU
Teknologiaosaamisen johtamisen koulutusohjelma
Ylempi ammattikorkeakoulututkinto

Mika Kähkönen

ROOLIPOHJAISEN KÄYTTÖVALTUUKSIEN JA RESURSSIEN KÄYTTÖÖNOTTO IDENTITEETINHALLINNASSA

Opinnäytetyö
Elokuu 2019

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Elokuu 2019
Teknologiaosaamisen johtamisen koulutusohjelma

Tikkarinne 9
80200 JOENSUU
+358 13 260 600

Tekijä
Mika Kähkönen

Nimeke
Roolipohjaisen käyttövaltuuksien ja resurssien käyttöönotto identiteetinhallinnassa

Toimeksiantaja
ICT-palvelualan yritys

Tiivistelmä

Kehitystehtävän tarkoituksena on tutkia ja toteuttaa rooli- ja resurssipohjainen toiminta Office 365 -palvelujen osalta kohdeorganisaation ylläpitämässä identiteetinhallinnan järjestelmässä. Kehitystehtävän tuloksena on suunnitelma toteutuksesta, jonka mukaan pystytään toteuttamaan rooli- ja resurssipohjainen toiminta Office 365 -palvelujen osalta.

Kehitystehtävä keskittyy sosiaali- ja terveydenhuollon Office 365 -palvelujen edellyttämien lisenssien allokoinnin toteuttamiseen rooli- ja resurssipohjaisen toiminnan kautta. Kehitystehtävä nostaa esille suurimpia haasteita sosiaali- ja terveydenhuollon osalta suunniteltaessa rooli- ja resurssipohjaista toiminnallisuutta Office 365 -palvelujen osalta.

Kehitystehtävästä saadun tuloksen pohjalta voidaan ottaa käyttöön rooli- ja resurssipohjainen toiminta sosiaali- ja terveydenhuollon identiteetinhallinnan järjestelmässä. Kehitystehtävän kautta hankittua tietoa hyödynnetään Office 365 -palvelujen lisäksi muiden resurssien allokoinnin osalta. Hankittua tietoa hyödynnetään myös muiden asiakasorganisaatioiden identiteetinhallinnan järjestelmien kehityssuunnitelmissa.

Kieli
suomi

Sivuja 57
Liitteet 2
Liitesivumäärä 2

Asiasanat
identiteetinhallinta, pilvipalvelu, Office 365 -palvelu

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
August 2019
Master's Thesis
Degree Programme in Technology
Competence Management

Tikkarinne 9
80200 JOENSUU
FINLAND
+ 358 13 260 600

Author (s)
Mika Kähkönen

Title
Introducing Role-Based Authority and Resources in Identity Management

Commissioned by
ICT services company

Abstract

The purpose of this development task was to research and implement role and resource based functionalities for Office 365 services, which are a part of an identity management system maintained by the target organization. The result of this development task was a plan for implementing role and resource-based action for the Office 365 services.

The development task focused on social welfare and healthcare Office 365 services required to allocate licenses through role and resource-based action. The development task raised the biggest challenges in planning the social welfare and healthcare related role and resource-based functionalities for Office 365 services.

Based on the result of the development task, the role and resource-based functionalities can be deployed in the identity management systems for social welfare and healthcare. The information acquired from the development task is utilized not only in the Office 365 services, but also in the allocation of other resources. The acquired information is also utilized in the system development plans of identity management systems of other customer organizations.

Language

Finnish

Pages 57
Appendices 2
Pages of Appendices 2

Keywords

identity management, cloud service, Office 365 service

Sisältö

Lyhenteet

IdM	Identity Management, identiteetin hallinta.
IAM	Identity and Access Management, identiteetin ja pääsyn hallinta.
GDPR	General Data Protection Regulation, yleinen tietosuoja-asetus.
HR	Human Resources, henkilöstöhallinto.
eDir	eDirectory, hakemistopalvelu.
AD	Active Directory, aktiivihakemisto.
AADC	Azure Active Directory Connect, azure -pilvipalvelu aktiivihakemistoliitos.
Azure AD	Azure Active Directory, azure –pilvipalvelu aktiivihakemisto.
SIEM	Security Information and Event Management, tietoturvainformaation ja -tapahtumien hallinta.
GUI	Graphical user interface, graafinen käyttöliittymä.
LDAP	Lightweight Directory Access Protocol, hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.
ADFS	Active Directory Federation Services, aktiivihakemiston federointipalvelu.
EU	European Union, Euroopan unioni.
IoT	Internet of Things, esineiden internet.
ICT	Information and Communication techonolgy, tieto- ja viestintätekniikka.
OU	Organizational Unit, organisaatioyksikkö.

1 Johdanto

1.1 Identity Management

Identity Management (IdM) vastaa kysymyksiin, kenen pitää päästä käsiksi resursseihin, miksi, mihin resursseihin ja miten. Identiteettejä säilytetään keskitetyssä tietovarastossa, joita voivat olla tietokannat, IdM-järjestelmät, hakemistot jne. Tietotekniikassa (sähköinen) identiteetti tarkoittaa kohdetta kuvailevien ominaisuuksien eli attribuuttien kokoelmaa. Kohteet ovat usein ihmisiä, tietojärjestelmien käyttäjiä, joita kuvailevia attribuutteja ovat esimerkiksi nimi, käyttäjätunnus ja valtuus tietyn palvelun käyttämiseen (Linden 2015, 14). Attribuutit voivat olla yksilöiviä tai kuvaavia, yksilöivä attribuutti voi esimerkiksi olla henkilöturvatunnus ja kuvaava attribuutti voi esimerkiksi olla organisaation nimi. Henkilöturvatunnuksella pystytään identiteetti kohdentamaan sen omistajaan, mutta kuvaavalla organisaation nimellä ei pystytä vielä päättelemään identiteetin omistajaa.

Tietovarastossa sijaitsevien identiteettien attribuuttien muutokset tapahtuvat manuaalisesti tai automaattisesti. Manuaalinen muutos suoritetaan ottamalla yhteys tietovarastoon esimerkiksi LDAP-työkalulla. Manuaalinen muutos voi koskea yhtä tiettyä identiteettiä tai useampaa identiteettiä yhtä aikaa. Yksittäisen identiteetin muutos voi koskea esimerkiksi tittelin muutosta olettaen, että kyseiseen attribuuttiin ei kohdisteta automaatiota. Yhtäaikainen muutos voi koskea tiettyä joukkoa identiteettejä, jolloin muutetaan yhtä aikaa kaikkien samaa attribuuttia, esimerkiksi halutaan muuttaa tietyn yksikön identiteettien kustannuspaikkanumeroa. Automaattiset muutokset tapahtuvat identiteetinhallintaan määriteltyjen ajurien avulla, esimerkiksi henkilöstöhallinnon järjestelmässä (HR) tapahtuvat muutokset kohdentuvat määritettyjen ehtojen mukaisten identiteettien attribuutteihin.

Organisaatioissa saattaa olla paljon erilaisia identiteettejä sisältäviä tietojärjestelmiä, joten on tärkeää määrittää päätietolähde. Päätietolähteellä tarkoitetaan sitä tietovarastoa, joka määrää identiteettien oikeellisuuden. Monesti päätietolähteenä käytetään HR-tietojärjestelmää, koska HR:ään syötetään työntekijöi-

den henkilötiedot työsuhteiden alussa, joten on luontevaa käyttää kyseistä tietojärjestelmää päätietolähteenä. Kun identiteetinhallintaan on määritetty päätietolähde, tämän jälkeen identiteetinhallinta pitää huolen siitä, että vaikka jokin muu tietojärjestelmä muuttaa identiteettien arvoja, niin identiteetinhallinta muuttaa kyseiset arvot takaisin HR:n määräämään muotoon. Identiteetinhallinnan järjestelmiä suunniteltaessa määritellään kunkin attribuutin päätietolähde.

1.2 Roolipohjainen hallinta

Roolit niputtavat resursseja ja käyttöoikeuksia yhteen. Käyttäjät saavat roolijäsenyyden joko anomisprosessin kautta, manuaalisesti asettamalla tai automaattisesti käyttäjän omaavan identiteetin tietoihin pohjautuen. Identiteettien profiloinnissa identiteeteille annetaan yksi tai useampia rooleja. Rooleihin on kytketty yksi tai useampi resurssi. Esimerkiksi johonkin rooliin on kytketty kaksi resurssia, toinen resurssi lisää kohdeidentiteetin aktiivihakemistossa haluttuun käyttöoikeusryhmään ja toinen resurssi antaa oikeudet resurssiin kytkettyyn kohdejärjestelmään.

Roolipohjainen hallinta auttaa identiteettien profiloinnissa. Identiteettien profiloinnilla tarkoitetaan sitä, että uuden työntekijän saama identiteetti profiloidaan annettujen sääntöjen mukaan. Esimerkiksi teknisen viraston uusi työntekijä saa identiteetin, joka on profiloitu teknisen viraston sääntöjen mukaan.

1.3 Lähtökohdat

Opinnäytetyön toimeksiantajan organisaation ylläpitämässä identiteetinhallinnassa ei ole käytössä roolipohjaista hallintaa. Identiteetteihin liitetyt resurssit toteutetaan erikseen luotujen sääntöjen avulla. Esimerkiksi on luotu ajuriin ehto, jossa tietyn kustannuspaikkanumeron omaavat identiteetit saavat halutun ryhmäjäsenyyden aktiivihakemistossa. Edellä mainittu esimerkki on kertaluontoinen toimenpide, eli ajuriin luotu ehto tekee määrityksen ja sen jälkeen kyseiseen määritykseen ei enää puututa. Kun määrittelyt tehdään ajurin sijaan rooliin

kytketyn resurssien avulla, tällöin pysyy yhteys annettuun aktiivihakemiston ryhmäjäsenyyteen ja resurssin poistuessa poistuu samalla kyseinen ryhmäjäsenyys. Roolipohjainen toiminta mahdollistaa paremman seurattavuuden ja raportoinnin. Office 365 -palvelujen osalta toimeksiantajan organisaatiossa on hyvin vähän identiteetinhallintaan pohjautuvia prosesseja.

1.4 Rakenne

Opinnäytetyö koostuu useista luvuista, joissa kunkin luvun aiheen sisältö pyritään tuomaan esille riittävällä syvyydellä. Luvussa kaksi esitellään toimeksiantaja, toimeksianto ja toimeksiantoon vaikuttavat keskeiset tekijät. Kolmannessa luvussa käydään läpi tietosuoja-asetusta identiteetin ja pääsynhallinnan (IAM) näkökulmasta, kyseistä tietosuoja-asetusta on sovellettu 25.5.2018 alkaen. Neljännessä luvussa käydään läpi pilvipalveluihin liittyviä seikkoja opinnäytetyöhön nojautuen, koska pilvipalvelut liittyvät olennaisesti opinnäytetyön toimeksiantoon. Viidennessä luvussa käydään läpi kehitystyön lähestymistavan, eli käytännössä kyseinen luku kertoo siitä, että mihin kysymykseen opinnäytetyö antaa vastauksen. Luvuissa kuusi ja seitsemän käydään läpi se, miten kehittämistehtävä käytännössä suunnitellaan ja toteutetaan. Luvussa kahdeksan esitellään opinnäytetyöhön liittyvät johtopäätöksen ja mahdolliset jatkotoimenpiteet tulevaisuuden näkymät huomioiden.

2 Viitekehys

2.1 Toimeksiantaja

Opinnäytetyön kehittämistehtävän toimeksiantaja on maakunnallinen IT-palveluntarjoaja, jatkossa tässä tekstissä käytetään kyseisestä organisaatiosta nimeä IT-palveluntarjoaja. IT-palveluntarjoaja on asiakkaidensa omistama voittoa tavoittelematon ICT-palveluyhtiö. Yhtiön juuret yltävät 1980-luvulle, mutta varsinainen toiminta nykyisessä laajuudessaan alkoi 2010-luvulla.

IT-palveluntarjoaja tarjoaa omistajilleen käytännössä kaikki tarvittavat tietotekniikkapalvelut, suurin osa palveluista tuotetaan omana tuotantona ja osa palveluista ostetaan kolmansilta osapuolilta. Työntekijöitä organisaatiossa on noin 140, joista valtaosa sijoittuu yhtiön päätoimipisteeseen ja loput sijoittuvat maakunnissa sijaitseviin toimipisteisiin.

Identiteetinhallintaan liittyvä ylläpitäminen ja kehittäminen toteutetaan kokonaan yhtiön omana palvelutuotantona. Identiteetinhallinnan palvelutuotanto kuuluu muiden teknisten ratkaisujen kanssa saman palvelualueen alaisuuteen. Kyseisen palvelualueen palvelujohtaja toimii opinnäytetyönohjaajana toimeksiantajan puolelta.

2.2 Toimeksianto

IT-palveluntarjoajan edustama palvelujohtaja antoi kehittämistehtävän, jossa tutkitaan ja toteutetaan rooli- ja resurssipohjainen toiminta Office 365 -palvelujen osalta IT-palveluntarjoajan ylläpitämässä identiteetinhallinnan järjestelmässä. Kehittämistehtävän kohteena on sosiaali- ja terveydenhuollon palvelut.

Toimeksianto kohdistuu sosiaali- ja terveydenhuollon palveluihin sen takia, että kyseiseen palvelualaan kohdistuu suurin osa identiteetteihin tapahtuvista muutoksista. Kyseinen suuri muutosten määrä johtuu kyseisen alan työntekijöiden työsuhteiden vaihteluista ja työroolien muutoksista. Sosiaali- ja terveydenhuollon alalla on yleistä, että työsuhteet ovat määräaikaisia, on paljon sijaisuuksia ja työsuhteet saattavat syntyä hyvinkin nopeasti.

2.3 Keskeiset tekijät ja niiden väliset suhteet

2.3.1 Asiakkaat

Asiakkaat ovat luonnollisesti tärkeä osa-alue, koska asiakkuudet määrittelevät koko organisaation olemassaolon. Asiakkuustapaamisissa sovitaan tietojen- ja tekojen vaihdannasta. Työnjaosta sopiminen tekojen osalta on eräs keskeisiä yrityksen kannattavuuteen ja asiakkuuden kehittymiseen liittyviä näkökohtia. Tämä merkitsee sitä, että asiakas panostaa tekojen osalta aikaa, työtä ja rahaa. Asiakkaan rooli ei näin ole vain tavaroita käyttävä objekti, vaan myös asiakkuuden kehittämiseen osallistuva subjekti (Storbacka & Lehtinen 2006, 47).

Asiakkaille identiteetinhallinnan olemassaolo näyttäytyy useammalla eri tavalla, pääasiallisesti graafisen käyttöliittymän ja automaattisen tietojen päivittymisen kautta. Graafisen käyttöliittymän kautta asiakkaat pääsevät tilaamaan, muuttamaan ja poistamaan käyttäjätunnuksia. Automaattisella tietojen päivittymisellä tarkoitetaan sitä, että ennakkoon määrättyjen sääntöjen mukaan identiteetinhallinta päivittää kohdeidentiteettien tietoja, esimerkiksi HR-järjestelmässä muuttuva kohdeidentiteetin kustannuspaikkanumero päivittyy automaattisesti haluttuun järjestelmään. Asiakkaan näkökulmasta paras mahdollinen tilanne on se, että identiteetinhallinta toimii taustalla mahdollisimman näkymättömissä, eli asiakkaan ei tarvitse puuttua identiteetinhallinnan toimintaan jokapäiväisissä työtehtävissä.

2.3.2 IT-palvelutarjoajan työntekijät

IT-palveluntarjoajan työntekijöille identiteetinhallinta näyttäytyy käyttäjätunnusten käsittelyn muodossa, eli kun asiakas on anonut uuden käyttäjätunnuksen tai muutoksen olemassa olevaan, tällöin IT-palveluntarjoajan työntekijä käsittelee pyynnön ja tämän jälkeen asiakas saa kuittauksen käyttäjätunnuksen käsittelystä. Identiteetinhallintaan liittyvissä kehitystöissä on pyrkimys asiakkaiden tavoin siihen, että identiteetinhallinta työllistää mahdollisimman vähän IT-

palveluntarjoajan työntekijöitä ja kaikki mahdollinen tapahtuu taustalla automaattisesti.

2.3.3 Tekniset ratkaisut

Tekniset ratkaisut käsittävät lähinnä palvelimet, työasemat ja tietoliikenneverkot. Identiteetinhallinnan tarjoamat palvelut on rajattu sisäverkkoon, eli palveluja ei voi käyttää julkisesta verkosta, vaan pelkästään sisäverkkoon kytketyiltä tietokoneilta. Identiteetinhallinnan käyttöön on asennettu muutamia palvelimia, LDAP-hakemistopalvelimia on vikasietoisuuden takia kaksi kappaletta, identiteetit varastoidaan kyseisille LDAP-hakemistopalvelimille. Graafinen käyttöliittymä (GUI) on asennettu omalle palvelimelle, GUI on web-palvelu, jonka kautta asiakkaat ja IT-palveluntarjoajan työntekijät käyttävät identiteetinhallinnan palveluja.

2.3.4 Kolmansien osapuolien järjestelmät

Kolmansien osapuolten ohjelmistot ovat niitä ohjelmistoja, joista tuodaan tietoa identiteetinhallintaan ja joihin viedään tietoa identiteetinhallinnasta. Hyvä esimerkki kolmannen osapuolen ohjelmistosta on HR-järjestelmä, eli ohjelmisto jota käytetään henkilöstöhallinnon tehtäviin. HR-järjestelmästä saatavaa tietoa käytetään yleensä kahdella eri tavalla, joko identiteetti perustetaan HR-järjestelmästä saatavan tiedon avulla tai HR-järjestelmästä saatavalla tiedolla täydennetään jo olemassa olevia identiteettejä.

3 Tietosuojalaki

3.1 Yleistä

Suomen ja Euroopan unionin (EU) tietosuojalait ovat uudistumassa. EU:n yleistä tietosuoja-asetusta sovelletaan 25.5.2018 alkaen kaikissa EU:n jäsenmaissa.

Tietosuoja-asetusta General Data Protection Regulation (GDPR) sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn (Tietosuojavaltuutetun toimisto 2019).

Tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista periaatteista, jotka ohjaavat rekisterinpitäjää käsittelemään henkilötietoja rekisteröidyn oikeuksia ja vapauksia kunnioittavalla tavalla. Periaatteet vastaavat monilta osin henkilötietolain periaatteita, vaikka asetuksessa osaa näistä periaatteista on täsmennetty.

Tietosuojaperiaatteet henkilötietojen käsittelyssä ovat seuraavat:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoituksen toteuttamista varten. (Tietosuojavaltuutetun toimisto 2019)

3.2 Tietosuojalaki tietohallinnon näkökulmasta

Tietohallinnon on käytävä kaikki järjestelmät läpi ja tehtävä niistä riskiluokittelu. Jokaisen järjestelmän kohdalla on myös tarkistettava, sisältääkö kohdejärjestelmä henkilötietoja ja näin ollen on henkilörekisteri. Täytyy selvittää, kuinka loki- ja muut kontrollit toimivat onko, esimerkiksi käytössä SIEM-järjestelmä.

SIEM-järjestelmän käytön tarkoituksena on kerätä useista lähteistä saadut lokit yhteen paikkaan sekä automatisoida eri järjestelmistä kerättyjen lokien käsittelyä mahdollisimman paljon (Aarnivuo-Seppinen 2014, 3). On suositeltavaa järjestää tietohallinnon työntekijöille tietosuoja-asetuksiin liittyvää koulutusta, jotta työntekijät pystyvät huomioimaan tietosuoja-asetukset työtehtävissään.

3.3 Tietosuojalaki IAM:n näkökulmasta

On selvitettävä, mitkä kaikki ympäristöt kuuluvat keskitetyn IAM:n piiriin. Edellä mainittua selvitystä edesauttaa palvelukuvaus tai tekninen kuvaus, muuten selvitystyö muuttuu työlääksi kyseisten kuvausten puuttuessa. Käyttäjätietovarastoja kartoittaessa on tehtävä yhteistyötä yli toimi- ja asiakkuusrajojen. Käyttäjätietovarastojen kartoitusvaiheessa on tärkeää pohtia sitä, mikä kannattaa ottaa IAM:n piiriin ja mikä kannattaa suosiolla jättää IAM:n ulkopuolelle. Kyseiset ulkopuolelle jäävät ympäristöt täytyy joka tapauksessa huomioida tietosuoja-asetusten vaatimalla tavalla. Kaikille järjestelmille on suoritettava riskiluokittelu. Kun on saatu kartoitettua ympäristöt, jotka on tarkoitus ottaa IAM:n piiriin, niin on käytävä keskustelua resursseista vastaavien tahojen kanssa ja perusteltava tietosuojan tuoma lisäarvo.

Käytön raportoitavuus, lokien hallinnan järjestäminen ja lokien eheyden varmistaminen on yksi suurimmista GDPR:n IAM:lle asettamista haasteista. Käytön raportoitavuudesta puhuttaessa voidaan käyttää muistisääntöä, kuka, mitä ja milloin. Eli kuka on käynnistänyt tai hyväksynyt työnkulkuja, mitä muutosta on anottu ja milloin työnkulku on käynnistynyt tai milloin se on käsitelty. Lokien hallinnan näkökulmasta lokit voidaan jakaa kahteen kategoriaan, virhelokit ja käyttölokit. Virhelokeja käytetään ongelmien ratkaisun apuna, eli toimintahäiriön ilmetessä otetaan virheloki avuksi. Käyttölokeihin tallennetaan sellaista tietoa, josta voidaan koostaa raportteja. Lokitietojen eheys on syytä suojata, koska muuten jää mahdollisuus lokitietojen väärentämiseen. Tietovarannon luonne sekä arkaluontoisuus määrittelevät lokien säilytysajan. Lokeille tallennetaan vain se määrä tietoa, mikä on välttämätöntä tietosuojavaatimusten näkökulmasta.

3.4 Henkilötietojen elinkaari

Identiteetti ei käytännössä koskaan ole muuttumaton, vaan se muuttuu ja kehittyy ihmisen mukana. Kuten ihmisen henkilökohtainen identiteetti, myös henkilön sähköinen identiteetti yrityksessä muuttuu ajan myötä (Sinesaari 2016, 16). Identiteetin elinkaari on yksinkertaistettuna syntyminen, jalostuminen ja päättyminen. Syntyminen voi tapahtua automaattisesti HR-järjestelmästä saatavan herätteen seurauksena tai tarvittavat valtuudet omaavan henkilön anomana. Jalostumisella tarkoitetaan identiteetin aktiivisena aikana tapahtuvia muutoksia, joita voivat olla nimikkeen vaihtuminen, käyttövaltuuksien muuttuminen, sukunimen vaihtuminen ja monet muut identiteetin attribuutteihin tapahtuvat muutokset. Identiteetin omaavalla henkilöllä on oikeus saada tietoa henkilötietojensa käsittelystä. Päättyminen tapahtuu silloin, kun kohdeidentiteetti poistuu identiteetinhallinnan piiristä. Identiteetin päättymisen jälkeen tapahtuviin toimenpiteisiin vaikuttavat liiketoimintavaatimukset, eli kuinka kauan on tarve säilyttää identiteettiin liittyviä henkilötietoja ja mitkä attribuutit ovat välttämättömiä säilytyksen kannalta. Henkilötietoja säilöttäessä on hyvä käyttää pseudonymisointia. Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Tällaiset lisätiedot täytyy säilyttää huolellisesti erillään henkilötiedoista (Tietosuojavaltuutetun toimisto 2019).

4 Pilvipalvelut

4.1 Yleistä

Pilvipalvelut on melko hajanainen nimitys palveluille, joita palvelun käyttäjä voi käyttää Internetin avulla riippumatta palvelun sijainnista ja päivitysajoista (Opetushallitus 2018). Pilvipalvelut voidaan jakaa kahteen eri kategoriaan, yksityiseen käyttöön ja organisaatioiden käyttöön tarjottavat pilvipalvelut.

Yksityisten pilvipalveluiden käyttäjien osalta voidaan yleistäen sanoa, että jokainen internetyhteyden omaava henkilö käyttää jotakin pilvipalvelua, esimerkiksi sähköposti, Linkedin ja Facebook.

Organisaatioiden näkökulmasta pilvipalvelut tarkoittavat sitä, että osa tai kaikki tarjottavat palvelut sijaitsevat On Premises -ympäristön ulkopuolella, yleisimpänä esimerkkinä sähköposti ja tiedostopalvelut. Hyvin pienet organisaatiot voivat ulkoistaa kaikki palvelunsa pilveen, mutta suurimpien organisaatioiden kohdalla käytetään pääsääntöisesti hybridimallia. Hybridimallilla tarkoitetaan sitä, että osa palvelusta tarjotaan pilvestä ja osa tarjotaan On Premises -ympäristöstä. Pilvipalveluiden käyttöönottoa suunniteltaessa on käytettävä tarkkaa harkintaa sen suhteen, mitä järjestelmiä lähdetään viemään pilveen ja mitkä on viisainta jättää On Premises -ympäristöön. Pilvipalvelut ovat vielä kohtalaisen uusi alusta erilaisille palveluille, joten alun perin On Premises -ympäristöön suunniteltujen palvelujen vienti pilveen voi olla erittäin haastavaa ja pahimmassa tapauksessa jopa mahdotonta.

4.2 Pilvipalvelut IT-palveluntarjoajan näkökulmasta

4.2.1 Sivistys

IT-palveluntarjoaja on tarjonnut Office 365 -palveluja opiskelijoille jo useamman vuoden ajan, joten kyseinen tuote on organisaatiolle tuttu. Opiskelijoille on tarjottu Office 365 -palvelujen kautta sähköposti, OneDrive, SharePoint ja monia muita lisenssien sallimia palveluja. Opiskelijoille tarjotaan hyvin vähän palveluja On Premises -ympäristöstä, koska opiskelijoille suunnatut palvelut on organisaation perustamisesta asti tarjottu Office 365 -palvelun kautta. Office 365 -palvelun edeltäjä oli Live@edu-palvelu. Office 365 -palvelu antaa opiskelijoille joustavuutta omien resurssien hallintaan. Esimerkiksi sähköposti, tiedostopalvelut ja SharePoint ovat saatavilla ajasta ja paikasta riippumatta. Opiskelijoille yleensä harvemmin tarjotaan etäkäyttömahdollisuutta On Premises -ympäristöön, joten opiskelijan on oltava sisäverkkoon kytketyllä tietokoneella päästäkseen koulun tarjoamiin tietoteknisiin resursseihin. Office 365 -palvelut mahdollistavat kevyemmän On Premises -ympäristön, koska näin ollen osa palvelimista sijaitsee Microsoftin hallinnoimissa konesaleissa.

4.2.2 Hallinto

Hallinnon käyttäjillä tarkoitetaan niitä henkilöitä, jotka käyttävät IT-palveluntarjoajan tarjoamia hallintoverkon palveluja, eli asiakkaat, asiakkaiden tytäryhtiöt ja muut ulkoiset käyttäjät. Hallintoverkon käyttäjille tarjottavat Office 365 -palvelut ovat olleet rajoitettuja. Suurin hallintoverkon Office 365 -palvelujen käyttäjäkunta on opetushenkilöstö. Syy opetushenkilöstön muita laajempaan Office 365 -palvelujen käyttöön on se, että oppilaiden ja opetushenkilöstön yhteistyö on sujuvampaa, kun käytettään samoja Office 365 -palveluja. Muiden hallintoverkon käyttäjien osalta Office 365 -palvelujen käyttöönotto tapahtuu hallituin askelin asiakas kerrallaan. Suurimpana haasteena on On Premises -ympäristössä tarjottavien sovelluksien ja Office 365 -palvelujen yhteensovittaminen.

4.2.3 Asiakkaat

Asiakkuuksia voidaan tarkastella kahdesta eri näkökulmasta, IT-palveluntarjoajan asiakkaat ja IT-palveluntarjoajan asiakkaiden asiakkaat. Asiakkaiden näkökulmasta Office 365 -palvelut tulevat tarjoamaan uusia mahdollisuuksia töiden tekemiseen. Palveluiden sijaitessa pilvipalvelussa yhteistyön tekeminen kolmansien osapuolten kanssa on helpompaa. Asiakkaat voivat esimerkiksi perustaa Teams tai SharePoint työtilan, johon he voivat kutsua kolmansien osapuolien edustajia.

4.3 Pilvipalvelut Identiteetinhallinnan näkökulmasta

4.3.1 Sivistys

Opiskelijoille tarjottavat Office 365 -palvelut ovat identiteetinhallinnan näkökulmasta melko suoraviivaista prosessointia. Identiteettien käsittely on käytännössä samanlaista jokaisen koulun osalta. Kouluilla itsellään on päätäntävalta siitä, minkä luokan opiskelijoille muodostetaan identiteetit Office 365 -palveluun. Opiskelijoiden identiteetit eivät muodostu suoraan opiskelijahallinnon järjestelmästä Office 365 -palveluun, vaan tunnus luodaan ensin identiteetinhallinnan kautta On Premises -ympäristössä sijaitsevaan aktiivihakemistoon ja sitä kautta Office 365 -palveluun. Opiskelijatunnusten luonti alkaa opiskelijahallinnon järjestelmästä, eli koulujen henkilöstön edustaja määrittää opiskelijahallinnon järjestelmään sen, että syntyykö opiskelijalle identiteetti Office 365 -palveluun. Identiteetinhallinta havaitsee opiskelijahallinnon järjestelmään tehdyn muutoksen ja muodostaa identiteetin On Premises -ympäristössä sijaitsevaan aktiivihakemistoon ja sen kautta opiskelijatunnus synkronoidaan Office 365 -palveluun.

4.3.2 Hallinto

Hallinnon käyttäjätunnuksia ei tällä hetkellä hallinnoida identiteetinhallinnan avulla Office 365 -palvelussa, eli hallinnon käyttäjätunnuksien hallinta koskee On Premises -ympäristöä. Identiteetinhallinta harvemmin hallinnoi käyttäjätunnuksia suoraan O365 -palvelussa, vaan hallinta tapahtuu On Premises -aktiivihakemiston kautta. Hallinta aktiivihakemiston kautta tapahtuu siten, että Azure Active Directory Connect (AADC) synkronoi identiteettejä ja käyttöoikeusryhmiä Office 365 -palveluun. Identiteettien synkronoinnissa pilveen hyödynnetään attribuutteja. Esimerkiksi aktiivihakemistossa kohdeidentiteetin attribuuttiin extensionAttribute7 asetetaan tietty arvo, AADC huomaa kyseisen arvon ja synkronoi identiteetin haluttuun O365 -tenanttiin. Pelkkä identiteetin synkronointi O365 -palveluun ei vielä riitä, vaan identiteettiin on sidottava lisenssi. Lisenssit ovat eräänlaisia tuotepaketteja, jotka sisältävät erilaisia sovelluksia ja ominaisuuksia. Tuotepakettien laajuus korreloi hinnan kanssa. Tuotepaketti voidaan osoittaa tiettyyn O365 -palveluun synkronoituun käyttöoikeusryhmään, jolloin kyseisen käyttöoikeusryhmän jäsenyyden omaavat identiteetit saavat tuotepaketin sovellukset ja ominaisuudet käyttöönsä.

Azure Active Directorystä (Azure AD) lohkaistaan kullekin asiakkaalle oma asiakaskohtainen hakemisto, jota kutsutaan Azure AD -tenantiksi. Tämä tenantti on varattu vain tämän asiakkaan käyttöön ja kunkin tenantin käyttäjät näkevät vain samassa tenantissa olevat tiedot ja tenantin pääkäyttäjä voi hallita vain oman tenanttinsa tietoja (Sulava Oy 2018). Käytännössä kaikki IT-palveluntarjoajan hallinnon asiakasorganisaatiot saavat halutessaan oman tenantin. Asiakaskohtaiset tenantit mahdollistavat paremmin asiakaskohtaiset räätälöinnit.

5 Kehitystyön lähestymistapa

5.1 Yleinen

Opinnäytetyö keskittyy sosiaali- ja terveydenhuollon palveluihin kohdistuvaan rooli- ja resurssipohjaiseen toimintaan Office 365 -palvelujen osalta. Edellä mainitun painotuksen johdosta tapahtuva suunnittelu koskee luonnollisesti myös muita asiakkaita. Suurimpana haasteena voidaan mainita roolien määrittelyprosessi. Kyseisessä tilanteessa roolien määrittelyprosessin tekee haastavaksi se, että sosiaali- ja terveydenhuollon alalla työskentelevien henkilöiden työtehtävät, fyysiset toimipisteet ja monet muut muuttuvat tekijät hankaloittavat käyttäjien profilointia.

Sosiaali- ja terveydenhuollon palveluiden lisäksi muiden asiakkaiden kohdalla on sama haaste, eli roolien määrittelyprosessia sovittujen yksilöivien tunnisteiden pysyvyys ja mahdollisten tulevien muutoksien tunnistettavuus. Asiakkaiden kanssa etukäteen sovitut yksilöivät tunnisteet saattavat muuttua asiasta sovittujen henkilöiden tietämättä. Kyseinen ennakoimaton muutos voi tapahtua esimerkiksi siten, että roolien määrittelyissä on käytetty kustannuspaikkanumeroita ja vuodenvaihteessa organisaatio päättää muuttaa kustannuspaikkarakennettaan. Edellä mainittu tilanne voisi johtaa pahimmillaan siihen, että kohdeidentiteeteille annettaisiin roolin kautta automaattisesti pääsy johonkin resurssiin, johon kyseisillä identiteeteillä ei saa olla pääsyä.

5.2 O365 -lisenssi

5.2.1 Tarjottavat lisenssit

Tarjottavien lisenssien määrittely on asiakkaiden toiveiden mukaan tapahtuva prosessi, eli eri asiakkaiden kanssa käydään neuvottelut tarjottavista lisenssipaketeista. Käytännössä lisenssipaketteja on muutamia ja keskusteluissa vain

päätetään se, että mitkä paketit annetaan automaattisesti millekin ammattitunnisteen omaavalle identiteetille.

5.2.2 Lisenssit roolien kautta resursseina

Etukäteen sovituille lisenssipaketeille määritetään resurssit ja resurssit kytketään haluttuihin rooleihin. Yksi resurssi voi kuulua useampaan rooliin, mikä on melko yleistä kyseisissä tilanteissa. Yksittäisen organisaation työntekijät saavat erilaisia rooleja riippuen asemasta tai kustannuspaikasta. Koko organisaatio saattaa käyttää yhtä ja samaa lisenssipakettia, joten tällöin sama lisenssipaketille määritetty resurssi liitetään kaikkiin tarvittaviin rooleihin.

5.2.3 Lisenssit anomisprosessin kautta

Asiakkaan palveluksessa olevat esimiestason tai muuta kautta valtuutetut henkilöt pystyvät tilaamaan identiteetinhallinnan kautta lisenssejä työntekijöille. Etukäteen asiakkaiden kanssa tehtävällä määrittelyllä varmistetaan se, että tilaajalle annetaan mahdollisuus tilata vain pelkästään edustamalleen organisaatiolle määriteltyjä lisenssejä.

5.3 Perusongelma resurssien myöntämisessä

5.3.1 Myöntäminen dynaamisten roolien kautta

Dynaamisesti roolien mukana tulevat kaikki ne lisenssit, jotka pystytään antamaan etukäteen tunnistetulle identiteetille. Tunnistus on tapahtunut annetun organisaatiotunnisteen avulla. Organisaatiotunnisteella tarkoitetaan sellaista attribuuttia, jolla käyttäjää ei yksilöidä henkilötasolla, vaan organisaatiotasolla. Organisaatiotasontunniste voi olla titteli, kustannuspaikka, työpaikanosoite tai

jokin muu, mikä ei suoraan viittaa tiettyyn identiteettiin. Tiettyyn identiteettiin viittaavat yksilötasontunnisteet ovat sosiaaliturvatunnus, sähköpostiosoite, mahdollinen henkilönumero ja muut vastaavat yksilöivät tunnisteet.

5.3.2 Myöntäminen anomisprosessin kautta

Erikseen anottaviksi resursseiksi jätetään ne samat lisenssipaketit, jotka muuten myönnetään dynaamisesti roolien mukana. Jos jostakin syystä työtekijän organisaatiotunnisteet eivät täytä dynaamiseen rooliin sidotun resurssin ehtoja, tällöin lähiesimies tai muuta kautta valtuutettu organisaation edustaja tilaa erikseen kyseisen lisenssipaketin.

5.3.3 Autentikointi

Autentikoinnilla tarkoitetaan identiteetin todentamista. Identiteetin todentaminen tarkoittaa, että identiteetin ja sitä tosielämässä vastaavan henkilön välille rakennetaan kytkös: tavalla tai toisella tietojärjestelmä varmistaa, että järjestelmään kirjautuu sisään juuri sama henkilö, jolle tietty järjestelmään luotu identiteetti kuuluu. (Linden 2015, 16)

Autentikointi tunnetaan yleisemmin tunnistautumisena. Tunnistautumiseen käytettäviä keinoja on olemassa useita: pankkitunnistautuminen, mobiilivarmenne, varmennekortti, salasana, sormenjälki jne. Palvelujen etenevässä määrin tapahtuva sähköistyminen aiheuttaa sen, että käyttäjällä voi olla useita eri käyttäjätunnuksia eri palveluihin ja näin ollen riskinä on käyttää samaa salasanaa eri käyttäjätunnuksissa. Useat palvelut käyttävät kaksivaiheista tunnistautumista, näin pystyttään paremmin varmistamaan palvelua käyttävän identiteetin oikeellisuus. EU:n tietosuoja-asetukset asettavat omat vaatimuksensa palvelutarjoajien käyttämiin tunnistuspalveluihin.

5.3.4 Profilointi

Käyttäjän tunnistamisen jälkeen on käyttäjä profiloitava. Profiloinnin kautta voidaan antaa tarvittavat valtuutukset. Profilointi muodostuu identiteettiin liitettyjen eri attribuuttien kokoelmasta.

5.3.5 Roolien määrittelyn lähestymistapa

Roolien määrittelyssä käytetään järjestelmäkeskeistä lähestymistapaa. Järjestelmäkeskeisessä lähestymistavassa roolien määrittely aloitetaan järjestelmätasolta yksittäisistä käyttöoikeuksista, joita lähdetään koostamaan yhteen (Mäkelä 2008, 38). Järjestelmäkeskeinen lähestymistapa on luonnollinen valinta O365 -palvelujen osalta, koska kyseessä on vain yksi järjestelmä.

5.4 Laskutus

Asiakkaita laskutetaan käyttäjätunnuksista tietyn määräajoin välein. Laskutus perustuu käytössä oleviin lisenssipaketteihin ja niiden määrään. Laskutuksen tärkeimmät seikat ovat mahdollisimman ajantasainen tieto lisenssien määrästä ja laskujen kohdentuminen oikeisiin kustannuspaikkoihin.

Lisenssien oikeanlaisen määrän varmistaminen etukäteen on haastavaa, koska tilanne elää koko ajan. Oikeanlaisilla prosesseilla varmistetaan se, että lisenssien määrä seuraa mahdollisimman hyvin identiteetteihin liittyviä muutoksia, eli prosessien on seurattava identiteettiä koko elinkaaren ajan. Identiteetin elinkaarella tarkoitetaan yleensä niitä vaiheita, joita identiteetti käy läpi olemassa olonsa aikana. Nämä vaiheet pystytään jakamaan neljään eri osioon, jotka ovat seuraavat: identiteetin luominen eli provisiointi, identiteetin käyttö, päivittäminen ja käytöstä poistuminen eli deprovisiointi. Lisäksi hallinnointi on osa identiteetin elinkaarta (Silander 2013, 8). Identiteetin luomisen yhteydessä lisenssi myönnetään automaattisesti rooliin mukana tai erikseen anoen. Identiteetin päivittämisen yhteydessä voidaan muuttaa lisenssipaketin koostumusta, jos kyseinen

toimenpide on sallittu. Identiteetin käytöstä poistamisen yhteydessä vapautetaan lisenssi toisten identiteettien käyttöön.

5.5 Raportointi

Raportointia käytetään laskutukseen, vallitsevan tilanteen seurantaan ja jäljitykseen. Laskutuksen ajankohdan lähestyessä identiteetinhallinnan järjestelmästä otetaan raportti lisenssien määrästä ja niiden sisällöistä. Säännöllisin määräajoin asiakkaat ja palveluntarjoaja hyödyntävät raportteja vallitsevan tilanteen seurantaan. Raporttien avulla suoritetaan tarkistuksia käytetyistä ja käyttämättömistä lisensseistä, sekä kuinka käytössä olevat lisenssit ovat kohdentuneet. Raportointia käytetään jäljitykseen silloin, kun on tarve jäljittää jokin tietty prosessi ja siihen liittyvä osatekijät.

5.6 Lokitus

Lokit voidaan jakaa käyttölokeihin ja virhelokeihin. Useasti raportointi nojaa käyttölokeihin, raportointiin ei käytetä kaikkea lokitietoa, vaan ainoastaan raportoinnin kannalta oleellista tietoa. Jos ilmenee raportoinnin ulkopuolelle jäänyt tapahtuma, niin tällöin aloitetaan käyttölokien syvällisempi tutkiminen. Raportoinnin lisäksi käyttölokia voidaan seurata muidenkin syiden takia, esimerkiksi tekniseen valvontaan. Virhelokeja tutkitaan silloin, kun järjestelmässä todetaan toimintahäiriö, eli jotakin toimintoja jää tapahtumatta tai jotkin prosessit johtavat väärään lopputulokseen.

5.7 Seuranta

Seurantaa toteutetaan silloin, kun jotakin resurssia on rajallisesti tarjolla ja sen riittävyyttä on seurattava. Teknisen ympäristön kannalta yksi seurattava resurssi on palvelimien levytilat, eli etukäteen määritetyn levytilan rajan ylittyessä järjestelmä antaa hälytyksen. Lisenssien määrän seuranta on tärkeää silloin, kun lisenssejä on rajallinen määrä. Lisenssien tilaaminen kolmansilta osapuolilta ei

välttämättä tapahdu hetkessä, joten oikeanlaisella seurannalla pystytään ennakoimaan liian alhaiset lisenssien määrät. Jos on käytössä volyymilisenssimalli, tällöin lisenssien seurannalle ei ole tarvetta.

5.8 Deprovisiointi

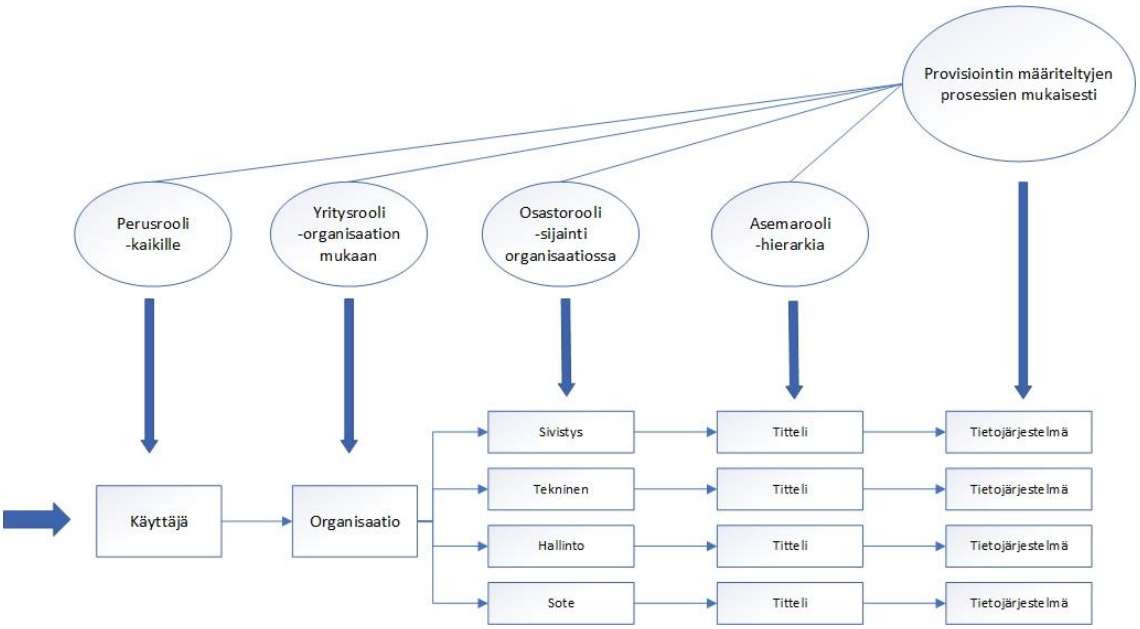
Deprovisiointi eli identiteetin käytöstä poisto aiheuttaa tietynlaisia toimenpiteitä. Identiteetin käytöstä poisto tapahtuu käytännössä silloin kun kohdeidentiteetin omaavan henkilön työsuhde loppuu. Työsuhteen loppumisesta tieto voidaan saada useampaa eri reittiä, yleisin on HR-järjestelmä, josta luetaan tieto päättyvistä työsuhteista identiteetinhallintaan. O365 -palvelun kannalta täytyy vähintään tapahtua lisenssien poisto ja kohdetilin lukitseminen. Jos identiteetin käytöstä poistossa kohdetiliä pidetään AD:ssa haluttu aika ennen lopullista poistamista, tällöin karsitaan kaikki resurssit pois ja samalla poistuu lisenssit O365 -palvelusta. Kun identiteetti poistetaan AD:sta, tällöin identiteetti siirtyy O365 -palvelussa roskakoriin, josta se poistuu määritetyn ajan jälkeen.

IT-palveluntarjoajan ylläpitämän identiteetinhallinnan piirissä on useampia organisaatioita ja kyseisten organisaatioiden välisissä henkilöstövaihdoksissa puhutaan myös deprovisioinnista. Organisaation vaihdoksessa kohdeidentiteetti poistetaan AD:sta ja samalla identiteetinhallinnassa karsitaan pois kaikki asiaan kuuluvat attribuutit ja näin kyseinen identiteetti on puhdas uuden organisaation käyttöön. O365 -palvelussa roskakoriin joutunut identiteetti ei aiheuta haittaa uudelle organisaatiolle, koska jokaisella organisaatiolla on oma tenantti O365 -palvelussa.

6 Käytännön suunnittelu

6.1 Organisaatiota koskeva roolien ja resurssien provisiointi

Uuden identiteetin luonnissa tapahtuva profilointi muodostuu siitä, mihin kohdeidentiteetti sijoittuu kohdeorganisaatiossa. Kuviossa 1 esitetään se, mistä eri rooleista käyttäjän profilointi koostuu.



Kuvio 1. Identiteetin profiloinnin muodostavat roolit.

6.1.1 Perusrooli

Jokainen uusi käyttäjä saa automaattisesti perusroolin. Perusrooliin voidaan kytkeä sellaisia resursseja, jotka annetaan kaikille käyttäjille. Perusrooli saatetaan kuitenkin poistaa jonkin toisen roolin toimesta, jos ilmenee ristiriita tai jokin muu määritelty sääntö.

6.1.2 Organisaatiorooli

Organisaatiorooli annetaan käyttäjille organisaatiokohtaisesti. Kun organisaatioon perustetaan uusi käyttäjä tai sinne siirtyy käyttäjä toisesta organisaatiosta, tällöin kyseinen henkilö saa kyseistä organisaatiota vastaavan organisaatioroolin. Organisaatiorooli yhdistetään käyttäjään yritysnumeron avulla.

6.1.3 Osastorooli

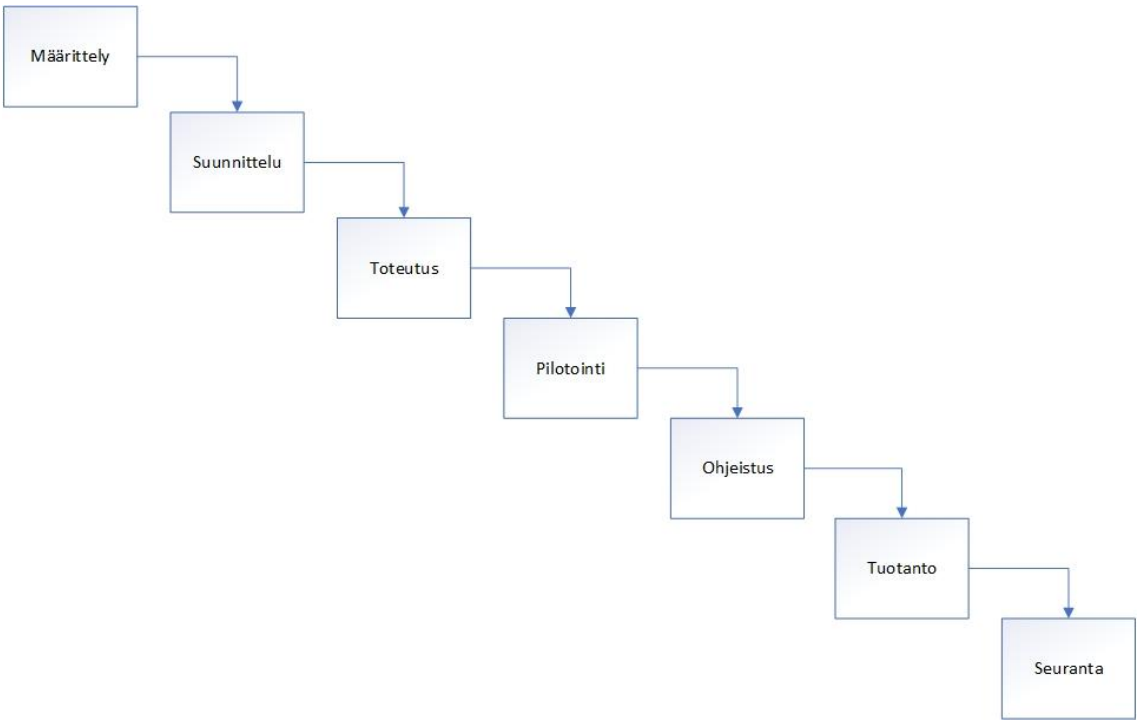
Osastorooli annetaan käyttäjille kustannuspaikkanumeron perusteella. Jokaisella identiteetinhallinnan piirissä olevalla käyttäjällä on kustannuspaikkanumero ja kyseistä numeroa hyödynnetään osastoroolin kytkemiseen.

6.1.4 Hierarkkinen rooli

Hierarkkinen rooli kytketään käyttäjien aseman perusteella ja asema kytketään rooliin tittelin perusteella. Hierarkkisessa roolissa haittapuolena on se, että käyttäjien tittelit voivat vaihdella organisaation eri osastoilla, vaikka työtehtävät olisivat samoja.

6.2 Yksittäisten roolien ja resurssien käyttöönoton suunnittelu

Kuviossa 2 esitetään yksittäisen roolin ja resurssin perustamiseen tarvittavat eri vaiheet.



Kuvio 2. Yksittäisen roolin ja resurssin käyttöönoton vaiheet.

6.2.1 Määrittely

Määrittely vastaa kysymykseen miksi, eli mitä varten kyseinen rooli tai resurssi luodaan. Luontitarve voi ilmetä monesta eri syystä, ympäristössä tapahtuvien muutosten kautta, oman kehitystyön kautta tai asiakkaalta saadun toiveen kautta.

6.2.2 Suunnittelu

Suunnittelu sisältää käytännön ja teknisen osuuden. Suunnitteluun otetaan mukaan kaikki ne tahot, joiden katsotaan olevan osallisia suunnittelun kohteena olevaan toimintoon. Esimerkiksi jos rakenteilla oleva resurssi kytkeytyy taloushallinnon järjestelmään, tällöin suunnitteluun otetaan mukaan taloushallinnon henkilöitä omasta organisaatiosta ja tarvittaessa asiakkaan organisaatiosta.

6.2.3 Toteutus

Toteutus tarkoittaa käytännössä roolin ja resurssin teknistä rakentamista. Esimerkiksi jos asiakkaan pyynnöstä on tarkoitus antaa taloushallinnon käyttäjille pääsy johonkin tiettyyn verkkokansioon, tällöin ensimmäisenä luodaan AD:hen käyttäjäryhmä, luodaan identiteetinhallintaan vastaava resurssi ja kytketään se AD-ryhmään. Resurssi liitetään olemassa olevaan rooliin tai perustetaan kyseistä toimintoa varten oma rooli. Uuden roolin tapauksessa määritetään kohdeidentiteetit, joille kyseinen rooli annetaan.

6.2.4 Pilotointi

Pilotointi eli testaaminen voi tapahtua tuotantoympäristöstä erillään olevassa kehitysympäristössä tai tuotantoympäristössä rajoitetulla käyttäjäryhmällä. Testaamisen tarkoituksena on varmistaa tekninen toimivuus ja roolien käyttäytyminen halutulla tavalla. Jos kyseinen toteutus näkyy asiakkaille, tällöin asiakkaan edustajat testaavat toimintoja ja antavat luvan käyttöönottoon, ellei ilmene lisäkehitystarpeita. Mitään ei saa koskaan ottaa tuotantoon ilman riittävän kattavaa testaamista, koska suunnittelupöydällä selkeältä näyttävät toiminnot saattavat tuotannossa toimia poikkeavalla tavalla muiden tuotannossa olevien tekijöiden vaikutuksesta.

6.2.5 Ohjeistus

Ohjeistetaan kaikkia tarvittavia tahoja tulevasta muutoksesta kohdennetulla asiakastiedotteella ja muutoksenhallinnan kautta oman organisaation henkilöstölle. Luodaan tarvittavat dokumentaatiot, jotka sisältävät tarvittavat kuvaukset ja ohjeistukset.

6.2.6 Tuotanto

Asetetaan kyseinen toiminto tuotantoon etukäteen sovittujen käytäntöjen mukaan. Tuotantoon otossa on aina oltava palautumissuunnitelma, eli jos jostain syystä tuotantoon otto menee pieleen, voidaan palautua nopeasti entiseen tilanteeseen.

6.2.7 Seuranta

Heti tuotantoon oton jälkeen aloitetaan seuranta, eli tarkistellaan teknistä toimivuutta ja tiedustellaan asiakkaiden mielipiteitä. Seurantaa jatketaan riittävän pitkän aikaa ja sen jälkeen siirrytään normaalin valvonnan tilaan.

6.3 Sosiaali- ja terveydenhuolto

6.3.1 Haasteet sosiaali- ja terveydenhuollon ympäristössä

Identiteetinhallinnan näkökulmasta suurin haaste sosiaali- ja terveydenhuollossa on työntekijöiden liikkuvuus, vaihtuvuus, määräaikaisuudet ja työroolien muuttuminen. Työntekijöiden liikkuvuudella tarkoitetaan sitä, että työntekijä saattaa lyhyehkön ajan sisällä työskennellä eri toimipisteissä erilaisissa rooleissa työajaltaan vaihtelevasti. Määräaikaiset työsuhteet ovat yleisiä sosiaali- ja terveydenhuollon alalla ja tämä aiheuttaa omat vaatimuksensa identiteetinhallinnalle. Käytännössä HR-järjestelmät eivät pysy nopeasti vaihtuvien työsuhteiden perässä ja muistakaan järjestelmästä on erittäin hankalaa saada reaaliaikaista tietoa identiteettejä koskien. Työroolin muuttumisella tarkoitetaan sitä, että työntekijä saattaa olla eri työpisteessä eri statuksella, välillä työntekijänä tai opiskelijana. Edellä mainituista syistä johtuen kaikki identiteetteihin liittyvän automaation täytyy perustua tarkasti sovittuihin sääntöihin.

Sosiaali- ja terveydenhuollossa on tärkeää varma ja nopea toiminta erilaisissa tietoteknisissä ratkaisuissa. Nopean toiminnan tarve johtuu sosiaali- ja tervey-

denhuollon alalla työskentelevien henkilöiden työtehtävien luonteesta. Esimerkiksi jollakin toisella toimialalla aloittava työntekijä ei välttämättä ensimmäisenä työpäivän tarvitse kaikkia tietoteknisiä palveluja täysimittaisina, mutta sosiaali- ja terveydenhuollon alalla uusi työntekijä tarvitsee heti pääsyn tietoteknisiin palveluihin. Uusien työntekijöiden lisäksi sijaisten on päästävä nopeasti tietoteknisiin palveluihin, koska hehän sijaistavat toista työntekijää. Sijaisilla on monesti jo olemassa identiteetti identiteetinhallinnassa, pitkä poissa olo on voinut hyllyttää käyttäjätunnuksen ja tämän johdosta käyttäjätunnuksen uudelleen aktivointi on sujuttava mahdollisimman vaivattomasti.

6.3.2 Resurssien määrittely kytkettäviin rooleihin

Organisaatiorooliin kytketään ne resurssit, jotka annetaan kaikille kyseisen organisaation käyttäjille, esimerkiksi yhteiset verkkolevyt tai muut vastaavat kaikkien käytössä olevat resurssit. Organisaatiorooli seuraa yritysnumeroa, eli mahdollisesti yritysnumeron vaihtuessa, vaihtuu organisaatiorooli vastaamaan uutta yritysnumeroa.

Osastorooliin kytketään ne resurssit, jotka annetaan kaikille kyseisen osaston käyttäjille, esimerkiksi osastokohtaiset SharePoint-sivustot tai muut vastaavat kohdeosaston käyttöön annettavat resurssit. Osastorooli seuraa yritysnumeroa ja kustannuspaikkanumeroa, eli organisaation sisällä tapahtuva kustannuspaikan muutoksen myötä vaihtuu osastorooli vastaamaan uutta kustannuspaikkanumeroa. Organisaation vaihtuessa vaihtuu osastorooli organisaatioroolin kanssa uuden organisaation mukaiseksi.

Asemarooliin kytketään sellaisia resursseja, jotka ovat riippuvaisia kohdehenkilön asemasta kyseisessä organisaatiossa. Asemarooliin kytkettäviä resursseja voivat olla tilausoikeuksia eri järjestelmiin tai muita vastaavia pelkästään esimiestason käytössä olevia resursseja. Asemaroolin haasteena on se, että joissain tapauksissa voi olla hankalaa tunnistaa kunkin identiteetin asema organisaatiorakenteeseen nähden. Asemarooli voi olla vaihtelevasti kytköksissä organisaatio ja osastorooliin, esimerkiksi henkilö voi olla yhtä aikaa esimiehenä

useammalle eri osastolla, joten tällöin yksi tietty osastorooli ja titteli eivät riitä kattamaan koko asemaroolin vaatimaa aluetta.

O365 lisenssit, eli eräänlaiset tuotepaketit vastaavat kukin yhtä resurssia. Kyseisissä resursseissa on ehtona se, että kohdeidentiteetti voi saada vain yhden tuotepaketin. Esimerkiksi ratkaisu voi olla se, että kaikille kohdeorganisaation henkilöille annetaan Organisaatioroolin kautta perustuotepaketti ja määriteltyjen sääntöjen mukaan eri identiteeteille myönnetään korkeampia tuotepaketteja.

6.3.3 Roolien kytkeminen identiteetteihin organisaation sisällä

Organisaatiorooli kytketään kunkin organisaation yritysnumeron mukaan. Osastorooli kytketään kunkin organisaation oman kustannuspaikkarakenteeseen perustuvan kustannuspaikkanumeron mukaan. Asemarooli kytketään kustannuspaikkanumeron, tittelin ja HR-järjestelmästä saatavan esimiestiedon mukaan. Muut automaattisesti identiteetteihin kytkettävät roolit liitetään etukäteen määritetyn tiedon mukaan, esimerkiksi tietyn katuosoitteen omaavat identiteetit voivat saada kyseisessä osoitteessa sijaitsevaan rakennukseen kohdistuvan roolin.

6.3.4 Resurssien kytkeminen rooleihin

Automaattisesti roolin mukana tulevat resurssit kytketään suoraan kiinni kohderooliin. Resursseja määriteltäessä voidaan asettaa ehto, joka estää ristiriitaisten resurssien kytkeytymisen. Mahdolliset ristiriitatilanteet käsitellään manuaalisesti tapaus kerrallaan.

6.3.5 Kuinka paljon pyritään kattamaan roolipohjaisella toiminnalla

On pohdittava sitä, että mitä on järkevää ottaa roolipohjaiseen toimintaan mukaan ja mikä kannattaa jättää manuaaliseen ylläpitoon. Mitä voidaan antaa suoraan automaattisesti roolin mukana, mitä loppukäyttäjä voi halutessaan ottaa vapaasti käyttöön, mikä vaatii järjestelmän pääkäyttäjän luvan, mikä vaatii esimiehen ja järjestelmän pääkäyttäjän luvan ja mikä pitää kierrättää IT-palveluntarjoajan kautta.

Asiakkuusnäkökulmasta on pohdittava sitä, että käytetäänkö neppari-, vetoketju- vai tarrastrategiaa. Eniten käytetty strategia on nepparistrategia, eli organisaatio tarjoaa asiakkaille lomakkeella vaihtoehdot, joista asiakas voi sitten valita haluamansa. Vetoketjustrategiaa käytetään yleensä lomakkeiden suunnitteluvaiheessa, eli asiakkaan kanssa keskustellaan heidän toiveistaan ja tarpeistaan.

Rooli- ja resurssinäkökulmasta on iso haaste pohtia sitä, mitkä roolien ja resurssien myöntämiset annetaan asiakkaiden tehtäviksi, mitkä tehdään itse ja mitkä automaattisesti. Vastuun asettelu on yksi näkökulma, eli pystyykö palveluntarjoaja päättelemään mitkä resurssit voi antaa kohdeidentiteeteille, vai pitääkö kyseinen päätös tehdä asiakkaan edustajan puolelta. Automaation suunnittelussa on oltava äärimmäisen tarkka sen suhteen, että missään tilanteessa automaation kautta ei anneta kiellettyjä oikeuksia.

6.4 Aineiston keruu

6.4.1 Olemassa oleva tieto

Olemassa oleva tieto on aiemmin karttunutta tietoa. Kyseistä tietoa on saatu esimerkiksi koulutusten kautta. Tärkein olemassa olevan tiedon lähde on kokemus, eli kokemuksen kautta matkan varrella saatua tietoa. Kokemuksella on tärkeä osa juuri kyseisen organisaation kannalta, koska palveluksen aikana saatu kokemus spesifioituu juuri kyseiseen organisaatioon ylläpitämiin ratkai-

suihin. Olemassa olevasta tiedosta riskialtteinta tietoa on ainoastaan yhden työntekijän tiedossa oleva hiljainen tieto.

Hiljainen tieto on luonteeltaan abstraktimpaa tietoa. Se on hyvin henkilökohtaista sisältäen henkilökohtaisia näkemyksiä, käsityksiä, intuitiota ja aavistuksia. Hiljainen tieto sisältää myös haltijansa kokemuksia, ideoita, arvoja ja tuntemuksia ja on juurtunut syvälle yksilöön. (Virtainlahti 2009, 43) Organisaatioissa on osaamisen johtamisen oltava kunnossa, jotta hiljaisen tiedon hyödyntäminen onnistuu parhaalla mahdollisella tavalla.

6.4.2 Dokumentaatiot

Dokumentaatiolla tarkoitetaan ohjekirjoja, keskustelupalstoja, artikkeleita, muistiinpanoja ja kaikkea muuta kyseiseen aiheeseen kirjoitettua materiaalia. Kaikkein luotettavinta dokumentaatiota ovat ohjelmiston valmistajan tekemät ohjekirjat. Ohjelmiston valmistajan tekemät ohjekirjat eivät läheskään aina anna ratkaisuja ongelmiin, koska niistä saa yleensä tietoja perusasioista, eli tällöin on ohjeita sovellettava. Internetistä löytyvistä keskustelupalstoista saatavaan tietoon on aina suhtauduttava tietyllä varauksella, koska keskustelupalstoilta löytyvien dokumentointien oikeellisuutta on hankala todentaa, koska kirjoittajan todellisesta osaamisesta ei ole varmuutta. Itse tehdyt organisaatiolle tarkoitetut ohjeet ovat tärkeimpiä, koska niissä on elintärkeää tietoa järjestelmän kannalta. Esimerkiksi jos ohjelmistoon tulee vikatilanne pääkäyttäjän poissa ollessa, tällöin voidaan turvautua kyseistä sovellusta koskevaan tehtyyn dokumentointiin. Kursseilta saatava dokumentaatio voidaan karkeasti jakaa kahteen eri kategoriaan, ohjelmistospesifinen dokumentaatio ja yleisemmälle tasolle tarkoitettu dokumentaatio.

6.4.3 Kyselyt

Kyselyt kohdistetaan etukäteen valittuihin organisaation työntekijöihin ja asiakkaiden edustajiin. Kyselytutkimusten etuna pidetään yleensä sitä, että niiden avulla voidaan kerätä laaja tutkimusaineisto: tutkimukseen voidaan saada pal-

jon henkilöitä ja voidaan myös kysyä monia asioita (Hirsjärvi, Remes & Sajavaara 1998, 191). Kyselyä laadittaessa on ensimmäisenä mietittävä sitä, mihin asioihin kyselyllä on tarkoitus saada vastauksia. Kyselyt voivat olla laadullisia tai määrällisiä. Laadullisella kyselyllä voidaan selvittää asiakkaan edustajilta esimerkiksi jonkin identiteetinhallinnan lomakkeen toimivuutta. Määrällisillä kyselyillä voidaan selvittää organisaation omilta työntekijöiltä esimerkiksi käyttäjätunnusten käsittelyihin liittyviä määreitä, tosin vastaavat asiat löytyvät monesti raportoinnin kautta.

6.4.4 Kehitystiimit

Kehitystiimit koostuvat pääsääntöisesti organisaation henkilöstöön kuuluvista työntekijöistä. Tiimejä voi olla useampia ja niissä kokoonpanot vaihtelevat kulloisenkin tarpeen mukaan. Esimerkiksi opettajien resursointiin liittyvässä kehitystiimissä on jäseninä niitä työntekijöitä, jotka ovat tekemisissä sivistyspuolen asioiden kanssa. Kehitystiimien kokoonpanoon kannattaa myös ottaa jäseniä kohdeaiheen ulkopuolelta, esimerkiksi asiakkuuksien kanssa olevia henkilöitä, jotka osaavat tarvittaessa ottaa kantaa asiakkuuksiin liittyvästä näkökulmasta.

6.4.5 Konsultit

Konsulteilta saatava tieto on monesti tärkeää, koska konsulttien puoleen yleensä käännytään siinä vaiheessa, kun organisaation omat resurssit eivät riitä tilanteen selvittämiseen. Konsulttien kanssa kannattaa toimia siten, että oman organisaation resursseilla tehdään kaikki mahdollinen ja konsulteilta otetaan ainoastaan se puuttuva tieto. Ei ole järkevää teettä konsultilla sellaista työtä, jonka omakin organisaatio pystyy tekemään.

7 Toteutus käytännössä

7.1 Tekninen ympäristö

Tekninen suunnittelu voidaan jakaa kahteen eri osa-alueeseen: On premises -ympäristössä suoritettaviin ratkaisuihin ja pilvessä suoritettaviin ratkaisuihin. Opinnäytteen kehittämistehtävän kohteena on sosiaali- ja terveydenhuollon palvelut. Teknisessä suunnittelussa on myös huomioitava sosiaali- ja terveydenhuollon palvelujen lisäksi kaikki muutkin organisaatiot, koska kaikki tehdyt toimenpiteet levitetään myöhemmin muiden organisaatioiden käyttöön.

Suunnittelun alussa kartoitetaan kohdejärjestelmät, joiden välillä halutaan identiteettien liikkuvan. Kun kohdejärjestelmät ja haluttu identiteettien liikkuminen on selvitetty, tämän jälkeen paneudutaan syvemmin identiteettien sisältöön, eli mitä attribuutteja halutut muutokset koskevat. Kun on selvitetty kohdeattribuutit, tällöin on hyvä piirtää attribuuttitasolle menevä taulukko. Taulukossa kuvataan identiteetin attribuuttien muoto jokaisen järjestelmän kohdalla. Taulukossa 1 on esimerkkitaulukko siitä, miten identiteetin eri attribuutit on oltava eri järjestelmissä. Lopullinen taulukko esitetään kaikille muutosta koskevien järjestelmien pääkäyttäjille. Taulukko antaa järjestelmien pääkäyttäjille selkeän kuvan identiteetin attribuuttien muodosta eri järjestelmissä ja antaa mahdollisuuden puuttua epäkohtiin.

Taulukko 1. Identiteetin attribuutit eri järjestelmissä.

Identity Vault	Active Directory Driver	Text Driver
Description	description	Description
preferredName	givenName	FirstName
Internet Email Address	mail	Email
mobile	mobile	WirelessPhone
Surname	sn	Lastname
Telephone Number	telephoneNumber	WorkPhone
Title	title	Title

Opinnäytetyötä koskevassa ympäristössä identiteettien käsittelyn ytimen muodostavat: eDirectory, Active Directory ja Azure Active Directory. Kuviossa 3 on havainnollistettu kyseiset kolme hakemistoa, joissa identiteettejä säilötään.

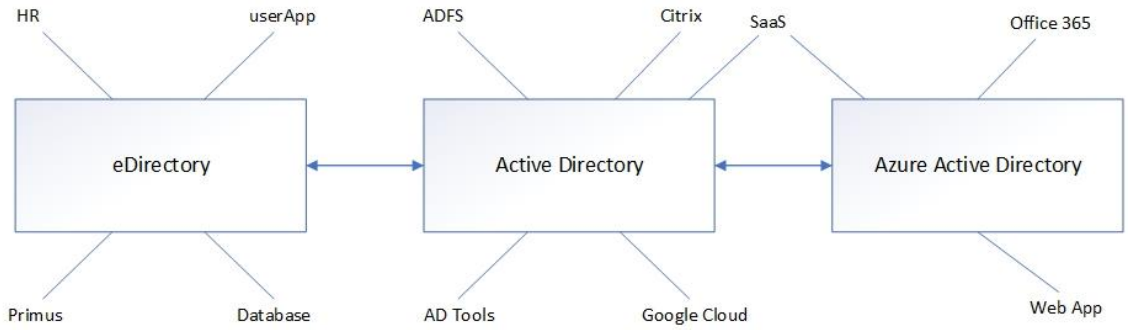
Kuvio 3. Hakemistot, joissa identiteettejä säilötään.

Kaikissa edellä mainituissa hakemistoissa säilötään ja käsitellään identiteettejä. Hakemistoissa identiteetit koostuvat attribuuteista ja attribuutit liikkuvat hakemistojen välillä annettujen sääntöjen mukaan. Jokaisessa hakemistossa on identiteetillä oltava jokin tietty attribuutin arvo, mikä pysyy aina samana identiteetin sijainnista riippumatta, koska aina on oltava varma tieto käsiteltävästä identiteetin omistajasta. Samaa identiteettiä eri ympäristöissä kuvaava attribuutti on ns. lyhyttunnus. Lyhyttunnus on eDirectoryssa (eDir) CN, Active Directoryssä (AD) SAM-Account-Name ja Azure AD:ssa SAM-Account-Name. EDir:n ja AD:n välillä identiteettien välinen synkronointi tapahtuu identiteetinhallinnan AD -ajurin avulla. AD:n ja Azure AD:n välillä identiteettien välinen synkronointi tapahtuu AADC –palvelun avulla. Kunkin hakemiston käyttötarkoitus määrää identiteeteissä olevat attribuutit, eli kaikkia eDir:ssa olevia attribuutteja ei synkronoida AD:hen. Esimerkiksi identiteetin henkilöturvatunnus on sellainen attribuutti, jota ei synkronoida eDir:sta eteenpäin tai jos synkronoidaan, tällöin viedään henkilöturvatunnuksen sijasta kryptattu arvo.

Identiteetinhallintaa rakennettaessa on huomioitava se, että mistä hakemistosta luodaan määräävä hakemisto. Määräävällä hakemistolla tarkoitetaan sitä hakemistoa, jossa on aina oikea tieto identiteetistä. Eli jos toisessa hakemistossa yritetään muuttaa jotakin identiteetin attribuuttia poikkeavaksi määräävän hakemiston arvosta, tällöin määräävä hakemisto muuttaa attribuutin takaisin alkuperäiseen arvoon. Yleensä määräävänä on metahakemisto, eli tässä tapauksessa eDir. Jos ei määritellä päähakemistoa, vaan annetaan kaikille hakemistoille yhtäläinen valta, tällöin kasvaa riski siihen, että samalla identiteetillä on eri hakemistoissa eriarvoisia attribuutteja. Päähakemisto ei päätä kaikista identiteettien attribuuteista, vaan tietyt attribuutit saavat määräytyä toisesta

hakemistosta. On myös mahdollista määrittää siten, että jokin attribuutti saa sen arvon, mikä sille on viimeiseksi asetettu jostakin hakemistosta. Esimerkiksi identiteetin salasana on sellainen attribuutti, jota voidaan päivittää useammasta eri lähteestä ja viimeisin asetettu arvo jää voimaan.

Hakemistopalveluihin liittyy useasti monta ulkopuolista järjestelmää, joista tuodaan tai joihin viedään tietoa identiteeteistä. Kuviossa 4 on kuvattuna identiteettejä säilövät hakemistot ja niihin liitettyjä järjestelmiä. Ulkopuoliset palvelut voivat myös käyttää hakemistoa identiteettien autentikoinnin varmistamiseen, esimerkiksi aktiivihakemiston federointipalvelu (ADFS).



Kuvio 4. Identiteettejä säilövät hakemistot ja niihin liitettyjä järjestelmiä.

Hakemistopalveluihin liitettyjen ulkopuolisten järjestelmien lisääntyminen aiheuttaa sen, että identiteetit ja niihin liitetyt attribuutit liikkuvat monimutkaisemmin. Edellä mainittu tilanne aiheuttaa tarvetta oikeanlaiseen suunnitteluun, muutoksenhallintaan ja dokumentointiin. Teknisestä näkökulmasta katsottuna suunnittelussa huomioidaan kohdejärjestelmän attribuuttien vastine eDir:ssa, attribuuttien liikkumissuunnat ja säännöt attribuuttien käsittelyyn. Kohdejärjestelmän ja eDir:n attribuuttien vastine toteutetaan schemamappauksella (liite 1). Schemamappauksessa kerrotaan eDir:lle haluttujen attribuuttien vastine kohdejärjestelmässä, esimerkiksi HR:ssä kustannuspaikka voi olla KP ja eDir:ssa costcenter. EDir:n schemaa laajentamalla voidaan lisätä attribuutteja, jos jo olemassa olevista ei löydy käyttötarkoitukseen sopivaa attribuuttia. Attribuuttien liikkumissuunnat eDirectoryn ja kohdejärjestelmän välissä tapahtuu filtterillä (liite 2). Filtterissä määritellään se, että saako attribuutti liikkua molempiin suuntiin, vai pelkästään toiseen suuntaan ja kumpi järjestelmä on määräävässä asemassa. Määräävä asema tarkoittaa sitä, että jos eDir:ssa ja kohdejärjestelmässä samal-

la attribuutilla on eri arvo, niin tällöin määräävä järjestelmä pakottaa kyseisen attribuutin samaan arvoon. Säännöillä eDir:ssa määritellään se, kuinka toimitaan attribuuttien arvojen muuttuessa. Esimerkiksi jos jonkin attribuutin arvo on 0, tällöin kohdejärjestelmässä ei tapahdu mitään, mutta jos vastaava arvo onkin 1, tällöin kohdejärjestelmässä tapahtuu ennalta määritelty tapahtuma

Muutoksen hallinnalla tarkoitetaan sitä, kun johonkin järjestelmään tehdään muutoksia, tällöin kyseisistä muutoksista tiedotetaan etukäteen asianmukaisella tiedotuskanavalla. Identiteetinhallinnan osalta muutoksen hallinnan tärkeys korostuu sitä enemmän, mitä enemmän järjestelmiä on kytketty identiteetinhallintaan. Pahimmassa tapauksessa johonkin identiteetinhallintaan kytkettyyn järjestelmään tehdään attribuutin merkitykseen liittyvä muutos, kyseistä muutosta ei suoriteta identiteetinhallintaan ja tämän johdosta identiteetit saattavat käyttäytyä poikkeavalla tavalla. Edellä mainittuja ongelmatilanteita pyritään ennakoimaan identiteetinhallinnan toimintaa suunniteltaessa, mutta kaikkiin poikkeamiin ei välttämättä pystytä etukäteen puuttumaan.

Muutoksen hallinnassa huomioidaan muutoksen vaikuttavuus. Pieniä muutoksia pystytään tekemään hyvin kevyelläkin tiedottamisella. Isommissa muutoksissa saatetaan joutua pyytämään johdontuki kohteena olevalle muutokselle ja muutoksesta on tehtävä oma projekti. Muutoksista tiedottaminen on hyvä tehdä laajalla skaalalla, koska näin ollen useampi organisaatioon kuuluva henkilö tietää järjestelmissä tapahtuvista muutoksista.

7.1.1 Dokumentointi

Dokumentointi voidaan jakaa yleiseen ja tekniseen dokumentointiin. Yleinen dokumentointi on sellainen, jossa näkyy identiteetinhallinnan toiminta yleisellä tasolla. Teknisessä dokumentaatiossa syvennytään identiteetinhallinnan toimintaan teknisellä tasolla. Dokumentoinnin tärkeys korostuu entisestään sitä mukaa, kun identiteetinhallinnan piiriin liitetään uusia järjestelmiä tai rakennetaan uusia toiminnallisuuksia.

Yleisestä dokumentaatiosta voidaan identiteetinhallinnan kohdalla puhua myös järjestelmäintegraatiodokumentaatiosta, koska identiteetinhallinta on käytännössä osa järjestelmäintegraatiota. Yhden haasteen dokumentointiin luo se, että dokumenttia käyttävät yleensä hyvin erilaiset ihmiset, ja kaikkien käyttäjien tulisi saada dokumentaatiosta selville omaan osa-alueeseensa liittyvä olennaiset asiat (Mäkisalo 2016, 28). Edellä mainitun haasteen lisäksi toinen merkittävä haaste on dokumentin päivittäminen ja tämän johdosta dokumentoinnin tulee olla olennainen osa muutosprosesseja.

Tekninen dokumentointi on suunnattu sellaiselle kohderyhmille, joilla on tekniset valmiudet ymmärtää kohdejärjestelmän toiminnallisuus. Laadukas tekninen dokumentaatio on hyvin suunniteltua, selkeätä ja riittävän yksinkertaista. Oleellista on saada dokumentaation kohde ymmärtämään käsiteltävä asia riittävällä tarkkuudella, jotta hän voisi sisäistää kuvattavan kohteen eri toiminnot. (Kokkonen 2016, 9)

7.2 On premises -toteutus

7.2.1 Active Directory

AD:ssa olevat ryhmät vastaavat identiteetinhallinnassa olevia resursseja. Ryhmiä voidaan hyödyntää O365 -palvelussa moneen eri tarkoitukseen: lisenssien hallinnointiin, SharePoint -oikeuksien määrittelyyn, sähköpostin jakelulistojen jäsenyyksien hallinnointiin, jaettujen kalentereiden hallinnointiin ja moniin muihin identiteetteihin liittyviin oikeuksien hallinnointiin.

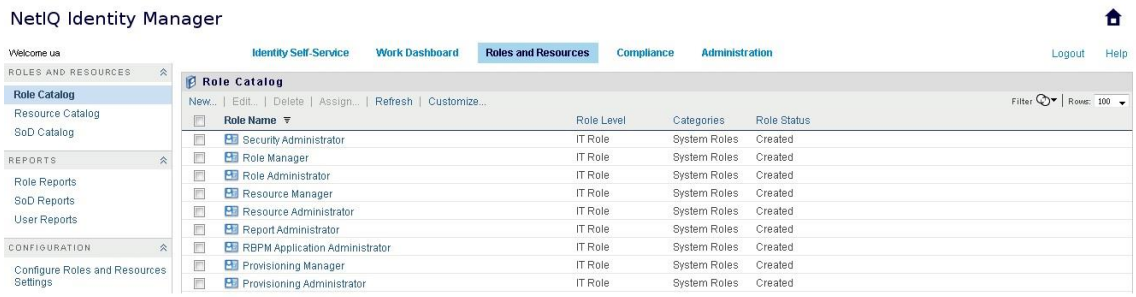
Ryhmät on järkevintä nimetä kunkin asiakasorganisaation nimeämiskäytäntöjen mukaan, näin ollen tarvittaessa ryhmän nimestä näkee sen, että mihin organisaation ryhmä kuuluu. Ryhmät sijoitetaan organisaatioyksiköihin (OU), jossa muutkin ryhmät sijaitsevat. Ryhmiin asetetaan ennalta määritettyyn ExtensionAttribute:n arvo, jonka mukaan kunkin Azure AD -tenantin AADC pystyy tunnistamaan ryhmän ja synkronoimaan sen Azure AD:hn. Jokainen Azure AD -

tenantti vaatii oman AADC:n, joten kukin tenantin AADC tunnistaa vain sitä koskevat tapahtumat.

Identiteetinhallinta lisää käyttäjät ryhmiin ajuria hyödyntäen, eli ajuri havaitsee identiteetinhallinnassa olevaan resurssiin tehdyt muutokset ja suorittaa käyttäjän lisäämisen ryhmään. On olemassa tilanteita, joissa täytyy jäsenyys antaa tapauskohtaisesti AD-työkaluja käyttäen, koska identiteetinhallinnan säännöillä ei pystytä kaikkea kattamaan. Pelkkä käyttäjän lisääminen synkronoitavaan ryhmään ei riitä, vaan kukin käyttäjä on erikseen synkronoitava Azure AD:hen. Käyttäjien synkronointi Azure AD:hen tapahtuu ryhmien tapaan ExtensionAttribute:n arvoa hyödyntämällä.

7.2.2 Rooli- ja resurssihakemisto

Roolit ja resurssit sijaitsevat metahakemistossa, kuin myös identiteetit sijaitsevat samassa metahakemistossa. Metahakemisto on NetIQ:n valmistama eDirectory LDAP-hakemisto. Roolien ja resurssien sijainnilla eDir:ssa ei ole merkitystä muokkaamisen kannalta. Roolien ja resurssien hallintaan on oma GUI, jonka kautta suoritetaan käytännössä kaikki tarvittavat toimenpiteet (kuva 1).



Kuva 1. Näkymä Identiteetinhallinnan rooli-luettelosta (NetIQ 2018).

AD:ssa sijaitsevat käyttäjäryhmät eivät ole ainoita identiteetinhallinnan ulkopuolisia resursseja, joita voidaan kytkeä identiteetinhallinnan sisäisiin resursseihin. Identiteetinhallinnan resurssin kautta on mahdollista luoda sähköpostilaatikko, käynnistää työnkulku, muuttaa kohdeattribuutin arvoa ja tehdä muita vastaavia

toimintoja. Opinnäytetyötä koskevassa työnannossa pysyttäydytään AD:ssa sijaitsevissa käyttäjäryhmissä.

7.2.3 Nimeäminen

Resurssit voidaan kytkeä identiteettiin roolin kautta, eli resurssi on kytketty tiettyyn rooliin tai rooleihin ja tällöin identiteetin saama rooli tuo resurssin mukanaan. Resurssi voidaan myös kytkeä suoraan staattisesti ajurin kautta, eli ajuriin asetettujen sääntöjen täytyttyä identiteetti saa kyseisen resurssin. Hallinnan ja seurattavuuden kannalta on parempi, että resurssit kiinnittyvät identiteetteihin roolien kautta.

Resurssin nimeämisessä kannattaa kiinnittää huomioita siihen, että nimi ei ole liian tekninen, vaan pikemminkin resurssia kuvaava. Hyvin kuvaava nimi tarkoittaa sitä, että jos resurssi saatetaan jossakin vaiheessa asiakkaan näkyville, tällöin asiakas pystyy helposti päättelemään resurssin toiminnallisuuden. Resurssin nimeämisessä on syytä unohtaa Roolin nimet, koska resursseja saatetaan kytkeä ristikkäin eri roolien kanssa.

Roolien nimeämistä suunniteltaessa on ensimmäiseksi mietittävä tulevia roolien käyttäjiä, yleensä kyse on loppukäyttäjistä. Roolin nimen on oltava kytköksissä kohdeidentiteetin profiloituun toimenkuvaan. Edellä mainittu profilointi tarkoittaa sitä, että uudet identiteetit profiloidaan ennalta määriteltyjen ehtojen mukaan ja täten profiloitu identiteetti saa määritellyn roolin automaattisesti. Automaattisen roolin lisäämisen lisäksi rooli voidaan myös anoa työnkulun kautta loppukäyttäjän toimesta ja tällöin roolin kuvaava nimi auttaa loppukäyttäjää.

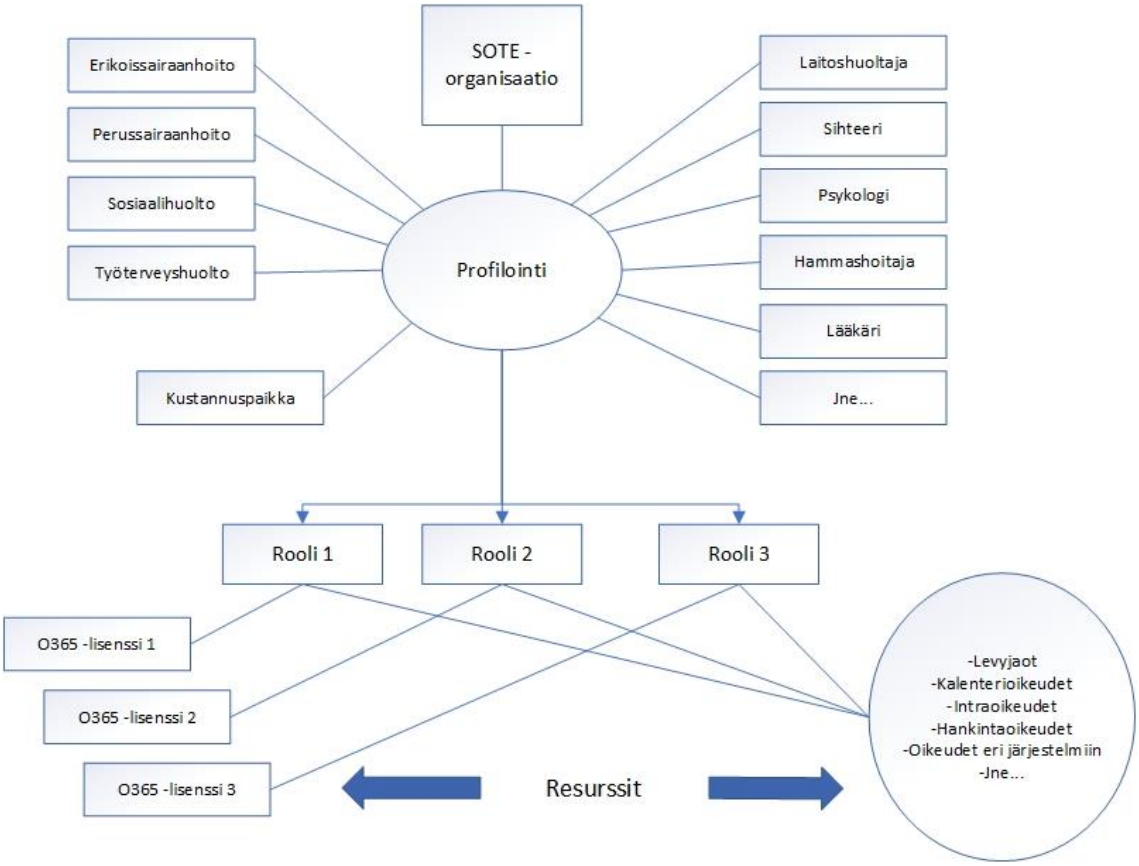
7.3 Azure Active Directory ja O365 -palvelu

O365 -palvelussa lisenssit voidaan kytkeä kohdeidentiteetteihin suoraan tai ryhmien kautta. Suoraan kytkettäessä voidaan käyttää kahta eri menetelmää, graafista käyttöliittymää (GUI) tai PowerShell komentotulkkia. GUI:n kautta lisenssin lisääminen tapahtuu internetselaimen kautta kirjautumalla admin -tason tunnuksilla O365 -palveluun. PowerShell komentotulkin kautta lisenssin lisääminen tapahtuu siten, että ensimmäiseksi käynnistetään etukäteen jo asennettu Azure AD Powershell moduuli, sitten kytkeydytään Azure AD:hn admin -tason tunnuksilla ja annetaan tarvittavat powershell komennot.

Lisenssin lisääminen ryhmien kautta tapahtuu siten, että ensin kirjaudutaan admin -tason tunnuksilla Azure AD -portaaliin ja sitten lisätään lisenssipaketti kohderyhmään. Lisenssipakettia lisättäessä voidaan halutessa antaa kohderyhmien jäsenille kaikki paketin sisältämät palvelut tai annetaan vain osa palveluista. Lisenssien lisäämisessä voidaan myös käyttää PowerShell komentotulkkia.

7.4 Identiteettien roolitus sosiaali- ja terveydenhuollon palveluissa

Kuviossa 5 on esitelty roolien luokittelumalli siitä, miten resurssit liitetään rooleihin ja roolit käyttäjiin. Resurssit on jo etukäteen liitetty sovittujen ehtojen mukaan rooleihin. Roolit liittyvät käyttäjiin määriteltyjen sääntöjen mukaan tai anomisprosessin kautta. Luokittelumallissa profilointi on keskiössä, eli profilointi muodostuu ympärillä olevista tekijöistä ja profiloinnin tapahduttua identiteettiin kytketään haluttu rooli.



Kuvio 5. Roolien luokittelumalli.

7.4.1 Profilointi

Luotu identiteetti profiloidaan etukäteen annettujen neljän eri tunnisteen mukaan. Profilointiin käytettävä toiminto on rakennettu siten, että identiteetti saa jokaisesta neljästä eri tunnisteesta aina jonkin arvon. Edellä mainittu toimenpide varmistetaan siten, että uutta identiteettiä luotaessa prosessi ei etene, kunnes kaikki tarvittavat arvot on annettu, käytännössä tämä tarkoittaa pakotettujen kenttien käyttämistä käyttäjätunnusten hakemiseen tarkoitetussa lomakkeessa.

7.4.2 Organisaatio

Sosiaali- ja terveydenhuollon organisaatioon luotava identiteetti tunnistetaan organisaation nimestä ja organisaation numerosta. Identiteetin tunnistamiseen organisaation osalta käytetään yritysnumeroa. Yritysnumeron käyttäminen orga-

nisaation tunnistamiseen on parempi vaihtoehto, kuin organisaation nimi. Organisaatio nimeen perustuvassa tunnistamisessa on se vaara, että jossain tapauksissa organisaatiot vaihtavat nimeään organisaationumeron kuitenkin pysyen ennallaan ja tällaisissa tilanteissa organisaation nimeen perustuvat tunnistamissäännöt on muutettava. Tunnusten hakijalle organisaatiotieto ei aiheuta minkäänlaista ongelmaa, koska on vain olemassa yksi sosiaali- ja terveydenhuollon organisaatio, johon on mahdollista anoa uusi käyttäjätunnus.

7.4.3 Alueet

Alueita Sosiaali- ja terveydenhuollon organisaatiossa on neljä kappaletta: erikoissairaanhoito, perussairaanhoito, sosiaalihuolto ja työterveyshuolto. Uuden työntekijän aloittaessa hän sijoittuu jollekin edellä mainitusta neljästä alueesta.

7.4.4 Kustannuspaikka

Kustannuspaikka koostuu kustannuspaikan numerosta ja kustannuspaikan kuvauksesta. Jokaisella Sosiaali- ja terveydenhuollon organisaatio kuuluvalla identiteetillä on aina jokin kustannuspaikka. Kustannuspaikka ei ole ainoastaan identiteetinhallinnassa käsiteltävä tietue, vaan samaa kustannuspaikkaa käytetään HR:ssä. Edellä mainitusta syystä identiteetinhallinnan ja HR:n välillä on yhteys, eli HR:ssä tapahtuvat kustannuspaikan muutokset siirtyvät myös identiteetinhallintaan. Kustannuspaikkoihin perustuviin sääntöihin liittyy se haaste, että organisaatioilla on tapana silloin tällöin uudistaa kustannuspaikkarakennetta. Jos kustannuspaikkarakenteen muutoksista ei ajoissa tiedoteta identiteetinhallinnan ylläpitäjiä, tällöin seurauksena voi olla identiteettien odottamaton käyttäytyminen identiteetinhallintaan kytköksissä olevissa järjestelmissä.

7.4.5 Toimenkuvat

Toimenkuvat ovat käytännössä kohdeidentiteetin omaavien henkilöiden titteleitä. Uutta käyttäjätunnusta anottaessa titteli voidaan valita valikosta, jos valikosta ei löydy sopivaa, sitten sen voi kirjoittaa. Jos uutta käyttäjätunnusta haettaessa titteli valitaan valikosta, tällöin kohdeidentiteetti saa spesifioidun roolin. Jos edellä mainitun valinnan sijaan titteli kirjoitetaan, tällöin kohdeidentiteetti saa yleisen roolin.

7.4.6 Roolit

Kohdeidentiteetti saa halutun roolin määriteltyjen ehtojen mukaan. Esimerkiksi sosiaali- ja terveydenhuollon organisaation työntekijä saa osastorooliin silloin, kun työntekijän identiteetin yritysnumero on organisaatioroolin edellyttämä ja kustannuspaikkanumero on osaston edellyttämä.

7.4.7 Yleiset resurssit

Yleisiä resursseja ovat niitä resursseja, jotka on tuotu O365 -resurssien lisäksi identiteetinhallinnan piiriin. Yleisiä resursseja voivat olla: levyjaot, kalenterioikeudet, hankintaoikeudet, oikeudet eri järjestelmiin ja kaikki muut identiteetinhallinnan piirissä olevat järjestelmät.

7.4.8 O365 -resurssit

O365 -resurssit jakautuvat lisenssien näkökulmasta Office 365 Enterprise E1 ja Office 365 Enterprise E3 -lisenssipaketteihin. E1 -lisenssi sisältää palvelut Exchange, OneDrive, SharePoint, Microsoft Teams ja Yammer. E3 -lisenssi sisältää samat palvelut kuin E1 -lisenssi ja lisäksi Office-sovellukset.

7.5 Vaihtoehtoiset ratkaisut

Jos kohdeidentiteetti on sellainen, että sitä ei saada profiloitua etukäteen suunnitellulla prosessilla, tällöin on oltava olemassa vaihtoehtoinen ratkaisu asiakkaan tarvitseman resurssin myöntämiseen. Ylipäätään roolipohjaisella toiminnalla ei ole tarkoituskaan kattaa kaikkia mahdollisia skenaarioita, vaan ne jotka on kohtuullisella vaivalla mahdollista profiloida etukäteen.

7.5.1 Erillinen pyyntölomake

Asiakkaalle tarjotaan erillinen pyyntölomake, jolla riittävät valtuudet omaava asiakkaan organisaation edustaja voi tilata tarjolla olevia lisenssipaketteja. Edellä mainittu tilanne voi tulla eteen sellaisessa tilanteessa, jossa kohdeidentiteetti on saanut profiloinnin kautta E1 -lisenssipaketin, mutta työtehtävien takia tarvitseekin E3 -lisenssipaketin.

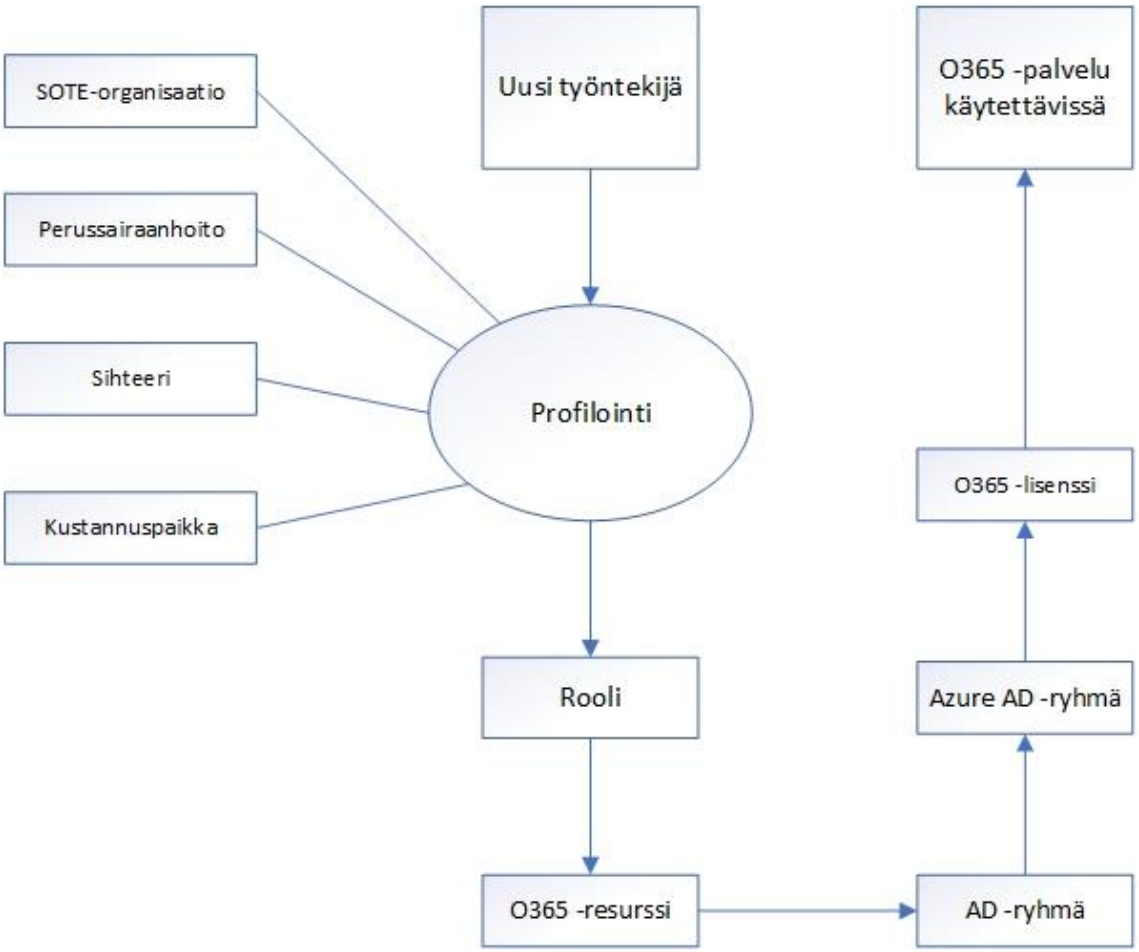
7.5.2 Muut yhteydenottokanavat

Kiireellisissä tapauksissa yhteydenotto tapahtuu puhelimitse tai IT-palvelu hallinnan kautta erillisellä tukipyynnöllä. Kiireellinen tapaus voi olla sellainen, että on nopea tarve käyttää Office 365 -palvelusta sellaisia ominaisuuksia, jota ei ole kohdeidentiteetille myönnetty ja kyseiseen toimenpiteeseen on saatu lupa valtuudet omaavalta asiakkaan organisaation edustajalta.

7.5.3 Esimerkki roolituksesta sosiaali- ja terveydenhuollon palveluissa

Kuviossa 6 on esitetty esimerkkitilanne, jossa sihteeri aloittaa työsuhteen perussairaanhoidon yksikössä. Identiteetinhallinnan kautta anotaan käyttäjätunnukset uudelle työntekijälle. Profiloinnin kautta kohdeidentiteetille luodaan jäse-

nyys tarvittavaan rooliin ja sitä kautta O365 -resurssiin. Kohdeidentiteetti saa AD:ssa ryhmäjäsenyyden O365 -resurssin kytköksen mukaan. AD:sta ryhmän jäsenyydet synkronoidaan Azure AD:hen ja näin ollen ryhmän uusi jäsen saa O365 -palvelut käyttöönsä.



Kuvio 6. Esimerkki roolituksesta.

8 Pohdinta

8.1 Tavoitteiden toteutuminen ja arviointi

Kehitystehtävän tarkoituksena oli tutkia ja toteuttaa rooli- ja resurssipohjainen toiminta Office 365 -palvelujen osalta kohdeorganisaation ylläpitämässä identiteetinhallinnan järjestelmässä. Kehitystehtävä painottui sosiaali- ja terveydenhuollon palveluun. Kehitystehtävässä käytiin läpi tarvittavat toimenpiteet siihen, kuinka otetaan identiteetinhallinnassa käyttöön roolipohjainen Office 365 -palvelujen hallinta. Kehitystehtävä ei anna tarkkaa ratkaisua käyttöönotettavaksi vaan paremminkin mallin, jonka mukaan on mahdollista toteuttaa rooli- ja resurssipohjainen toiminta Office 365 -palvelujen osalta ja sama toiminnallisuus on myöhemmin kopioitavissa muihin järjestelmiin. Oleelliset kohdat tavoitteiden toteutumisen kannalta olivat käytännön suunnittelu ja toteutus käytännössä.

Käytännön suunnittelu sisältää tarvittavat tiedot, joiden perusteella pystytään siirtymään toteutukseen. Suunnittelussa huomioitiin sosiaali- ja terveydenhuollon ympäristön luomat haasteet, joita ovat esimerkiksi työntekijöiden liikkuvuus, vaihtuvuus, määräaikaisuudet ja työroolien muuttuminen. Office 365 -palvelujen osalta suunnittelussa muodostuu tärkeäksi tekijäksi asiakkaiden kanssa käytävät neuvottelut lisenssipakettien osalta, koska kyseisten pakettien sisällöt vaikuttavat lisenssien hintoihin. Office 365 -palvelujen osalta resurssien tekeminen on suoraviivaista toimintaa. Roolien automaattinen määrittely sosiaali- ja terveydenhuollon ympäristössä osoittautui haastavaksi toimenpiteeksi, koska aiemmin mainitut sosiaali- ja terveydenhuollon haasteet aiheuttavat sen, että identiteettejä ei pystytä profiloimaan ehdottomalla varmuudella kovinkaan syvälle. Syvyydellä tarkoitan sitä, että esimerkiksi organisaatiotason rooli on helppo määrittää, mutta edetessä syvemmälle organisaatiorakenteessa profiloinnin ehdottomuus muuttuu epävarmaksi. Ehdottomuudella tarkoitan sitä, että identiteetti on profiloitu varmasti oikein annettujen ehtojen mukaan, koska vääränlaisen profiloinnin tapahtuessa kohdeidentiteetti saattaa saada sille kuulumattomia resursseja.

Toteutus jakautuu kahteen eri osaan, tekniseen rakentamiseen ja roolien luokittelun mallin mukaisesti identiteettien profiloinnin toteuttamiseen. Pilvipalveluiden osalta vastaavia toteutuksia on jo olemassa, koska pilvipalvelujen näkökulmasta ei ole väliä sillä, että millä keinoilla identiteetti on lisätty ryhmään On Premises AD:ssa. On Premises AD:n osalta kerrottiin kuinka ryhmät on syytä nimetä vastaaviksi identiteetinhallinnan resurssien kanssa. Identiteetinhallinnan näkökulmasta katsottuna kerrottiin seikkaperäisesti identiteettien attribuuttien merkitykset ja niihin kohdistuvat muutokset eri identiteettejä säilövien hakemistojen kannalta.

Roolien luokittelumallissa käytiin läpi identiteetin profiloiminen. Kyseinen malli mahdollistaa identiteetin profiloimisen sosiaali- ja terveydenhuollon palvelujen osalta. Mallissa kerrottiin kaikki profilointiin vaikuttavat osatekijät ja miten O365 -lisenssipaketit kytketään niihin. Jos suunnitteluvaiheessa on profiloinnin ehdot saatu sovittua, tällöin tekninen toteuttaminen on suoraviivaista toimintaa. Luokittelumallin riskinä on jo aiemmin mainittu mahdollisuus siihen, että kustannuspaikat ja tittelit saattavat asiakkaan puolelta vaihdella identiteetinhallinnan ylläpitäjien tietämättä.

Kokonaisuutena opinnäytetyö vastaa annettuun toimeksiantoon. Toimeksiantoon liittyen on huomioitava se, että opinnäytetyönprosessin aikana kehitystyön kohteena oleva ympäristö on kokenut muutoksia ja kaikkia näitä muutoksia ei ole pystytty huomioimaan opinnäytetyössä. Tietyissä kohdissa opinnäytetyötä teksti on identiteetinhallintaan liittyvää teknistä sanastoa ja osalle lukijoista tämä aiheuttaa hämmennystä. Asiakkuuksiin ja pilvipalveluihin liittyvistä seikoista olisi pystytty kertomaan enemmänkin, mutta päätettiin pitää painopiste toimeksiantoon liittyen rooli- ja resurssipohjaisessa toiminnassa. Identiteetinhallintaan liittyvistä tulevaisuuden suunnitelmista kerrottiin yleisellä tasolla, koska kyseiseen aiheeseen liittyy monia eri tekijöitä ja niitä kaikkia ei pystytä hallitsemaan palvelun tarjoajan organisaation puolelta.

8.2 Johtopäätökset

Identiteettien tunnistamisen kautta tapahtuva profilointi on suurin haaste identiteettien roolienmäärittelyssä sosiaali- ja terveydenhuollon organisaatiossa. On tarkkaan pohdittava ne keinot, joilla pystytään riittävällä varmuudella profiloimaan sosiaali- ja terveydenhuollon organisaatiossa työskentelevät henkilöt. Profiloinnin kautta annettavat roolit sisältävät sellaisia resursseja, joilla on lupa kohdentua ainoastaan niille tarkoitettuihin identiteetteihin. Jos profiloinnissa on mahdollisuus poikkeamiin, tällöin kyseisen profiloinnin kautta tapahtuvaa roolien myöntämistä ei pidä toteuttaa. Jos jokin tietty rooli on myönnettävä kohdeidentiteetille ilman automaattisesti tapahtuvaa profilointia, tällöin myöntämisen on tapahduttava erillisen anomisprosessin kautta ja tästä tapahtumasta tallennetaan lokitieto.

Roolien oikean määrän määrittäminen on mietittävä sen kautta, että mitä kaikkea roolien kautta halutaan tuoda identiteetinhallinnan piiriin. Sitä parempi, mitä enemmän yksi rooli sisältää resursseja. Jos suunnittelu on menossa siihen suuntaan, että jokaiselle resurssille on oltava oma rooli, tällöin on syytä pohtia uudestaan roolien ja resurssien suhdetta. On olemassa suuri riski siinä, että roolipohjaista identiteetinhallintaa suunnitellessa takerrutaan vähemmän tärkeisiin resursseihin, kun enneminkin pitäisi ensin haarukoida suurimmat tarpeet.

Muutoksien tunnistaminen ja tämän myötä tapahtuva identiteetinhallinnan konfigurointi on tärkeässä asemassa identiteetinhallinnan luotettavan toiminnan kannalta. Osa muutoksista tapahtuu ylläpitäjien oman havaintojen kautta, esimerkiksi lokitietoja tutkittaessa löydetään poikkeama ja tämän johdosta suoritetaan tarvittavat korjaustoimenpiteet. Tietoturvapäivitykset, lakimuutokset ja muut etukäteen tiedossa olevat muutostarpeet ovat normaalia järjestelmän ylläpitämiseen liittyvää toimintaa. Ylläpitäjien huomaamatta jääneet poikkeamat nousevat esille arkipäiväisen toiminnan kautta ja niistä oman organisaation tai asiakasorganisaation edustajat ilmoittavat sähköisiä viestintäkanavia pitkin. Etukäteen tiedostettavia muutoksia ovat myös identiteetinhallintaan liitettyjen järjestelmien muutokset ja näissä muutoksissa on alusta alkaen hyvä pitää identiteetinhallinnan ylläpitäjät mukana. Identiteetinhallintaan liitettyjen järjestelmien muutokset ilman ennakkotietoja on suuri haaste, koska järjestelmistä

vastaavat tahot saattavat työskennellä asiakasorganisaatiossa ja heillä ei välttämättä ole tietoa siitä, että mihin kaikkeen kyseisestä järjestelmästä on kytköksiä. Uusien järjestelmien käyttöönotoissa on syytä luoda johdettu projekti, jossa huomioidaan kaikki uutta järjestelmää koskevat osapuolet. Uusien järjestelmien käyttöönottoprosessia ei pelkästään tarkastella identiteetinhallinnan kannalta, vaan myös muiden järjestelmien kannalta, esimerkiksi uuden järjestelmän dokumentointi ja varmistukset.

Asiakasorganisaation ja identiteetinhallinnan ylläpitäjien vallan ulkopuolella ovat kolmansien osapuolien järjestelmät. Näissä tapauksissa identiteetinhallinnan ylläpitäjät ovat täysin järjestelmää tuottavien organisaatioiden tiedottamisen varassa. Tämän johdosta on erittäin tärkeää seurata järjestelmää tuottavien organisaatioiden tiedotteita, uutissivustoja, blogeja ja muita mahdollisia tiedotuskanavia. Esimerkiksi Microsoftin toimittama O365 -palvelu on sellainen, että sitä kehitetään jatkuvasti ja tämän johdosta on oltava jatkuva seuranta tulevia ominaisuuksia silmällä pitäen. Jatkuva seuranta mahdollista varautumisen tuleviin muutoksiin ja näin ollen tulevista muutoksista voidaan ottaa irti paras mahdollinen hyöty.

Kohdassa 7.5 vaihtoehtoiset ratkaisut käytiin läpi vaihtoehdot, jos kohdeidentiteetin saama rooli ei sisälläkään tarvittavaa resurssia. Kyseinen muutostarve voi kohdata asiakasta vaikka esimerkiksi siten, että asiakkaalle on roolin kautta annettu E1 -lisenssipaketti, mutta nopeasti muuttuneen työtilanteen takia hän tarvitseekin E3 -lisenssipaketin. Kyseinen työtilanteen muutos voi olla sellainen, että se ei näy missään identiteetinhallintaan liitetyssä järjestelmässä ja tämän johdosta automaattisesti ei pystytä tunnistamaan kohdeidentiteetin profiiliin tapahtunutta muutosta.

Niin kauan kun ihmiset tekevät päätöksiä, niin poikkeamilta ei voida välttyä. Poikkeamat kuuluvat inhimilliseen toimintaan, joten niistä ei pidä tuomita ketään, elleivät poikkeamat ole tahallisesti tehtyjä. Poikkeamiin liittyvät ennaltaehkäisy, raportointi ja seuranta. Ennaltaehkäisyyn liittyy etukäteen määritetyt oikeudet rooleihin ja sitä kautta resursseihin. Tietyn organisaation tiedot omaavalle identiteetille pystytään kohdistamaan vain määritetyt roolit ja näin ollen järjestelmä estää poikkeamien syntymisen. Järjestelmästä saatavia raportte-

ja tarkastellaan yhdessä asiakkaiden edustajan kanssa ja tarpeen vaatiessa pystytään korjaamaan poikkeamien mahdollisuudet, jos tällaisia mahdollisuuksia on jäänyt suunnitteluvaiheen jälkeen identiteetinhallintaan. Kun ilmenee tarve jälkikäteen selvittää tapahtunutta poikkeamaa, tällöin hyödynnetään seurantaan tarkoituksenmukaisesti määriteltyä lokitusta.

8.3 Jatkotoimenpiteet ja tulevaisuuden ajatukset

8.3.1 Identiteetinhallinnan näkökulma

Opinnäytetyön kehitystehtävässä keskityttiin rooli- ja resurssipohjaisen toiminnan toteutukseen Office 365 -palvelujen osalta sosiaali- ja terveydenhuollon organisaatiossa. Kyseinen toteutus koskee käytännössä lisenssipakettien jakelua halutuille rooleille. Seuraavaksi on tutkittava tarkemmin Office 365 -palvelujen kautta tarjottavia sovelluksia ja kuinka niitä olisi mahdollista tuoda identiteetinhallinnan piiriin. Esimerkiksi voidaanko Office 365:n Teams tiimityön kanavien oikeuksien hallinta toteuttaa identiteetinhallinnan roolien avulla siten, että esimiesasemassa olevilla on automaattisesti omistajaoikeus ryhmäkeskusteluihin ja ilman esimiesasemaa olevilla on jäsenyysoikeus.

Office 365 -palvelujen käyttö tulee laajenemaan sosiaali- ja terveydenhuollon organisaation lisäksi muissakin saman identiteetinhallinnan piirissä olevien organisaatioiden kohdalla, joten kyseinen konsepti on kopioitavissa muiden organisaatioiden käyttöön. Jokaisen organisaation kanssa on erikseen neuvoteltava Office 365 -palvelujen käytön vaativien lisenssipakettien sisällöstä ja muista aiheeseen liittyvistä seikoista.

Jatkossa identiteetinhallinnan palveluiden on asiakkaiden näkökulmasta mentävä siihen suuntaan, että mahdollisimman paljon asioita tapahtuu piilossa taustalla. Silloin kun identiteetinhallinta edellyttää ihmisen puuttumista prosessiin, tällöin kyseinen tapahtuma kannattaa tarjota asiakkaalle itsepalveluna niin pitkälle kuin se on mahdollista. Edellä mainittu itsepalvelu on asiakkaiden kanssa sovittua työnjakoa, eli kyseessä on tekojen vaihdantaa.

Storbacka ja Lehtinen kiteyttävät tekojenvaihdannan seuraavalla tavalla: Työnjaosta sopiminen tekojen osalta on eräs keskeisiä yrityksen kannattavuuteen ja asiakkuuden kehittämiseen liittyviä näkökohtia. Tämä merkitsee sitä, että asiakas panostaa tekojen osalta aikaa, työtä ja rahaa. Asiakkaan rooli ei näin ole vain tavaroita käyttävä objekti, vaan myös asiakkuuden kehittämiseen osallistuva subjekti. (Storbacka & Lehtinen 2006, 47)

Monella eri alalla työn tekeminen on muuttumassa liikkuvammaksi, eli työntekijöillä ei enää välttämättä ole nimettyjä työpisteitä ja töitä tehdään paljon oman toimiston ulkopuolella. Etätyö on jo normaalia toimintaa monella työpaikalla ja samalla työaikojen joustavuus muuttaa työn tekemisen luonnetta. Työn liikkuvuus ja aikaan sitomattomuus asettavat identiteetinhallinnalle vaatimukset palvella kellon ympäri. Identiteetinhallinnan palveluiden on oltava päätelaiteriippumattomia.

Pilviratkaisut ovat jo osa organisaatioiden IT-ratkaisuja ja tulevaisuudessa pilvipohjaiset ratkaisut tulevat lisääntymään. Office O365 -palvelun myötä käyttäjien identiteetit sijaitseva Azure AD -käyttäjähakemistossa. Tällä hetkellä tyypillisesti identiteetit synkronoidaan On Premises AD:sta O365 -palveluun. Tulevissa ratkaisuissa tilanne voi olla se, että tunnukset viedään suoraan Azure AD -hakemistoon ilman On Premises AD:ta. Tällä hetkellä on jo olemassa toteutuksia, joissa perusasteen koulujen oppilaiden tunnukset synkronoidaan suoraan oppilashallintojärjestelmästä O365 -palveluun. Edellä mainitut seikat on huomioitava identiteetinhallinnan järjestelmiä suunniteltaessa, koska pilvipalvelut ovat osa identiteetinhallintaa.

Identiteetinhallinnan ohjelmistotoimittajan vaihtaminen saattaa tulla ajankohtaisesti moninaisista syistä. Oli ohjelmiston vaihtamisen syy mikä tahansa, niin joka tapauksessa on kyseessä iso projekti. Identiteetinhallinnan ohjelmistovaihtoprojektin suuruus riippuu sitä, että miten laajasti käytössä oleva identiteetinhallinnan ohjelmisto on integroitu toisiin järjestelmiin. Identiteetinhallinnan ohjelmistotoimittajan vaihtaminen saattaa myös toteutua mahdollisesti voimaan astuvan maakuntauudistuksen myötä. Mahdollisen maakuntauudistuksen toteutuessa Vimana Oy:n rooli tarkentunee maakuntien käytössä olevien ohjelmistojen määrittelijänä.

Pilvipalvelut kehittyvät jatkuvasti siten, että yhä enemmän On Premises -ympäristössä tarjottavista palveluista ovat myös tarjolla pilvipalveluissa. Esimerkiksi SQL-tietokanta- ja palvelinresurssit ovat jo tarjolla pilvipalveluissa. Internet of Things (IoT), eli esineiden internet on kovassa kasvussa ja tässä on pilvipalvelut avainasemassa. Tulevaisuudessa monet kodinkoneet on kytkettävissä verkkoon ja niitä sitten hallinnoidaan mobiilisovellusten avulla.

Robottiohjelmien enenevässä määrin lisääntyvä käyttö aiheuttaa sen, että ihmisten hoitamia työtehtäviä osittain korvataan robottiohjelmien avulla. Robottiohjelmien tehdessä ihmisten tekemiä töitä herää kysymys, että pitäisikö robottiohjelmalla olla identiteetti identiteetinhallinnan järjestelmässä. SailPointin perustaja Mark McLain kertoo Computerworld:n artikkelissa, että SailPoint on julkaissut identiteetinhallinnan tuotteen, jolla pystytään hallinnoimaan myös robottiohjelmien omaamia identiteettejä (Computerworld 2019).

8.3.2 Yleisiä näkökulmia

Eri medioista saamme jatkuvasti lukea siitä, kuinka ammatit tulevat tulevaisuudessa muuttumaan. Nyt on jo poistunut tiettyjen alojen ammatteja ja toisaalta samalla on syntynyt tilalle uusia ammatteja.

Työn tekemisen näkökulmasta olemme enenevässä määrin siirtymässä kohti lisääntyvää vuorovaikutusta, eli eri organisaatioiden työntekijät ovat yhä enemmän työajastaan vuorovaikutuksessa toisiin työntekijöihin. Vuorovaikutus ei rajoitu pelkkään fyysiseen läsnäoloon toisten työntekijöiden kanssa, vaan erilaiset sähköiset viestintävälineet luovat jatkuvaa vuorovaikutusta, esimerkiksi Skype:n kautta hoidettavat palaverit ja Teams:n kautta käytävät ryhmäkeskustelut. Vuorovaikutuksella tarkoitetaan myös sitä, että työntekijät haluavat tekemästään työstään mahdollisimman nopeasti palautetta, koska palaute on yksi tärkeä osa työntekijän ammatillista kehittymistä. Digitaalisten työvälineiden lisäksi etätyö lähentää ihmisten vapaa-aikaa ja työaikaa. Uudessa työmaailmassa ei tarvita erikseen työ- ja kotiminää, sillä jokaisen tulee saada olla ja viihtyä työssä omana itsenään (Wilenius 2015, 224).

Maakunta- ja sote-uudistuksen on tarkoitus tulla voimaan 1.1.2021. Tällöin sosiaali- ja terveyspalvelujen, pelastustoimen ja kasvupalvelujen järjestämisvastuu siirtyisi maakunnille (Valtioneuvosto 2019). Maakunta- ja sote-uudistus on niin iso uudistus, että maallikon on hankalaa muodostaa siitä kokonaiskuvaa kaikkine vaikutuksineen. Yksi kyseisen uudistuksen kohde on palvelujen nykyaikaistaminen. Palveluja uudistetaan digitaalisiksi, asiakaslähtöisiksi ja kustannustehokkaiksi. Tavoitteena on tuottaa palveluja sujuvasti ja hyödyntää uusia toimintatapoja (Valtioneuvosto 2019).

Maakunta- ja sote-uudistuksen myötä ICT:n näkökulmasta katsottuna muutoksessa ovat vahvasti mukana Vimana Oy- ja SoteDigi Oy -palvelukeskukset. Vimana on valtion omistama yhtiö, joka toimii Valtiovarainministeriön ohjauksessa. Maakuntauudistuksen tullessa voimaan 90 prosenttia omistuksesta siirtyy maakunnille ja 10 prosenttia jää valtiolle (Vimana 2019). Vimanan tehtävänä on tuottaa maakunnille digitaalisia palveluja. SoteDigi on laissa säädettävää erityistehtävää toteuttava erityistehtäväyhtiö. Valtio omistaa yhtiön sataprosenttisesti, mutta maakunta- ja sote-uudistuksessa omistus siirtyy pääosin maakunnille.

Tätä opinnäytetyötä kirjoitettaessa maakunta- ja sote-uudistus ovat siinä vaiheessa, että eduskunta on käsittelemässä lakiesitystä. Entuudestaan kuntien- ja sairaanhoitopiirien ICT-palveluja tarjoavien yhtiöiden on tulevissa päätöksenteoissaan huomioitava maakunta- ja sote-uudistuksen mahdollisesti tuomat muutokset.

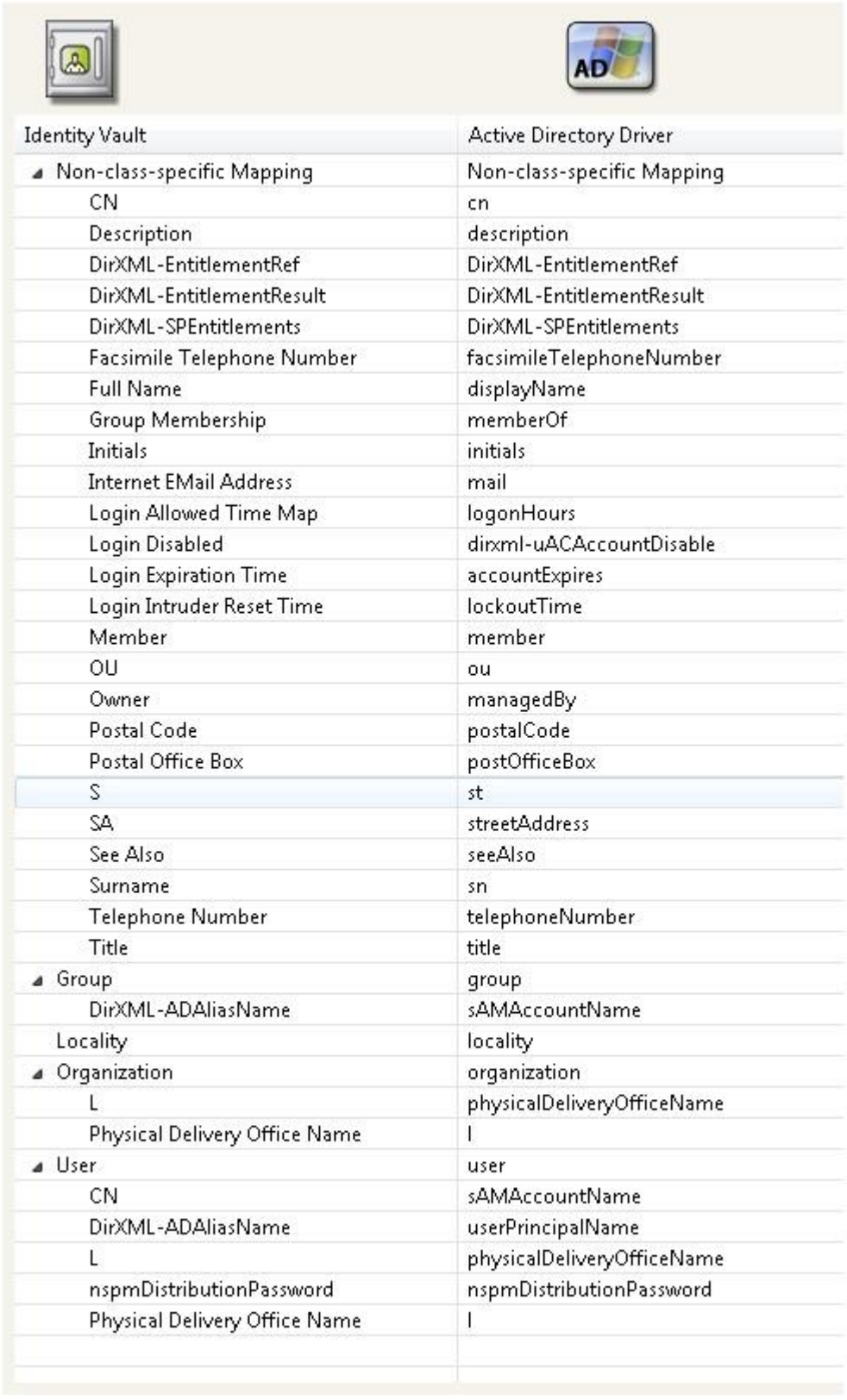
Organisaatioissa tapahtuvat muutokset ovat normaalia yritysten elinkaareen liittyvää toimintaa. Organisaatioiden sisällä rakenteet muuttuvat, organisaatio saattaa fuusioitua toisen vastaavan organisaation kanssa tai jokin toinen taho ostaa koko organisaation osakekannan. Työntekijän näkökulmasta maailma on muuttunut entiseen verrattuna, jolloin saatettiin jäädä ensimmäisestä työpaikasta eläkkeelle. Nykyään työntekijä voi työuransa aikana vaihtaa työpaikkaa monesti ja alakin saattaa vaihtua. On luonnollista, että nykytyöelämän haasteet aiheuttavat työntekijöille ylimääräistä stressiä, koska osaamista on päivitettävä jatkuvasti ja aiemmin mainitut organisaatiomuutokset luovat väistämättä tietynlaista epävarmuutta. Aina on kuitenkin muistettava, että muutoksessa on mahdollisuus.

Lähteet

Aarnivuo-Seppinen, M. 2014. SIEM ulkoistettuna palveluna Case: Julkishallinto. Metropolia Ammattikorkeakoulu. Insinöörityö. http://urn.fi/URN:NBN:fi:amk-201405086711. 2.3.2019.
Computerworld. 2019. Bots: The new challenge for identity management. https://www.computerworld.com.au/article/645589/bots-new-challenge-identity-management. 6.4.2019.
Hirsjärvi, S., Remes, P. & Sajavaara, P. 1998. Tutki ja kirjoita. Helsinki: Kirjayhtymä Oy.
Kokkonen, J. 2016. Tietojärjestelmän teknisen dokumentaation päivittäminen. Hämeen ammattikorkeakoulu. Opinnäytetyö. http://urn.fi/URN:NBN:fi:amk-2016113018323. 16.7.2018.
Linden, M. 2015. Identiteetin- ja pääsynhallinta. Tampereen teknillinen yliopisto. Tietotekniikan laitos. Raportti 6.
https://tutcris.tut.fi/portal/files/3087873/linden_identiteetin_ja_paasynhallinta.pdf. 8.8.2018.
Mäkelä, N. 2008. Identiteetit ja roolit identiteetinhallintajärjestelmissä. Tampereen yliopisto. Pro gradu -tutkielma.
https://tampub.uta.fi/bitstream/handle/10024/79839/gradu03152.pdf?sequence=1 14.7.2018.
Mäkisalo, L. 2016. Järjestelmäintegraatioiden dokumentointi. Tampereen ammattikorkeakoulu. Opinnäytetyö. http://urn.fi/URN:NBN:fi:amk-201605249399 6.1.2019.
Opetushallitus. Edu.fi – opettajan verkkopalvelu.
http://www.edu.fi/valo_opas/hankintaopas/pilvipalvelut. 15.9.2018.
Silander, J. 2013. Katsaus identiteetinhallinnan teknologioihin ja niiden tulevaisuu-den näkymiin. Aalto-yliopisto. Diplomityö.
https://aaltodoc.aalto.fi/bitstream/handle/123456789/10426/master_Silander_Jon_2013.pdf?sequence=1. 15.7.2018.
Sinesaari, J. 2016. Identiteetin-ja käyttöoikeuksien hallinnan kustannus-ja tulosvaikutukset. Lappeenrannan teknillinen yliopisto. Diplomityö.
http://lutpub.lut.fi/handle/10024/124444 29.3.2019.
Storbacka, K & Lehtinen, J. 2006. Asiakkuuden ehdoilla vai asiakkaiden armoilla. Helsinki: WSOY
Sulava Oy. Azure Active Directory kayttajatietojen hallintaa pilvessä.
https://www.sulava.com/azure-active-directory-kayttajatietojen-hallintaa-pilvessa. 15.9.2018.
Tietosuojavaltuutetun toimisto. EU:n tietosuojauudistus.
http://www.tietosuoja.fi/fi/index/euntietosuojauudistus. 10.2.2018.
Tietosuojavaltuutetun toimisto. Henkilötietojen käsittely.
https://tietosuoja.fi/henkilotietojen-kasittely. 29.3.2019.
Tietosuojavaltuutetun toimisto. Pseudonymisoidut ja anonymisoidut tiedot.
https://tietosuoja.fi/pseudonymisointi-anonymisointi. 23.4.2019.
Valtioneuvosto. Maakunta- ja sote-uudistuksen aikataulu.
https://alueuudistus.fi/aikataulu. 06.1.2019.
Valtioneuvosto. Mikä on maakuntauudistus. https://alueuudistus.fi/mika-on-maakuntauudistus. 06.1.2019.

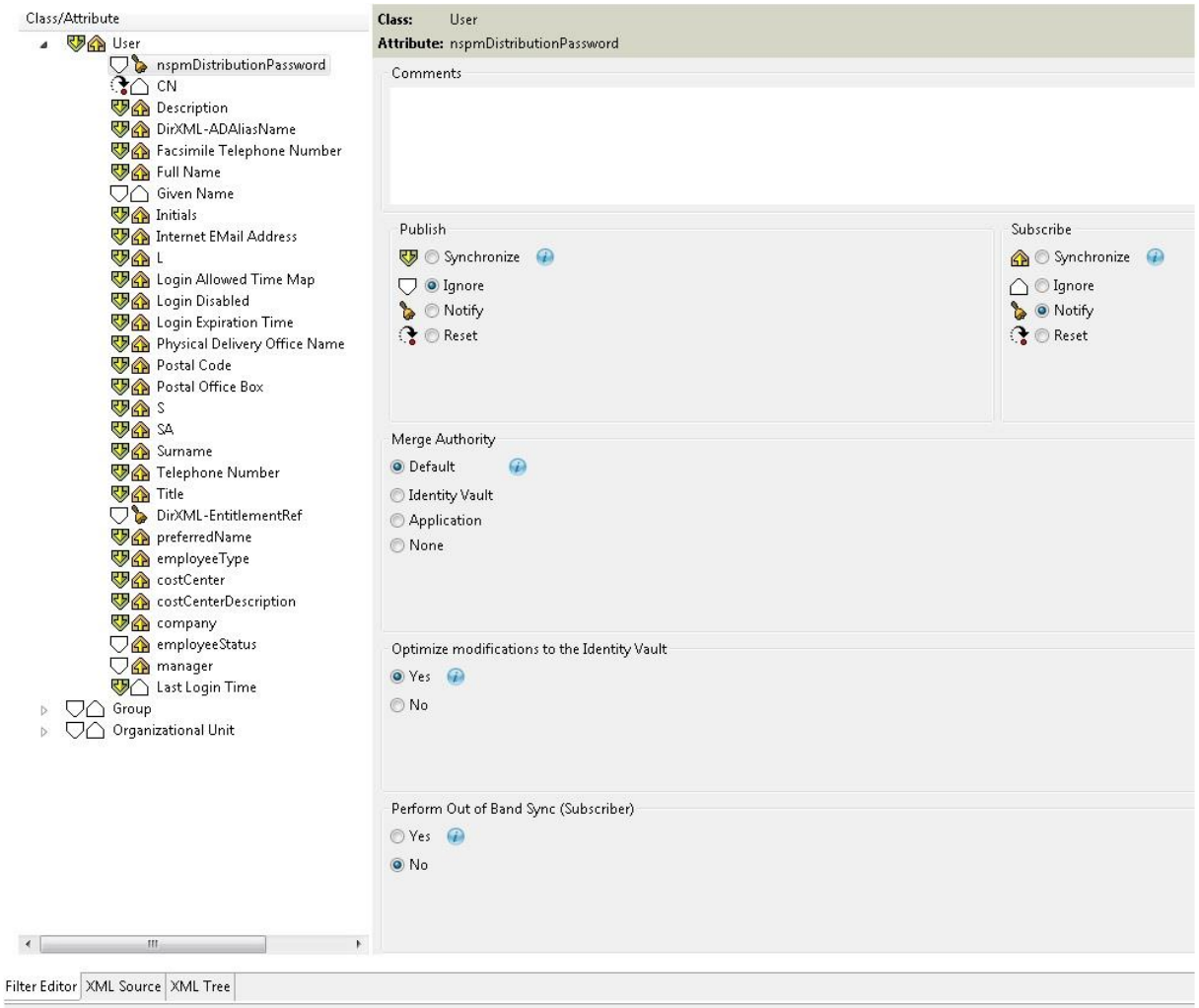
Vimana Oy. Tietoa meistä. https://www.vimana.fi/tietoa-meista/organisaatio. 12.1.2019.
Virtainlahti, S. 2009. Hiljaisen tietämyksen johtaminen. Helsinki: Talentum.
Wilenius, M. 2015. Tulevaisuuskirja : metodi seuraavan aikakauden ymmärtämiseen. Helsinki: Otava.

Schemamappaus



Identity Vault	Active Directory Driver
Non-class-specific Mapping	Non-class-specific Mapping
CN	cn
Description	description
DirXML-EntitlementRef	DirXML-EntitlementRef
DirXML-EntitlementResult	DirXML-EntitlementResult
DirXML-SPEntitlements	DirXML-SPEntitlements
Facsimile Telephone Number	facsimileTelephoneNumber
Full Name	displayName
Group Membership	memberOf
Initials	initials
Internet EMail Address	mail
Login Allowed Time Map	logonHours
Login Disabled	dirxml-uACAccountDisable
Login Expiration Time	accountExpires
Login Intruder Reset Time	lockoutTime
Member	member
OU	ou
Owner	managedBy
Postal Code	postalCode
Postal Office Box	postOfficeBox
S	st
SA	streetAddress
See Also	seeAlso
Surname	sn
Telephone Number	telephoneNumber
Title	title
Group	group
DirXML-ADAliasName	sAMAccountName
Locality	locality
Organization	organization
L	physicalDeliveryOfficeName
Physical Delivery Office Name	l
User	user
CN	sAMAccountName
DirXML-ADAliasName	userPrincipalName
L	physicalDeliveryOfficeName
nspmDistributionPassword	nspmDistributionPassword
Physical Delivery Office Name	l

Filtteri


Class/Attribute
User
nspmDistributionPassword
CN
Description
DirXML-ADAliasName
Facsimile Telephone Number
Full Name
Given Name
Initials
Internet EMail Address
L
Login Allowed Time Map
Login Disabled
Login Expiration Time
Physical Delivery Office Name
Postal Code
Postal Office Box
S
SA
Surname
Telephone Number
Title
DirXML-EntitlementRef
preferredName
employeeType
costCenter
costCenterDescription
company
employeeStatus
manager
Last Login Time
Group
Organizational Unit
Class: User
Attribute: nspmDistributionPassword
Comments
Publish
Synchronize
Ignore
Notify
Reset
Subscribe
Synchronize
Ignore
Notify
Reset
Merge Authority
Default
Identity Vault
Application
None
Optimize modifications to the Identity Vault
Yes
No
Perform Out of Band Sync (Subscriber)
Yes
No
Filter Editor
XML Source
XML Tree