IDENTITEETINHALLINTAJÄRJESTELMÄN SUUNNITTELU JA KÄYTTÖÖNOTTO

Case Point Transaction Systems Oy

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, 5.6.2013

Heli Saarinen

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Hämeenlinna
Tietojenkäsittelyn koulutusohjelma
eLearning ja multimedia

Tekijä Heli Saarinen **Vuosi** 2013

Työn nimi Identiteetinhallintajärjestelmän suunnittelu ja käyttöönotto

TIIVISTELMÄ

Opinnäytetyön toimeksiantajana oli Point Transaction Systems Oy. Tämä opinnäytetyö tehtiin, koska yrityksellä oli tarve sähköistää työntekijöiden käyttöoikeudet omaan identiteetinhallintajärjestelmään (myöhemmin IdM-järjestelmä). Tässä työssä käydään läpi järjestelmän suunnittelu ja käyttöönotto.

Opinnäytetyössä kerrotaan, mitä yrityksen tulee ottaa huomioon identiteetinhallintajärjestelmän käyttöönotossa. Työssä käydään läpi myös, mitä yritys järjestelmältä haluaa ja miten järjestelmä pystyy vastaamaan näihin vaatimuksiin. IdM-järjestelmä, jonka käyttöönotto esitellään myöhemmin työssä tarkemmin, kattaa sisällään niin työntekijöiden käyttöoikeudet ja käyttöoikeustasot yrityksessä käytettäviin ohjelmistoihin ja järjestelmiin kuin kulunvalvonta- ja kassakaappioikeudetkin.

Teoriaosuudessa käydään läpi identiteetinhallintajärjestelmän valintaan vaikuttavat PCI DSS -vaatimukset yrityksen auditoinnin ja raportoinnin kannalta. Tämän jälkeen vertaillaan avoimeen lähdekoodiin perustuvia identiteetinhallintajärjestelmiä sekä maksullisia kaupallisia järjestelmiä. Kun valinta käytettävästä järjestelmästä on tehty, kerrotaan työssä mitä kaikkea pitää ottaa huomioon IdM-järjestelmää suunniteltaessa. Työssä kerrotaan niin projektisuunnitelmasta, gap-analyysista, käyttötapauksista kuin huomioonotettavista laeistakin. Käytännön osuudessa kerrotaan palvelimien sekä itse IdM-järjestelmän asennuksesta sekä käydään läpi yksityiskohtaisempi järjestelmän konfigurointi.

Työn tuloksena yritykselle saatiin vaatimukset täyttävä identiteetinhallintajärjestelmä. Kehitysehdotuksena voisi mainita järjestelmän integroimisen muihin yrityksen käytettävissä oleviin järjestelmiin. Integroimisen myötä saataisiin minimoitua varsinkin IT-tuen manuaalista työtä vielä entuudestaan.

Avainsanat IdM-järjestelmä, PCI DSS, identiteetinhallinta, käyttöoikeus, RM5 IdM

Sivut 26 s.

Hämeenlinna
Degree Programme in Business information Technology
eLearning and multimedia

Author Heli Saarinen **Year** 2013

Subject of Bachelor's thesis Planning and implementing an identity management system

ABSTRACT

The commissioner of this thesis was Point Transaction Systems Oy. This thesis was done because the company did not have an electric identity management system of employees' rights. The company was in need of that kind of system. Planning and implementation of the identity management system is described in this topic.

This thesis describes what should be taken into account when implementing an identity management system. The thesis contains also what the company wants for the system and how the system is able to meet these demands. IdM system includes both access rights of employees and access right levels used in the company's software.

The theory part handled PCI DSS requirements and their influence on the company's strict audit and reporting demands. Both open source identity management systems and commercial systems were compared in the theory part of the thesis. When IdM system had been chosen in the thesis it is told what should been taken into account especially when a company is deploying a new IdM system. The project plan, gap analysis, use cases and observed laws are also represented in the thesis. The practice part handled the installation of used test and production servers and the installation of IdM system itself. Also more specific configuration is described at the end of the practice part.

As a main result the company got an identity management system which fulfilled the strict requirements of the company. One development idea is to integrate the IdM system to the other systems used in the company. It helps manual work of the Service Desk for doing the integrations.

Keywords IdM system, PCI DSS, identity management, access rights, RM5 IdM

Pages 26 p.

SISÄLLYS

ASV	Approved Scanning Vendor. Yritys, joka harjoittaa PCI-verkkoskannausta
Auditointi	Yleisten toimien sekä laadunvarmistuksen arviointi
Gap-analyysi	Analyysi, joka tehdään yritykselle esimerkiksi PCI DSS:n alaisuuteen siirryttäessä: mikä on yrityksen nykytila ja mitä pitää tehdä, jotta yritys täyttäisi PCI-vaatimukset
HR-järjestelmä	Human Resources. Henkilöstöhallintoon käytettävä sähköinen järjestelmä
IdM-järjestelmä	Identiteetinhallintajärjestelmä, jolla hallitaan muun muassa työntekijöiden käyttöoikeuksia
Konfigurointi	Asetusten päättäminen tai asettaminen esimerkiksi ohjelmaa asennettaessa. Yleensä asetuksia voidaan myös muuttaa, jolloin puhutaan uudelleen konfiguroimisesta
Loki	Tapahtumarekisteri, johon kirjautuu esimerkiksi tietokoneohjelmassa tapahtuvat muutokset
PCI DSS	Payment Card Industry Data Security Standard. Maksukorttialan tietoturvastandardi, joka määrittelee maksutapahtumia käsittelevien yritysten vähimmäisvaatimukset
PCI SSC	Payment Card Industry Security Standards Council. Luottokorttiyhtiöistä koostuva neuvosto, jonka hallinnassa ovat PCI-turvakäytänteet
Provisiointi	Ohjelman tai sovelluksen automatisointi käyttöönotossa niin, ettei esimerkiksi it-asiantuntijoilta vaadita osallistumista sovelluksen käyttöönottoon
QSA	Qualified Security Assessor. PCI SSC -neuvoston hyväksymä PCI-tietoturva-auditoija, joka tarkastaa yrityksen käytännöt tietoturvastandardin noudattamisen suhteen
Service Desk	Yrityksen sisäinen IT-tuki. Informaatioteknologian ja tietotekniikan tukihenkilö.
System Owner	Järjestelmän vastuuhenkilö. Henkilö, joka valtuuttaa käyttöoikeuspyynnöt kyseessä olevaan järjestelmään

1 JOHDANTO

Maksupalvelujen tarjoaminen on yleistynyt yritysten keskuudessa huomattavasti viime vuosien aikana. Tämän vuoksi myös säädökset ja vaatimukset ovat tiukentuneet maksupalvelujen tarjoajille. Yrityksille asetetaan tarkat minimivaatimukset, joita tulee noudattaa. Nämä minimivaatimukset määrittää PCI Data Security -standardi (myöhemmin PCI DSS).

Yksi PCI-standardin vaatimuksista on käyttöoikeushallintatyökalujen käyttöönotto yrityksessä. Tässä opinnäytetyössä paneudutaan tuohon vaatimukseen syvemmin sekä esitellään erilaisia vaihtoehtoja identiteetinhallintajärjestelmäksi (myöhemmin IdM-järjestelmä). Näitä IdM-järjestelmiä voidaan käyttää nimenomaan käyttöoikeuksien hallintaan. Työssä kerrotaan myös, miten PCI DSS -vaatimukset vaikuttavat yrityksen identiteetinhallintaan. Lisäksi käydään tarkemmin läpi yhden IdM-järjestelmän suunnittelu- sekä käyttöönottovaiheet.

Työn toimeksiantaja Point Transaction Systems Oy (myöhemmin Point) on Suomen markkinoiden johtava maksupäätetoimittaja sekä palveluntarjoaja. Pointin Suomen toimipisteessä työntekijöitä on noin 130. Point on toimittanut Suomen markkinoille yli 100 000 maksupäätettä ja sirulukijaa. Point keskittyy tarjoamaan asiakkaille korttimaksamiseen liittyviä kokonaisratkaisuja kattaen sisällään niin maksupäätteiden myynnin, huollon kuin erilaiset maksukortteihin sekä -päätteisiin liittyvät palvelut. Näiden lisäksi Point on vastikään aloittanut myös verkkomaksupalvelujen tarjoamisen. Juuri verkkomaksupalvelujen tarjoaminen asettaakin yritykselle aiempaa tiukemmat tietoturvavaatimukset.

Aluksi työssä esitellään, mitä PCI-vaatimukset ovat ja mitä ne merkitsevät yrityksen toiminnalle sekä auditointitarpeille. Tämän jälkeen paneudutaan erilaisiin markkinoilla oleviin IdM-järjestelmiin sekä kerrotaan käytettävän IdM-ohjelmiston valintaprosessista. Työssä kerrotaan sekä avoimeen lähdekoodiin pohjautuvista että kaupallisista järjestelmistä, joita markkinoilla tällä hetkellä tarjotaan identiteetinhallintaan. Valintaprosessin jälkeen kerrotaan enemmän itse suunnitteluvaiheesta; mitä PCI DSS vaatii IdM-järjestelmältä, ja mitä pitää ottaa huomioon tällaista järjestelmää käyttöönotettaessa. Suunnittelun jälkeen kerrotaan ohjelmisto- ja tietokantapalvelimen asennuksesta, minkä jälkeen käydään läpi itse järjestelmän asennus ja yksityiskohtaisempi konfigurointi. Lopuksi esitellään järjestelmän käyttöönotto sekä tulokset.

Opinnäytetyönä valmistunut IdM-järjestelmä on apuna PCI-auditoinneissa erilaisten järjestelmästä ajettavien raporttien vuoksi. Raporteista saa esimerkiksi selville, keillä on oikeudet johonkin tiettyyn järjestelmään ja minkä tasoiset oikeudet ovat. Näitä tietoja muun muassa PCI-auditoijat vaativat. Useissa yrityksissä työntekijöiden käyttöoikeuksia ja käyttöoikeustasoja hallitaan paperilla. Tämän opinnäytetyön tarkoituksena on sähköistää tuo paperiversio.

Tavoitteena on saada kattava tietopaketti eri IdM-järjestelmistä ja kokonaisvaltainen selvitys siitä, mitä on hyvä ottaa huomioon kun yritys siirtyy PCI DSS:n määritysten alaisuuteen. Työssä paneudutaan nimenomaan niihin PCI-vaatimusten kohtiin, joissa puhutaan käyttöoikeushallintatyökalujen käyttöönotosta.

2 MAKSUKORTTIALAN TIETOTURVASTANDARDI

Maksukorttialan tietoturvastandardi eli PCI DSS määrittelee vaatimukset, joita jokaisen maksutapahtumia käsittelevän yrityksen on noudatettava. Tällaisiin yrityksiin kuuluvat esimerkiksi kauppiaat, pankit, erilaiset palveluntarjoajat sekä maksunvälittäjät. PCI DSS:n alainen maksukorttitapahtumien käsittely kattaa niin korttitietojen tallentamisen, hallussapidon kuin välittämisenkin. PCI DSS on kehitetty suojaamaan kortinhaltijan tietoturvaa sekä ylläpitämään yhtenäisen linjan tietoturvakäytänteissä. (Luottokunta n.d.)

Tämän maksukorttialan tietoturvastandardin on kehittänyt PCI Security Standards Council -neuvosto. Neuvostoa ovat olleet perustamassa vuonna 2006 kansainväliset luottokorttiyhtiöt American Express, Discover Financial Services, JBC, MasterCard Worldwide ja Visa International. (PCI DSS Quick Reference Guide 2010, 6.)

2.1 PCI DSS -vaatimukset

PCI DSS:n määrittämiä tietoturvakäytänteitä noudatetaan maksukorttialalla ympäri maailmaa. PCI-tietoturvastandardi on jaettu 12 kohtaan, jotka näkyvät taulukossa 1. (Luottokunta 2010.)

Taulukko 1. PCI-tietoturvastandardin 12 kohtaa (Luottokunta 2010, 5)

Ryhmä	PCI DSS -vaatimukset
Turvallinen verkko	1. Tietojen suojaaminen turvataan asentamalla ja ylläpitämällä toimiva palomuuriratkaisu. 2. Ohjelmistotoimittajan määrittämiä oletussalasanoja tai -asetuksia ei käytetä.
Kortinhaltijoiden tietojen suojaus	3. Tallennetut kortinhaltijatiedot suojataan. 4. Kortinhaltijoiden tiedot ja muut luottamukselliset tiedot siirretään salattuina julkisissa tietoverkoissa.
Haavoittuvuudenhallinta	5. Viruksentorjuntaohjelmistoja käytetään sekä päivitetään säännöllisin väliajoin. 6. Turvallisten järjestelmien ja sovellusten kehittäminen ja ylläpitäminen on suotavaa.
Käyttöoikeushallintatyökalujen käyttöönotto	7. Tietoja rajoitetaan niin, että ne ovat saatavilla vain niille, jotka liiketoiminnallisista syistä tietoja tarvitsevat. 8. Jokaiselle tietojärjestelmän käyttäjälle luodaan yksilöllinen käyttäjätunnus. 9. Kortinhaltijoiden tietoihin pääsyä rajoitetaan fyysisesti.
Verkkojen valvonta ja testaaminen	10. Kaikkea, mikä liittyy verkkoresursseihin ja kortinhaltijoiden tietojen käyttöön valvotaan ja seurataan. 11. Suojamenetelmät ja -prosessit tulee testata säännöllisin väliajoin.
Tietoturvakäytännöt henkilöstölle	12. Koko henkilöstöä koskevat tietoturvakäytännöt luodaan.

2.2 PCI-auditointi

Yritykset, jotka tarjoavat maksupalveluja, tarvitsevat toimiakseen lain säätelemän maksulaitosluvan. Maksulaitosluvan myöntää Finanssivalvonta, joka osaltaan tutkii, täyttääkö maksulaitoslupaa hakeva yritys maksulaitoslaissa säädetyt edellytykset ja vaatimukset (Finanssivalvonta 2012). Maksulaitosluvan saamisen jälkeen Finanssivalvonta valvoo, että lain säätelemät minimivaatimukset täyttyvät yrityksessä myös jatkossa. Tämän takia yrityksiltä vaaditaan erilaisia raportteja ja todistuksia. Tarkastusta, jossa katsotaan, onko etukäteen asetetut vaatimukset täytetty, sanotaan auditoinniksi.

PCI-auditoinnilla tarkoitetaan tarkastusta, jossa tarkistetaan, täyttääkö auditoinnin kohteena oleva yritys PCI DSS -vaatimukset. PCI-auditointeja saavat tehdä ainoastaan yritykset, jotka PCI SSC -neuvosto on hyväksynyt. Näistä PCI SSC:n hyväksymistä PCI-tietoturva-auditoijista käytetään myös kansainvälistä nimitystä QSA eli Qualified Security Assessor. QSA tekee vuosittain yrityksessä paikan päällä tarkastuksen, jossa auditoidaan niin yrityksen järjestelmät kuin yrityksen harjoittamat käytännötkin. Auditointikertoja toistetaan, kunnes yritys täyttää kaikki sille asetetut vaatimukset.

QSA:t, jotka auditoivat suomalaisia PCI DSS:n alaisia yrityksiä, ovat israelilainen Comsec Consulting, IBM:n omistuksessa oleva ISS eli Internet Security Systems, Nixu Oy Suomesta, norjalais-ruotsalainen Secode sekä O-C Group ja Sysnet Irlannista (Pertti Hämäläinen 2009). QSA:n lisäksi yrityksien auditoinnissa on mukana myös PCI-verkkoskannauksia tekevät yritykset. Näistä yrityksistä käytetään nimeä ASV eli Approved Scanning Vendor. PCI SSC -neuvosto valitsee PCI-tietoturva-auditoijien tavoin myös verkkoskannauksia tekevät yritykset hyväksyttävien yritysten listalle. Näitä ASV:n tekemiä ulkopuolelta tulevia PCI-verkkoskannauksia tehdään neljä kertaa vuodessa (Pertti Hämäläinen 2009).

2.3 Raportointi

Identiteetinhallinnassa raportoinnilla tavoitellaan nimenomaan ajantasaisen tiedon saamista ulos järjestelmässä. Raportointityökaluilla tutkitaan järjestelmän eri identiteettien ja käyttövaltuuksien tilaa kyseisenä ajankohtana. Tilanteesta riippuen on mahdollista, että raportit halutaan nykyhetkestä, mutta joissain tilanteissa tarvitsee raportteja ajaa myös esimerkiksi vuosi sitten vallinneesta tilanteesta.

Identiteetinhallintajärjestelmästä ajettavasta raportista halutaan usein nähdä käyttäjälistaus eri järjestelmien osalta, järjestelmälistaus yhden käyttäjän osalta ja lista rooleihin kytketyistä käyttöoikeuksista.

3 IDM-OHJELMISTON VALINTA

IdM-ohjelmiston valintaan vaikuttaa suuresti se, mitä yritys järjestelmältä haluaa ja millaisia vaatimuksia yrityksellä järjestelmän suhteen on. Käytettäväksi ohjelmistoksi voi valita niin avoimeen lähdekoodiin pohjautuvan kuin kaupallisenkin järjestelmän. Vaihtoehtoja löytyy monia molemmista kategorioista. Tässä luvussa esitellään muutamia avoimen lähdekoodin sekä kaupallisen puolen järjestelmiä. On tärkeää, että ennen kuin vaihtoehtoja lähdetään pohtimaan tarkemmin, tulee yrityksellä olla selvillä, mitä identiteetinhallinnalla ylipäätään tarkoitetaan yritysmaailmassa.

3.1 Mitä on identiteetinhallinta?

Identiteetillä tarkoitetaan yritysmaailmassa käyttäjän tunnistamista. Identiteetinhallinnalla varmistetaan, että käyttäjällä on pääsy ainoastaan liiketoiminnallisista syistä tarvittaviin yrityksen järjestelmiin ja tietoihin. Ilman toimivaa identiteetinhallintaa eivät käyttöoikeudet usein ole ajan tasalla.

Helpoiten yrityksen identiteettejä hallitaan omassa IdM-järjestelmässä, johon työntekijöiden käyttöoikeudet syötetään. Kaikki käyttäjien oikeuksien muutokset, lisäykset ja poistot tulisi olla kirjattuna ylös sekä tarvittaessa raportoitavissa ja auditoitavissa. Yksi identiteetin elinkaaren hallinnan keskeisimmistä tehtävistä onkin juuri raportointi ja auditointi. Kun työntekijälle myönnetään oikeuksia, poistetaan niitä tai kun käyttöoikeuksiin tehdään muutoksia, tulee kaikista näistä jäädä merkinnät. Auditoinneissa halutaan saada raporttien avulla selville, kuka on käyttöoikeudet myöntänyt ja kuka suorittanut.

Keskeisimmät kysymykset, joihin identiteetinhallinjärjestelmän halutaan antavan vastauksen, ovat esitettynä taulukossa 2.

Taulukko 2. Identiteetinhallintajärjestelmän keskeiset kysymykset

Ryhmä	**Kysymykset**
Käyttöoikeuksien omaaminen	1. Kenellä on tai on ollut yrityksen järjestelmiin käyttöoikeudet? 2. Minkä tasoiset käyttöoikeudet työntekijällä on tai on ollut?
Käyttöoikeuspyyntöjen hyväksyminen	3. Kuka on hyväksynyt käyttöoikeuslisäykset ja -muutokset?
Käyttöoikeuspyyntöjen suorittaminen	4. Kuka on suorittanut käyttöoikeuksien lisäys-, poisto- ja muutospyynnöt?
Perustelut	5. Perustelu, miksi työntekijä hakee tai tarvitsee käyttöoikeutta. 6. Perustelu, minkä takia työntekijän käyttöoikeuspyyntö on hyväksytty tai hylätty.

Raporttien lisäksi eräs identiteetinhallintajärjestelmään haluttavista ominaisuuksista ovat ilmoitukset ja varoitukset, joita järjestelmä lähettää. Muun muassa määräaikaisista työntekijöistä voidaan lähettää käyttöoikeuden tarkistusilmoituksia esimiehelle tai järjestelmän omistajalle. Näin myös esimerkiksi kesätyöntekijöiden käyttöoikeuksia ei jää niin sanotusti virheellisesti roikkumaan eri järjestelmiin. Jotta identiteetinhallinta on mielekästä, tulee IdM-järjestelmässä olevat tiedot olla ajan tasalla. Tämän takia myös työntekijöiden kouluttaminen järjestelmän käyttöön on ensiarvoisen tärkeää. Käytettävän järjestelmän käyttöliittymä kannattaa mukauttaa mahdollisemman loogiseksi, jotta työntekijöiden olisi helpompi omaksua järjestelmä.

3.2 Avoimeen lähdekoodiin pohjautuvat järjestelmät

Identiteetinhallintaan on saatavilla nykyään monia erilaisia järjestelmiä. Yksi vaihtoehto on käyttää avoimeen lähdekoodiin perustuvaa järjestelmää. Hyvä puoli avoimen lähdekoodin järjestelmissä on se, että ne ovat kustannustehokas vaihtoehto yritykselle. Identiteetinhallintaan käytettävät avoimen lähdekoodin järjestelmät ovat kuitenkin melko uusia ja saattavat vaatia järjestelmän pystyttäjältä teknisempiä taitoja, kuin jos käytettäisiin kaupallista järjestelmää. Alla on esiteltynä muutamia avoimeen lähdekoodiin pohjautuvia järjestelmiä, joissa jokaisessa keskitytään hieman eri asioihin.

3.2.1 OpenIAM Identity Manager

OpenIAM Identity Manager on avoimeen lähdekoodiin pohjautuva järjestelmä. Se on yksi vanhimmista identiteetinhallintajärjestelmistä. Järjestelmä pohjautuu Javaan, mutta sisältää myös HTML- sekä XML-koodia. OpenIAM käyttää arkkitehtuurina palvelukeskeistä tapaa, mikä tarkoittaa sitä, että järjestelmän toiminnot on suunniteltu toimimaan itsenäisinä ja avoimina palveluina. Yksi OpenIAM:n huonoista puolista on se, että se käyttää provisioinnissa SPML-kieltä eli Service Provisioning Markup Languagea. SPML on XML-kieleen pohjautuva kieli, joka on jo hieman vanhanaikainen kieli, eikä sitä enää juurikaan kehitetä. (nLight 2009.)

Kehityksen puutteen lisäksi OpenIAM:n dokumentointi on todella vaikeaselkoista ja lähdekoodia on hankala saada. Lähdekoodista ei ole saatavilla minkäänlaisia muutoslokeja, joten OpenIAM:n kehittymistä on työlästä seurata. Hankalan saatavuuden vuoksi voidaankin jopa kyseenalaistaa se, voiko OpenIAM:ää ylipäänsä edes kutsua avoimeen lähdekoodiin pohjautuvaksi järjestelmäksi.

3.2.2 ForgeRock - OpenIDM

OpenIDM on ForgeRock-nimisen yhtiön kehittelemä avoimeen lähdekoodiin pohjautuva järjestelmä. ForgeRockin perustivat vuonna 2010 ohjelmistoyhtiö Sunilta lähteneet työntekijät. Yhtiö on rekisteröity Norjassa, mutta toimipisteitä sijaitsee Norjan lisäksi myös Yhdysvalloissa, Iso-Britanniassa sekä Ranskassa. Forgerockin muita tuotteita ovat OpenIDM:n lisäksi muun muassa OpenAM sekä OpenDJ.

OpenIDM rakentuu joukosta komponentteja, jotka JavaScript nitoo yhteen. JavaScriptiin pohjautuva koodi vaatii kehittäjältä paljon työtä, joten helppo vaihtoehto IdM-järjestelmäksi OpenIDM ei ole. OpenIDM on kuitenkin varteenotettava vaihtoehto avoimeen lähdekoodiin pohjautuvaksi järjestelmäksi, sillä lähdekoodi on tuoretta ja sitä kehitetään koko ajan aktiivisesti. Sekä etuna että riskinä OpenIDM:n valitsemisessa on kuitenkin se, että koodissa käytetty teknologia on niin uutta, että sen toiminnallisuudesta ei ole täyttä varmuutta. Tämän takia kannattaakin odottaa muutamia vuosia, että nähdään mihin ForgeRock kehityksessään pääsee.

3.2.3 Grouper

Grouper on yliopistomaailmassa tunnettu kevyt avoimeen lähdekoodiin pohjautuva IdM-järjestelmä. Se on suunnattu hieman suuremmalle määrälle käyttäjiä, sillä se on nimenomaan yliopisto ja -koulutusmaailmassa tunnettu sekä käytetty. Tämän takia Grouperia ei tässä projektissa valittu käytettäväksi järjestelmäksi.

3.2.4 Apache Syncope

Apache Syncope on erittäin hyvin rakennettu ja pitkälle suunniteltu avoimen lähdekoodin järjestelmä. Tirasa-niminen yhtiö perusti Syncope IdM:n vuonna 2010, mutta sittemmin se on liittynyt Apache Software Foundationiin (ASF). ASF:ään liittyminen muutti Syncope IdM:n nimeksi Apache Syncopen. Apache Syncopea päivitetään ja parannetaan jatkuvasti, mikä on käyttäjän kannalta positiivinen asia. (Tirasa Apache Syncope n.d.)

3.2.5 MidPoint

MidPoint on työkalu, jolla sidotaan yhteen useita identiteettivarastoja (Evolveum 2011). MidPoint tuntuu hyvältä ratkaisulta, mutta ongelmana ovat hankalat ja laajatkin raportointivaatimukset, jotka yrityksellä on ja tämän takia myös tämä avoimeen lähdekoodiin perustuva järjestelmä unohdettiin.

3.3 Kaupalliset IdM-järjestelmät

Kaupallisiin IdM-järjestelmiin on helpommin saatavilla tukea sekä itse järjestelmän pystytys ei tuota yritykselle niin paljon työtä. Kaupalliset järjestelmät ovat usein melko kalliita, mutta monissa tapauksissa saa rahoille myös hyvää vastinetta. Suurinta osaa kaupallisista järjestelmistä myös parannellaan koko ajan ja niiden kehityksen jatkuvuus on yleensä turvattu.

Haasteena kaupallisissa IdM-järjestelmissä on se, että yrityksen tulee tarkoin selvittää, kuinka mutkattomasti valittava järjestelmä mukautuu kyseessä olevalle yritykselle sopivaksi. Lisäksi on kannattavaa miettiä, kuinka hyvin yrityksen IT-henkilöstö pystyy järjestelmää muokkaamaan vai tarvitaanko aina ulkopuolista, mahdollisesti maksavaa tukea tai konsultin käyntiä paikan päällä.

Kaupallisia IdM-järjestelmiä on monia kymmeniä hieman erityylisiä ja eri asioihin fokusoituneita. Tässä työssä esitellään Quest ActiveRoles-, Microsoft Forefront Identity Manager- sekä RM5 IdM -identiteetinhallintajärjestelmät sekä esitellään niiden hyviä ja huonoja puolia.

3.3.1 Quest ActiveRoles

Quest ActiveRoles on kaupallinen järjestelmä, joka on hyvin AD-orientoitunut. Järjestelmä on kevyt sekä yksinkertainen konfiguroida. Suomessa on ainoastaan yksi Questin tuotteita myyvä yritys. Lisäksi monimutkaisemmat hyväksymisketjut vaativat hieman haasteellisempaa konfiguroimista, eikä se välttämättä onnistu ilman ulkopuolisen konsultin apua.

Questin tuote on selvästi suunnattu pienille ja keskisuurille yrityksille. Mikäli yrityksen koko, tai toisin sanoen käyttäjämäärä, nousee yli 350 henkilön, tulee lisensointi kalliiksi. Lisäksi monimutkaisemmat hyväksymisketjut ja muut vaativammat konfiguroinnit saattavat aiheuttaa haasteita, eikä muutosten tekeminen välttämättä onnistu suoraan järjestelmän käyttöliittymästä.

Koska kyseessä on suuri amerikkalaisyritys, ei konfigurointeja tai yrityskohtaisia muutoksia tehdä juurikaan itse järjestelmään, vaan kaikki konfiguroidaan suoraan asiakkaan ympäristöön. Tämä saattaa aiheuttaa hankaluuksia esimerkiksi järjestelmän päivityksessä. Voidaankin pohtia, kuinka hyvin yrityksessä erikseen määritellyt konfiguraatiot toimivat päivityksen jälkeen.

Raportointityökalut ovat Questin tuotteessa hyvin suunniteltu ja käytettävissä on valmiina monimutkaisempiakin raportteja. Myös auditointivaatimukset olisivat täyttyneet tämän järjestelmän kohdalla.

3.3.2 Microsoft Forefront Identity Manager

Microsoftin identiteetinhallintaan suunnittelema tuote, Microsoft Forefront Identity Manager, sisältää pitkälle kehittynyttä identiteetinhallintaa. Tuote on tarkoitettu selvästi isoille yrityksille ja on täten melko raskas hieman päälle sadan työntekijän yrityksen käyttöön. Microsoftin paikallinen tuki on myös hyvin rajoitettua, joten ongelmia kohdatessa saattaa joutua etsimään apua pitkäänkin.

Microsoftin tuote on huomattavasti kalliimpi kuin yllä esitelty Questin tuote. Kun käyttäjämäärä alkaa lähentyä 10 000 käyttäjää, alkavat kustannukset kääntyä edukseen. Tätä tuotetta valitessa kannattaakin miettiä, onko Microsoftin tuote hieman liian raskas, mikäli kyseessä on pienempi yritys.

Tuotteessa itsessään IdM-järjestelmänä ei ole vikaa. Raportointi- sekä auditointivaatimukset täyttyvät tämän tuotteen kohdalla sekä käyttöoikeudet saa helposti ajettua järjestelmään. Tuotetta myös kehitetään jatkuvasti, joten tuotteen elinkaari ei ole lopussaan. Mutta kuten jo aiemmin mainittiin, saattaa hintalappu pienemmissä yrityksissä olla se syy, jonka vuoksi Microsoftin tuote jää valitsematta.

3.3.3 RM5 IdM

RM5 Software on suomalainen yritys, joka on perustettu vuonna 2009. RM5 on Suomen johtava identiteetinhallintajärjestelmän toimittaja. RM5 IdM -järjestelmän avulla onnistuvat monimutkaisemmatkin hyväksymisketjut. Hyviä puolia on myös se, että tuki on lähellä sekä helposti saatavilla. Koska tuotteen kehitys on suomalaisten käsissä, ovat tuotteen päivitykset nopeasti sekä helposti noudettavissa.

Positiiviseksi puoleksi nousee esille myös se, että RM5 tekee suuret konfiguraatiomuutokset suoraan itse järjestelmään. Tämä tarkoittaa käytännössä sitä, että konfiguraatiot ja erilaiset toiminnot ovat kaikkien RM5:n tuotetta käyttävien yritysten saatavilla näin haluttaessa. Yrityskohtaista konfigurointia pyritään välttämään, sillä se saattaa aiheuttaa haavoittuvuuksia ohjelmistopäivityksissä.

Integraatiomahdollisuudet ovat hyvät, sillä tuotteen saa helposti integroitua erilaisiin HR-järjestelmiin. Myös AD-integrointi on pitkälle kehitettyä ja se onnistuu melko kätevästi asiakasyrityksen näin halutessa.

Riskinä tämän tuotteen valinnassa voi mainita sen, että tuotetta kehittävä yritys on melko pieni. Tähänkin saatiin tosin ratkaisu, sillä Suomen johtava yritysten IT-palvelunhallinta- ja työntekijöiden itsepalveluratkaisujen ohjelmistotoimittaja Efecte Oy, teki yrityskaupat ja osti RM5 Software Oy:n 13.2.2013. (Efecte Oy 2013.)

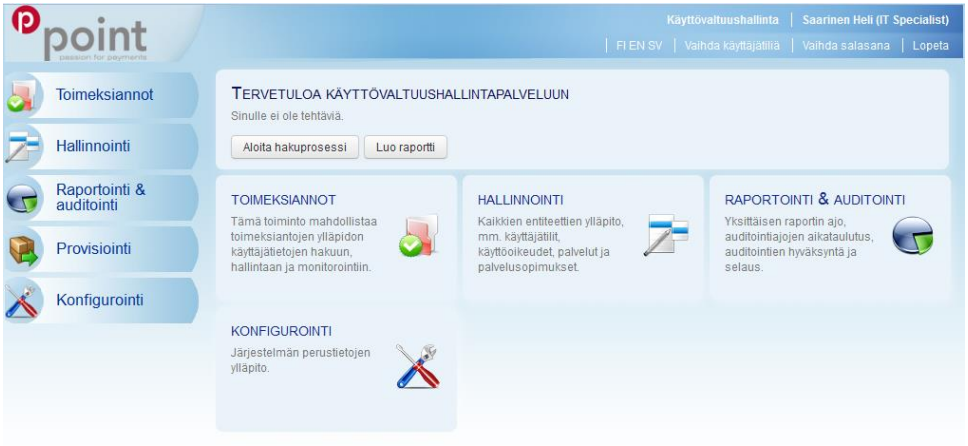
3.4 IdM-ohjelmistoksi valittu järjestelmä

Point valitsi käytettäväksi järjestelmäksi suomalaisen RM5 IdM:n tuotteen. Valintaperusteet olivat muun muassa hyvä hinta-laatu -suhde, suomalaisuus, miellyttävä käyttöliittymä, raportointi- ja auditointivaatimusten täyttyminen sekä nopea järjestelmän toimitus.

Avoimen lähdekoodin järjestelmiä ei valittu siitä syystä, että ne eivät täyttäneet suoriltaan yrityksen vaatimuksia raportoinnin osalta. Tämän lisäksi järjestelmien pystytys olisi vienyt huomattavan paljon kauemmin aikaa kuin kaupallisen järjestelmän käyttöönotto.

Muut kaupalliset järjestelmät RM5 IdM voitti hyvillä ominaisuuksillaan. Ominaisuuksien ja toiminnallisuuksien lisäksi järjestelmän tuen saatavuuden suhteen oltiin tyytyväisiä. Mikäli järjestelmää haluaa jatkossa kehittää entisestään yrityksessä, onnistuu se helposti ottamalla yhteyttä yritykseen.

Yksi tärkeimmistä valintaperusteista oli RM5 IdM:n käyttöliittymä. Käyttöliittymä on toimiva sekä looginen käyttää. Alla olevassa kuvassa 1 näkyy RM5-pääkäyttäjän etusivun näkymä.



Kuva 1. RM5 IdM -pääkäyttäjän näkymä

4 IDM-JÄRJESTELMÄN SUUNNITTELU

IdM-järjestelmän suunnittelu aloitettiin jo järjestelmän valintavaiheessa. Tarkemmin suunnittelua lähdettiin miettimään kuitenkin vasta, kun valinta käytettävästä IdM-järjestelmästä oli tehty. IdM-järjestelmäksi Pointin tapauksessa valittiin suomalaisen RM5 Softwaren tuote RM5 IdM.

IdM-järjestelmän suunnitteluvaihe on kokonaisuuden kannalta hyvin merkittävä, sillä suunnitteluvaiheessa käydään läpi käyttötapaukset, aikataulutetaan projekti sekä tehdään gap-analyysi. Suunnitteluvaihe alkaa projektisuunnitelman tekemisellä.

4.1 Projektisuunnitelma

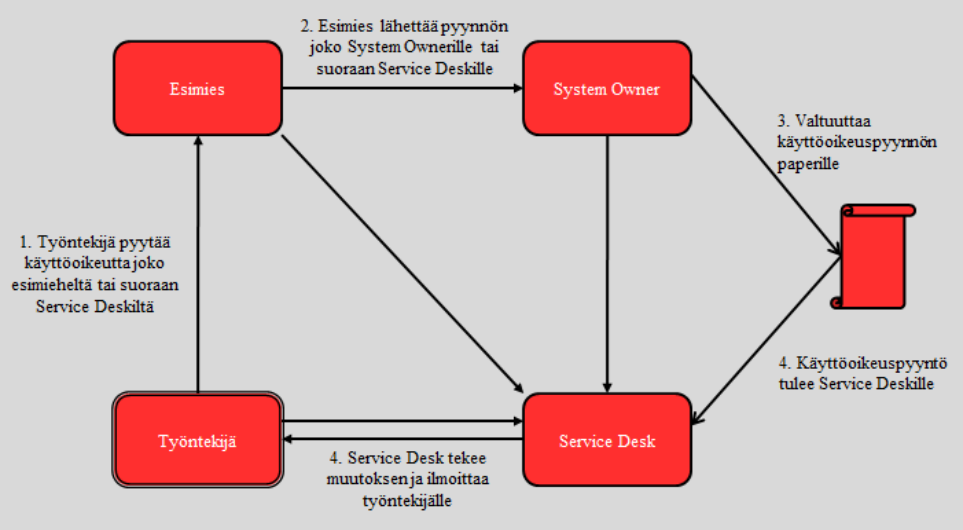
Projektisuunnitelmassa yksi tärkeimmistä kohdista on projektin aikataulutus sekä vastuualueet. Tämä projekti aikataulutettiin alkamaan joulukuussa 2012 ja päättymään huhtikuussa 2013. Suunnitelmassa esitetään myös tarkasti, mitkä ovat toimittajan vastuualueet ja mitkä asiakkaan. Toimittajan vastuulla on toimittaa tuote asiakkaan määrittelyjen mukaan sekä täyttäen asiakkaan vaatimukset. Asiakkaan vastuualue sen sijaan on määritellä toimittajalle käyttötapaukset ja vaatimukset, sekä kerätä IdM-järjestelmään ajettavat tiedot valmiiksi. Tiedoilla tarkoitetaan tässä tapauksessa yrityksen henkilöstöä sekä tämän hetkisiä käyttöoikeuksia ja käyttöoikeuskohteita. Käyttöoikeuskohteet ovat yrityksen käytössä olevia järjestelmiä.

Projektisuunnitelmassa käydään läpi myös mahdolliset testaukset ja järjestelmän koulutukset. Koulutuksia järjestetään usein niin IdM-järjestelmän peruskäyttäjälle kuin pääkäyttäjällekin. Pointin tapauksessa valittiin ainoastaan pääkäyttäjäkoulutus. Henkilökunnan koulutus järjestetään sisäisesti Pointin IT-järjestelmäasiantuntijoiden toimesta.

4.2 Gap-analyysi

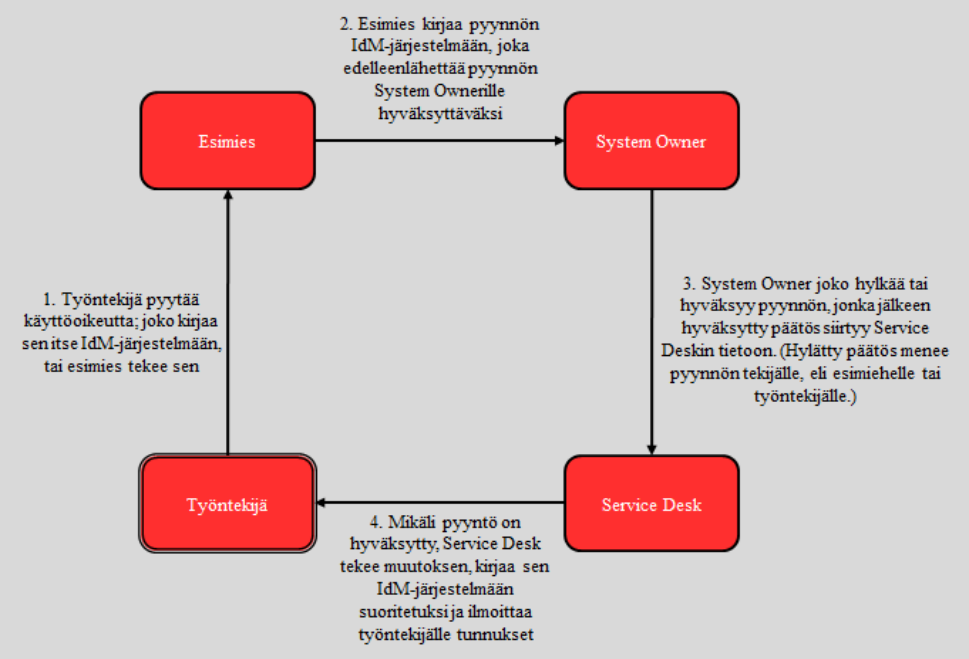
Gap-analyysilla tarkoitetaan selvitystä, jossa tutkitaan mikä on yrityksen tämänhetkinen tila ja mitä vaaditaan, jotta haluttu tavoitetila täyttyisi. Alla on selvennyksenä kuva 2, jossa on kuvattu, miten yrityksen käyttöoikeuspyyntöprosessi ennen IdM-järjestelmää toimi.

Kuvassa käyttöoikeuspyynnön tekee joko työntekijä tai esimies. Työntekijä saattaa pyytää käyttöoikeutta esimieheltä tai suoraan Service Deskiltä. Mikäli pyyntö tulee esimieheltä, lähettää esimies tämän jälkeen pyynnön joko järjestelmän vastuuhenkilölle tai Service Deskille. Kun tieto on saavuttanut kyseessä olevan järjestelmän vastuuhenkilön, valtuuttaa hän käyttöoikeuspaperille pyynnön ja tämän seurauksena Service Desk toteuttaa pyynnön ja ilmoittaa työntekijälle. Mikäli pyyntö on hylätty, on esimiehelle ja työntekijälle mennyt siitä tieto suoraan Service Deskiltä.



Kuva 2. Identiteetinhallintaa ennen IdM-järjestemän käyttöönottoa

Niin kuin kuvasta 2 näkee, ei identiteetinhallinta ollut kovinkaan selvä ja järjestelmällinen. Käyttöoikeuspyynnöt tulivat eri lähteistä ja seurasivat usein väärää reittiä. Pyyntöjen toimeenpaneminen saattoi kestää pitkään, mikäli pyyntö oli mennyt esimerkiksi väärälle henkilölle. IdM-järjestelmä hankitaan nimenomaan yksinkertaistamaan tämä malli. Alla olevasta kuvasta 3 näkeekin, mikä on tavoitetila, joka IdM-järjestelmällä halutaan yrityksessä saavutettavan.



Kuva 3. IdM-järjestelmän avulla saavutettava tavoitetila identiteetinhallinnassa

Käyttöoikeuspyyntöjen lisäksi IdM-järjestelmällä haluttiin yksinkertaistaa ja helpottaa raportointia sekä auditointeja. Kun kaikki käyttöoikeudet ovat IdM-järjestelmässä, on sieltä helppo ajaa haluttu raportti ulos auditointeja varten.

4.3 Käyttötapaukset

Projektisuunnitelman sekä gap-analyysin teon jälkeen käydään läpi käyttötapaukset, jotka projekti tulee sisältämään. Käyttötapauksilla kuvataan tapaukset, jotka järjestelmän tulee täyttää sen ollessa valmis. Mikäli testausvaiheessa käyttötapauksissa kuvattuja tapauksia ei pystytä järjestelmässä toteuttamaan, on projekti usein toimittajan kohdalla siltä osin epäonnistunut. Tämän vuoksi määrittelyvaihe on erityisen tärkeä tämänkaltaisessa projektissa, jottei epäselvyyksiä järjestelmän toiminnallisuuden suhteen tulisi. Käyttötapaukset listattiin yhdessä toimittajan ja Pointin kesken. Käyttötapauksia tuli yhteensä 20 kappaletta. Oheisessa taulukossa 3 on listattu kaikki käyttötapaukset, jotka projektin alussa määriteltiin.

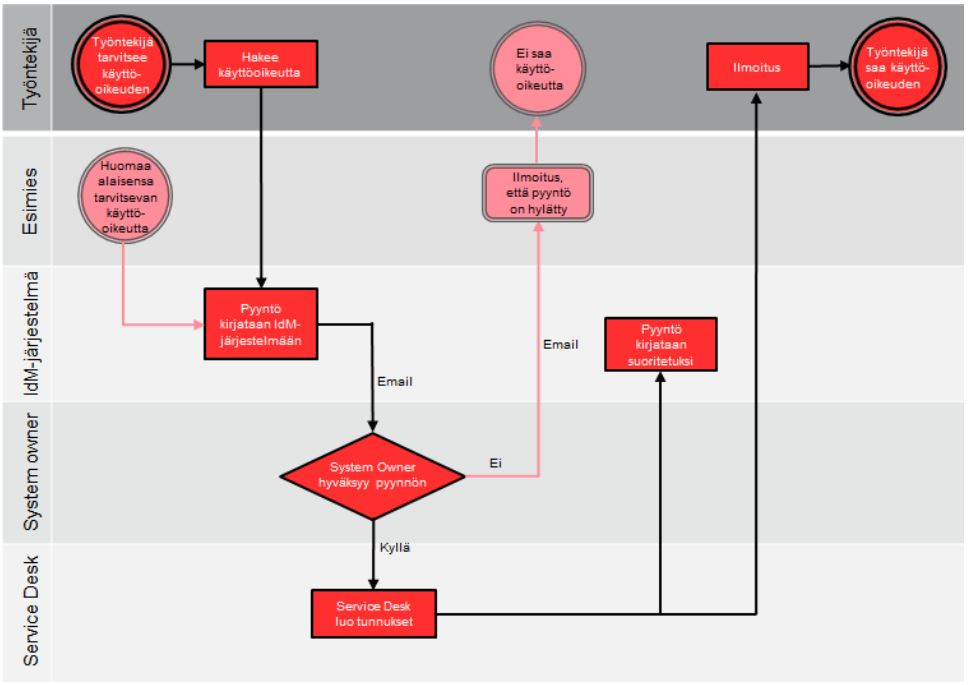
Taulukko 3. Käyttötapauslista

Käyttötapaukset
1. Uuden työntekijän luominen järjestelmään sekä peruskäyttöoikeuksien antaminen
2. Uuden ulkomaalaisen työntekijän luominen ja peruskäyttöoikeuksien antaminen
3. AD- eli toimialuetunnuksen luominen työntekijälle
4. Työntekijä pyytää käyttöoikeutta itselleen
5. Laajennettujen käyttöoikeuksien anominen työntekijälle
6. Laajennettujen käyttöoikeuksien hyväksyminen
7. Laajennettujen käyttöoikeuksien poiston anominen
8. Työntekijän työnkuvan vaihtuminen
9. Työntekijän organisaation tai osaston vaihtuminen
10. Työntekijän esimiehen vaihtuminen
11. Käyttöoikeuksien manuaalinen provisiointi
12. Työntekijöiden käyttöoikeuksien tarkistus esimiehen toimesta
13. Esimiehen tai vastuuhenkilön määrittäminen
14. Esimiesaseman poistaminen työntekijältä
15. Työntekijän pitkä poissaolo (esimerkiksi pidemmän sairasloman tai raskauden vuoksi)
16. Varoitusviestit esimiehille määräaikaisten työntekijöiden sopimusten päättymisen lähestyessä
17. Työntekijän sopimuksen päättyminen
18. Sisäisen tai ulkoisen työntekijän poistaminen järjestelmästä
19. Kassakaappioikeuksien hallinnointi
20. Kulkuluvan anominen työntekijälle

Nämä kaikki kuvattiin omiksi käyttötapauksikseen. Jokaista käyttötapausta varten määriteltiin käyttötapauksen nimi, lyhyt kuvaus, käyttötapauksen toimijat, esivalmistelut ja triggerit. Toimijoilla tarkoitetaan henkilöitä, jotka liittyvät käyttötapaukseen ja ovat mukana käyttötapauksen toimeenpanemisessa. Triggereillä tarkoitetaan asioita, jotka tulee olla tehtynä, jotta kyseessä oleva käyttötapaus voidaan toteuttaa. Esimerkiksi, jotta pystytään luomaan käyttäjälle AD- eli toimialuetunnus, tulee itse työntekijä olla luotuna IdM-järjestelmään. Valmiissa IdM-järjestelmässä testataan kaikkien käyttötapauksien toimivuus.

Alla olevassa kuvassa 4 esitetään yksityiskohtaisemmin gap-analyysissa esitelty tavoitetila käyttöoikeuspyyntöprosessin kulusta. Tämä on yksi käyttötapauksista. Tässä käyttötapauksessa työntekijä pyytää käyttöoikeutta johonkin kyseessä olevaan järjestelmään. Työntekijä kirjaa pyynnön IdM-järjestelmään. Vaaleanpunaisella kuvataan vaihtoehtoinen käyttöoikeudenpyyntöprosessi. Pointin tapauksessa myös esimiehellä on oikeus pyytää alaisilleen käyttöoikeutta. Kun käyttöoikeus on kirjattu IdM-järjestelmään, joko työntekijän tai esimiehen toimesta, lähtee siitä kyseessä olevan järjestelmän vastuuhenkilölle (kuvassa System Owner) sähköposti. Vastuuhenkilö kirjautuu sisään IdM-järjestelmään ja joko hyväksyy tai hylkää pyynnön. Mikäli vastuuhenkilö hyväksyy pyynnön, lähtee siitä yrityksen sisäiselle IT-tuelle (kuvassa Service Desk) sähköposti käyttöoi-

keuden toimeenpanemiseksi. IT-tuki kirjaa työpyynnön tehdyksi IdM-järjestelmään sekä ilmoittaa työntekijälle järjestelmän tunnukset.



Kuva 4. Identiteetinhallinnan käyttötapaus, jossa työntekijälle pyydetään uutta käyttöoikeutta järjestelmään

4.4 Henkilötietolaki ja tietosuoja

Koska järjestelmään ajetaan tiedot työntekijöistä, myös henkilötietolaki on otettava huomioon. Henkilötietolain tarkoituksena on turvata jokaisen henkilön yksityisyyden suojaa. Henkilötietolakia tulee noudattaa silloin, kun henkilötietoja tallennetaan nimenomaan henkilötietorekisteriksi, niin kuin tämän IdM-järjestelmän osalta tapahtuukin. Henkilön tietoja tulisi käsitellä ainoastaan IdM-järjestelmässä siihen alun perin tarkoitetulla tavalla, eikä tietoja saa käyttää muuhun tarkoitukseen. Henkilötietolain nojalla yrityksessä tehdään henkilörekisterianomus tästä IdM-järjestelmästä. (Henkilötietolaki 1999.)

5 JÄRJESTELMÄN ASENNUS

IdM-järjestelmän perusteellisen suunnittelun jälkeen aloitettiin palvelinten asennukset. Asennusvaiheeseen kuului niin palvelimien ja ohjelmistojen asennus kuin järjestelmän konfigurointikin.

5.1 Palvelimen asennus

IdM-järjestelmää varten asennettiin palvelin sekä testikäyttöä että itse tuotantoa varten. Palvelimista tehtiin virtuaalipalvelimia asentamalla ne pyörimään VMwaren päälle. Käyttöjärjestelmäksi valittiin Linux Red Hat Enterprise 6, 64-bittinen versio. IdM-järjestelmän olisi voinut asentaa myös

Windowsin päälle, mutta Linux on tiettävästi huomattavasti helpompi ylläpidettävä, joten valinnaksi osui tämän takia Red Hat Enterprise -käyttöjärjestelmä. Palvelimet saavat tietoturvapäivitykset Red Hat Satelliten kautta, joten manuaalisesti niitä ei tarvitse erikseen hakea. Näin palvelimet saadaan pidettyä ajan tasalla ja päivitettyinä.

Palvelimiin konfiguroitiin muistia neljä gigatavua ja levytilaa 10 gigatavua. Oletusvaatimuksena RM5:lla oli edellä mainittua hieman suuremmat lukemat, mutta koska Pointilla on käyttäjiä melko vähän, noin 130 työntekijää, riittävät alemmat muistin määrät sekä levytilat.

5.2 Ohjelmiston asennus

Tietokannaksi asennettiin MySQL 5.1.3 ja ohjelmistopalvelimeksi Glassfish 3.1.2. Molemmat ovat avoimeen lähdekoodiin pohjautuvia ilmaisia järjestelmiä. Näiden lisäksi järjestelmä käyttää Javaa, joten Javasta asennettiin versiot JDK 1.6 sekä JCE 6.

5.3 Järjestelmän konfigurointi

Järjestelmän konfigurointi aloitettiin Excel-tiedoston täyttämisellä. Jotta vältyttäisiin manuaaliselta konfiguroinnilta käyttöliittymän kautta, täytettiin Excel-tiedosto niin tarkasti ja monipuolisesti kuin mahdollista. Kaikki tiedot, mitä Exceliin täytettiin, olisi ollut mahdollista konfiguroida myös käyttöliittymän kautta. Aikaa säästyi tosin huomattavasti täyttämällä Excel alusta lähtien oikeilla tiedoilla. Excelin sai myöhemmin ajettua järjestelmään sisään ja tämän jälkeen yksityiskohtaisempaa konfigurointia voi jatkaa käyttöliittymän kautta.

Exceliin kirjattiin kaikki työntekijät, heidän yhteystietonsa, esimiehensä sekä heidän tämänhetkiset oikeutensa. Tämän lisäksi kirjattiin kymmenen käytössä olevaa järjestelmää sekä järjestelmien kuvaukset. Loput järjestelmät, joita yrityksessä käytetään, kirjataan manuaalisesti IdM-järjestelmän käyttöliittymästä.

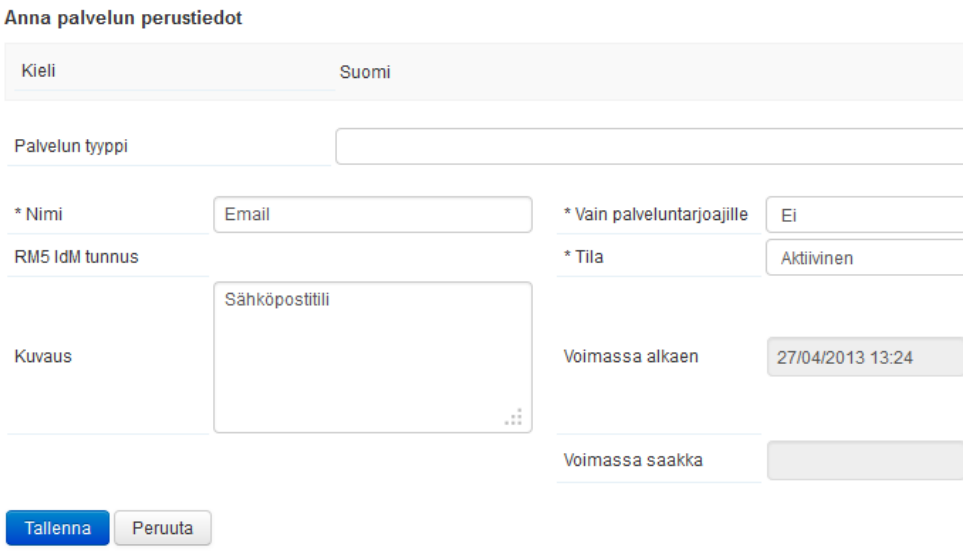
Edellä mainittujen lisäksi Exceliin määriteltiin tehtävät ja tehtävätyypit. Tähän osioon kuvailtiin, minkälaisia tehtäviä yrityksessä on sekä minkälaista prosessia seurataan näitä kyseessä olevia tehtäviä suoritettaessa. Tässä tapauksessa tehtävillä tarkoitetaan muun muassa työntekijän peruskäyttöoikeuksien anomista, käyttöoikeuksien poistamista, laajennettujen käyttöoikeuksien anomista ja kulkuluvan ja -kortin anomista.

Käyttötapauksiin on määritelty, minkälainen prosessi työntekijöiden käyttöoikeuden anominen on. Käyttöoikeutta pystyy anomaan työntekijä itse, hänen esimiehensä ja IdM-järjestelmän pääkäyttäjät. Kun käyttöoikeutta on anottu, lähtee pyyntö peruskäyttöoikeuksien hyväksyjälle. Hyväksyjä on voitu määrittää aiemmin mainittuun Exceliin tai sen voi määrittää käyttöliittymän kautta. Hyväksynnän jälkeen siirtyy pyyntö suorittajalle eli tässä tapauksessa IT-tuelle.

Alla käydään läpi peruskäyttöoikeuden anominen. Esimerkissä määritellään anomiseen tarvittavat palvelut, järjestelmäroolit, käyttäjätilit, käyttäjäryhmät, tehtävätyypit ja toimeksiantotyypit. Alla käydään läpi myös konfigurointi IdM-järjestelmään järjestelmän käyttöliittymästä.

5.3.1 Palvelun määrittely

Ennen koko prosessin konfiguroimista, pitää luoda prosessissa käytettävät palvelut ja järjestelmäroolit. Palvelu määritellään ensin ja sen jälkeen järjestelmärooli. Kun palvelu ja järjestelmärooli tai -roolit on luotu, ne liitetään yhteen. Esimerkkinä käytetään sähköpostitunnuksia ja niiden anomista. Ensin luodaan palvelu nimeltä Email sekä määritellään sille kuvaus, tila sekä voimassaolo (kuva 5).

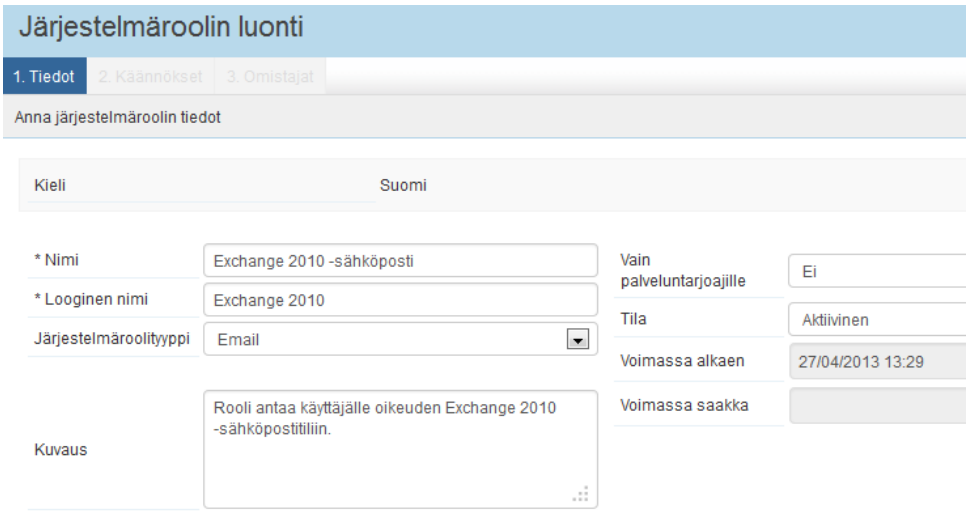


Kuva 5. Sähköposti-palvelun luominen

Tämän jälkeen palvelulle saadaan määritettyä vastuuhenkilö. Tätä vastuuhenkilöä voi esimerkiksi myöhemmin käyttää hyväksyjänä tämän palvelun käyttöoikeuspyynnölle. Vastuuhenkilöitä voi myös määritellä useampia tarvittaessa.

5.3.2 Järjestelmäroolin määrittely

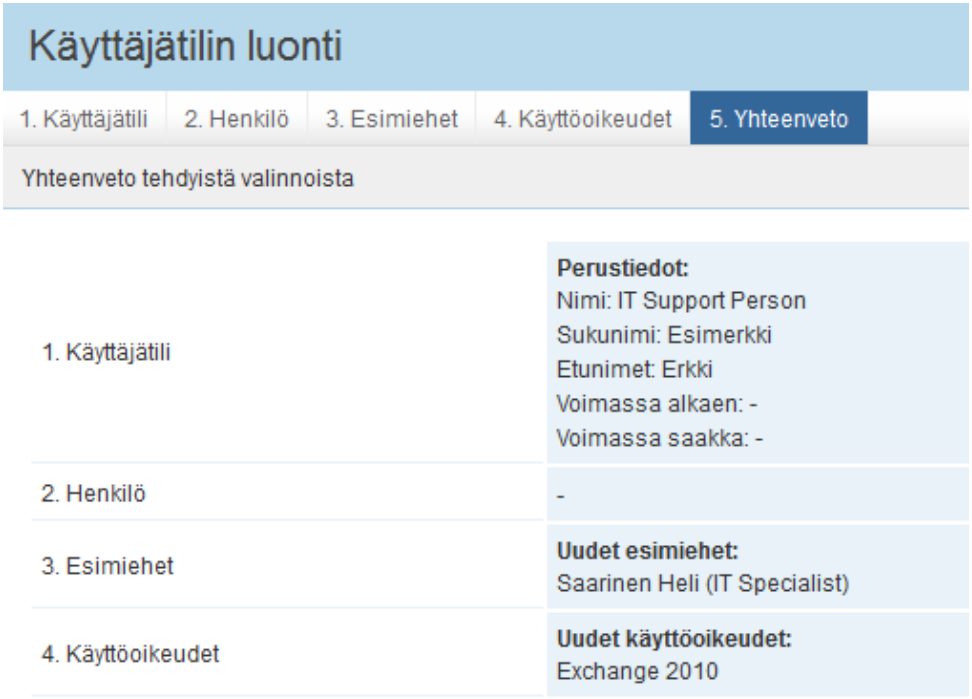
Kun palvelu on luotu, määritetään IdM-järjestelmään tämän palvelun järjestelmärooli tai -roolit (kuva 6). Esimerkissä luodaan järjestelmärooli nimeltä Exchange 2010 -sähköposti. Roolille annetaan nimi, looginen nimi sekä järjestelmäroolityyppi, joka tässä tapauksessa on siis äsken luotu palvelu. Näin saadaan linkitettyä järjestelmärooli siihen kuuluvaan palveluun.



Kuva 6. Exchange 2010 -sähköposti -järjestelmäroolin luominen

5.3.3 Käyttäjätilin luominen

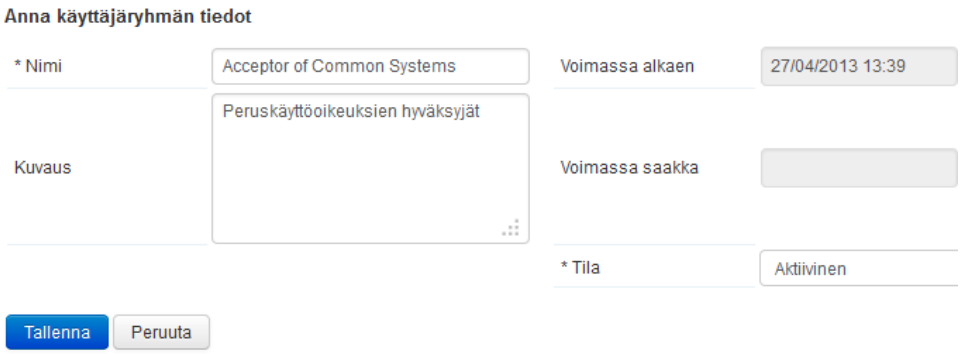
Käyttäjätilit tarkoittavat yrityksen työntekijöitä, joille jokaiselle on IdM-järjestelmässä oma tili. Uusia tilejä saa luotua käyttäjätilityökalulla. Käyttäjätiliä muodostettaessa annetaan työntekijän titteli, nimi, puhelinnumero, sähköpostiosoite sekä mahdollinen kulku- tai hälyavaimen numero. Lisäksi käyttäjätilille valitaan listasta esimies sekä määritetään mahdolliset suoraan annettavat käyttöoikeudet. Esimerkissä on annettu käyttöoikeudeksi äsken määritetyn Email-palvelun alta Exchange 2010 -järjestelmärooli (kuva 7).



Kuva 7. Käyttäjätilin luominen: Yhteenveto

5.3.4 Käyttäjäryhmän luominen

Käyttäjätilit kuuluvat määriteltäviin käyttäjäryhmiin. Esimerkissä luodaan peruskäyttöoikeuksien hyväksyntään tarvittava käyttäjäryhmä nimeltä Acceptor of Common Systems (kuva 8). Tallennuksen jälkeen tähän käyttäjäryhmään saa lisättyä käyttäjätilin tai -tilejä. IdM-järjestelmässä olevien käyttäjien ei ole pakko kuulua yhteenkään ryhmään. Toisaalta taas käyttäjät voivat kuulua myös useampaan ryhmään. Käyttäjä voi olla esimerkiksi hyväksyjä useissa eri toimeksiannoissa.



Kuva 8. Käyttäjäryhmän luominen

5.3.5 Tehtävätyypin määrittely

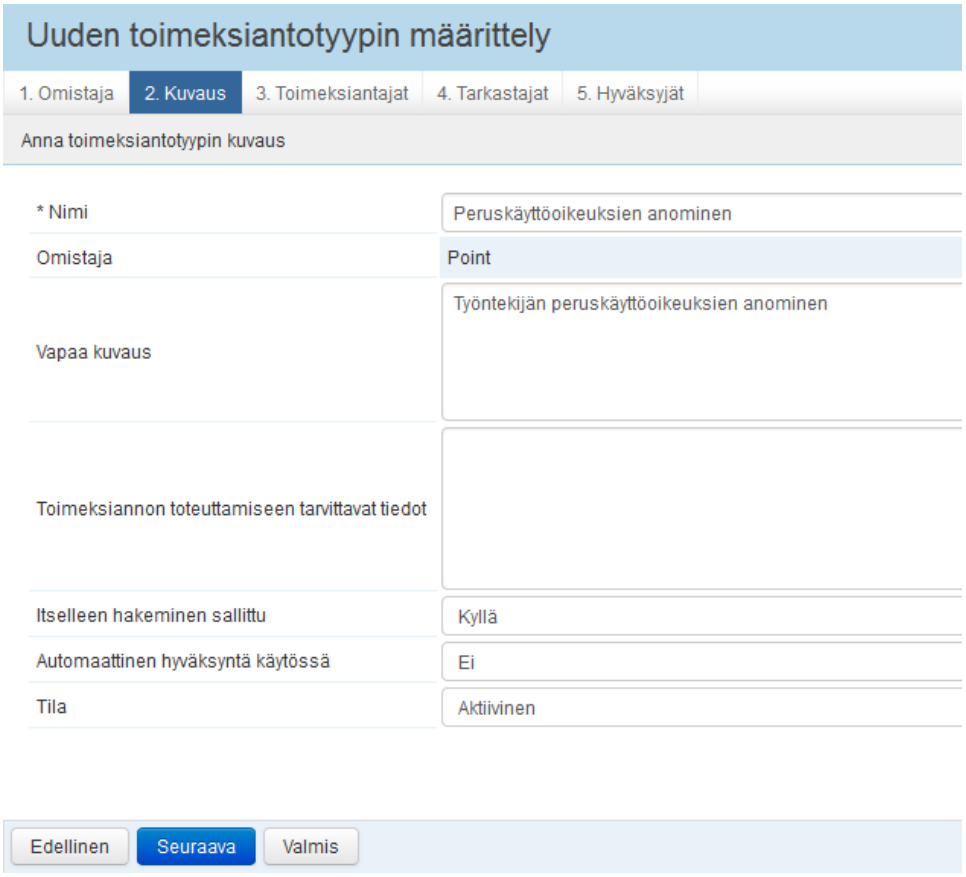
Tehtävätyyppejä tarvitaan, jotta toimeksiantoketjuja voi luoda. Tehtävät voidaan linkittää tiettyyn palveluun ja tiettyyn järjestelmärooliin. Alla olevassa kuvassa 9 luotu tehtävä on linkitetty Email-palveluun ja sen sisällä Exchange 2010 -järjestelmärooliin. Tehtävä siirtyy toimeksiantoketjussa hyväksynnän jälkeen suorittajalle, joka saa ohjeistuksen sen mukaan, miten tähän tehtävään on merkitty.

Kuva 9. Tehtävätyypin määrittely

5.3.6 Toimeksiantotyypin määrittely

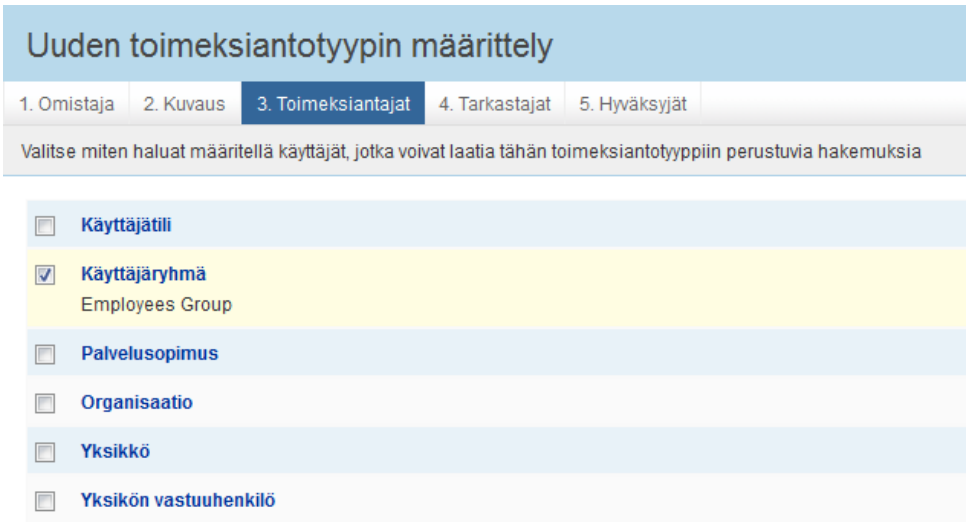
Viimeinen vaihe tässä esimerkissä on toimeksiantotyypin määrittely. Toimeksiantotyypin määrittelyä varten tulee olla luotuna palvelu, järjestelmärooli sekä tehtävä. Toimeksiantotyypin voi määritellä suoraan käyttöliittymästä IdM-järjestelmään.

Toimeksiantotyypin määrittelyn ensimmäisessä kohdassa omistajaksi valitaan Point. Tämän jälkeen kuvaukseen kirjataan toimeksiannon nimi, kuvaus sekä valitaan pystyykö toimeksiantoa hakemaan itselleen vai ei. Tässä tapauksessa työntekijä saa hakea käyttöoikeutta itselleen. Näiden lisäksi valitaan, onko automaattinen hyväksyntä käytössä, eli meneekö toimeksianto läpi ilman hyväksyntää vai ei. Tässä tilanteessa hyväksyntä vaaditaan (kuva 10).



Kuva 10. Toimeksiantotyypin määrittely: Kuvaus

Kuvauksen jälkeen valitaan, kuka pystyy toimimaan toimeksiantajana, eli kenellä on oikeus anoa tätä oikeutta. Tässä tapauksessa valitaan Käyttäjäryhmä ja sen alta Employees Group (kuva 11). Employees Group on ryhmä, joka on määritelty aiemmin Exceliin ja siihen kuuluvat kaikki Pointin työntekijät.



Kuva 11. Toimesantotyypin määrittely: Toimeksiantajat

Toimeksiantajan määrittelyn jälkeen valitaan toimeksiannon tarkastaja tai tarkastajat. Tämä tarkoittaa sitä, että kun toimeksianto on laitettu alulle toimeksiantajan toimesta, menee pyyntö sen jälkeen tässä kohdassa määritetylle tarkastajalle hyväksyttäväksi. Tässä esimerkissä, jossa on kyse työntekijän peruskäyttöoikeuden anomisesta, valitaan aiemmin luotu käyttäjäryhmä Acceptor of Common Systems (kuva 12). Tähän ryhmään kuuluvat henkilöt saavat tämän prosessin mukaisen käyttöoikeuspyynnön hyväksyttäväksi. Hyväksymispyyntö lähetetään sähköpostitse. Tarkastajan tulee aina perustella, miksi hän hyväksyy jonkun pyynnön.

Kuva 12. Toimeksiantotyypin määrittely: Tarkastajat

Tarkastajien valinnan jälkeen valitaan viimeisenä toimeksiannon hyväksyjä (kuva 13). Hyväksyjä tarkoittaa tässä tilanteessa toimeksiannon suorittajaa. Hyväksyjäksi valitaan tässä tapauksessa ja monissa muissakin tapauksissa Yksikkö ICT eli yrityksen sisäinen IT-tuki. Kun tarkastaja on ylem-

pänä hyväksynyt pyynnön, lähtee siitä IT-tuelle ilmoitus. Ilmoituksen perusteella IT-tukihenkilö kirjautuu järjestelmään ja kirjaa työn tehdyksi.

Kuva 13. Toimeksiantotyypin määrittely: 5. Hyväksyjät

Näiden kohtien jälkeen on uusi toimeksiantoprosessi määritetty. Toimeksiantotyyppiin tulee uudeksi kohdaksi välilehti Käyttövaltuudet ja tehtävät. Tähän kohtaan määritetään, mitä käyttövaltuuksia ja tehtäviä kyseessä oleva toimeksiantotyyppi koskee. Tähän kohtaan valitaan siis esimerkiksi taloushallinnon ohjelmat, toimialuetunnus tai aiemmin luotu sähköposti.

5.4 Käyttöoikeuden hakeminen

Kun kaikki tarvittavat työkalut on luotu ja määritelty, pystyy työntekijä hakemaan esimerkiksi Exchange 2010 -sähköpostitunnuksia itselleen. Mikäli hakija on perustyöntekijä, näkee hän ainoastaan itsensä toimeksiannon kohteena. Jos kyseessä olisi esimies, näkee hän itsensä sekä alaisensa listalla.

Kohteen valitsemisen jälkeen valitaan listasta toimeksiantotyyppi eli esimerkiksi yllä luotu Peruskäyttöoikeuksien anominen. Tämän jälkeen saadaan lista toimeksiantotyypin määrittelyvaiheessa määritetyistä käyttövaltuuksista ja tehtävistä. Tästä listasta valitaan aiemmin luotu sähköposti. Tätä seuraa Kuvaus-välilehti, jossa on Lisätiedot-kenttä. Aina kun tekee käyttöoikeuspyyntöä, on hakuprosessiin kirjattava perustelu, minkä takia käyttöoikeutta haetaan ja mihin sitä tarvitaan. Tämä kirjataan nimenomaan Lisätiedot-kenttään. Käyttöoikeuspyyntö on nyt valmis.

Jokainen työntekijä pystyy hakemaan käyttöoikeuksia itselleen. Riippuen käyttäjän osastosta, ovat haettavat käyttöoikeudet hieman erilaisia.

5.5 Käyttöoikeuspyynnön hyväksyminen

Käyttöoikeuspyyntö lähtee tämän jälkeen valitun järjestelmän taakse määritellylle hyväksyjälle sähköpostitse. Tässä tapauksessa hyväksyjänä oli Acceptor of Common Systems -käyttäjäryhmä. Hyväksyjä saa sähköpostin, jossa kerrotaan odottavasta pyynnöstä IdM-järjestelmässä. Kun hyväksyjä kirjautuu sisään, näkee hän tiedot, jotka pyynnön tekijä on kirjannut. Samanlainen Lisätiedot-kenttä kuin hakijalla oli, tulee näkyviin myös käyttöoikeutta hyväksyttäessä. Hyväksyjän tulee perustella hyvin jokainen hyväksymänsä pyyntö auditointeja varten.

Mikäli pyyntö jostain syystä hylätään, lähtee siitä käyttöoikeuden pyytäjälle sähköposti. Jossain tilanteissa lähtee tieto myös pyytäjän esimiehelle. Mikäli toimeksiannon tekijä on ollut kohteen esimies, lähtee tieto hylätystä päätöksestä ainoastaan esimiehelle. Myös hylkäämistapauksessa hyväksyjän on perusteltava valinta.

5.6 Käyttöoikeuspyynnön suorittaminen

Kun hyväksyjä on käynyt kuittaamassa pyynnön hyväksytyksi, lähtee siitä sähköposti yrityksessä käytössä olevaan tikettijärjestelmään IT-tuen tiketeiksi. Yrityksen sisäinen IT-tuki käsittelee tiketin, tekee tarvittavat muutokset ja käy kuittaamassa pyynnön tehdyksi ja valmiiksi IdM-järjestelmässä. Myös suoritusvaiheessa tulee IT-tuen kirjata Lisätiedot-kenttään oma kommenttinsa tehtävän suorituksesta. IT-tuki toimittaa tunnukset toimeksiannon kohteelle eli tässä tapauksessa käyttöoikeuden pyytäjälle. Näin prosessi on kokonaisuudessaan valmis.

Jälkikäteen pystyy IdM-järjestelmän pääkäyttäjät listaamaan kaikki käyttöoikeuspyynnöt, hyväksymiset sekä suoritukset. Kaikki perustelut on tarvittaessa katsottavissa. Mikäli hyväksyjänä tai suorittajana on ryhmä, tallentaa järjestelmä sen henkilön tiedot, joka on kirjautuneena järjestelmään. Näin varmistetaan se, että aina saadaan tietoon henkilö, joka on pyynnöt tosiasiassa hyväksynyt, tarkistanut ja suorittanut.

6 KÄYTTÖÖNOTTO JA TULOKSET

Ympäristön testaus aloitettiin testipuolen palvelimella. Testauksessa käytiin läpi kaikki käyttötapaukset, jotka olivat ylempänä listattuna taulukkoon 3. Kun ympäristö oli testattu toimivaksi testipuolella, siirryttiin tuotantoon. Tuotantopalvelimelle tuotiin viimeisimmät päivitetyt tiedot, jotta IdM-järjestelmä olisi ajan tasalla ja järjestelmässä olevat tiedot valideja.

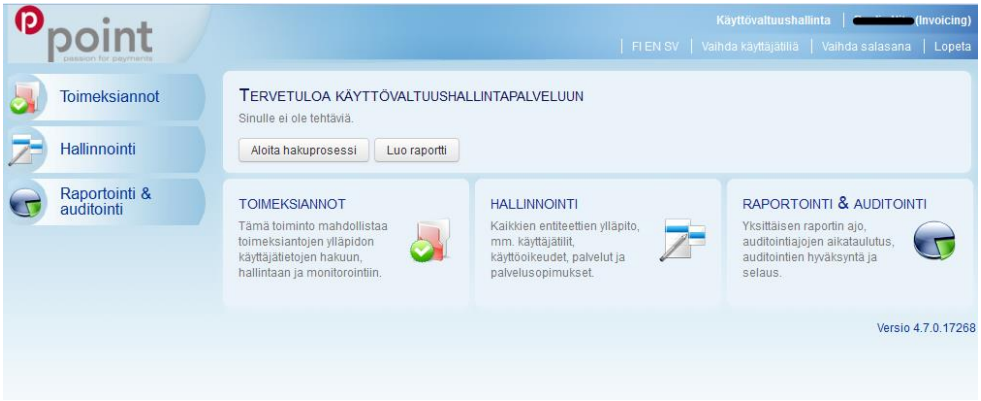
Sähköpostipalvelimen asetukset konfiguroitiin tuotantopalvelimelle tässä vaiheessa. Sähköpostiasetuksia ei konfiguroitu ollenkaan testipuolen palvelimelle. Tämä sen takia, että testauksia pystyy jatkossakin tekemään rauhassa testipuolella niin, ettei jokaisesta pyynnöstä lähde järjestelmän hyväksyjille ja suorittajille turhia sähköposteja.

Järjestelmän käyttöönotto toteutettiin askel kerrallaan. Koska tämäntyylistä järjestelmää ei ole ollut käytössä työpaikalla, vaati se työntekijöiden koulutusta ja perehdytystä järjestelmän käyttöön. HR-henkilöstölle tehtiin oma sähköpostipohja, jonka täyttämällä ja lähettämällä he voivat ilmoittaa tulevista ja lähtevistä työntekijöistä IdM-järjestelmän pääkäyttäjille. HR-henkilöstö on tärkeä kouluttaa toimimaan oikein, jotta tiedot IdM-järjestelmässä eivät vanhene. On tärkeää, että tiedot myös luovutetaan ajoissa, jotta IT-henkilöstö ehtii reagoimaan pyyntöihin muun muassa uuden työntekijän käyttöoikeuksien osalta.

Sitä mukaa kun uusia järjestelmiä otetaan työpaikalla käyttöön, on ne lisättävä myös identiteetinhallintajärjestelmään. Tämän lisäksi jokaisen työntekijän käyttöoikeudet pitää käydä tasaisin väliajoin läpi. Järjestelmästä lähtee kaksi kertaa vuodessa esimiehille lista heidän alaisistaan sekä alaisten käyttöoikeuksista. Näin esimiehet pystyvät tarkistamaan helposti, pitävätkö järjestelmässä olevat tiedot edelleen paikkansa. Mikäli tiedoissa on puutteita tai tiedot ovat virheellisiä, voi esimies kirjautua IdM-järjestelmään ja pyytää kyseessä olevalle alaiselleen muutoksia käyttöoikeuksiin. Näin saadaan kaikki pyynnöt, muutokset, poistot ja lisäykset lokitietoihin ja ne ovat tarvittaessa raportoitavissa. Lisäksi määräaikaisista työntekijöistä lähtee niin sanottu varoitusviesti esimiehelle, kun työntekijän sopimus on loppumassa. Mikäli sopimuksen loppumiseen ei reagoida, poistetaan työntekijältä käyttöoikeudet.

Huomioon tulee ottaa tällaisissa projekteissa ja järjestelmien käyttöönotoissa myös mahdollinen työntekijöiden muutosvastarinta. Kun uusi järjestelmä otetaan käyttöön, saattaa se aiheuttaa epämieluisia tuntemuksia työntekijöissä ja työntekijät saattavat kokea, että heidän työmääränsä vain lisääntyy tämän myötä. Saatetaan myös ajatella, ettei tämä järjestelmä tuo lisäarvoa työnteolle. Myös tämän takia on tärkeää, että työntekijät tietävät, miten heidän kuuluu järjestelmän kanssa toimia ja mitä kaikkea he voivat järjestelmän kautta saada. Näin saadaan minimoitua muutosvastarinnan mahdollisuus, kun järjestelmää osataan alusta lähtien käyttää oikein ja järjestelmä on mahdollisimman yksinkertainen ja looginen käyttää.

Jotta järjestelmä saatiin näyttämään Pointin järjestelmältä, muokattiin web-käyttöliittymää vielä värimaailman osalta sekä lisättiin Pointin logo vasempaan yläkulmaan. Näiden lisäksi perustyöntekijöiden näkymää rajattiin näyttämään ainoastaan tarpeelliset linkit ja heidän tarvitsemansa osiot. Ainoastaan järjestelmän pääkäyttäjillä on näkymä, jossa on kaikki mahdollinen näkyvissä aina provisiointiasetuksista konfigurointityökaluihin. Alla olevassa kuvassa 14 näkyy peruskäyttäjän näkymä. Pääkäyttäjän näkymä näkyi ylempänä kuvassa 1.



Kuva 14. Peruskäyttäjän näkymä

Näkymästä on rajattu pois kaikki, mikä ei peruskäyttäjälle kuulu. Peruskäyttäjä pystyy näkemään omat toimeksiantopyyntönsä sekä omat tietonsa. Näiden lisäksi peruskäyttäjä pystyy halutessaan tekemään raportin omista oikeuksistaan.

Mikäli järjestelmän käyttäjä on esimies, pystyy hän näkemään omien pyyntöjensä ja tietojensa lisäksi myös alaistensa tiedot. Omia tietojaan pystyy muokkaamaan kaikki käyttäjät. Toimeksiantopyynnöt on rajoitettu niin, että käyttäjä pystyy hakemaan vain hänen osastonsa mukaan määriteltyjä mahdollisia käyttöoikeuksia. Laajemmat käyttöoikeudet voi hakea esimies. Pääkäyttäjätasoisia käyttöoikeuksia pystyvät hakemaan ainoastaan yrityksen IT-asiantuntijat sekä IdM-järjestelmän pääkäyttäjät. Näin vältytään siltä, että työntekijä ei hae sellaisia oikeuksia, jotka eivät tämän työnkuvaan kuulu.

7 YHTEENVETO

Identiteetinhallintajärjestelmää suunniteltaessa tulee ottaa huomioon useita asioita. Tulee pohtia, käytetäänkö avoimeen lähdekoodiin pohjautuvia järjestelmiä vai kaupallisia maksullisia järjestelmiä. Molemmissa on omat hyvät ja huonot puolensa ja valintaan vaikuttaa suuresti kyseessä olevan yrityksen tarpeet ja toiveet järjestelmän toiminnallisuuden suhteen.

Tässä opinnäytetyössä esiteltiin muutamia vaihtoehtoja identiteetinhallintaan. Lisäksi käytiin kokonaisvaltaisesti läpi prosessi, joka suoritetaan identiteetinhallintajärjestelmää käyttöönotettaessa.

Opinnäytetyössä saavutettiin asetetut tavoitteet ja tuotos oli sen mukainen, mikä projektisuunnitelmassa oli määritelty. Työn tuloksena saatiin yritykselle räätälöity identiteetinhallintajärjestelmä. Järjestelmä täyttää nyt yrityksen tiukat raportointi- ja auditointitarpeet, jotka PCI DSS on yritykselle asettanut.

Opinnäytetyön tuotoksena saatua identiteetinhallintajärjestelmää voisi kehittää vielä pidemmälle integroimalla siihen eri järjestelmiä. Muun muassa AD-integraatio voisi olla seuraava askel järjestelmän kehittämisessä. Näin uudet työntekijät siirtyisivät suoraan AD:seen ja manuaalista työtä saatai-

siin vähennettyä. Monet yrityksen käytössä olevista järjestelmistä on itse kehitettyjä ja ohjelmoituja, joten myös niihin integroituminen ei pitäisi olla kovinkaan haastavaa.

Työtä tehdessä oppi sen, että projektit eivät aina etene niin kuin alun perin oli suunniteltu. Koska sidosryhmiä ja toimijoita oli useita, vaati se enemmän työtä projektinhallinnassa sekä tapaamisten järjestämisessä. Myös aikataulusta jouduttiin joustamaan sairaslomien, talvilomien sekä äkillisen resurssipulan vuoksi.

Kaiken kaikkeaan projekti sujui kuitenkin hyvin ja lopputulos oli odotetun kaltainen. IdM-järjestelmä korvasi vanhanaikaisen paperiversion ja yrityksen identiteetinhallinta on nyt täysin PCI-vaatimusten mukainen.

LÄHTEET

Efecte Oy. 2013. Efecte ostaa RM5 Software Oy:n. Viitattu 01.04.2013. Saatavilla: http://www.efecte.com/about-efecte/news/news/efecte-oy-to-purchase-rm5-software-oy

Evolveum. 2011. MidPoint. Viitattu 14.3.2013. Saatavilla: http://evolveum.com/midpoint.php

Finanssivalvonta. 2012. Maksupalvelun tarjoajat. Viitattu 20.1.2013. Saatavilla: http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Palveluntarjoajat/Maksupalvelu/Pages/Default.aspx

Luottokunta Oy. n.d. PCI. Viitattu 21.1.2013. Saatavilla: http://www.luottokunta.fi/Luottokunta/Toimialatietoa/PCI/

Luottokunta Oy. 2010. PCI DSS 2.0 – Vaatimukset ja turvallisuuden arviointimenetelmät. Viitattu 23.1.2013. Saatavilla: http://www.luottokunta.fi/Global/Liitteet/Luottokunta/PCI/PCI%20DSS%20v2.0_FI.pdf

nLight. 2009. Open Source Identity Management Systems. Viitattu 2.2.2013. Saatavilla: http://www.nlight.eu/documents/open-source-idm/

PCI Security Standards Council. 2010. PCI Data Security Standard V2.0. Viitattu 27.1.2013. Saatavilla: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

PCI Security Standards Council. 2010. PCI DSS Quick Reference Guide. Viitattu 27.1.2013. Saatavilla: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

Pertti Hämäläinen. 2009. Turvallisen korttimaksun teoria ja käytäntö. Viitattu 27.1.2013. Saatavilla: http://www.tietokone.fi/lehti/tietokone_1_2009/turvallisen_korttimaksun_teoria_ja_kaytanto_513

Tirasa Apache Syncope. n.d. The Origin. Viitattu 5.3.2013. Saatavilla: http://syncope.tirasa.net/site/syncope/live/hctsite_en/common/apache.htm