

Opinnäytetyö (AMK)

Tietojenkäsittely

Tietojärjestelmät

2013

Aapo Sillanpää

SAP NETWEAVER IDENTITY MANAGEMENT – OHJELMISTON EVALUOINTI

– Case: HK Ruokatalo



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojenkäsittely | Tietojärjestelmät

Syyskuu 2013 | 54 sivua

Ohjaaja: Tuomo Helo

Aapo Sillanpää

SAP NETWEAVER IDENTITY MANAGEMENT- OHJELMISTON EVALUOINTI

– Case: HK Ruokatalo

Opinnäytetyö on tehty toimeksiantona HK Ruokatalolle, joka on kiinnostunut kartoittamaan SAP-toiminnanohjausjärjestelmän käyttäjähallintaratkaisuja. Työssä tutkitaan SAP NetWeaver Identity Management -ratkaisua.

Opinnäytetyön tavoitteena on selvittää SAP NetWeaver Identity Management -ratkaisun mahdollisia hyötyjä sekä arvioida sen sopivuutta yritykselle. Työn yhtenä tavoitteena on myös perehtyä Single Sign-On -menetelmään.

Opinnäytetyö kartoittaa SAP Identity Management -ratkaisun ominaisuuksia. Työssä vertaillaan myös Identity Management -ratkaisua SAP CUA -käyttäjähallintaratkaisuun. Vertailun avulla pyritään selvittämään ratkaisujen eroavaisuudet. Opinnäytetyössä verrataan SAP NetWeaver Identity Management -ratkaisun ominaisuuksia yrityksen SAP-käyttäjähallinnalle asetettuihin vaatimuksiin, näin voidaan tarkastella ratkaisun soveltuvuutta yrityksen tarpeisiin.

Työn teoriaosuus koostuu käyttäjähallinnan, vaatimusmäärittelyn ja ohjelmistojen käyttöönoton ja vertailuperiaatteiden teoriasta.

Opinnäytetyön empiirinen osa koostuu kohde yrityksen vaatimusten keräämisestä, käyttäjähallintaratkaisujen vertailusta ja NetWeaver Identity Management -ratkaisun soveltuvuuden tutkimisesta.

Työn tuloksina syntyi suositus, josta selviää onko NetWeaver Identity Management -ratkaisu sopiva yrityksen ympäristöön. Lisäksi tuloksista havaitaan sen mahdolliset hyödyt. Tuloksena syntyi myös selvitys siitä miten NetWeaver Identity Management -ratkaisu ja miten yrityksen nykyinen käyttäjähallintaratkaisu eroavat toisistaan.

ASIASANAT: SAP, ERP, käyttäjähallinta, käyttäjäroolit, vaatimusmäärittely, ohjelmiston käyttöönotto

Aapo Sillanpää

EVALUATING – SAP NETWEAVER IDENTITY MANAGEMENT SOFTWARE

– Case: HK Ruokatalo

This Bachelor's thesis is an assignment from HK Ruokatalo. Target corporation is interested in identifying SAP – ERP user management solutions. This thesis focuses on studying SAP NetWeaver Identity Management solution that is especially designed for user management in SAP environments.

The aims of this thesis are to determine possible benefits of SAP NetWeaver Identity Management software and to evaluate the suitability of NetWeaver Identity Management to target corporation. One aim is also to familiarize with Single Sign-on method.

The thesis lists the benefits and features of SAP NetWeaver Identity Management software. The thesis also compares the NetWeaver Identity Management software with corporation's current identity management solution. Based on the comparison the differences between the two solutions can be identified. This thesis also compares the NetWeaver Identity Management software features with corporation's SAP user management requirements. Through this comparison the suitability of the NetWeaver Identity Management software to corporation can be assessed.

The theoretical part of the thesis consists of the theory of user management, requirements analysis and software deployment. The theoretical part also includes the theory of software comparison.

The empirical part of the thesis consists of specifying corporation's SAP user management requirements. The empirical part also consists of comparison of the identity management softwares and evaluating the suitability of the NetWeaver Identity Management software to corporation.

The result of this thesis is a recommendation to to corporation, which identifies the suitability of NetWeaver Identity Management software for corporation's SAP – environment. Another result is to state the differences between corporation's current identity management solution and the NetWeaver Identity Management software.

KEYWORDS: SAP, ERP, identity management, user roles, requirement specification, software implementation

SISÄLTÖ

KÄYTETYT LYHENTEET	6
1 JOHDANTO	8
2 HK RUOKATALO OY JA SAP (SALATTU OSIN)	10
3 OHJELMISTON KÄYTTÖÖNOTON LÄHTÖKOHDAT JA VAIHEISTUS	13
3.1 Käyttöönottoprosessi	13
3.2 Käyttöönottomallit	14
4 VAATIMUSMÄÄRITTELY (SALATTU OSIN)	15
4.1 HK Ruokatalon SAP-ympäristön käyttäjähallintaprosessin kulku (SALATTU)	16
4.2 HK Ruokatalon käyttäjienhallinnan vaatimukset SAP-ympäristössä (SALATTU)	16
5 OHJELMISTOJEN VERTAILUPERIAATTEET	16
6 KÄYTTÄJIEN HALLINTA	20
6.1 Keskitetty käyttäjien hallinta	21
6.2 Käyttäjien todentaminen	22
6.3 Käyttäjäroolien hallinta	23
7 SAP CENTRAL USER ADMINISTRATION	25
8 SAP NETWEAVER IDENTITY MANAGEMENT	31
8.1 Arkkitehtuuri	32
8.2 Ominaisuudet	36
8.3 Single sign-on (SSO)	37
8.4 The Security Assertion Markup Language (SAML)	38
9 OHJELMISTOJEN VERTAILU	39
10 JOHTOPÄÄTÖKSET (SALATTU OSIN)	42
10.1 SAP NetWeaver Identity Managementin hyödyt	42
10.2 Suosituksia HK Ruokatalolle (SALATTU)	43
LÄHTEET	44

LIITTEET

Liite 1. SAP-asiantuntijan haastattelu Espoossa 19.3.2012

Liite 2. Haastattelu HK Ruokatalon SAP-käyttöoikeuksista vastaavan henkilön kanssa
25.10.2012

KUVAT

Kuva 1. SAP Maintain User näkymä.....	26
Kuva 2. Loppukäyttäjän roolit.....	26

KUVIOT (SALATTU OSIN)

Kuvio 3. SAP:n autorisointikonsepti.....	30
Kuvio 4. SAP NetWeaver Identity Management arkkitehtuuri.....	33
Kuvio 5. Identity Centerin komponentit.....	34

TAULUKOT

Taulukko 1. SAP käyttäjähallintasovellusten vertailu.....	41
---	----

KÄYTETYT LYHENTEET

ABAP	Advanced Business Application Programming. Korkean tason ohjelmointikieli, jonka on kehittänyt SAP (Searchsap 2010).
CUA	Central User Administration, keskitetty käyttäjien hallinta (Help SAP 2012).
ERP	Enterprise Resource Planning, tietojärjestelmä, joka integroi yrityksen toimintoja yhteen järjestelmään.
Horeca	Hotel, Restaurant, Cafe. Elintarvikekaupan suuriasiakasryhmä. Siihen sisältyy ravintoloita, hotelleja sekä muita ruokapalveluyrityksiä (Kesko 2011).
IDM	Identity Management yksittäisten identiteettien hallinta tietojärjestelmän sisällä tai tietojärjestelmärajojen yli (Linkies & Host 2010, 169-170).
J2EE	Java 2 Platform, Enterprise Edition. Ohjelmistokehitysalusta Java-sovellusten kehittämiseen ja suorittamiseen (IBM 2013).
LDAP	Lightweight Directory Access Protocol. Protokolla, jonka avulla käytetään hakemistopalveluja. Sen yleisimpiä käyttötarkoituksia on käyttöoikeuksien tarkistus ja käyttäjätunnistus (Gracion 2008).
NW	NetWeaver SAP:n teknologia-alusta sovellusten käyttöönottoon (SAP 2011f).
PPS	Procurement for Public Sector. Julkishallinnon ostotarpeisiin räätälöity SAP moduuli (Help SAP 2011).
SAML	Security Assertion Markup Language ulkopuolinen auktorisointia kontrolloiva teknologia (Wun-Young ym. 2008, 70).
SAP	SAP AG, saksalainen ohjelmistoyritys, joka on erikoistunut toiminnanohjausjärjestelmien ja niiden tukituotteiden kehittämiseen (SAP 2011f).
SCM	Supply Chain Management osa SAP Business Suitea. Se on toimitusketjujen hallintaan tarkoitettu ohjelmisto (SAP 2011g).
SSL	Secure Sockets Layer tietoliikenneverkoissa käytetty salausprotokolla (Wun-Young ym. 2008, 33).

SSO

Single Sign-On auktorisointitekniikka, joka yhdistää yhden käyttäjätunnuksen ja salasanan alle monia tietojärjestelmiä (Wun-Young ym. 2008, 34-35).

1 JOHDANTO

SAP-toiminnanohjausjärjestelmä on laaja ja monimutkainen ohjelmisto, jolle on tarjolla monia erilaisia käyttäjienhallintaratkaisuja. Opinnäytetyöni päätavoite on vertailla ja arvioida yrityksen SAP -toiminnanohjausjärjestelmän nykyistä CUA-käyttäjienhallintaratkaisua, uuteen SAP:n tarjoamaan SAP NetWeaver Identity Management -käyttäjienhallintaratkaisuun. Tavoitteen saavuttamiseksi työssä selvitetään ensiksi nykyisen järjestelmän ominaisuudet, minkä jälkeen niitä verrataan SAP NW IDM -järjestelmän vastaaviin ominaisuuksiin. Työssäni kartoitan myös yrityksen käyttäjien hallinnan vaatimuksia ja niiden perusteella selvitan miten NW IDM sopisi kohde yritykselle. Opinnäytetyössäni kartoitan SAP NetWeaver Identity Management-ohjelmiston hyötyjä ja haittoja yrityksille. Opinnäytetyössäni tutkin SSO- ja SAML- tekniikoita käyttäjien hallinnassa. Edellä mainittujen kartoitusten ja määrittelyjen perusteella voidaan ruveta mahdollisesti tulevaisuudessa valmistelemaan uuden käyttäjienhallintasovelluksen käyttöönottoa.

SAP NetWeaver Identity Management -ohjelmisto on uusi kokonaisvaltainen käyttäjienhallintasovellus, jolla voidaan korvata SAP:n vanhat käyttäjienhallintamekanismit kuten CUA. SAP:n Central User Administration on ainoastaan ABAP-pohjaisten järjestelmien käyttäjien hallintaan suunniteltu ratkaisu. (Gergen ym. 2010, 70.)

Työssäni olen käyttänyt hyväkseni monia tutkimusmenetelmiä. Pääasiallisina tutkimusmenetelminäni ovat olleet kirjallisuuskatsaus ja asiantuntijoiden haastattelut. Kirjallisuuskatsauksen avulla selvitin, aihepiirini aikaisemmat tutkimukset ja artikkelit. Haastattelujen avulla saan tärkeää tietoa alan asiantuntijoilta. Työssäni haastattelin SAP Finland Oy:n asiantuntijaa Olli-Pekka Lindströmiä ja HK Ruokatalon asiantuntijaa Eija Sillanmäkeä. Tutkimusstrategianani toimivat kvalitatiivinen tutkimusstrategia sekä tapaustutkimus. Tapaustutkimuksen avulla tutkin rajattua kokonaisuutta, käyttämällä monipuolisia ja eri menetelmillä hankittuja tietoja. Kvalitatiivisen

tutkimusstrategian avulla pyrin ymmärtämään tutkimuskohteen laatua, ominaisuuksia sekä sen merkitystä kokonaisvaltaisesti. Työtäni varten sain käyttööni HK Ruokatalon sisäisiä Power Point -esityksiä Tuomo Suonkoskelta ja Ritva Vierulalta.

Motivaationani opinnäytetyöni tekemiseen toimi tieto, että työn edetessä kartutan taitojani SAP-toiminnanohjausjärjestelmästä. SAP-taitoja arvostetaan työelämässä todella paljon, joten päätin ottaa vastaan opinnäytetyön aiheen liittyen SAP:n käyttäjien hallintaan ja tietoturvaan.

2 HK RUOKATALO OY JA SAP (SALATTU OSIN)

HKScan Oyj on Pohjois-Euroopan suurimpia ruoka-alan yrityksiä. Yhtiön kotimarkkina-alue muodostuu Suomesta, Ruotsista, Tanskasta, Baltian maista ja Puolasta. Yhtiöllä on toimintaa yhdeksässä eri maassa ja sen palveluksessa on noin 11 000 henkilöä, joista Suomessa on noin 2 330. Konsernin pääkonttori sijaitsee Turussa. (HKScan 2013a.)

HKScan konsernin liikevaihto oli vuonna 2012 2 503,1 miljoonaa euroa. Suomen markkina-alueen liikevaihto oli vuonna 2012 842,6 miljoonaa euroa. Konsernin Suomen markkina-alueen liikevoitto oli vuonna 2012 18,4 miljoonaa euroa. (HKScan 2013b.)

HKScan Oyj syntyi nyky muodossaan vuonna 1988 LSO Osuuskunnan teollisuuden ja markkinoinnin yhtiöittämisen seurauksena. Vuonna 1997 HK Ruokatalo uudisti rakenteensa ja listautui Helsingin pörssiin. HKScan-nimi otettiin kuitenkin käyttöön vasta vuonna 2007, kun HK Ruokatalo Group osti Ruotsin suurimman liha-alan yrityksen Scan AB:n. Konsernin nimi päätettiin vaihtaa lisääntyneen kansainvälisyyden vuoksi. (HKScan 2013c.)

HK Ruokatalo Oy on HKScan Finland Oy:n kokonaisuudessaan omistama tytäryhtiö. HK Ruokatalo Oy vastaa tuotteiden valmistuksesta, markkinoinnista, logistiikasta ja kuljetuksista. HK Ruokatalon yritysarvoiksi ilmoitetaan, luottamus, vastuullisuus, osaaminen, jatkuva parantaminen ja kehittäminen, asiakastytyväisyys sekä kannattavuus. (HKScan 2013d; HKScan 2013e.)

HKScan Finland Oy:n muita tytäryhtiöitä ovat HK Agri Oy ja Järvi-Suomen Portti Oy. HK Agri vastaa sikojen, nautojen ja broilereiden hankinnasta HK Ruokatalon käyttöön. Lisäksi HKScan Finland Oy on osakkaana Kivikylän Kotipalvaamo Oy:ssä sekä Lihatukku Harri Tamminen Oy:ssä. HKScan Finland Oy vastaa HKScan-konsernin liiketoiminnasta Suomessa. (HKScan 2013c.)

HKScan valmistaa, myy ja markkinoi pääasiallisesti sian-, naudan- ja siipikarjanlihaa, lihavalmisteita ja valmiita ruokia. Pääasiallisina asiakkaina toimivat vähittäiskaupat, HoReCa-asiakkaat, teollisuus sekä vientiasiakkaat. (HKScan 2013a.)

HKScan Oy:n tunnetuimpia tuotemerkkejä Suomessa ovat HK, Kariniemen, Tamminen, Kivikylän ja Portti (HKScan 2013c).

SAP AG

SAP AG on maailman neljänneksi suurin ohjelmistovalmistaja ja maailman suurin yritysohjelmistojen valmistaja. Euroopassa SAP AG on selkeästi suurin ohjelmistovalmistaja. SAP AG:n pääkonttori sijaitsee Waldorffissa Saksassa. SAP perustettiin vuonna 1972 Mannheimissa Saksassa. Sen perustivat viisi entistä IBM:n työntekijää. (SAP 2013.)

SAP:lla on yli 176 000 asiakasta maailmanlaajuisesti. SAP työllistää yli 54 000 työntekijää. Toimipaikkoja SAP:lla on yli viidessäkymmenessä maassa ympäri maailman. (SAP 2011a.)

SAP:n ensimmäinen moduuli RF julkaistiin vuonna 1973. RF moduuli kehitettiin yrityksen kirjanpidon hallintaan. Samana vuonna aloitettiin myös monien muiden moduulien kehitystyö. Kehitetyt moduulit yhdistettiin samaan järjestelmään, josta syntyi SAP R/1. Jo vuonna 1974, kaksi ja puoli vuotta yrityksen perustamisen jälkeen, asiakasyrityksiä oli jo yli 40. Vuonna 1975 SAP lanseerasi RM-järjestelmän, jonka avulla yritykset pystyivät hallinnoimaan ostojaan, varastojaan ja laskutustaan. (SAP 2011b.)

SAP pyrki kehittämään ohjelmistoaan nopeasti eteenpäin vastaamaan yrityksien kokonaistarpeita. Niinpä se aloitti SAP R/2-järjestelmän kehityksen jo vuonna 1979. Vuonna 1981 SAP sai valmiiksi vakaan version seuraavan sukupolven järjestelmästä SAP R/2:sta. Samana vuonna SAP saavutti 200 asiakasyrityksen rajan ja laajensi tarjontaansa tuotannonohjaukseen. (SAP 2011b.)

Vuonna 1984 SAP palkkasi 48 uutta työntekijää, jolloin työntekijöiden kokonaismäärä kasvoi jo 163:een. Suurin osa uusista työntekijöistä työllistyi tuotekehitykseen. SAP alkoi kehittää uusia moduuleita kuten PPS. Vuonna 1984 SAP perusti myös uuden tytäryhtiön SAP (International) AG:n Sveitsiin. Tytäryhtiön tarkoituksena on tukea ulkomaankauppaa sekä markkinointia. (SAP 2011c.)

SAP alkoi kehittää uutta versiota toiminnanohjausjärjestelmästänsä vuonna 1989. Sen nimeksi muodostui SAP R/3. Saman vuonna SAP julkaisi käyttäjäystävällisemmän käyttöliittymän R/2 järjestelmänsä sekä uuden ABAP/4 ohjelmointiympäristön. (SAP 2011c.)

Vuonna 1991 SAP esitteli ensimmäistä kertaa uutta R/3 järjestelmänsä ulkopuolisille. Asiakkaiden suhtautuminen uuteen järjestelmään oli positiivinen. R/3-järjestelmä sisälsi lukuisia parannuksia, kuten yhtenäisen graafisen ulkoasun ja tuen relaatiotietokannoille. SAP:lla oli vuoden 1991 loppuun mennessä 14 toimipistettä ja yli 2200 asiakasta ympäri maailman. (SAP 2011d.)

Virallisesti SAP julkaisi R/3 toiminnanohjausjärjestelmänsä vuonna 1992. Vuonna 1994 SAP julkaisee R/3 järjestelmänsä Microsoft Windows NT alustalle ja aloitti yhteistyön Microsoftin kanssa. SAP järjestelmään kehitettiin etäkäyttömahdollisuus vuonna 1996. (SAP 2011d.)

SAP julkaisi vuonna 2004 uuden integraatio- ja sovelluskehitysympäristön, SAP NetWeaverin. SAP NetWeaverin avulla asiakkaat voivat integroida kolmansien osapuolien tekemiä sovelluksia omaan SAP järjestelmänsä. SAP NetWeaverin suosio ylitti kaikki SAP:n ennusteet. Vuonna 2010 SAP teki suuren luokan yritysoston. SAP osti Yhdysvaltojen suurimman mobilisaatioon keskittyvän ohjelmistoyrityksen Sybasen. Yritysoston avulla SAP pyrki vahvistamaan osaamistaan mobiiliteknologioiden saralla. Vuonna 2011 SAP julkaisi myös uuden muistiteknologiansa HANA:n. (SAP 2011e.)

3 OHJELMISTON KÄYTTÖÖNOTON LÄHTÖKOHDAT JA VAIHEISTUS

Tietojärjestelmän kehittämishanke aloitetaan esitutkimuksen laatimisella. Esitutkimuksen tarkoituksena on selvittää edellytykset hankkeen toteutumiselle. Esitutkimus-vaiheen jälkeen seuraa määrittelyvaihe, jonka tarkoituksena on selvittää, mitä toteutettavan järjestelmän tulee tehdä. Määrittely pyritään tekemään toteutusriippumattomasti analysoimalla esitutkimuksessa kerätyjä asiakasvaatimuksia. Määrittelyvaihe tuottaa toiminnallisen määrittelyn dokumentin. Määrittelyvaiheen jälkeen toteutetaan suunnittelu. Suunnitteluvaiheen tarkoituksena on muuntaa asiakkaan tarpeiden mukaan tehty toiminnallinen määrittely tekniseksi määrittelyksi, joka kuvaa tulevan järjestelmän toteutuksen. Toteutusvaiheessa ohjelma tai sen osa toteutetaan jollakin sovelluskehittimellä tai ohjelmointikielellä. Ennen ohjelmiston käyttöönottoa se testataan kattavasti, jotta mahdolliset virheet löydetään. (Paananen 2005, 344-345.)

Ohjelmiston käyttöönotto voidaan määritellä monella tavalla. Määritelmään vaikuttavat käyttöönoton näkökulma sekä lähestymistapa. Näkökulmia voivat olla muun muassa tekninen, ohjelmistotoimittajan ja loppukäyttäjän näkökulma. (Kettunen & Simons 2001, 25.)

Teknisen näkökulman kannalta tietojärjestelmän käyttöönotto tarkoittaa valitun järjestelmän implementointia, parametrisointia ja vanhojen tietojen siirtoa uuteen järjestelmään. (Kettunen & Simons 2001, 25.)

3.1 Käyttöönottoprosessi

Käyttöönottoprosessiin kuuluu suunnittelua, käyttäjien koulutusta, toimenpiteitä liittyen uuteen järjestelmään siirtymiseen sekä uuden järjestelmän seuranta. Seurannan avulla varmistutaan siitä, että uusi järjestelmä toimii oikein. (Paananen 2005, 345.)

Käyttöönottoprosessissa toteutettu ja testattu ohjelmisto otetaan käyttöön. Käyttöönottoon liittyy monia huomioitavia tekijöitä, jotka tulisi valmistella huolellisesti ennen käyttöönottoa. Tällaisia tekijöitä ovat muun muassa olemassa olevien tietojen, tiedostojen ja tietokantojen siirto uuteen järjestelmään. Käyttöönottoon kuuluu myös mahdolliset järjestelmän räätälöinnit, käyttäjien koulutukset sekä harjoituskäytöt. (Paananen 2005, 345.)

Käyttöönottovaiheen yksi keskeisimmistä tehtävistä on käyttäjien koulutus uuteen järjestelmään. Koulutuksen avulla koko organisaatio ja henkilöstö saadaan mukaan käyttöönottoon, jolloin käyttöönottoprosessin läpivieminen helpottuu. Myös ylläpitohenkilökunnan koulutus on tärkeää. (Paananen 2005, 345) Ilman koulutusta käyttäjien tuottavuus laskee huomattavasti, koska järjestelmän käytön opettelu vie aikaa. Näin ollen ohjelmistoprojektin kokonaiskustannukset kasvavat sekä järjestelmän käyttöaste pysyy matalana.

3.2 Käyttöönottomallit

Käyttöönotto voidaan toteuttaa monella eri tavalla. Yleisimmät käyttöönottomallit ovat vaiheittainen, kertasiirtymä, rinnakkainen tai pilotointi. Vaiheittaisessa käyttöönotossa siirtyminen uuteen järjestelmään toteutetaan esimerkiksi toimipisteittäin tai käyttöönotto ajastetaan (Turban ym. 2002, 638). Vaiheittaisessa käyttöönotossa järjestelmän käyttäjäoikeuksien antamista voidaan porrastaa eri käyttäjäryhmien osalta. Käyttäjäoikeuksien porrastaminen tarkoittaa käytännössä sitä, että kaikille käyttäjille ei tarvitse antaa oikeuksia järjestelmään heti. Kertasiirtymätoteutuksessa tietojärjestelmä otetaan käyttöön koko organisaatiossa samanaikaisesti. Rinnakkaisessa käyttöönotossa uutta sekä vanhaa tietojärjestelmää käytetään aluksi rinnakkain. Lopulta siirrytään käyttämään vain uutta järjestelmää, jolloin vanha järjestelmä poistetaan käytöstä. Pilotointi-käyttöönottomallissa uusi järjestelmä otetaan käyttöön ensimmäiseksi tietyssä alaryhmässä. Lopulta käyttöönotto laajennetaan koskemaan koko käyttäjäryhmää. (Turban ym. 2002, 638.)

4 VAATIMUSMÄÄRITTELY (SALATTU OSIN)

Vaatimusmäärittelyn tekeminen on tärkeä osa ohjelmistotuotantoa. Sen tarkoitus on asiakasvaatimusten muuntaminen täsmällisiksi ohjelmistovaatimuksiksi. (Haikala & Märijärvi 2004, 39.)

Vaatimusmäärittelyn tärkeimpänä tavoitteena on kerätä järjestelmälle asetetut vaatimukset mahdollisimman tarkasti. Tarkasti selvitettyjen vaatimusten perusteella eri osapuolet pystyvät keskustelemaan, millainen ohjelmiston tulee olla (JUHTA 2009, 13). Huolellisesti laaditulla vaatimusmäärittelyllä mahdollistetaan onnistunut järjestelmähankinta ja käyttöönottovaiheessa pystytään toteamaan järjestelmän ominaisuuksien vastaavan asetettuihin vaatimuksiin. (JUHTA 2009, 13.)

Vaatimusmäärittelydokumentti laaditaan yleensä heti asiakkaan vaatimusten selvittämisen jälkeen. Usein ennen vaatimusmäärittelyn tekemistä ohjelmiston toimittaja on tehnyt esitutkimuksen. (Haikala & Märijärvi 2004, 37.)

Esitutkimuksen tarkoituksena on asettaa yleiset järjestelmävaatimukset tulevalle järjestelmälle. Sen tarkoituksena on myös tuottaa tietoa tietojärjestelmän kehityksestä vastaaville henkilöille ja määrittellä lähtökohdat mahdolliselle järjestelmän hankinnalle (JUHTA 2009, 11). Esitutkimusvaiheessa toimittaja määrittelee asiakkaan tarpeet, mutta ei ota kantaa siihen, millainen järjestelmä täyttää asiakkaan vaatimukset. Yleensä esitutkimus vastaa kysymykseen, miksi ohjelmisto tai järjestelmä tulisi tehdä. (Haikala & Märijärvi 2004, 37-39.)

Esitutkimuksen laatiminen on vaiheena erityisen tärkeä, sillä vääristä asiakasvaatimuksista on vaikea päätyä toimivaan ratkaisuun. Esitutkimusvaiheen suurin ongelma on asiakkaan todellisten tarpeiden selvittäminen ja niiden perusteellinen ymmärtäminen. (Haikala & Märijärvi 2004, 37.)

Esitutkimusvaihetta seuraa määrittelyvaihe. Määrittelyvaihe jaetaan yleisesti kahteen vaiheeseen: asiakkaan vaatimusten kartoittamiseen sekä toteutettavan ohjelmiston määrittelyyn. Määrittelyvaiheessa voidaan määrittellä joko koko järjestelmä, koko ohjelmisto tai jokin ohjelmiston osa. (Haikala & Märijärvi 2004, 78-79.)

Määrittelyvaiheen tärkein tehtävä on asiakasvaatimusten analysointi. Analyysin perusteella toimittaja pystyy kartoittamaan ohjelmistovaatimukset, jotka määrittelevät tulevan järjestelmän (Haikala & Märijärvi 2004, 39, 78-79). Kartoitettujen ohjelmistovaatimusten priorisointi on tärkeää. Priorisoinnin avulla pystytään hallitsemaan järjestelmän ominaisuuksia tärkeysjärjestyksessä. Tärkeimmät vaatimukset ovat prioriteetiltaan korkealla, jotta niiden toteutus pystytään varmistamaan jo hankkeen alkuvaiheessa (JUHTA 2009, 15). Määrittelyvaiheeseen liittyy oleellisesti myös projektin tarpeellisuuden ja toteuttamiskelpoisuuden selvittäminen. Lisäksi tässä vaiheessa asetetaan projektin tavoitteet sekä vaatimukset. Projektin ratkaisumalli luodaan myös määrittelyvaiheen aikana. Määrittelyvaiheen tuloksena syntyy ainakin toiminnallinen määrittely -dokumentti. Muitakin dokumentteja voi syntyä kuten, alustava järjestelmätestaussuunnitelma, toteutusprojektin projektisuunnitelma sekä alustava käyttöohje. (Haikala & Märijärvi 2004, 39, 78-79.)

Toiminnallisessa määrittelyssä on kuvattu ohjelmiston toiminnot ja toteutukselle asetetut ei-toiminnalliset vaatimukset. Toimintojen yhteydessä määritellään ohjelmiston toteuttamat ominaisuudet, käyttöliittymä ja yhteydet muihin järjestelmiin. Ei-toiminnallisiin vaatimuksiin kuuluvat esimerkiksi vasteaika, suoritusteho ja käytettävyys. (Haikala & Märijärvi 2004, 39.)

4.1 HK Ruokatalon SAP-ympäristön käyttäjähallintaprosessin kulku
(SALATTU)

4.2 HK Ruokatalon käyttäjienhallinnan vaatimukset SAP-ympäristössä
(SALATTU)

5 OHJELMISTOJEN VERTAILUPERIAATTEET

Uutta ohjelmistoa hankittaessa vastaan voi tulla monia toimittajia ja ratkaisuja. Suurin osa ratkaisuista näyttää sisältävän samat toiminnallisuudet, mutta ne

voivat toimia hyvinkin erilaisesti. Samankaltaisten ohjelmistojen vahvuudet ja heikkoudet voivat olla myös hyvin erilaiset. (Hollander 2005, 78.)

Ohjelmistojen ja niiden komponenttien oikeanlaisen valinnan huomioiminen on todella tärkeää. Väärällä valinnalla voi olla huomattavia tuotantotaloudellisia vaikutuksia. Hankitun ohjelmiston käyttö voi myös jäädä vähäiseksi, jollei sen käyttö vastaa sille asetettuja vaatimuksia. Valinnan onnistumisen takaa oikeanlainen ohjelmiston arviointi. (Hollander 2005, 78.)

Ensimmäiseksi arvioijan tulisi tietää ohjelmistolle asetetut vaatimukset sekä tarpeet, jotka sen tulee täyttää. Arvioijan tulisi priorisoida liiketoiminnan kannalta tärkeät vaatimukset. Hänen tulisi myös arvioida, mitkä ominaisuudet tulevassa ohjelmistossa ovat pakollisia ja mitkä eivät ole. Priorisointia tehtäessä arvioijan kannattaa keskustella loppukäyttäjien kanssa ja selvittää, mitkä ominaisuudet parantaisivat heidän työskentelyään ja tuotteitaan (Pendergraft & Blakely 2010, 41). On tärkeää löytää sopiva ehdokas, jonka vahvuuksia ovat arvioijan asettamat vaatimukset ja tarpeet. (Hollander 2005, 78.)

Toisena arvioijan tulisi pystyä arvioimaan ohjelmistolle asetettujen vaatimusten kehitystä tulevaisuudessa. Kasvua tavoittelevien yritysten on erityisen tärkeää pystyä arvioimaan vaatimuksiensa kehitystä tulevaisuudessa. Oikeanlaisella vaatimusten arvioinnilla voidaan välttää kalliit ohjelmistohankinnat sekä muutostarpeet, koska vanha ohjelmisto vastaa edelleen sille asetettuihin vaatimuksiin. Valittavan ohjelmiston on siis hyvä olla skaalautuva, joustava ja konfiguroituva, jotta se pystyisi vastaamaan liiketoiminnan mahdollisesti muuttuviin vaatimuksiin. (Hollander 2005, 78.)

Uuden ohjelmiston valitsijan tai valitsijoiden on hyvä testikäyttää useampiakin ratkaisuja ennen päätöksentekoa. Testikäytöstä saatujen tuloksien perusteella pystytään varmistumaan siitä, sopiiko juuri tämä ohjelmisto yrityksen liiketoimintaan. (Hollander 2005, 78.)

Ohjelmistoja ja toimittajia vertaillessa kannattaa ohjelmiston toimittajilta kysyä asiakasreferenssejä liittyen haluttuun ratkaisuun. Julkisten asiakasreferenssien kanssa kannattaa käydä keskusteluja liittyen ohjelmistojen ja toimittajien toimintaan ja varmistaa, että sekä ohjelmistot ja toimittajat ovat luotettavia

(Hollander 2005, 78). Käytäessä keskusteluja toimittajan asiakasreferenssien kanssa, kannattaa heiltä tiedustella erinäisiä asioita liittyen ohjelmistoon ja sen toimittajaan. Heiltä ei kannata kysyä ainoastaan, miten ohjelmisto on toiminut, koska toimittaja ei julkistaisi referenssinään tyytymätöntä asiakasta. Toimittajan julkaisemilta referensseiltä kannattaa kysyä seuraavia asioita:

- Jos he ottaisivat ohjelmiston uudelleen käyttöön, mitä he tekisivät toisin?
- Pysyikö käyttöönotto aikataulussa ja budjetissa?
- Oliko käyttöönotossa ongelmia?
- Ovatko he tyytyväisiä toimittajan tarjoamaan koulutukseen?
- Ovatko he tyytyväisiä toimittajan dokumentointiin?
- Ovatko he tyytyväisiä käyttöönoton jälkeiseen ylläpitoon? (Pendergraft & Blakely 2010, 42.)

Ennen toimittajan valintaa kannattaa varmistaa, että toimittaja on tarkastellut ja ymmärtänyt ohjelmistolle asetetut vaatimukset. Ennen lopullista valintaa olisi myös suositeltavaa järjestää testitilaisuus, jossa toimittaja esittelisi, miten ohjelmisto käytännössä vastaa sille asetettuja vaatimuksia. (Pendergraft & Blakely 2010, 42.)

Tärkeätä on myös selvittää, voiko ohjelmistoa räätälöidä liiketoiminnan tarpeiden mukaan. Jos hankitaan valmis sovellus, voidaan olettaa, että jotkin sen ominaisuudet toimivat heti. Kuitenkin joitain ominaisuuksia voidaan joutua räätälöimään liiketoimintaan sopiviksi. Jos räätälöinti ei onnistu tai se vie todella paljon aikaa, resursseja tai on investointina todella suuri verrattuna hyötyihin, kannattaa ratkaisusta luopua. (Hollander 2005, 78.)

Yhtäaikaisten käyttäjien määrän selvittäminen on myös tärkeää. Ohjelmiston arvioijien tulee selvittää, kuinka monta käyttäjää tulee käyttämään ohjelmistoa samanaikaisesti ja miten se vaikuttaa ratkaisun suorituskykyyn. Ohjelmiston hankkijan tulee ottaa myös selvää, missä ohjelmistossa olevia yrityksen tietoja säilytetään. (Hollander 2005, 78.)

Ratkaisun tulevaisuuden näkymät kannattaa selvittää. Onko toimittaja panostamassa ratkaisun kehitykseen tulevaisuudessa? Tärkeiden

ohjelmistopäivitysten saanti tietyin väliajoin takaa ohjelmiston toimivuuden ja tietoturvallisuuden. Ohjelmistopäivitysten hinnoittelu on myös tärkeä asia vertailtaessa eri ratkaisuja toisiinsa. (Hollander 2005, 78.)

Piilokustannusten selvittäminen on tärkeässä roolissa liittyen ohjelmistojen vertailuun. Ratkaisujen kustannukset saattavat erota toisistaan huomattavasti, mutta piilokustannusten selvittämisen jälkeen kustannukset saattavat olla hyvinkin lähellä toisiaan. Suurimmat kustannuserät ovat käyttäjäkoulutus ja migraatio vanhasta ohjelmistosta uuteen. Yritys voi joutua ostamaan myös uusia laitteistoja, jotka tukevat uutta ohjelmistoa (Hollander, H. 2005, 78). Ohjelmiston kokonaiskustannuksiin pitkällä aikavälillä vaikuttavat myös toimittajan julkaisemat ohjelmistopäivitykset ja niiden implementointi. (Pendergraft & Blakely 2010, 40.)

6 KÄYTTÄJIEN HALLINTA

Organisaatioiden heterogeenisten it-ympäristöjen käyttäjien hallinta on haasteellista. Ohjelmistoympäristöt monimutkaistuvat koko ajan, sekä käyttäjien vastuut ja työtehtävät voivat muuttua nopeasti. Yritysten tulee seurata järjestelmiään tarkasti, jotta tiedetään kuka käyttää mitäkin sovellusta ja mihin aikaan. (SAP AG 2011a.)

Monissa yrityksissä käyttäjentunnistusprosessi aloitetaan pääsynhallintalomakkeella tai -hakemuksella. Kaikki pääsynhallintalomakkeet ja -hakemukset hyväksytetään esimiehellä, jolloin varmistetaan, että hakemus on paikkansapitävä. Jos hakemus hylätään, se palautetaan hakijalle kommentoituna. Kun hakemus on korjattu, niin hakijalle myönnetään oikeudet hakemiinsa toimintoihin (Wun-Young ym. 2008, 40). Työntekijälle myönnetään ainoastaan työn suorittamiseen tarvittavat oikeudet. Jos oikeuksia myönnetään liikaa, voi työntekijällä olla pääsy tietoihin tai järjestelmiin, joihin hänen ei kuuluisi päästä. Jos taas oikeuksia myönnetään liian vähän, ei työntekijä voi suorittaa työtehtäviään. Oikeuksien myöntämisen jälkeen hakijalle ilmoitetaan, että hakemus on hyväksytty ja hän on saanut pääsyn toimintoihin. (Wun-Young ym. 2008, 40.)

Kun työntekijän työsuhde päättyy, saa tietoturvahenkilöstö siitä ilmoituksen. Ilmoituksen saatuaan tietoturvahenkilöstön tulisi lukita vanhan työntekijän käyttäjätunnus, vaihtaa käyttäjän lisenssityyppiä ja asettaa sisäänkirjautumiselle jokin asiallinen takaraja. (Wun-Young ym. 2008, 40.)

Käyttäjäoikeuksien luomisprosessi voi kestää jopa viikkoja, koska se vaatii koordinoitua ja yhteistoimintaa yrityksen eri osastojen välillä. Tällainen monimutkainen prosessi voi aiheuttaa yritykselle turhia kuluja, koska uusi työntekijä ei voi suorittaa työtehtäviään ilman asianmukaisia oikeuksia tarpeellisiin järjestelmiin. (Wun-Young ym. 2008, 41.)

Tehokkaan käyttäjienhallinnan tulisi nopeuttaa käyttäjäoikeuksien muuttamista, jos työntekijä ylennetään tai hän lähtee organisaatiosta. Käyttäjäoikeuksien luonnin nopeuttamisella ja prosessia yksinkertaistamalla yhteydenotot

helpdeskiin vähenevät ja työntekijöiden tuottavuus paranee. Näin ollen yritys säästää kustannuksissa. (Wun-Young ym. 2008, 41.)

Monilla yrityksen henkilöillä on käyttöoikeuksia useisiin eri järjestelmiin. Jokaisen järjestelmän käyttäjätunnuksen ja salasanan muistaminen on hankalaa. Niinpä monet työntekijät ovat valinneet tunnuksikseen mahdollisimman yksinkertaisia sanoja tai lauseita. Yleisesti he myös käyttävät samoja tunnuksia useissa järjestelmissä. Jotkut käyttäjät myös kirjoittavat muistiin omat tunnuksensa, jotta he muistaisivat ne. Tällainen toimintamalli sisältää lukuisia riskejä. Tunnukset voidaan varastaa, jolloin ulkopuolisella henkilöllä voi olla pääsy kaikkiin yrityksen tietojärjestelmiin.

Useat eri järjestelmät ja niiden vaatimat autentikointitiedot vaativat ohjelmistojen ylläpitäjiltä huomattavia resursseja. Jokaisella järjestelmällä on tietyt autentikointiprotokollat, salasanat, käyttäjätunnukset sekä muut tunnistusmenetelmät. Näiden tietojen hallinta ohjelmistokohtaisesti on todella hankalaa. Autentikointitietojen hallinta helpottuu huomattavasti keskittämällä käyttäjien hallinta.

6.1 Keskitetty käyttäjien hallinta

Nykyajan yritysympäristöissä käyttäjien hallinnan tulee pystyä hallitsemaan yksittäisten henkilöiden käyttöoikeuksia läpi erilaisten järjestelmäympäristöjen. Helpoin tapa tämän tyypiseen käyttäjähallintaan on integroida käyttäjien hallinta vain yhteen järjestelmään. (Wun-Young ym. 2008, 41.)

Käyttäjien hallinnan integrointi tarkoittaa käyttäjätietojen ja auktorisointitietojen yhdistämistä monista järjestelmistä, keskitettyyn tietovarastoon. Kaikki käyttäjien hallintaan liittyvä tieto ylläpidetään vain yhdessä keskitetyssä järjestelmässä, jonka kanssa muiden järjestelmien tulee synkronoitua, jotta ne saavat tarvittavat oikeudet käyttäjille. Tämä tarkoittaa sitä, että jos käyttäjän käyttöoikeudet kytketään pois hallintajärjestelmästä, niin ohjelmisto kytkee ne pois kaikista järjestelmistä. Keskitetyllä käyttäjienhallinnalla saavutetaan hyötyjä. Tietojen ylläpidettävyys helpottuu, päällekkäisten tietojen määrä vähenee, ylläpidon kulut vähenevät, läpinäkyvyys paranee sekä tietoturva kasvaa. (Wun-Young ym. 2008, 41.)

6.2 Käyttäjien todentaminen

Yrityksen tietojärjestelmäarkkitehtuuriin saattaa kuulua monia tietojärjestelmiä. Järjestelmät voivat poiketa toisistaan hyvinkin paljon. Kuitenkin kaikkien järjestelmien tulee todentaa sitä käyttävät henkilöt. Todennuksen avulla voidaan määrittää käyttäjän oikeudet sekä varmistaa, että henkilö on yrityksen palveluksessa.

Käyttäjien todentamisprosessin tarkoituksena on pyrkiä varmistamaan käyttäjien, ohjelmien, ja palveluiden identiteetit. Vain todentamisprosessin läpäisseet ohjelmat, käyttäjät ja palvelut, saavat käyttöoikeuden tietojärjestelmiin. Käyttäjien todentaminen on tärkeää, koska sillä varmennetaan käyttäjän identiteettiä. Todentaminen on tärkeää myös, koska tietoturvaohauhat kuten virukset, madot ja identiteettivarkaudet ovat lisääntyneet. Näiden uhkien toteutuessa yrityksen tuottavuus voi kärsiä ylimääräisten virustarkistusten ja tietoturvapäivitysten asennuksen takia. (Wun-Young ym. 2008, 31-32.)

Kaikki SAP NetWeaver -tuotteet tukevat oletuksena käyttäjätunnuksella ja salasanalla toteutettua autentikointia. Salasana ja käyttäjätunnus eivät aina riitä estämään tietoturvahyökkäyksiä. Tietoturvaa voidaan parantaa ottamalla käyttöön ulkoisia autentikointiratkaisuja. Ulkoiset ratkaisut parantavat tietoturvaa, koska ne tukevat tietojen salausta ja niille on voitu myöntää viranomaisien hyväksymä sertifikaatti. (Wun-Young ym. 2008, 32.)

Biometriset tunnistet

Viime vuosien aikana biometriset tunnistusmenetelmät ovat kehittyneet nopeasti ja niiden soveltaminen on myös yleistynyt. Biometrisiä tunnistetietoja käytetään usein automatisoidun todentamis- ja tunnistamismenettelyn yhteydessä. Erityisen usein biometrisiä tunnistetietoja käytetään valvottaessa pääsyä sekä fyysisille että virtuaalisille alueille. Fyysisillä ja virtuaalisilla alueille tarkoitetaan usein sähköisiä järjestelmiä ja palveluita. Ennen biotunnisteiden käyttö rajoittui selkeästi DNA:n ja sormenjälkien osa-alueille. (Tietosuojatyöryhmä 2003, 2.)

Biometriset järjestelmät koostuvat biometrinen tekniikoiden sovelluksista. Ne mahdollistavat henkilöiden automatisoidun tunnistamisen ja hänen henkilöllisyytensä todentamisen. (Tietosuojatyöryhmä 2003, 3.)

Biometriset tekniikat voidaan jakaa kahteen pääryhmään, fysiologisiin ja käyttäytymiseen perustuviin tekniikoihin. Fysiologisilla tekniikoilla mitataan henkilön fysiologisia ominaisuuksia. Käyttäytymiseen perustuvilla tekniikoilla analysoidaan henkilön käyttäytymistä. (Tietosuojatyöryhmä 2003, 3.)

Fysiologisiin tekniikoihin kuuluvat muun muassa sormenjälkien tunnistaminen, sormen kuvan analysointi, iiriksen tunnistaminen, verkkokalvon tunnistus, kasvojen tunnistus, kehon hajun tunnistus ja henkilön äänen analysointi. (Tietosuojatyöryhmä 2003, 3.)

Käyttäytymiseen perustuvia tekniikoita ovat muun muassa kirjoitetun allekirjoituksen todentaminen, henkilön liikkeiden analysointi ja näppäinkosketuksen tunnistaminen. (Tietosuojatyöryhmä 2003, 3.)

Biometrinen tunnistaminen avulla pystytään kontrolloimaan luotettavasti pääsynvalvontaa organisaation eri osa-alueilla. Yleisin käyttökohde on varmastikin rakennusten pääsynvalvonta, mutta biometrisiä tekniikoita voidaan soveltaa myös tietojärjestelmien käyttäjien tunnistamisessa. Osassa kannettavista tietokoneista on jo melko kauan ollut mahdollisuus sormenjälkitunnistukseen.

6.3 Käyttäjäroolien hallinta

Käyttäjäroolit ovat määriteltyjä luokkia, joita voidaan asettaa käyttäjille heidän työtehtäviinsä tai muihin kriteereihin perustuen. Roolit rakennetaan käyttöoikeuskokonaisuuksista, eri roolit sisältävät erilaisia käyttöoikeuksia. Roolien ympärille rakennetaan organisaation järjestelmien kulunvalvonta. Roolia käytetään yleisimmin esittämään mukautettuja versioita käyttöliittymistä tai näkymistä, erilaisiin käyttäjätyppeihin perustuen. Samaa käyttäjäroolia voidaan jakaa monelle samaa työtehtävää suorittavalle käyttäjälle. (Microsoft 2013a.)

Käyttäjäroolien hallinnassa on tärkeää, että käyttöoikeudet ovat liitetty rooleihin, joita asetetaan loppukäyttäjille asianmukaisella tavalla. Roolitus helpottaa sekä yksinkertaistaa käyttöoikeuksien hallintaa. Organisaation sisällä erilaisille työtehtäville on luotu erilaiset roolit. Loppukäyttäjille asetetaan asianmukaiset roolit heidän vastualueisiinsa ja pätevyksiinsä perustuen. Loppukäyttäjälle annettu rooli pystytään helposti vaihtamaan toiseen. (Microsoft 2013a.)

Rooleihin pystytään luomaan uusia käyttöoikeuksia tarvittaessa, esimerkiksi kun organisaatio ottaa käyttöön uuden tietojärjestelmän. Rooleista pystytään myös poistamaan käyttöoikeuksia tarvittaessa.

7 SAP CENTRAL USER ADMINISTRATION

SAP Central User Administration-ohjelmisto kehitettiin vain ABAP-pohjaisten sovellusten hallintaan. Sen päätehtävänä on luoda ja jakaa kaikki käyttäjätilit, käyttäjäroolit ja profiilit keskitetysti yhdestä ABAP-pohjaisesta järjestelmästä. (Gergen ym. 2010, 70.)

Kuten kuvasta 1 nähdään, SAP CUA:n Maintain User toiminto saadaan käynnistettyä SU01-transaktiolla. Toiminnon käynnistyttyä avautuu käyttäjien perustiedot sekä useita välilehtiä, joiden kautta voidaan hallita käyttäjien tietoja. Maintain User -toiminto näyttää käyttäjälle, kuka on viimeksi muokannut kyseistä käyttäjäroolia ja koska muokkaus on tehty. Toiminto ilmoittaa myös roolin tilanteen Status-kohdassa, joka on tässä tapauksessa Saved. SAP CUA:n Address välilehden kautta pystytään tarkastelemaan käyttäjälle määritettyjä yleisiä tietoja. Tarkasteltavia tietoja ovat muun muassa käyttäjän nimi, osasto ja työhuoneen numero. Roles-välilehden kautta pystytään määrittämään käyttäjälle hänen käyttäjäroolinsa ja profiilinsa.

The screenshot shows the SAP Maintain User interface. At the top, there is a menu bar with 'Users', 'Edit', 'Goto', 'Information', 'Environment', 'System', and 'Help'. Below the menu bar is a toolbar with various icons. The main area is titled 'Maintain User' and displays the following information:

User	GANTER			Status	Saved
Last Changed On	TOEWEU	06.03.2009	19:25:34		

Below this information are several tabs: Address, Logon data, SNC, Defaults, Parameters, Roles, Profiles, and Gr... The 'Person' section contains the following fields:

Title	Ms.				
Last name	Bathelt				
First name	Sabine				
Academic Title					
Format	Sabine Bathelt				
Function	Trainer				
Department	Schulung, SAP LGD				
Room Number	D3.37	Floor	3	Building	WDF02

The 'Communication' section contains the following fields:

Language		Other communication...			
Telephone		Extension			
Mobile Phone					
Fax		Extension			
E-Mail					
Comm. Meth					

Below the communication section are two buttons: 'Assign other company address...' and 'Assign new company address...'. The 'Company' section contains the following text:

SAP AG / Neurottstr. 16 / D-69190 Walldorf

Kuva 1. SAP Maintain User -näkyvä.

Käyttäjärooleja pystytään hallinnoimaan käyttäjäkohtaisesti CUA:n avulla, Roles välilehdeltä (kuva 2). Roolit voidaan myöntää käyttäjälle vain tietyksi ajaksi, Valid From ja Valid To -toimintojen avulla. CUA:lla nähdään käyttäjälle myönnettyjen roolien tilanne, Status-sarakkeesta. Roolien tilannetta kuvataan erivärisillä indikaattoreilla, kuvassa vihreällä. CUA:lla nähdään myös roolin tyyppi Type-sarakkeesta eli onko käyttäjälle myönnetty rooli yksittäinen vai yhdistelmä eri rooleista. Rooleja kuvaavat nimet näkyvät Name-kohdassa.

The screenshot shows the SAP 'Maintain User' interface. At the top, there is a menu bar with 'Users', 'Edit', 'Goto', 'Information', 'Environment', 'System', and 'Help'. Below the menu bar is a toolbar with various icons. The main area is titled 'Maintain User' and contains a form for user details. The 'User' field is set to 'GANTER'. The 'Last Changed On' field shows 'TOEWEU' on '06.03.2009' at '19:25:34'. The 'Status' is 'Saved'. Below the form are several tabs: 'Address', 'Logon data', 'SNC', 'Defaults', 'Parameters', 'Roles', 'Profiles', and 'Gr...'. The 'Roles' tab is selected, showing a table of role assignments. The table has columns for 'St...', 'Role', 'Type', 'Valid From', 'Valid to', and 'Name'. The roles listed are:

St...	Role	Type	Valid From	Valid to	Name
	SAP_EPM_PLANT_MANAGER		02.08.2001	31.12.9999	Role for Plant Manager Role
	SAP_EPM_PLANT_MANAGER_ADMIN		02.08.2001	31.12.9999	Administrator for Plant Manager
	Z_L0215_BD		02.08.2001	31.12.9999	Stammdaten R/3
	Z_L0215_MRP		02.08.2001	31.12.9999	Planungsfunktionen R/3
	Z_L0215_MRP_MINI		02.08.2001	31.12.9999	MRP Miniapplikationen
	Z_SCM310		02.08.2001	31.12.9999	SCM310 Sammelrolle für sp
	Z_SCM310_SFC		02.08.2001	31.12.9999	PP-SFC Auftragsverwaltung

Kuva 2. Loppukäyttäjän roolit.

CUA asennetaan yhteen ABAP-pohjaiseen järjestelmään. Asennuksen jälkeen keskitetyn käyttäjähallinnan piiriin tulevat ABAP-järjestelmät integroidaan järjestelmään, johon CUA on asennettu. Hallitsevalla järjestelmällä voidaan keskitetysti suorittaa SAP:n eri järjestelmien, käyttäjien hallintaa sekä roolitusta. Muutokset jotka tehdään hallitsevassa järjestelmässä, allokoidaan automaattisesti siihen integroituihin järjestelmiin. (Gergen ym. 2010, 70.)

CUA:n käyttäjätietojen jakelu perustuu toiminnalliseen Application Link Enabling -teknologiaan. Application Link Enabling -teknologia on integraatiotekniikka, jonka avulla voidaan siirtää tietoa SAP:n ja sen kumppaneiden kehittämien sovellusten välillä. Kyseistä teknologiaa käyttämällä tietoja voidaan vaihtaa

järjestelmästä toiseen kontrolloidusti ja varmasti menettämättä tiedon yhtenäisyyttä. (SAP 2011f.)

SAP CUA:n suurimpina hyötyinä voidaan pitää käyttäjähallinnan helppoutta sekä mahdollisuutta keskittää käyttäjähallinnan toimet yhteen järjestelmään. CUA:ta suosivat useat yritykset, jotka hankkivat käyttöönsä monia ABAP – pohjaisia SAP-moduuleita lisäämään SAP ERP:n toiminnallisuutta. Yleisiä toiminnallisuutta lisääviä moduuleita olivat muun muassa SAP NetWeaver BW ja SAP APO. (Gergen ym. 2010, 70.)

CUA on vieläkin todella suosittu ratkaisu SAP:n käyttäjien hallintaan, vaikka se ei enää pysty tarjoamaan muuta kuin hyvät integraatiomahdollisuudet ABAP-ympäristössä. CUA:ssa ei ole rajapintoja Workflow'ille eikä Portalille, jolloin niiden integraatiot tulee tehdä itsenäisesti.

Workflow eli työnkulku koostuu erilaisista perättäisistä tehtävistä, joiden suorittaminen johtaa tiettyyn tulokseen. Työnkulku voidaan kuvata vuokaaviona, jossa on alku ja loppu. (Microsoft 2013b.)

CUA ei myöskään huomioi roolitukseen liittyviä riskejä. Käyttäjille pystytään myöntämään rooleja, jotka voivat sisältää vaarallisia työyhdistelmiä. Vaarallisten työyhdistelmien huomioiminen on täysin SAP-käyttöoikeuksista vastaavan henkilön vastuulla. SAP CUA ei myöskään tue loppukäyttäjien itsepalveluominaisuuksia salasanojen vaihtamiseen. CUA:n kautta käyttäjäroolien hallinta on mahdollista ainoastaan hallitsevasta ABAP-järjestelmästä. (Gergen ym. 2010, 70.)

Roolien luonti SAP CUA:n onnistuu manuaalisesti transaktiokoodilla PFCG. Kyseinen transaktiokoodi käynnistää SAP:n Profile Generatorin, jonka kautta roolien luonti tapahtuu. Profile Generatorin avulla pystytään helpottamaan roolien luontia, sillä se luo käyttäjäprofiilit sekä lisää määritykset automaattisesti. Profile Generator nopeuttaa ja virtaviivaistaa käyttäjien hallintaa, sekä sen avulla voidaan luoda räätälöityjä valikkoja SAP:n loppukäyttäjille. (Gergen ym. 2010, 70.)

SAP CUA:ssa on selkeitä puutteita verrattuna esimerkiksi NW IDM -ratkaisuun. SAP on lopettanut CUA:n kehitystyön kokonaan, korjauksia kuitenkin julkaistaan vielä. Oheinen seikka osoittaa selvästi, että SAP ei enää halua tarjota asiakkailleen CUA-ratkaisua käyttäjien hallintaan, vaan pyrkii tarjoamaan uudempia ja kehittyneempiä ratkaisuja. Käyttäjän uudelleen nimeäminen on SAP CUA:ssa hankalaa. Käyttäjän nimeä vaihdettaessa hänet pitää luoda kokonaan uudelleen. SAP CUA:n ominaisuudet eivät kata mobiililaitteiden käyttäjien hallintaa. Mobiililaitteiden käyttäjien hallinta on nykyisin tärkeä osa-alue organisaatioiden tietoturvallisuuden hallinnassa. CUA ei myöskään sisällä Workflow-ominaisuutta, toisin kuin NW IDM. (Olli-Pekka Lindström 19.3.2012, haastattelu.)

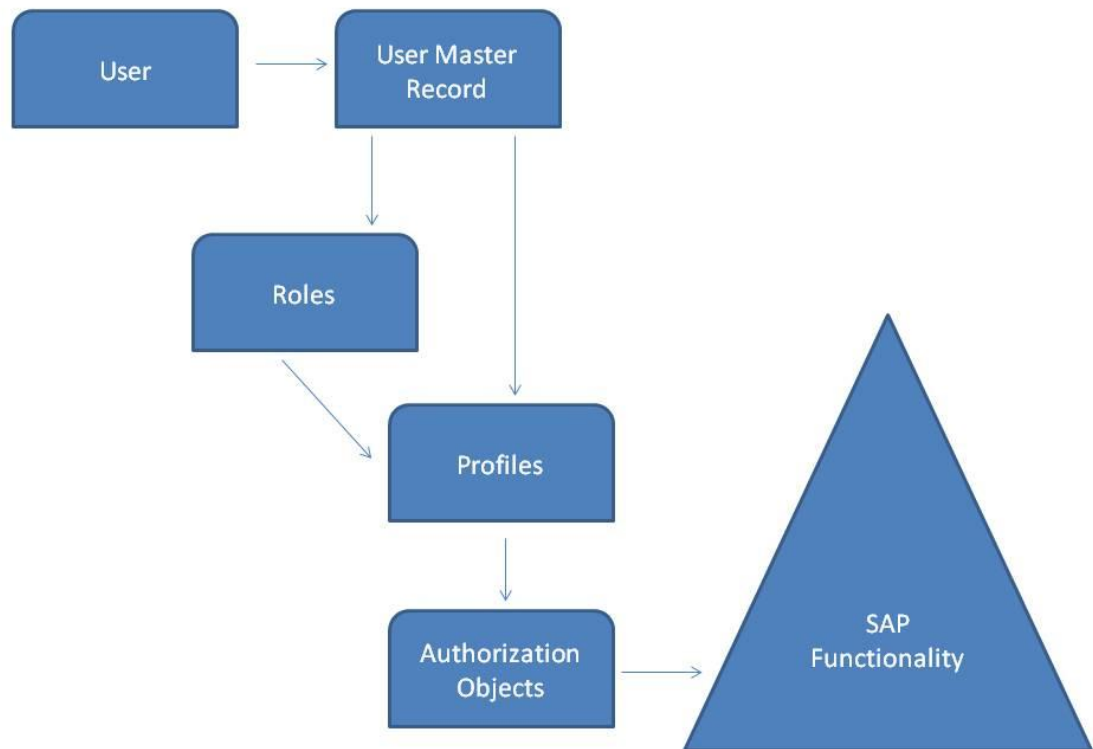
SAP profiilit ja roolit

SAP:n autorisointikonsepti perustuu profiileihin ja rooleihin. Niiden avulla loppukäyttäjät saavat käyttöoikeudet järjestelmään. SAP-järjestelmään määritetyt käyttäjät, profiilit ja roolit sijaitsevat User Master Recordissa (kuvio 3). (Help SAP 2013.)

Profiilit sisältävät itse autorisointiin tarvittavan informaation. SAP-järjestelmässä voi olla erilaisia profiileja perustuen niiden luontitapaan tai ominaisuuksiin. SAP-profiileja voidaan luoda manuaalisesti tai Profile Generatorin avulla. SAP suosittelee vahvasti Profile Generatorin käyttöä profiilien luomiseen ja ylläpitoon. Profiileja voi olla yksittäisiä sekä yhdistelmiä eli Composite-profiileja. Composite-profiili koostuu monista yhdistetyistä profiileista. (Help SAP 2013.)

SAP:n rooli on kokoelma käyttöoikeuksia eli profiileja. Rooli voi sisältää monia profiileja, mutta sen täytyy sisältää ainakin yksi profiili (kuvio 3). Roolien avulla pystytään luomaan työtehtäväkohtaisia roolituksia. SAP:n roolit voidaan jakaa kahteen ryhmään, Composite ja Single. Composite-rooli koostuu useista Single-rooleista. Single-rooli on yksittäinen rooli. Roolit voidaan määrittää loppukäyttäjille transaktioilla SU01 tai PFCG. PFCG-transaktio käynnistää Profile Generatorin, jonka avulla pystytään luomaan ja ylläpitämään rooleja. (Help SAP 2013.)

SAP-järjestelmässä toimintojen suorittaminen sekä pääsy tietoihin on suojattu Authorization Objectien avulla, kuten kuviosta 3 nähdään. Authorization Objectit mahdollistavat monimutkaisien tarkastuksien luonnin, jotka voivat sisältää useita erilaisia ehtoja. Ehtojen täyttymisen perusteella käyttäjä saa tietynlaiset oikeudet käyttöönsä. (Help SAP 2006.)



Kuvio 3. SAP:n autorisointikonsepti (Sym-Corp 2010).

8 SAP NETWEAVER IDENTITY MANAGEMENT

SAP NetWeaver on teknologia-alusta SAP:n ohjelmistoille. SAP NetWeaver tarjoaa monia toimintoja ja työkaluja yrityksille. Sen päätehtävä on kuitenkin toimia teknisenä alustana yrityksen palvelukeskeiselle arkkitehtuurille. NetWeaverin avulla SAP-ohjelmistot voivat olla vuorovaikutuksessa muiden ohjelmistojen kanssa. NetWeaverin avulla yritys pystyy kehittämään sovelluksiaan vastaamaan paremmin liiketoimintansa vaatimuksia. (Muir & Kimbell 2008, 62, 299-300.)

SAP NetWeaver yhdistää monia teknologioita ja toimintoja. Teknologiat ja toiminnot ovat kiinteitä ja niitä käyttävät kaikki SAP:n ohjelmistot, jotka tukevat yrityksen SAP-järjestelmää. Tukevia ohjelmistoja ovat muun muassa SAP NetWeaver Exchange Infrastructure, SAP NetWeaver Portal, SAP NetWeaver Web Application Server ja SAP NetWeaver Business Intelligence. (Muir & Kimbell 2008, 62.)

SAP NetWeaver auttaa yrityksen osastoja kommunikoimaan paremmin keskenään. Se auttaa työntekijöitä organisoimaan tietoa ja parantamaan tiedon saatavuutta sekä suorittamaan liiketoimintaprosesseja, tarjoamalla integraatioalustan eri ohjelmistoille. NetWeaver tarjoaa myös avoimiin standardeihin perustuvan kehitysympäristön SAP-ohjelmistoille. (Muir & Kimbell 2008, 62, 299-300.)

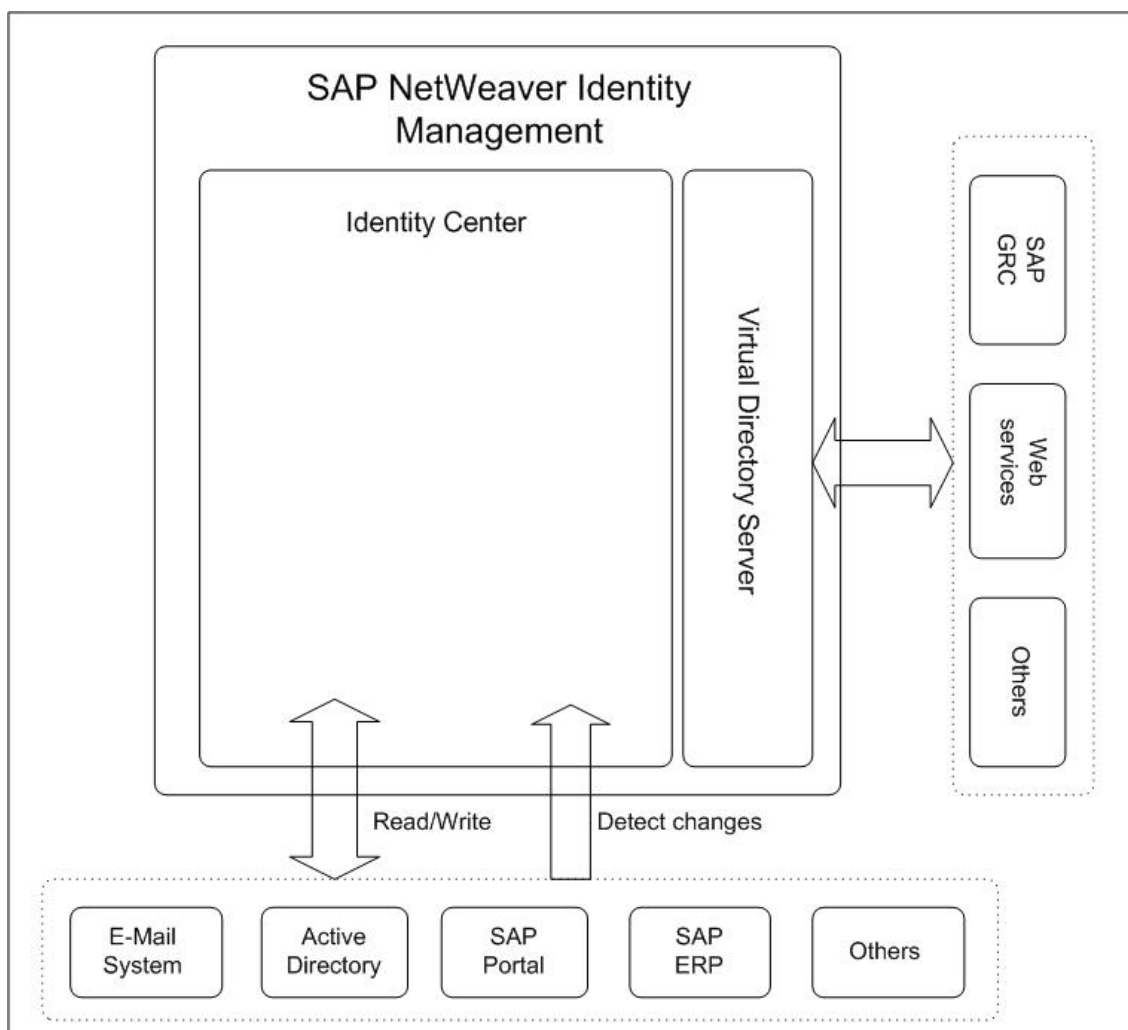
CUA:n integraatiomahdollisuuksien riittämättömyyden sekä muiden puutteiden takia SAP tarvitsi tarjontaansa sovelluksen, joka vastaisi paremmin nykyaikaisten yritysten käyttäjien hallinnan vaatimuksia. Tärkeimpänä vaatimuksena uudelle sovellukselle oli heterogeenisen järjestelmäarkkitehtuurin tukeminen. Tavoitteena siis oli, että uuden ratkaisun piiriin saataisiin muun muassa kaikki SAP-, Windows-, tietokanta- ja räätälöidyt-ohjelmistot, jotka tarvitsevat autentikointitietoja. (Gergen ym. 2010, 77.)

SAP hankki lisää käyttäjähallintaosaamista vuonna 2007 ostamalla yrityksen nimeltä MaxWare. Yrityksen tuotteisiin kuului MaxWare IDM Suite, joka oli käyttäjähallintaan suunniteltu sovellus. Sovellus sisälsi monia liittyviä erilaisiin järjestelmiin, myös muihin kuin SAP:n järjestelmiin. SAP investoi hankkimansa järjestelmän tekniseen kehitykseen. SAP lisäsi järjestelmään laajemmat integraatiomahdollisuudet. Lopulta tuote sai nimen SAP NetWeaver Identity Management nimellä. SAP NetWeaver IDM:ssä on markkinoilla olevista käyttäjähallintasovelluksista korkein integrointiaste SAP-järjestelmiin. SAP NW IDM on myös täysin integroitu SAP:n teknologia-alustaan. (Gergen ym. 2010, 277.)

8.1 Arkkitehtuuri

SAP NetWeaver Identity Management on SAP -NetWeaver alustan päälle rakennettu käyttäjähallintasovellus. Se mahdollistaa keskitetyn käyttäjätietojen hallinnan ja jakelun koko organisaation järjestelmäympäristössä. (Gergen ym. 2010, 78.)

NW IDM -ratkaisuun pystytään integroimaan erilaisia ratkaisuja, kuten SAP Governance, Risk and Compliance-ratkaisuja, web-palveluita sekä useita muita ratkaisuja, kuten kuvioista 4 nähdään. Integraatio tapahtuu Virtual Directory Serverin kautta, joka on toinen SAP NW IDM:n pääkomponenteista. VDS:n kautta tietoa voidaan kuljettaa Identity Centeristä siihen liitettyihin järjestelmiin tai järjestelmistä Identity Centeriin (kuvio 4).

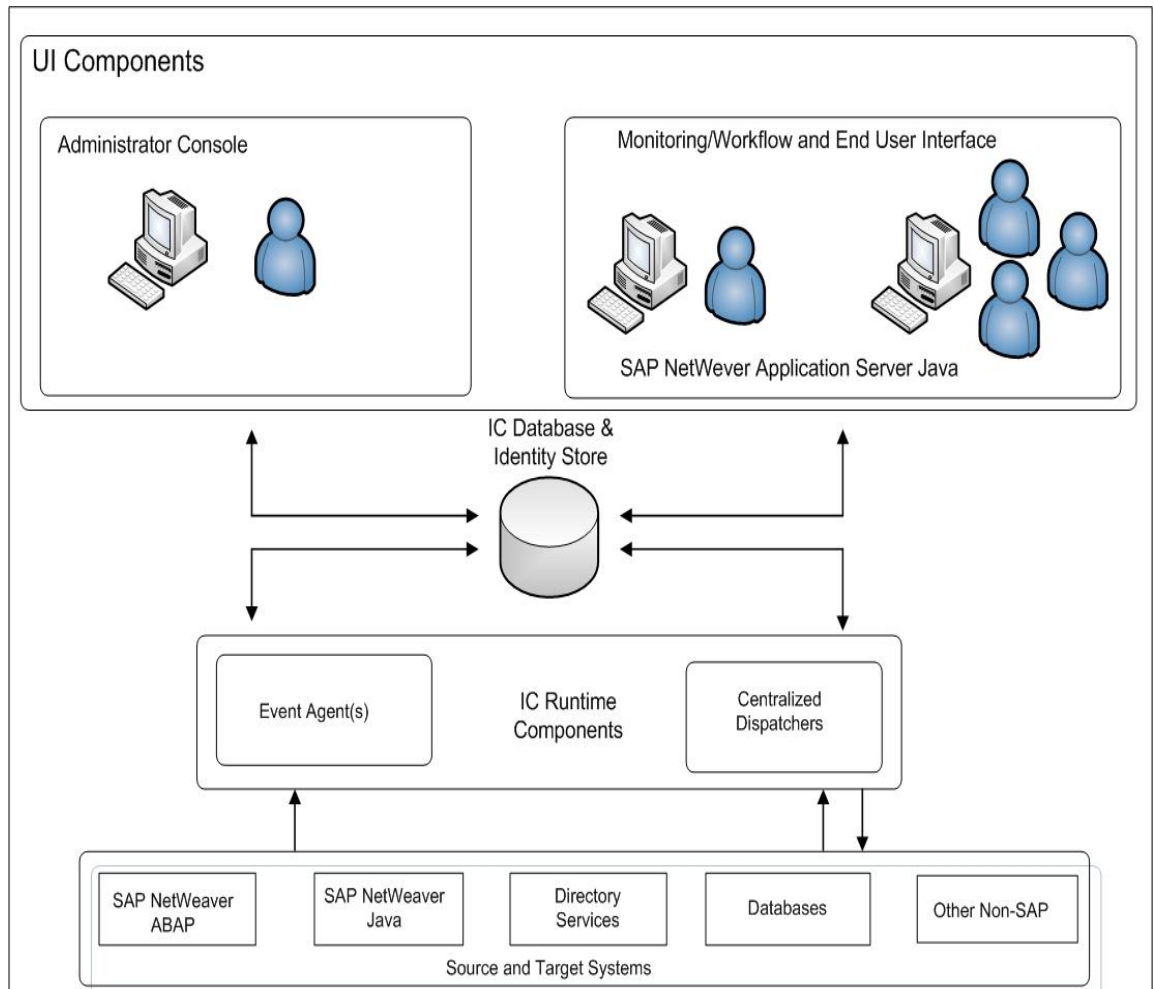


Kuvio 4. SAP NetWeaver Identity Management arkkitehtuuri (SAP AG 2010).

Toinen pääkomponentti on Identity Center, jonka läpi NW IDM järjestelmään voidaan integroida muun muassa Microsoft Active Directory, SAP Portal, SAP ERP sekä sähköpostisovelluksia, kuten kuvioista 4 nähdään. Identity Centeriin integroidut järjestelmät voivat hakea ja muokata Identity Centerin tietoja. Osa integroiduista ratkaisuista reagoi tapahtuviin muutoksiin muissa komponenteissa ja ilmoittaa niistä Identity Centerille.

Virtual Directory Server toimii väliohjelmistona, joka tuottaa toiminnallisuksia virtualisoiduille ja standartoiduille liittymille. Se tarjoaa muutosfunktioita sekä tukee tiettyjä protokollia, kuten LDAP. SAP VDS on NW IDM-arkkitehtuurin valinnainen komponentti, jolla on kuitenkin keskeinen rooli erilaisten järjestelmien välisessä integraatiossa sekä tiedonkeruussa muista tietolähteistä.

VDS:ää käytetään esimerkiksi Human Capital Management -moduulin integraatioissa ja integroitaessa SAP Business Objects Access Control järjestelmää. (Gergen ym. 2010, 85-86.)



Kuvio 5. Identity Centerin komponentit (Gergen ym. 2010, 79).

Identity Center on relaatiotietokantapohjainen ratkaisu, joka muodostaa NW IDM järjestelmän ytimen. (Gergen ym. 2010, 78.) Identity Center voidaan jakaa kolmeen pääkerrokseen (kuvio 5):

- User Interface Components.
- Database and Identity Stores.
- Runtime Components. (Gergen ym. 2010, 78.)

User interface components kerros koostuu kahdesta osasta (kuvio 5):

- *Administration Console*: Administration Consolen avulla ylläpitäjät pystyvät kehittämään, kustomoimaan ja konfiguroimaan Identity Centeriä ja sen toimintoja, kuten käyttöoikeuksia ja työnkulkua. (Gergen ym. 2010, 79.)
- *SAP NetWeaver IDM UI*: SAP NetWeaver IDM UI sisältää kaksi erilaista toiminnallisuutta. Workflow and End User Interfacen kautta suoritetaan kaikkien loppukäyttäjien rekisteröinnit järjestelmään. Käyttöliittymän kautta loppukäyttäjät pääsevät käyttämään itsepalveluominaisuuksia. Kyseisen käyttöliittymän kautta voidaan palauttaa ja nollata salasanoja sekä ottaa vastaan erilaisia tehtäviä. Monitoring User Interfacen avulla pystytään tarkkailemaan järjestelmän tilaa, tarkastuksia ja logeja päivittäisten operaatioiden aikana. (Gergen ym. 2010, 79.)

Database and Identity Stores kerros rakentuu yhdestä komponentistä (kuvio 5):

- *Identity Center Database*: Sisältää tiedot käyttöoikeuksista, työkuluista ja käyttäjistä. Identity Center Databasen kirjataan myös järjestelmän tapahtumat. (Gergen ym. 2010, 85.)

Runtime Components kerros koostuu kahdesta osasta (kuvio 5):

- *Dispatchers*: Dispatcherit suorittavat työtehtäviä ja jakavat käyttöoikeuksia. Dispatchereita voidaan muokata tekemään erilaisia tehtäviä, muuttamalla niiden määrittelyjä. Esimerkiksi tietty dispatcheri hoitaa ainoastaan tietynlaisia, sille määriteltäviä tehtäviä, sille määriteltävien aikarajojen puitteissa. (Gergen ym. 2010, 84.)

Dispatchereita on edelleen saatavilla sekä Windows- että Java-ympäristöihin, koska NW IDM:iin liitetään usein Windows-ympäristön käyttäjätilit Windows Active Directoryn kautta. SAP:n tavoitteena on kuitenkin käyttää tulevaisuudessa ainoastaan Java-ympäristöä, joka

takaisi SAP:lle IC runtime -komponenttien alustariippumattomuuden. (Gergen ym. 2010, 84.)

- *Event Agent*: Event Agentit voidaan konfiguroida toimimaan, kun erilaisissa tietovarastoissa, esimerkiksi hakemistopalvelimessa tapahtuu muutoksia. Event Agent huomaa muutokset ja lähettää tiedon muutoksista Identity Centeriin, joka lisää muuttuneen tiedon Identity Databaseen. (Gergen ym. 2010, 85.)

Event Agent-toiminnallisuudet on saatavilla ainoastaan seuraavissa käyttötapauksissa:

- objektien monitorointi, lisääminen, muuttaminen tai poistaminen Microsoft Active Directorysta
- muutosten monitorointi tietokannoissa
- tiedostojen ja hakemistojen monitorointi
- muutosten monitorointi LDAP-hakemistoissa (Gergen ym. 2010, 85.)

8.2 Ominaisuudet

SAP NetWeaver IDM tarjoaa monia ominaisuuksia organisaation käyttäjien hallintaan. Ominaisuudet voidaan kiteyttää seuraaviin kohtiin:

- *Metadirectory*: Synkronoitu, yhdistetty ja keskitetty relaatiotietokanta, joka sisältää organisaation käyttäjätiedot, lisäksi sen tietomallia pystytään kehittämään joustavasti.
- *Process control*: Process control mahdollistaa monimutkaisten työkulujen kehityksen, käyttäjien tietojen sekä auktorisointi pyyntöjen hallintaan.

- *Automated and rule-based provisioning:* Ominaisuuden avulla pystytään luomaan, muokkaamaan, lukitsemaan ja poistamaan käyttäjiä, NW IDM:iin liitetyistä ja sillä hallinnoituista järjestelmistä.
- *Password management:* Password managementin avulla organisaation salasanoja pystytään hallinnoimaan keskitetysti.
- *Reporting and audit:* Reporting and audit-ominaisuuden avulla voidaan luoda raportteja nykyisistä tai vanhoista aineistoista, käyttämällä SAP Business Objects Crystal Reports raportointityökalua. (Gergen ym. 2010, 77.)

8.3 Single sign-on (SSO)

Yrityksissä käytetään päivittäin monia eri tietojärjestelmiä, itse työn suorittamiseen sekä suorittamisen tukemiseen. Usein työntekijät joutuvat kirjautumaan kaikkiin tarvitsemiinsa järjestelmiin yksitellen. Moniin järjestelmiin kirjautuminen yksitellen kuluttaa turhaan työaika. Työntekijän tulee myös muistaa kaikkien järjestelmien käyttäjätunnuksensa ja salasanasensa. Tämä ei ole helppoa, ja näin ollen työntekijät kirjoittavat tunnuksiaan ja salasanojaan muistiin, esimerkiksi tekstitiedostoon tai paperille helpottaakseen niiden muistamista. Oheinen toimintapa ei ole tietoturvallinen eikä parhaiden käytäntöjen mukainen. Nämä ongelmat voidaan ratkaista kertakirjautumisen avulla.

Kertakirjautuminen on mekanismi, jonka avulla käyttäjä voidaan autentikoida ja auktorisoida moneen eri järjestelmään, yksillä käyttäjätunnuksilla. Kertakirjautuminen mahdollistaa siis käyttäjän kirjautumisen yksillä käyttäjätunnuksilla kaikkiin yrityksen järjestelmiin tai tietoteknisiin laitteisiin, joihin hänelle on luotu käyttäjätunnukset. (Opengroup 2010.)

8.4 The Security Assertion Markup Language (SAML)

Tietojärjestelmien autentikointi voidaan toteuttaa monella eri tavalla. Opinnäytetyöni puitteissa en kuitenkaan voi perehtyä kaikkiin autentikointimekanismeihin. Työssäni perehdyn erityisesti SAML-tekniikkaan. SAML on J2EE-pohjainen mekanismi. SAP:n kanssa yhteensopivia mekanismeja on ainakin kahta eri tyyppiä, ABAP-pohjaisia sekä J2EE-pohjaisia. Muita ratkaisuja ovat muun muassa Kerberos, SAP Logon Tickets, SSL ja SNC.

SAML on XML-pohjainen viitekehys, joka mahdollistaa autentikointi ja auktorisointitietojen vaihtamisen servereiden välillä. Tietojen vaihto tapahtuu käyttäjien näkymättömissä, HTTP-yhteyden yli. SAML-tekniikan kehityksen perustana on ollut tieto siitä, että jokaisella ohjelmistoalustalla on omanlaisensa autentikointi ja auktorisointi periaatteensa. Niinpä käyttäjien tiedot vaihdetaan standardien mukaisella XML - tekniikalla. SAML perustuu OASIS nimisen web palveluiden standardointia harjoittavan yrityksen avoimeen standardiin. (Oasis-open 2005.)

9 OHJELMISTOJEN VERTAILU

Tässä luvussa selvitetään SAP NW IDM ja SAP CUA -järjestelmien merkittävimmät eroavaisuudet. Taulukossa 1 kuvataan, SAP CUA:lla voidaan hallita vain ABAP-pohjaisia kohdejärjestelmiä. SAP NW IDM:n kohdejärjestelminä voi olla sekä ABAP-pohjaisia että muita ratkaisuja. Tämä on suurin eroavaisuus näiden kahden järjestelmän välillä.

SAP CUA ei tue Workflow-ominaisuutta toisin kuin SAP NW IDM. Työnkulun avulla voidaan saavuttaa monia etuja. Työnkulku eliminoi prosessissa tapahtuvat virheet sekä nopeuttaa prosessin läpivientiä, koska prosessi voidaan osittain automatisoida. Prosessin nopeampi läpivienti sekä virheiden eliminointi mahdollistavat kustannussäästöjä. Käyttäjähallinnassa työnkulkua on mielekästä käyttää ainakin käyttäjän lisäämisessä ja poistamisessa.

Roolihierarkian mallinnuksen avulla rooleja ja niiden hierarkioita pystytään esittämään kuvina. Tämä ominaisuus helpottaa roolien ymmärtämistä. SAP NW IDM tukee roolihierarkioiden mallinnusta, eli järjestelmä pystyy mallintamaan roolit ja niiden hierarkiat automaattisesti (taulukko 1). SAP CUA ei tue automaattista roolihierarkioiden mallinnusta lainkaan.

SAP NetWeaver IDM tukee täydellisesti automaattista järjestelmäriippumatonta roolien jakelua. Tämä ominaisuus mahdollistaa esimerkiksi SAP käyttäjäroolien jakamisen muihin järjestelmiin. Näin ollen rooleja ei tarvitse luoda aina uudelleen jokaiseen järjestelmään, vaan ne luodaan kerran, ja jaetaan kaikkiin järjestelmiin. SAP CUA:lla pystytään jakamaan rooleja vain muihin ABAP-pohjaisiin järjestelmiin ja itse jakaminen tapahtuu manuaalisesti.

LDAP-protokollan integraatiomahdollisuus on tärkeä ominaisuus. Monet järjestelmät käyttävät LDAP-protokollaa käyttäjien tunnistukseen sekä käyttöoikeuksien tarkistamiseen. Se on yleisesti käytössä oleva protokolla. SAP CUA pystyy synkronoimaan LDAP-hakemiston. Synkronoinnin avulla CUA pystyy tunnistamaan käyttäjiä ja tarkistamaan käyttöoikeuksia LDAP:n läpi. SAP

NetWeaver IDM tukee kokonaisvaltaisesti LDAP-hakemiston käyttöä käyttäjien tunnistamiseen ja käyttöoikeuksien tarkistamiseen.

Salasanojen hallinta tapahtuu vertailtavissa ohjelmistoissa myös eri tavalla (taulukko 1). SAP CUA mahdollistaa salasanojen keskitetyn hallinnan ja jakelun. Kun SAP ympäristöön lisätään uusi käyttäjä, tulee hänelle määrittää salasana. SAP CUA:ssa uusien käyttäjien ensimmäiset salasanat määritetään keskitetysti, ylläpitäjien toimesta. Ensimmäisen salasanan jälkeen loppukäyttäjä pystyy vaihtamaan itselleen haluamansa salasanan. SAP NW IDM järjestelmässä loppukäyttäjä pystyy itse määrittämään oman salasanaan alusta alkaen. NW IDM:lla loppukäyttäjä pystyy myös itse resetoimaan tai vaihtamaan salasanaan omasta käyttöliittymästään.

Molemmat ohjelmistot tarjoavat graafisen käyttöliittymän, kuten taulukosta 1 näemme. SAP CUA:ssa graafinen käyttöliittymä käynnistetään transaktiolla SU10. SAP NW IDM tarjoaa graafisen käyttöliittymän lisäksi tuen käyttäjätietojen massamuutoksiin CSV-tiedostojen avulla.

SAP CUA sisältää raportointiominaisuuksia transaktion SUIM kautta (taulukko 1). SAP NetWeaver Identity Management -ohjelmisto tarjoaa myös raportointiominaisuuksia. NW IDM tuottaa standardoituja raportteja SAP NetWeaver Business Warehousen ja SAP Crystal Reports -työkalujen kautta.

SAP CUA -ohjelmisto ei mahdollista ilmoitusten lähettämistä sähköpostitse, kuten taulukossa 1 on mainittu. SAP NetWeaver Identity Management tukee sähköpostijärjestelmien integraatiota ja näin mahdollistaa ilmoitusten lähettämisen sähköpostin välityksellä.

Taulukko 1. SAP käyttäjähallintasovellusten vertailu (SAP AG 2011b).

Toiminnallisuus	SAP CUA	SAP NetWeaver Identity Management
Kohdejärjestelmät	Vain ABAP - pohjaiset	SAP:n ja muiden toimittajien sovellukset
Workflow (työnkulku) tuki	Ei	Kyllä
Roolihierarkian mallinnus	Ei	Kyllä
Järjestelmäriippumaton roolien jakelu	Manuaalinen	Kyllä, automaattinen
LDAP hakemiston integraatio	Ainoastaan LDAP synkronointi	Kyllä
Salasanojen hallinta	Kyllä, keskitetty alustavien salasanojen hallinta ja jakelu	Kyllä, käyttöliittymä mahdollistaa keskittämättömän salasanojen vaihdon
Graafinen käyttöliittymä	Kyllä, transaktion SU10 kautta	Kyllä, tukee massamuutoksia CSV tiedostojen kautta
Raportointi	Kyllä, transaktion SUIM kautta	Kyllä, standardoituja raportteja SAP Business warehousen tai SAP Crystal Reportsin kautta
Sähköposti-ilmoitukset	Ei	Kyllä

10 JOHTOPÄÄTÖKSET (SALATTU OSIN)

Työssäni vertailin SAP NetWeaver IDM käyttäjienhallintaratkaisua SAP CUA ratkaisuun.

10.1 SAP NetWeaver Identity Managementin hyödyt

SAP NetWeaver Identity Managementin käyttöönoton avulla yritykset voisivat saavuttaa monia etuja verrattuna CUA-ratkaisuun.

SAP NW IDM:n avulla yritykset pystyisivät eliminoimaan vaaralliset työyhdistelmät SAP-ympäristöstään. Vaarallisten työyhdistelmien eliminoinnilla pystyttäisiin estämään väärinkäytöksiä ja virheiden tapahtumista kriittisissä prosesseissa.

SAP NW IDM:n integrointimahdollisuuksien ansiosta yritykset pystyisivät integroimaan kaikki SAP -ratkaisuna keskitetyn SAP-käyttäjähallinnan piiriin. Käyttäjäroolit, käyttäjätunnukset ja käyttöoikeudet voitaisiin hallita keskitetysti yhdellä ratkaisulla.

Loppukäyttäjien itsepalveluominaisuuksien kautta yritykset pystyisivät nopeuttamaan käyttäjien hallintaan liittyviä muutoksia. Ominaisuuden avulla loppukäyttäjät pystyvät tekemään tiettyjä muutoksia itsenäisesti, esimerkiksi uusimaan salasanaan. Tiettyissä muutoksissa heidän ei tarvitsisi ottaa yhteyttä käyttäjien hallinnasta vastaavaan tahoon.

SAP NW IDM:n avulla yritykset pystyisivät rakentamaan todella kattavan raportoinnin loppukäyttäjistä ja käyttäjähallinnan tilasta. NW IDM:n raportointi integroituu todella hyvin Crystal Reports ja Business Warehouse -pohjaiseen raportointiin.

SAP NW IDM-ratkaisun hyödyt:

- vaarallisten työyhdistelmien eliminointi
- kaikki SAP -järjestelmät keskitetyn käyttäjähallinnan piiriin

- loppukäyttäjien itsepalveluominaisuus, jonka avulla pystytään vähentämään ylläpidon työtehtäviä
- monipuolinen raportointi SAP NetWeaver Business Warehouse ja Crystal Reports ratkaisuihin
- automaattinen käyttäjien hallinta perustuen työnkulkuun
- roolienhallinta työtehtäviin perustuen
- Single Sign-On ratkaisu, joka tukee standardeja.

10.2 Suosituksia HK Ruokatalolle (SALATTU)

LÄHTEET

Alter, S. 2002. Information Systems. The Foundation of e-business. 4., uudistettu painos. New Jersey: Prentice-Hall.

Gergen, P.; Heilig, L. & Muller, A. 2010. Understanding SAP NetWeaver Identity Management. Boston: Galileo Press. Translator: Lemoine International.

Gracion 2008. What is LDAP? Viitattu 5.11.2013 <http://www.gracion.com/server/whatldap.html>

Haikala, I & Märijärvi, J. 2004. Ohjelmistotuotanto. 10., uudistettu painos. Helsinki: Talentum Media Oy.

Help SAP 2006. Authorization Objects. Viitattu 6.11.2013 http://help.sap.com/saphelp_470/helpdata/en/5c/73ba3bd14a6a6ae10000000a114084/content.htm

Help SAP 2009. SAP NetWeaver. Integration. Viitattu 15.3.2012 http://help.sap.com/saphelp_nw04/helpdata/en/30/c4461ff69d5a438f1286e344b545fa/content.htm

Help SAP 2011. Procurement for public sector. Viitattu 22.2.2012. http://help.sap.com/saphelp_srm70/helpdata/en/c9/8d47ed4a5548c08521615d84a590e6/content.htm

Help SAP 2012. Central User Administration. Viitattu 1.2.2012. http://help.sap.com/saphelp_nw04s/helpdata/en/bf/b0b13bb3acd607e10000000a11402f/content.htm

Help SAP 2013. AS ABAP Authorization Concept. Viitattu 5.11.2013 http://help.sap.com/saphelp_nw2004s/helpdata/en/52/671285439b11d1896f0000e8322d00/content.htm

HKScan 2013a. HKScan Oyj on Pohjois-Euroopan johtavia liha- ja ruokayhtiöitä. Viitattu 3.12.2013 <http://www.hkscan.com/fi/hkscan>

HKScan 2013b. Tulos ja tunnusluvut. Viitattu 18.11.2013 http://www2.hkscan.com/portal/suomi/hkscan/sijoituksena/tulos_ja_tunnusluvut/

HKScan 2013c. Historiaa. Viitattu 3.12.2013 <http://www.hkscan.com/fi/historiaa>

HKScan 2013d. Suomi. Viitattu 3.12.2013 <http://www.hkscan.com/fi/suomi>

HKScan 2013e. HK Ruokatalo Oy. Viitattu 3.12.2013 http://www2.hkscan.com/portal/suomi/suomi/hk_ruokatalo_oy/

Hollander, H. 2005. Evaluating software: Finding the right fit. Stone World, 22(8), 78-78. Viitattu 21.11.2012 <http://search.proquest.com/docview/213596644?accountid=14446>

IBM 2013. Java 2 Platform, Enterprise Edition (J2EE) specification. Viitattu 5.11.2013 http://pic.dhe.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=%2Fcom.ibm.websphere.express.doc%2Finfo%2Fexp%2Fae%2Fcovr_j2ee.html

JUHTA 2009. JHS 173 ICT palvelujen kehittäminen: Vaatimusmäärittely. Viitattu 18.9.2013 <http://docs.jhs-suositukset.fi/jhs-suositukset/JHS173/JHS173.pdf>

Kesko 2011. Sanasto. Viitattu 5.3.2012 <http://www.kesko.fi/fi/Kesko-yrityksena/Sanasto/>

Kettunen, J & Simons, M. 2001. Toiminnanohjausjärjestelmän käyttöönotto pk-yrityksessä. Teknologialähtöisestä ajattelusta kohti tiedon ja osaamisen hallintaa. Viitattu 14.3.2012 <http://www.vtt.fi/inf/pdf/julkaisut/2001/J854.pdf>

Linkies, M & Host, K. 2010. SAP Security and Risk Management. 2., uudistettu painos. Boston: Galileo Press.

Microsoft 2013a. Johdanto käyttäjärooleihin. Viitattu 30.9.2013.
<http://office.microsoft.com/fi-fi/infopath-help/johdanto-kayttajarooleihin-HP010165118.asp>

Mircosoft 2013b. Johdanto työnkulkujen käyttämiseen. Viitattu 5.11.2013
<http://office.microsoft.com/fi-fi/windows-sharepoint-services-help/johdanto-tyonkulkujen-kayttamiseen-HA010164124.aspx>

Muir, N & Kimbell, I. 2008. Discover SAP. 1., renewed edition. Boston: Galileo Press.

Oasis-open 2005. SAML V2.0 Executive Overview. Viitattu 14.3.2012 <http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>

Opengroup 2010. Sinlg Sign-on. Viitattu 14.3.2012 <http://www.opengroup.org/security/sso/>

Paananen, J. 2005. Tietotekniikan peruskirja. Jyväskylä: Docendo Finland Oy.

Pendergraft, L., C.R.M., & Blakely, A. F. (2010). Ten steps for evaluating and selecting software and service providers. Information Management, 44(1), 40-42,44. Viitattu 27.8.2013
<http://search.proquest.com/docview/227764122?accountid=14446>

SAP AG 2010. SAP NetWeaver Identity Management. Technical Overview Presentation. Viitattu 26.11.2012 http://nicx.co.uk/uploaded_files/identity%20management.pdf

SAP AG 2011a. SAP NetWeaver ID Management Solution Details. SAP Solution in Detail 5/11.

SAP AG 2011b. SAP NetWeaver Identity Management: The Time is now. Replace CUA – Set a strategic course in user administration 11/04.

SAP 2011a. About SAP AG. Viitattu 24.1.2012 <http://www.sap.com/corporate-en/our-company/index.epx>

SAP 2011b. The First 10 Years. Viitattu 24.1.2012 <http://www.sap.com/corporate-en/our-company/history/1972-1981/index.epx>

SAP 2011c. The SAP R/3 Era. Viitattu 24.1.2012 <http://www.sap.com/corporate-en/our-company/history/1982-1991/index.epx>

SAP 2011d. The Age of E-Business. Viitattu 24.1.2012 <http://www.sap.com/corporate-en/our-company/history/1992-2001/index.epx>

SAP 2011e. SAP Today. Viitattu 27.1.2012 <http://www.sap.com/corporate-en/our-company/history/2002-today/index.epx>

SAP 2011f. NetWeaver. Viitattu 1.2.2012. <http://www.sap.com/platform/netweaver/index.epx>

SAP 2011g. Supply Chain Management. Viitattu 14.2.2012
<http://www.sap.com/solutions/business-suite/scm/index.epx>

SAP 2011i. SAP NetWeaver: Components and Tools. Viitattu 13.3.2012
<http://www.sap.com/platform/netweaver/components/index.epx>

SAP 2013. About SAP AG. 1971-1981: the early years. Viitattu 5.11.2013
<http://global.sap.com/corporate-en/our-company/history/1972-1981.epx>

Searchsap 2010. ABAP. Viitattu 5.11.2013 <http://searchsap.techtarget.com/definition/ABAP>

Sym-Corp 2010. SAP Security 101: Introduction to SAP security. Viitattu 5.11.2013
<http://www.sym-corp.com/archived-webinars/item/153-sap-security-101-introduction-to-sap-security>

Turban, E.; McLean, E. & Wetherbe, J. 2002. Information technology for Management. Transforming business in the digital economy. 3., uudistettu painos. New York: John Wiley & Sons.

Wun-Young, L.; Hirao, J.; Hirao, J.; Choi, M.; Cox, P. & Passer, L.S. 2008. SAP Security Configuration and Deployment. Burlington: Syngress.

TIETOSUOJATYÖRYHMÄ. 2003. Valmisteluasiakirja biotunnisteista. Viitattu 22.11.2012
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_fi.pdf

SAP-asiantuntijan haastattelu Espoossa 19.3.2012

Haastattelija: Aapo Sillanpää

Haastateltava: Olli-Pekka Lindström – SAP Finland

Paikka: SAP-Finland Oy, Espoo

SAP NetWeaver IDM yleisesti:

- Kerrotko lyhyesti NW IDM-ratkaisun tietoturvaominaisuuksista?
- Mitä hyötyjä NW IDM-järjestelmän käyttöönotosta olisi organisaatiolle?
- Miten käyttöönottoprojekti etenisi ja kuinka vaativa se olisi?
- Kertoisitko mitkä ovat NW IDM-ratkaisun ja SAP CUA-ratkaisun, suurimmat erot?
- Onko hyödyllistä käyttää molempia ratkaisuja (NW IDM. SAP CUA)?
- Mitkä ovat NW IDM-ratkaisun suurimmat heikkoudet/puutteet?

SAP CUA heikkoudet:

- Kerrotko lyhyesti SAP CUA-ratkaisun ominaisuuksista?
- Mitä hyötyjä SAP CUA voisi tarjota organisaatioille?
- Mitkä ovat SAP CUA-järjestelmän suurimmat heikkoudet/puutteet?

Haastattelu HK Ruokatalon SAP-käyttöoikeuksista vastaavan henkilön kanssa 25.10.2012

Haastattelija: Aapo Sillanpää

Haastateltava: Eija Sillanmäki

Paikka: HK Ruokatalo Oy

- Lähtötilanteen kartoitus, mitä ongelmia, haasteita, heikkouksia CUA:ssa oli? Eli minkä takia se tarvitsisi korvata?
- HK:n vaatimukset uudelle käyttäjähallintajärjestelmälle/palvelulle? Eli onko jonkinlaisia vaatimusmäärittely dokumenttia olemassa?
- Minkälainen uusi järjestelmä/palvelu on?
- Pystyisitkö vielä kertomaan miksi HK:n SAP käyttäjähallinta ulkoistettiin? Eli minkälaisia syitä taustalla oli esim. kustannussyyt, liian paljon aikaa vievää ym.
- Käyttääkö GRC Nordic etäkäyttönä HK:n CUA:ta vai onko heillä oma CUA käytössä?
- Voisitko lyhyesti kuvailla (sanallisesti tai kuva) käyttäjähallintaprosessin kulkua, siitä kuin uusi henkilö tulee HK:lle töihin ja hänelle luodaan SAP tunnukset, siihen asti kun hän lähtee yrityksen palveluksesta?