



TAMPEREEN
AMMATTIKORKEAKOULU

TUTKINTOTYÖRAPORTTI

KESKITETTY KÄYTTÄJÄTUNNUSTEN HALLINTA
Hallintasovelluksen määrittely ja kuvaus Metso Automationille

Tuomo Seppänen

Tietojenkäsittelyn koulutusohjelma
helmikuu 2006
Työn ohjaaja: Harri Hakonen

TAMPERE 2006



Tekijä(t)	Tuomo Seppänen	
Koulutusohjelma(t)	Tietojenkäsittely	
Tutkintotyön nimi	Keskitetty käyttäjätunnusten hallinta Hallintasovelluksen määrittely ja kuvaus Metso Automationille	
Työn valmistumis- kuukausi ja -vuosi	helmikuu 2006	
Työn ohjaaja	Harri Hakonen	Sivumäärä: 35

TIIVISTELMÄ

Käyttäjätunnusten ja identiteetin hallinta on viime vuosina herättänyt tietotekniikka-alalla runsaasti keskustelua. Ohjelmistovalmistajat ovat kilpaa tuoneet markkinoille identiteetin hallintaan soveltuvia tuotteita ja yrityksetkin ovat havahtuneet reagoimaan asiaan. Tehokkaalla käyttäjätunnusten hallinnalla yritys voi saavuttaa sekä tiukemman tietoturvan että taloudellista säästöä.

Metsolla oli alun perin tarkoituksena toteuttaa koko konsernin laajuinen sovellus keskitettyä käyttäjätunnusten hallintaa varten. Tämän hankkeen viivästyttyä päätettiin Metso Automationilla toteuttaa oma sovellus. Työssä esitellään keskitettyyn käyttäjätunnusten hallintaan liittyviä yleisiä asioita, määritellään Metso Automationin hallintasovellukselta vaatimat toiminnallisuudet sekä kuvataan toteutettu sovellus. Sovellus käsittelee ainoastaan käyttäjätunnustietoja, ei salasanoja. Tämä tutkintotyö on tehty toimeksiantona Metso Automationille.

Aiheen laajuuden vuoksi työssä on keskitytty Metso Automationin projektin kannalta tärkeisiin asioihin. Samasta syystä työssä ei ole esitelty kaupallisten tuotteiden ominaisuuksia, vaikka se mielenkiintoista olisi ollutkin.

Sovellus saatiin käyttöön suunnitellussa aikataulussa, ja se on osoittautunut toimivaksi ja hyödylliseksi. Sen kehittäminen tulee kuitenkin jatkumaan, sillä toistaiseksi sovellus on aktiivisesti käytössä vain Tampereen toimipisteessä. Tarkoitus on laajentaa käyttö kattamaan ainakin Metso Automationin kaikki Suomen toimipisteet.



Author(s)	Tuomo Seppänen	
Degree Programme(s)	Business Information Systems	
Title	Centralized user account management Specification and description of management software for Metso Automation	
Month and year	February 2006	
Supervisor	Harri Hakonen	Pages: 35

ABSTRACT

User account and identity management have raised a lot of discussion on IT-sector during last couple of years. Software companies have raced to the market with their identity management products and customers have become more aware of the subject. Companies can achieve both tighter security and financial savings with efficient user account management.

Originally Metso was going to implement concern wide application for centralized user management. This project was delayed and Metso Automation decided to implement its own application. This final thesis details general matter concerning centralized user account management, defines requirements of the application and describes implemented application. The application manages only user account information, not passwords.

Because the subject is so extensive, this final thesis is focused on matters that are important for Metso Automation's project. For the same reason, the thesis doesn't present the features of commercial products, even though it would have been interesting.

Application was implemented in planned schedule and it has proven to be working and useful. The development will however continue. At the moment the application is actively in use at Tampere office. The plan is to implement the application at least to all Metso Automation's Finland offices.

Sisällysluettelo

1	JOHDANTO	5
2	METSO	6
2.1	YRITYKSEN ESITTELY (METSO CORPORATION 2005)	6
2.2	METSON TIETOTEKNINEN YMPÄRISTÖ	6
3	TAUSTAA	8
3.1	MITÄ KESKITETTY KÄYTTÄJÄTUNNUSTEN HALLINTA TARKOITTAAN?	8
3.2	MIKSI KESKITETTY KÄYTTÄJÄTUNNUSTEN HALLINTA?	10
3.3	TAUSTAA METSON PROJEKTISTA	11
3.4	KÄYTTÄJÄHALLINNON LÄHTÖTILANNE	12
4	SOVELLUKSEN VAATIMUKSET	15
4.1	YLEISET VAATIMUKSET	15
4.2	TOIMINNALLISET VAATIMUKSET	15
4.3	SOVELLUKSEN KÄYTTÖTASOT	16
4.4	TAVOITEPROSESSI	17
4.5	NÄKYMÄT	18
4.6	RAJOITUKSET	18
5	SOVELLUKSEN KUVAUS	20
5.1	YLEISTÄ	20
5.2	YLEISKUVAUS	20
5.3	PROSESSIKUVAUS	21
5.4	SOVELLUKSEN OSAT	22
5.4.1	Järjestelmät	23
5.4.2	SQL Server	23
5.4.3	NotesSQL	24
5.4.4	Käyttäjätunnustietokanta (MASA).....	25
5.4.5	Työprosessien hallintakanta (MAINT)	27
6	KÄYTTÖÖNOTTO	30
7	SOVELLUKSEN JATKOKEHITYS	31
8	TYÖN ARVIOINTI	33
9	LÄHTEET	34
10	LIITTEET	35

1 Johdanto

Alun perin tutkintotyöni piti käsitellä Metsossa vuoden 2004 syksyllä käynnistynyttä projektia. Sen tarkoituksena oli toteuttaa Metso-konsernin laajuinen sovellus keskitettyä käyttäjähallintoa varten. Sovellukselle määriteltiin kaksi pääasiallista käyttötarkoitusta. Ensiksi sen kautta piti olla mahdollista tehdä tilauksia, muutoksia ja poistoja eri järjestelmien käyttäjätunnuksiin. Sovelluksen piti pystyä käsittelemään näiden pyyntöjen työprosessi. Toiseksi sen piti toimia tietokantana, josta pystytään tarkistamaan reaaliaikainen tilanne eri järjestelmissä olevista käyttäjätunnuksista tai hakemaan tieto, mihin järjestelmiin tietyllä henkilöllä on tunnukset. Hanke todettiin niin laajaksi, että sen toteuttaminen viivästyi toistaiseksi.

Tulossa olevan Sarbanes-Oxley –tietoturva-auditoinnin tarpeiden pohjalta Tampereen Metso Automationilla päätettiin toteuttaa oma Lotus Notes -pohjainen käyttäjätunnusten hallintasovellus. Näin saatiin tiedot käyttäjätunnuksista kerättyä keskitetysti yhteen paikkaan sekä luotua selkeä toimintamalli tunnuspyyntöjen hallintaan.

Sain Metso Automationilta toimeksiannon tehdä sovelluksen tärkeimmistä ominaisuuksista vaatimusmäärittelyn, osallistua toteutukseen sekä kuvata toteutuvaa järjestelmää. Tarkoituksena on saada aikaan Tampereella toimiva ratkaisu, josta tiedot voidaan viedä myöhemmässä vaiheessa mahdollisesti toteutuvaan konsernitaseiseen sovellukseen tai laajentaa sovelluksen käyttöä konsernissa.

Tässä työssä esitellään lyhyesti Metson projekti tähän saakka, annetaan tärkeimpien vaatimusten avulla kuva siitä, mitä toiminnallisuuksia sovellukselta toivotaan sekä kuvataan toteutuneen sovelluksen toiminta.

2 Metso

2.1 Yrityksen esittely (*Metso Corporation 2005*)

Metso on kansainvälinen teknologiakonserni, joka toimittaa prosessiteollisuuden koneiden ja järjestelmien huolto- sekä asiantuntija-palveluita. Asiakkaina ovat lähinnä paperi- ja selluteollisuus, kiven ja mineraalien käsittelylaitokset, energia- ja prosessiteollisuus sekä levyteollisuus.

Metso syntyi tammikuun lopulla 1999, kun Rauma- ja Valmet-konsernit fuusioituivat. Metsoon kuuluu neljä eri liiketoiminta-alueita:

- Metso Paper, joka on maailman johtavia paperi-, kartonki- ja seluvalmistuslinjojen toimittajia.
- Metso Automation, joka toimittaa kone- ja prosessiautomaatio- sekä säätöteknologiaratkaisuja pääasiassa sellu-, paperi- ja energia- ja prosessiteollisuudelle.
- Metso Minerals, joka on erikoistunut kiven- ja materiaalienkäsittelyjärjestelmien sekä murskainten toteuttamiseen louhoksille, kaivos- ja maanrakennusteollisuudelle sekä murskeentuottajille.
- Metso Ventures, jonka alla toimivat
 - Metso Panelboard, levyteollisuuden (kuitu-, lastu- ja OSB-levyt) tuotantolinjat, laitteet ja huollot
 - Metso Powderment, pulverimetallurgiaan perustuva materiaalteknologia sekä komponenttien suunnittelu
 - Metson valimot, rauta- ja teräsvalutut komponentit
 - Valmet Automotive, erikoisautojen sopimusvalmistus

Konserni työllistää yli 50 maassa yhteensä n. 22000 henkilöä, joista lähes 40 % on Suomessa. Sen liikevaihto vuonna 2004 oli n. 4 miljardia euroa.

Metso Automation syntyi vuoden 1999 fuusiossa, kun Valmet Automation ja Neles Controls yhdistettiin. Sillä on palveluksessaan 36 maassa yhteensä noin 3300 työntekijää.

2.2 Metson tietotekninen ympäristö

Konsernitasolla tietotekniikkaa ohjaa Metso IT Shared Services. Se on yksikkö, joka tuottaa tietotekniikkapalveluja kaikille liiketoiminta-alueille, vastaa Metson verkkorakenteesta sekä kehittää käyttöönotettavia tietoteknisiä ratkaisuja.

Tämän lisäksi jokaisella liiketoiminta-alueella on oma pienehkö tietotekniikkahenkilöstönsä, joka vastaa tietotekniikan käytännön tarpeista, kuten

laitehankinnoista, omassa organisaatiossaan. Varsinainen käyttäjätuki on ulkoistettu.

Tampereen Metso Automationilla päätoimisissa tietotekniikkatehtävissä työskentelee viisi omaa henkilöä sekä seitsemän henkilöä ulkoistetussa käyttäjätuessa. Oman henkilöstön ylläpitoon kuuluvat mm. toiminnanohjausjärjestelmä, Lotus Notes-, sekä tietoturva-asiat. Loppukäyttäjien työasematuen hoitaa ulkoistettu yhteistyökumppani.

Metsossa on maailmanlaajuisessa käytössä Windows Active Directory, johon työasemien toiminta perustuu. Metson Active Directory on jaettu viiteen eri toimialueeseen geologisten alueiden mukaan ja sen jokapäiväinen hallinta on hajautettu paikallisille IT-organisaatioille. Suuremmat muutokset tekee Metso IT.

Toinen suuri tekninen ympäristö Metsossa on Lotus Notes. Lotus Notes on monipuolinen työryhmä-ohjelmisto. Se sisältää sähköpostin, LDAP-pohjaisen osoitekirjan sekä tekstipohjaisia dokumenttitietokantoja. Tietokannat pystytään myös julkaisemaan suoraan www-sivuiksi. Tietokannat eivät ole varsinaisesti relaatiotietokantoja, mutta niitä pystytään lukemaan peilaamalla ne relaatiopohjaisiksi NotesSQL-ohjelman avulla, jolloin niihin voidaan tehdä kyselyitä SQL-kielillä.

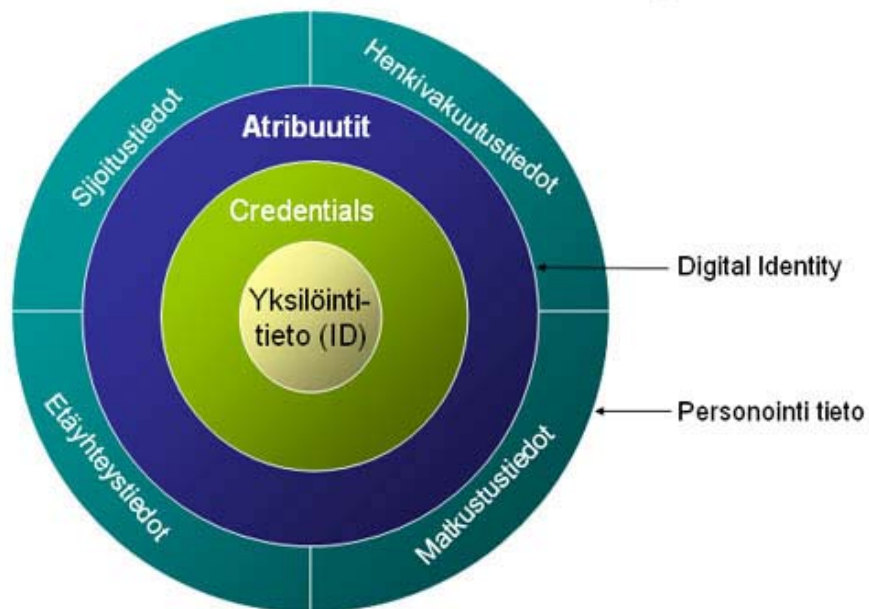
Koko Metso-konsernissa on käytössä Lotus Notesin sähköposti. Notesissa on myös huomattava määrä liiketoimintaa tukevia sovelluksia. Lähes jokaisella projektilla on oma Notes-kantansa projektin työryhmän tiedonvälitykseen ja dokumentointiin. Kokonaisuudessaan aktiivisten Notes-kantojen lukumäärä on tuhansia. Notesin käyttöön on sitouduttu koko konsernissa hyvin vahvasti.

Näiden lisäksi liiketoiminta-alueilla on käytössä yhteensä kymmeniä eri tarkoituksiin käytettyjä, yleensä tietokantapohjaisia järjestelmiä, joiden tunnukset halutaan saada mukaan keskitetyn järjestelmän piiriin. Tampereen Metso Automationilla tällaisia järjestelmiä on hieman toistakymmentä. Näihin kuuluvat muun muassa henkilöstöhallinta-, toiminnanohjaus-, palkkahallinta-, matkalasku- sekä kulunvalvontajärjestelmät.

3 Taustaa

3.1 Mitä keskitetty käyttäjätunnusten hallinta tarkoittaa?

Keskitetyn käyttäjätunnusten hallinnan määrittely tuntuu käyvän sitä vaikeammaksi, mitä enemmän aiheeseen tutustuu. Useissa tilanteissa puhutaan digitaalisen identiteetin hallinnasta. Digitaalinen identiteetti tarkoittaa kokonaisuutta, joka käsittää identiteetin yksilöivän tunnisteiden (ID) sekä sille kuuluvia oikeuksia (credentials) ja attribuutteja (Kuvio 1). Tällöin tietyn järjestelmän käyttäjätunnus on osa sen omaavan henkilön digitaalista identiteettiä. Valitsin tähän työhön termiksi käytännönläheisemmän käyttäjätunnusten hallinnan. (Lehmus 2005.)



Kuvio1 Digitaalinen identiteetti (Lehmus 2005)

Keskitetty käyttäjätunnusten hallinta voidaan katsoa kokonaisuudeksi, joka muodostuu yrityksen prosesseista, menettelytavoista ja teknologiasta. Näiden avulla hallitaan käyttäjien pääsyä yrityksen eri resursseihin ja estetään luvaton pääsy luottamuksellisiin tietoihin. Karkeasti ottaen keskitettyyn käyttäjätunnusten hallintaan kuuluu ainakin kaksi pääelementtiä: suunniteltu prosessi siitä, miten käyttäjätunnusten muutoksia tehdään ja sovellus, josta löytyvät tiedot kunkin käyttäjän olemassa olevista tunnuksista. (Microsoft Identity...2004.)

Prosessissa määritellään, ketkä saavat tilata uusia tunnuksia ja tehdä muutos- ja poistopyyntöjä. Siihen kuuluvat myös pyyntöjen hyväksymismenettely, viestin kulku toteuttajille, tehtyjen muutosten kuittaustapa sekä ilmoitus toteutuneesta muutoksesta pyytäjälle. Toimintatapa on saatava niin toimivaksi, että kaikki noudattavat sitä. Jos prosessia ei noudateta, hyvin-

kin toteutettu sovellus jää nopeasti käyttökelvottomaksi, kun se ei pysy ajan tasalla.

Sovellukseen kuuluu myös käyttäjätunnustietokanta, josta löytyvät vähintään käyttäjän perustiedot sekä tieto hänelle myönnettyistä käyttäjätunnuksista. Laajemmissa toteutuksissa tietokannassa voi olla hyvinkin paljon tietoa käyttäjistä kuten puhelinnumero, kustannuspaikka, autentikointitietoja, sekä roolit, jotka käyttäjällä on eri järjestelmissä.

Perinteisesti jokaisella tietojärjestelmällä on oma tietokantansa, jossa säilytetään tieto kyseisen järjestelmän käyttäjistä ja salasanoista. Tämän mallin ongelmana on se, että yleensä mistään ei löydy keskitettyä tietoa siitä, mihin järjestelmiin kenelläkin on oikeus. Tällöin kaikkien tunnusten poistaminen käyttäjän lähtiessä on käytännössä hyvin vaikeaa varsinkin suuremmissa yrityksissä, joissa saattaa olla kymmeniä eri järjestelmiä. Lisäksi eri järjestelmiä hallinnoi yleensä eri henkilö. Tällöin jo yrityksen työntekijöiden normaali vaihtuminen aiheuttaa vuodessa suuren määrän tunnusten hallintaan liittyvää työtä useille eri ihmisille. (Microsoft Identity...2004.)

Keskitetyssä mallissa yrityksessä on käytössä keskitetty käyttäjätietokanta, josta kaikkien käyttäjien tunnukset löytyvät. Tämä mahdollistaa käyttäjän tunnusten nopean poiston. Useat sovellukset mahdollistavat myös käyttäjätunnusten automaattisen luonnin, provisioinnin, tietyn tapahtuman laukaisemana. Jos esimerkiksi henkilöstöhallintajärjestelmään luodaan uusi henkilö, voidaan hänelle automaattisesti luoda sähköpostiosoite ja verkkokäyttäjätunnus. Pidemmälle vietyinä tämä mahdollistaa myös single sign-on -ominaisuuden. Tällöin käyttäjä autentikoidaan hänen kirjautuessaan työasemalle ja hän pääsee suoraan, ilman erillisiä tunnuksia ja salasanoja, käyttämään kaikkia järjestelmiä, joihin hänelle on myönnetty oikeudet. (Microsoft Identity...2004.)

On huomion arvoista, että keskitetyn käyttäjätunnusten hallinnan käyttöönotto yrityksessä ei ole suinkaan pelkästään tietotekninen projekti. Itse asiassa tekninen toteutus on helpoin osa projektista. Hankalampaa on luoda toimiva työprosessi tunnusten tilauspyyntöjä ja niiden toteutusta varten sekä saada tämä työprosessi ajettua läpi organisaatiossa. Ihmiset ovat luonnostaan konservatiivisia ja muutosvastarintaa on aina.

Keskitettyyn käyttäjätunnusten hallintaan tarkoitettuja sovelluksia alkaa löytyä yhä enemmän markkinoilta. Ominaisuuksiltaan sovellukset ovat nykyään hyvin monipuolisia ja kirjavia. Tärkeää onkin löytää parhaiten yrityksen tarkoitukseen soveltuva ohjelmisto. Olennaista on mieltä valmiiksi, minkälaisia järjestelmiä sovelluksen piiriin halutaan ja halutaanko saman sovelluksen pystyvän toteuttamaan myös työpyyntöjen hallinta.

3.2 Miksi keskitetty käyttäjätunnusten hallinta?

Keskitetyn käyttäjätunnusten hallinnan edut ovat kiistattomia, mutta niitä on usein vaikea perustella liiketoiminnallisin lähtökohdin. Kyse on yleensä tietoturvasta ja taloudellisen hyödyn laskeminen sille voi olla hankalaa. Taloudellista etua voidaan saada siitä, että joidenkin järjestelmien tunnukset aiheuttavat kuluja. Ainakin ulkoa hankitut etäyhteys- tai muiden järjestelmien tunnukset maksavat yritykselle. Samoin yrityksen sisäisiä IT-kuluja, ainakin suuremmissa yrityksissä, saatetaan jyvittää esimerkiksi sähköpostitunnusten perusteella eri osastoille. Kun ylimääräiset tunnukset saadaan karsittua, saadaan myös taloudellista säästöä.

Pääasiallinen peruste sovelluksen toteuttamiselle on yleensä kuitenkin tietoturvan parantaminen. Uusien käyttäjien tunnukset tulevat kyllä yleensä luoduiksi, siitä pitää huolen itse käyttäjä tai hänen esimiehensä. Järjestelmiä kun ei pääse käyttämään ilman tunnuksia. Vaikka tunnusten poistaminen käyttäjän lähtiessä onkin vähintään yhtä tärkeä osa prosessia, siitä ei välttämättä tule ollenkaan tietoa tietohallintoon. Käyttäjätunnusten hallinnan tehostaminen lisää automaattisesti tietoturvaa. Sovelluksen ja etenkin toimintamallien ollessa kunnossa saadaan poistuvien käyttäjien tunnukset nopeasti ja tehokkaasti pois käytöstä. Tällöin riski avoimiksi jääneiden tunnusten väärinkäytöstä poistuu. (Microsoft Identity...2004.)

Oma lukunsa ovat partneri-käyttäjät. Nämä ovat konsultteja tai muita yhteistyökumppaneita, jotka eivät ole yrityksen palkkalistoilla, mutta kuitenkin toimivat yrityksen toimitiloissa ja tarvitsevat yhteydet yrityksen verkkoon tai muihin järjestelmiin. Nämä henkilöt vaihtuvat tiheään ja muodostavat potentiaalisen tietoturvauhan. Partnereille ei yleensä anneta samoja oikeuksia kuin omille työntekijöille. Tämän lisäksi heidän tunnuksiaan tulisi seurata tarkemmin. Hyvä käytäntö on antaa heille määräaikaisten tunnuksien, jotka lakkaavat toimimasta tietyn ajan kuluttua, ellei niiden voimassaoloa uusita.

Keskitetyn käyttäjätunnustenhallintasovellusten avulla voidaan myös automatisoida tunnusten hallintaa. Puhutaan käyttäjätunnusten provisioinnista ja deprovisioinnista. Nämä tarkoittavat tunnusten automaattista luontia tai poistoa tiettyjen ennalta luotujen sääntöjen mukaisesti. On mahdollista valita jokin pääjärjestelmä. Usein pääjärjestelmänä toimii henkilöstöhallintajärjestelmä. Kun uusi henkilö kirjataan pääjärjestelmään, luodaan hänelle määriteltyjen sääntöjen mukaan, automaattisesti tunnukset haluttuihin järjestelmiin. Näin saadaan vähennettyä pääkäyttäjien kuormaa tunnusten tekemisessä sekä vähennettyä inhimillisten virheiden määrää tunnusten luonnissa. (Microsoft Identity...2004.)

Tutkimuksesta riippuen noin 15 - 25 % helpdeskiin tulevista puheluista koskee salasanoja. Eri sovellusten avulla on mahdollista toteuttaa käyttäjille palvelu, jonka kautta he pystyvät itse palauttamaan salasanansa. To-

teutustavat voivat vaihdella henkilökohtaisista kysymyksistä puhetunnistukseen. Tällaisen toteutuksen avulla on suurissa yrityksissä mahdollista huomattavasti vähentää helpdeskiin tulevia puheluita.

Monet tietoturvastandardit tai muut säännökset vaativat käyttäjätunnusten hallinnan kunnossa olemista. Ei siis välttämättä ole kyse yrityksen halusta toteuttaa tarvittava sovellus, vaan lain tai määräyksen noudattamisesta. Yhdysvalloissa toimivien pörssiyhtiöiden tulee täyttää Sarbanes-Oxley -lain (SOX) määräykset. Sarbanes-Oxley on Yhdysvalloissa vuonna 2002 voimaan saatettu laki, jonka tarkoituksena on sijoittajien luottamuksen palauttaminen yrityksiin sekä yritysten taloudellisen raportoinnin luotettavuuden parantaminen. Laki koskee kaikkia yrityksiä, joiden osakkeita on listattuna Yhdysvaltain arvopaperimarkkinoita valvovan SEC:in alaisissa pörsseissä. Pääasiassa Sarbanes-Oxley on taloushallintoa koskeva laki, mutta koska kaikki taloushallinnon järjestelmätkin toimivat tietokoneilla, on laissa myös tietotekniikkaa koskevia asioita. Tietohallinnon kannalta tärkeintä on juuri käyttäjätunnusten tarkka hallinta sekä eri järjestelmien valvonnan kunnossa oleminen. Tämä takaa sen, että tiedetään tarkkaan, kenellä on pääsy mihinkin järjestelmiin. Valvonnan kautta on mahdollista jälkikäteenkin tarkistaa, kuka on tehnyt mitä, milloin ja missä järjestelmässä. (Lindh 2004.)

Nykyisessä dynaamisessa työelämässä myös yritysten uudelleenjärjestelyt aiheuttavat haasteita tietohallinnolle. Järjestelmien ja käyttäjätunnusten yhtenäistäminen yritysostojen tai fuusioiden jälkeen on työlästä. Se, että käyttäjätunnusten hallinta on ajan tasalla, helpottaa kahden organisaation järjestelmien yhdistämistä ja lyhentää yhdistämiseen kuluva aikaa. Tällöin saadaan uuden organisaation työntekijöille mahdollisimman nopeasti oikean tasoiset käyttöoikeudet. Lisäksi on helpompaa tunnistaa tarpeettomat käyttäjätunnukset ja hallintaprosessit sekä poistaa ne käytöstä. (Microsoft Identity...2004.)

3.3 Taustaa Metson projektista

Vuoden 2004 syksyllä Tampereen Metso Automationilla alettiin suunnitella käyttäjätunnussovelluksen toteuttamista ja käyttöönottoa. Koska Metso Paperilla Jyväskylässä oli toteutettuna Lotus Notes -pohjainen sovellus, päätettiin tutustua siihen ja tutkia, olisiko mahdollista ottaa siitä mallia tai jopa kopioida ja muokata kyseinen sovellus Automationille. Kuultuaan tästä muutkin liiketoimintayksiköt kiinnostuivat aiheesta. Tällöin sovittiin yhteinen tapaaminen ja alettiin selvittää, olisiko mahdollista toteuttaa koko konserni-tasoinen tunnustenhallintajärjestelmä.

Nopeasti selvisi, että Metso Paperin sovelluksen ominaisuudet eivät riittäneet konsernitasoisiksi työkaluksi. Sovellus oli toteutettu alun perin omana työnä ja siinä oli liikaa sovelluksen sisään ohjelmoituja asioita. Uuden järjestelmän lisääminen sovelluksen piiriin oli melko työlästä ja sovellus oli

suunniteltu nimenomaan Metso Paperin käyttöön. Lisäksi Lotus Notes toteutus-
alustana ei olisi pystynyt käsittelemään koko konsernitason tarvittavia tietomääriä.

Tällöin perustettiin työryhmä, jonka tarkoituksena oli kartoittaa eri liiketoimintayksiköiden tarpeet ja vaatimukset sekä luoda näiden pohjalta vaatimusmäärittely sovellukselle. Ryhmään kuului henkilöitä eri liiketoiminta-alueilta ja sitä koordinoi Metso IT. Se kokoontui muutaman kerran ja sai muodostettua alustavan listan vaatimuksista sekä tutustuttua muutamaa tuote-esittelyyn. Alkuvuodesta 2005 projekti kuitenkin hautautui eikä tapaamisia kutsuttu kokoon. Päälimmäisinä syinä olivat havainto hankkeen laajuudesta ja monimutkaisuudesta sekä resurssien vähyys. Työryhmän keräämät vaatimukset ja toivomukset eri tahoilta olivat moninaisia ja jopa ristiriitaisia. Eri tahoilla oli hyvinkin erilaiset odotukset sovellukselta eikä Metso IT:llä ollut tarvittavia resursseja hankkeen vetämiseksi tuolla hetkellä. Hanke hautautui syksyyn saakka.

Alkusuksystä 2005 Metso IT päätti, että konsernitason käyttäjätunnussovelluksen toteutusta siirretään toistaiseksi. Metso Automation tietohallinto Tampereella päätti tällöin toteuttaa oman sovelluksensa. Tampereen oman tietohallinnon henkilöt alkoivat kehittää pikkuhiljaa Lotus Notes - pohjaista sovellusta. Tällöin tehtäväkseni jäi laatia sovelluksesta karkeahko vaatimusmäärittely, olla mukana toteutusta suunnittelemassa sekä laatia kuvaus sovelluksen toiminnasta.

3.4 Käyttäjähallinnon lähtötilanne

Nykyisen Metso-konsernin taustalla on sekä valtiojohtoisia että yksityissektorin yrityksiä. Näiden yhdistymisen seurauksena toimintamallit eri liiketoimintayksiköissä ovat olleet hyvin erilaisia. Tätä ei myöskään ole helpottanut se, että liiketoimintayksiköiden välinen yhteistyö ei ole aiemmin ollut kovin tiivistä. Vasta aivan viime vuosien aikana yhteistyö varsinkin tietotekniikan alueella on kasvanut konsernin käynnistäessä laajan tietoteknisten ratkaisujen yhtenäistämiskampanjan.

Metsolla ei varsinaisesti ole keskitettyä käyttäjätunnusten hallintaa. Kuitenkin koko konsernille yhteisiin tietojärjestelmiin kuten Lotus Notes - sähköpostiin ja etäyhteyksien ratkaisuihin, tunnukset tilataan yhteisen Notes-pohjaisen sovelluksen kautta. Järjestelmä toimii kuitenkin enemmän työpyyntöjenhallintajärjestelmänä kuin käyttäjätunnusten säilyttämisessä. Kunkin liiketoimintayksikön omiin järjestelmiin tunnuksia pyydetessä toimintamallit vaihtelevat melkoisesti.

Metso Paperilla on käytössään itse kehitelty Notes-sovellus käyttäjätunnusten hallintaan. Tietotekniikkatukihenkilöt voivat kirjata järjestelmään tunnuspyyntöjä. Tehty pyyntö tarkastetaan tietohallinnon toimesta ja tarkistuksen jälkeen se ohjautuu järjestelmäkohtaisesti pääkäyttäjälle. Hän

tekee pyydetyn muutoksen ja kuittaa sen tietohallinnolle tehdyksi. Tietohallinto merkitsee sovellukseen tunnuksen tehdyksi, jolloin pyynnön tekijälle lähtee viesti tunnuksesta. Sovelluksesta löytyvät tiedot käyttäjillä olevista tunnuksista sekä tunnuspyyntöjen suorituksista. Tietotekniikkatukihenkilö hoitaa osastonsa tietotekniikkaan liittyviä asioita sekä toimii tietohallinnon ja oman osastonsa tiedonvälittäjänä. Näitä henkilöitä Metso Paperilla on jokaisella osastolla ja he hoitavat roolinsa oman työnsä ohella. Tämän on osoittautunut varsin toimivaksi käytännöksi.

Metso Paperin sovellus on toimiva yrityksen omassa ympäristössä. Sovelluksen heikkoutena on sen tekotapa. Sitä ei alun perin ole suunniteltu modulaarisesti ja sen muokkaaminen nykyisestäään on hankalaa. Uuden järjestelmän lisääminen sovelluksen piiriin vaatii paljon työtä.

Metso Mineralsilla tunnuspyynnöt hoidetaan myös Notes-sovelluksen kautta. Saman sovelluksen kautta tehdään myös uusien ohjelmistojen asennuspyynnöt. Sovellus toimii ainoastaan työprosessin hallintatyökaluna. Suoritetuista töistä jää järjestelmään historiatieto, mutta sen kautta ei voida nähdä kenellä on tunnus mihinkin järjestelmään. Sovelluksesta ei lähde viestejä tai kuittauksia automaattisesti kenellekään, vaan sitä on seurattava aktiivisesti.

Kuka tahansa voi tehdä sovellukseen pyynnön tunnuksista tai ohjelmistotasenuksesta. Yleensä pyynnön kuitenkin tekee esimies. Tietohallinto tarkistaa pyynnöt, minkä jälkeen ne ohjautuvat toteutettavaksi joko tietohallinnon omille henkilöille tai ulkoistetulle lähituella. Työn suorituksen jälkeen tekijä kuittaa sen sovellukseen tehdyksi.

Metso Automationilla ei toistaiseksi ole käyttäjätunnushallintaan tarkoitettua sovellusta. Eri toimipisteiden välillä on eroa toimintatavassa. Helsingin toimipisteessä on ollut käytössä Excel-pohjainen lomake, jolla esimiehet ovat tehneet tunnusten hallintaan liittyviä pyyntöjä. He ovat lähettäneet lomakkeen tukihenkilöille, jotka ovat tarkastaneet määritellyltä listalta, että kyseinen henkilö saa pyyntöjä tehdä.

Tampereen toimipisteessä tunnusten luonti on tapahtunut omalla painollaan. Toisin sanoen käyttäjän tarvitessa tunnukset järjestelmään, hän itse tai hänen esimiehensä ottaa yhteyttä järjestelmän pääkäyttäjään. Osa tunnuspyynnöistä kulkee Metson helpdeskin kautta, joka ohjaa pyynnöt järjestelmien pääkäyttäjille. Käyttäjän poistuessa talosta hänen on täytynyt kuitata tunnukset poistetuiksi sähköpostitse kulkevalla lomakkeella ennen lopputilin maksamista.

Metso Automationilla on lisäksi jatkuvasti useita kymmeniä partnerikäyttäjiä. Yritys käyttää paljon konsultteja projekteissaan. Samat henkilöt käyvät vuosien varrella tekemässä useita projekteja ollen välillä poissa, välillä paikalla. Heidän tunnuksensa pitäisi saada tarkempaan seurantaan. On mahdollista, että partnerin poistuessa talosta, hänen tunnuksiaan ei olekaan poistettu. Partnerien tunnukset ovat kuitenkin järjestelmissä pää-

asiassa määräaikaista ja menevät siten lukitus-tilaan, jos tunnuksia ei vähään aikaan käytetä. Se, että tunnuksia saattaa jäädä poistamatta johtuu yleensä siitä, ettei tietohallinto ole saanut tietoa partnerin lähdöstä. Tämä osoittaa sen, että tunnusten hallintaan täytyy olla olemassa selkeä prosessi, jota kaikki noudattavat. Metso Automationille uusi selkeä prosessi tullaan ottamaan käyttöön tämän käyttäjätunnussovelluksen käyttöönoton yhteydessä. Prosessi lanseerataan henkilöstöhallinto-osaston toimesta yhteistyössä tietohallinnon kanssa.

4 Sovelluksen vaatimukset

4.1 Yleiset vaatimukset

Tämä määrittely koskee Metso Automation Tampereelle suunnitella olevaa keskitettyä käyttäjätunnusten hallintasovellusta.

Sovelluksella tullaan hallitsemaan käyttäjätunnukset eri tietojärjestelmiin. Sillä hallitaan tunnusten pyyntöön ja käsittelyyn liittyvä työnkulku sekä nähdään jatkuvasti ajantasainen tieto siitä, mitä käyttäjätunnuksia kullakin henkilöllä on. Aluksi sovelluksen piiriin halutaan liittää seuraavat järjestelmät:

- Active Directory
- Aton (Product data management)
- Lean (toiminnanohjausjärjestelmä)
- TietoPersona HR (Henkilöstöhallintajärjestelmä)
- Lotus Notes (sähköposti / työryhmäohjelmisto)
- Etäyhteystunnukset (VPN, dial-up, Global Internet Access)

Sovelluksessa tulee olla järjestelmäkohtaisesti mahdollista määritellä lisätietokenttiä, jotka tunnusten tilaajan on täytettävä. Jatkossa sovellukseen on pystyttävä helposti lisäämään uusia järjestelmiä. Sovelluksen pääkäyttäjän tulee pystyä tekemään uuden järjestelmän lisääminen. Käyttökielen tulee olla englanti. Toteutuslueksi halutaan joko Lotus Notes- tai www-pohjainen sovellus.

4.2 Toiminnalliset vaatimukset

Käyttäjiä sovelluksen piiriin on alkuvaiheessa tulossa noin 1500. Sovelluksen on pystyttävä huolehtimaan kyseisen käyttäjämäärän tunnuksista sekä hoitamaan tunnustilausten työprosessi ja ylläpitämään historiatieto tunnusten tilauksista. Sovelluksesta tulee löytyä ainakin seuraavat tiedot jokaisesta sen piirissä olevasta käyttäjästä:

- Henkilönumero tai muu yksilöivä tieto
- Etunimi
- Sukunimi
- Sähköposti
- Yritys
- Kustannuspaikka
- Esimies

- Työsuhteen päättymispäivä sekä määräaikailla että partnerikäyttäjillä
- Tieto kaikista järjestelmistä, joihin käyttäjällä on käyttäjätunnus. Salasanaja ei tallenneta sovellukseen.

Käyttäjätunnusten hallintaan kuuluu tunnusten luominen, muuttaminen ja poistaminen. Tarkoitus on, että uudelle käyttäjälle pystytään tilaamaan tunnukset kaikkiin tarvittaviin järjestelmiin kerralla yhden lomakkeen kautta. Kunkin järjestelmän osalta sovellukseen pitää kuitenkin kirjautua oma pyyntönsä, joka voidaan ohjata kyseisen sovelluksen pääkäyttäjälle. Olemassa olevalle käyttäjälle on pystyttävä tilaamaan tunnuksia uusiin järjestelmiin, tekemään muutospyyntöjä sekä poistamaan tunnuksia. Käyttäjän poistuessa yrityksestä on hänen kaikki tunnuksensa pystyttävä poistamaan yhdellä pyynnöllä, josta lähtee viesti eri järjestelmien pääkäyttäjille.

Jokaisella työpyynnöllä tulee olla työvaiheen tila, jotta työn edistymistä on mahdollista seurata. Työn tila muuttuu aina, kun joku työprosessin varrella tekee jotakin pyynnölle. Sarbanes-Oxley määritysten mukaisen seurannan takia sovelluksesta tulee olla nähtävissä tunnuspyynnön tekijä, hyväksyjä ja toteuttaja sekä näiden tapahtumien ajankohdat. Tunnuspyyntöjen historia täytyy myös pystyä erikseen arkistomaan sen kasvaessa liian suureksi.

Suurena ongelmana nykyään ovat nimenomaan partnerikäyttäjät eli konsultit sekä muut yhteistyökumppanit. Siksi halutaan, että heidän tunnuksensa ovat voimassa tietyn määräajan kerrallaan. Ennen määräajan umpeutumista partnerin kontaktihenkilölle lähtee sovelluksesta viesti, johon vastaamalla tunnusten voimassaoloa jatketaan. Mikäli määräaika umpeutuu eikä lisäaikaa haeta, otetaan partnerin tunnukset automaattisesti pois käytöstä.

4.3 Sovelluksen käyttötasot

Lähtökohtana on, että kuka tahansa ei saa tilata tunnuksia. Tilausoikeudet ovat esimiehillä ja heidän nimeämillään sihteereillä tai muilla yhteyshenkilöillä. Tilausoikeuden omaavilla henkilöillä täytyy olla oikeantasoiset oikeudet sovellukseen. He pystyvät tekemään tilauksia, mutta eivät pysty esimerkiksi kuittaamaan tunnuksia tehdyksi.

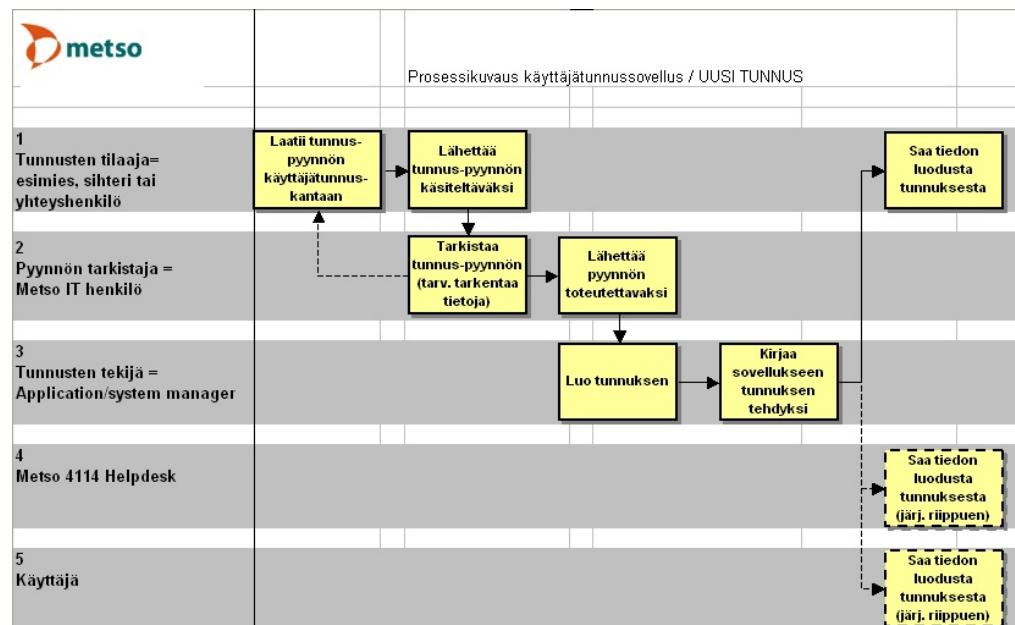
Tietohallinto-osaston nimetyillä henkilöillä tulee olla oikeus hyväksyä tai hylätä sovellukseen tehty pyyntö ennen kuin pääkäyttäjä luo tunnuksen. Heillä täytyy olla oikeudet nähdä muiden tekemät pyynnöt sekä hyväksyä ne toteutettavaksi tai tarvittaessa hylätä pyyntö.

Järjestelmien pääkäyttäjillä tulee olla oikeudet nähdä muiden tekemät pyynnöt ja kuitata järjestelmään luotu tunnus tehdyksi. Heillä saattaa myös tilanteesta riippuen olla oikeus tehdä tilauksia.

Lisäksi sovelluksessa täytyy olla pääkäyttäjiä, joilla on oikeus tehdä kaikki edellä mainittu sekä tehdä muutoksia sovelluksen asetuksiin. Pääkäyttäjän täytyy mm. pystyä muuttamaan muiden henkilöiden käyttöoikeuksia tähän sovellukseen ja tarvittaessa lisätä uusia järjestelmiä käyttöön.

4.4 Tavoiteprosessi

Pääsääntöisesti tunnuksia tilaavat esimiehet tai heidän valtuuttamansa yhteyshenkilöt. Uuden henkilön saapuessa heidän tulee tilata hänen tarvitsemansa tunnukset ja henkilön poistuessa tehdä välittömästi tunnusten poistopyyntö. Sovellukseen haetaan omien työntekijöiden henkilötiedot henkilöstöhallintajärjestelmästä. Konsulttien tai muiden yhteistyökumppanien henkilötiedot on syötettävä sovellukseen tilausta tehdessä. Työprosessi on lähes samanlainen sekä tunnuksia tilatessa että muutettaessa tai poistettaessa, joten tässä esitellään uusien tunnusten tilausprosessi (kuvio 2).



Kuvio 2 Prosessikuvaus tavoiteprosessista

Palkattaessa uutta henkilöä tuleva esimies ja henkilöstöhallinto toimivat yhteistyössä. Kun lopullinen päätös on tehty, kirjaa henkilöstöhallinto pal-kattavan tiedot henkilöstöhallintajärjestelmään. Kun tiedot ovat henkilöstöhallintajärjestelmässä, ne saadaan näkyviin tunnusten tilaussovellukseen ja työntekijälle voidaan tilata tunnuksia. Jos kyseessä on partneri, kirjataan hänen henkilötietonsa sovellukseen samalla, kun tilataan halutut tunnukset. Tunnuksen tilaaja täyttää tarvittavat tiedot sovellukseen ja lähettää tunnuspyynnön eteenpäin.

Sovelluksesta lähtee tieto tunnuspyynnöstä sähköpostilla tunnusten tarkistajalle, joka on Metson tietohallinnon henkilö. Viestissä on mukana linkki, joka avaa sovelluksen. Hän tarkastaa, että annetut tiedot ovat järkeviä ja ettei pyynnössä ole mitään omituista. Tarvittaessa tarkistaja on yhteydessä tunnuksen pyytäjään ja tarkentaa tietoja. Tämän jälkeen hän lähettää pyynnot toteutettavaksi.

Järjestelmän pääkäyttäjä saa ilmoituksen pyynnöstä sähköpostilla. Hän luo pyydytyt tunnukset ja kuittaa ne sovellukseen tehdyiksi. Tunnuksipyynnön luojalle lähtee tällöin viesti pyynnön toteutumisesta. Järjestelmästä ja tilanteesta riippuen viesti lähetetään myös käyttäjälle ja Metso4114-helpdeskiin, mikäli tunnuksen käyttöönotto edellyttää ohjelmiston asennusta. Itse käyttäjätunnus ja salasana toimitetaan myös tilanteesta riippuen joko käyttäjälle tai esimiehelle salatulla sähköpostiviestillä tai tekstiviestillä. Mikäli järjestelmän pääkäyttäjä ei reagoi tunnuksipyynnön tietyn ajan sisällä, lähetetään hänelle sovelluksen toimesta muistutusviesti tekemättömästä tunnuksesta.

4.5 Näkymät

Tietokannassa on yleensä ottaen paljon tietoa. Mikäli se kaikki yritetään näyttää kerralla, on siitä hyvin vaikea löytää etsimäänsä tietoa. Näkymällä tarkoitetaan valmiiksi määriteltyä hakua tietokannasta, joka tuo näkyviin vain halutun tiedon.

Sovellukseen halutaan ainakin seuraavat näkymät:

- Kaikki käyttäjät (kaikki käyttäjät ja käyttäjien tunnukset näkyvät)
- Määräaikaiset (kaikki määräaikaiset ja työsuhteen päättymispäivämäärät näkyvät)
- Partneri-tunnukset / Ulkopuoliset (kaikki ulkopuoliset käyttäjät ja työsuhteen päättymispäivämäärät näkyvät)
- Tunnukset poistettu (kaikki käyttäjät, joiden tunnukset on poistettu)
- Pyynnot (eri statuksittain eroteltuna / eri järjestelmittäin eroteltuna)
- Henkilöt esimiehittäin/yhteyshenkilöittäin

4.6 Rajoitukset

Sovelluksella ei tulla hallitsemaan järjestelmien sisäisiä oikeuksia kuten tuotannonohjausjärjestelmän rooleja tai Active Directoryn käyttäjäryhmiä. Järjestelmäkohtaisesti voidaan tehdä lisäkenttä, johon esimies voi kirjoittaa pääkäyttäjälle tiedoksi halutun roolin järjestelmän sisälle, mutta itse sovellus ei asiaan sen kummemmin puutu. Pääkäyttäjän tulee tarvittaessa selvittää minkälaiset oikeudet järjestelmän sisällä käyttäjälle kuuluvat.

Itse sovellukseen ei tehdä työnimikkeisiin perustuvia roolipohjaisia järjestelmäoletuksia. Tämä tarkoittaa sitä, että myyntipäälliköllä ei automaattisesti ole oikeuksia tiettyihin järjestelmiin, vaan kaikki on pyydettävä erikseen. Työnimikkeiden perusteella tehtävien oletusoikeuksien määrittely on niin vaikeaa, että siitä luovuttiin ainakin tässä vaiheessa. Se tarvitsisi kokonaan oman projektinsa.

5 Sovelluksen kuvaus

5.1 Yleistä

Tässä kappaleessa kuvataan toteutunut sovellus sellaisena kuin se on Metso Automationilla virallisesti käyttöön otettaessa.

Käyttäjätunnusten hallintasovellus toteutettiin Lotus Notes -alustalle. Notes valittiin, koska se on laajalti käytössä Metsossa ja Notes-osaamista löytyy paljon oman talon henkilöiltä. Näin sovellukseen tehtävät muutokset on jatkossa mahdollista toteuttaa omin voimin. Jos oman talon osaajien aika ei riitä, voidaan muutostyöt ostaa myös ulkopuolisilta tahoilta. Todettiin myös, että vastaavan kaltaisia sovelluksia on Metsossa jo valmiina, joten niistä voidaan saada pohjaa tämänkin sovelluksen toteutukseen. Myös kaupallisia sovelluksia harkittiin, mutta Notes todettiin sopivammaksi vaihtoehdoksi.

Sovellus täyttää pääpiirteittäin sille asetetut alustavat vaatimukset ja siihen tuli toteutuksen aikana myös lisää ominaisuuksia. Lisäksi tunnustentilausprosessi muovautui hieman toteutuksen aikana. Pääsyy tähän oli se, että sovellukseen haluttiin hieman lisää automatiikkaa.

Sovellus toteutettiin melko nopeasti, sillä sen pitää olla käytössä 1.1.2006 mennessä. Tämä on takaraja siihen, kun Metson tulee täyttää SOX-auditoinnin vaatimukset. Itse auditointi tapahtuu myöhemmin, mutta silloin täytyy olla mahdollista näyttää, että vaatimukset on täytetty 1.1.2006 lähtien. Auditointiin kuuluu, että taloushallinnon ohjelmien käyttäjätunnuspyynnöt on toteutettu ennalta suunnitellun toimintamallin mukaan ja että tunnuspyynnön eri vaiheista jää merkinnät siitä, kuka on toteuttanut ja koska.

Sovelluksen toteutus ja suunnittelu hoidettiin pääasiallisesti Metson oman tietotekniikkahenkilöstön voimin. Notes-kantojen ohjelmoinnissa käytettiin myös ulkopuolisen konsultin palveluja.

5.2 Yleiskuvaus

Sovelluksen avulla hoidetaan käyttäjätunnusten tilaukset, muutokset ja poistot Metso Automationin yleisimpiin järjestelmiin. Se sisältää sekä tilausten vaatiman työprosessin hallinnan että ajantasaisen käyttäjätunnustietokannan.

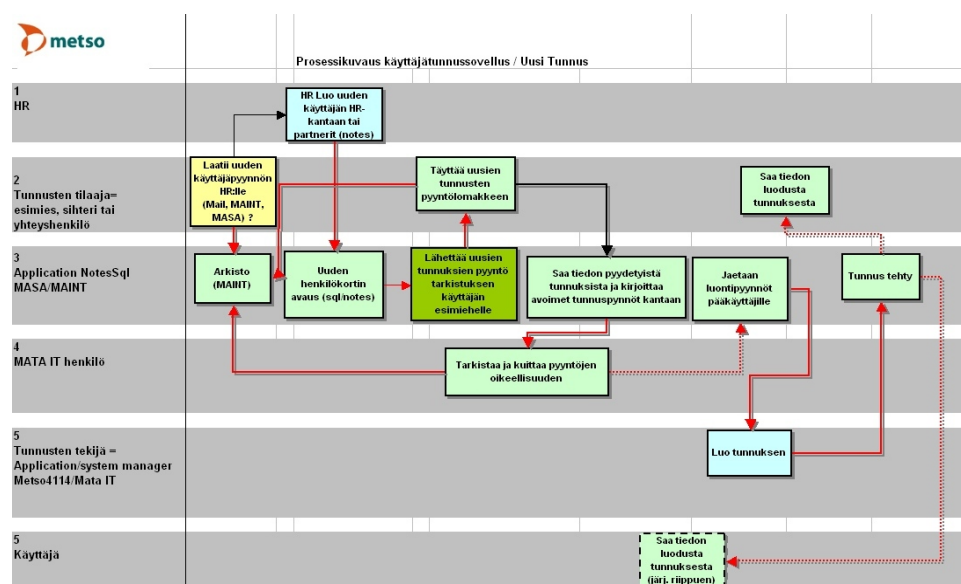
Työprosessi hallitaan Lotus Notes -kannalla, jonka nimi on MAINT. Pääasiassa tilaukset tehdään käyttäjätunnuskannan kautta, mutta itse työt generoituvat tähän kantaan. Tilaaja voi pyytää samalle käyttäjälle kerralla tunnuksia useisiin järjestelmiin, mutta jokaisen järjestelmän tunnuspyynnöstä luodaan kantaan oma työnsä, jotta ne voidaan ohjata oikeille toteuttajille. Näin myös jokaisen tunnuspyynnön edistymistä voidaan seurata erikseen. Tällainen työprosessin hallinta on Notesilla helppoa. Lisäksi samantyyliisiä työprosessikantoja on Metsolla jo käytössä.

Käyttäjätunnustietokanta (MASA) on myös toteutettu Notes-kannalla. Se ei kuitenkaan ole pelkkä tietokanta vaan sisältää myös toiminnallisuuksia. Tämä on kanta, joka tullaan näyttämään tunnustenpyytäjille. He voivat sen kautta nähdä käyttäjillä jo olevat tunnuksia ja tehdä pyyntöjä uusista tunnuksista. Pyyntöstä avautuu työ MAINT-kantaan, minkä lisäksi siitä lähtee sähköposti kunkin järjestelmän pääkäyttäjille. Pääkäyttäjät seuraavat MAINT-kannasta tehtyjä pyyntöjä ja luotuaan tunnuksen kuittaavat pyynnön suoritetuksi.

5.3 Prosessikuvaus

Prosessikuvaus on esitetty graafisessa muodossa kuviossa 3. Kuvion suurennettu versio on työn lopussa liitteenä 1.

Kun yritykseen palkataan uusi henkilö, toimitetaan allekirjoitettu työsopimus henkilöstöhallintoon. Henkilöstöhallinto kirjaa henkilön tiedot henkilöstöhallintajärjestelmään. Kun tieto on kirjattu sinne, se siirtyy seuraavana yönä automaattisesti käyttäjätunnussovellukseen, joka käyttää henkilöstöhallintajärjestelmää pääsovelluksenaan.



Kuvio 3 Prosessikuvaus uuden tunnuksen luonnista (suurennettuna liitteessä 1)

Mikäli kyseessä on yhteistyökumppani, joiden tietoja ei hallita Metson oman henkilöstöhallintajärjestelmän kautta, kirjataan tarvittavat tiedot henkilöstä suoraan MASA-käyttäjätunnustietokantaan. Kanta toimii samalla myös rekisterinä Metso Automationissa työskentelevistä yhteistyökumppaneista.

Käyttäjätunnussovelluksesta lähtee esimiehelle sähköpostilla pyyntö tilata uudelle henkilölle tarvittavat tunnukset. Sähköposti sisältää linkin käyttäjätunnuskannan tunnustentilausnäkyvyyteen. Esimies valitsee lomakkeesta järjestelmät, joihin työntekijä tarvitsee tunnukset sekä järjestelmäkohtaisesti mahdollisesti käyttäjän roolin. Lomake tallentuu käyttäjätunnussovellukseen. Tällöin pyyntö kirjautuu sovellukseen avoimena työnä. Järjestelmäkohtaisesti on myös mahdollista lisätä hyväksyntäketjuun järjestelmän omistaja, mikäli tämä nähdään tarpeelliseksi.

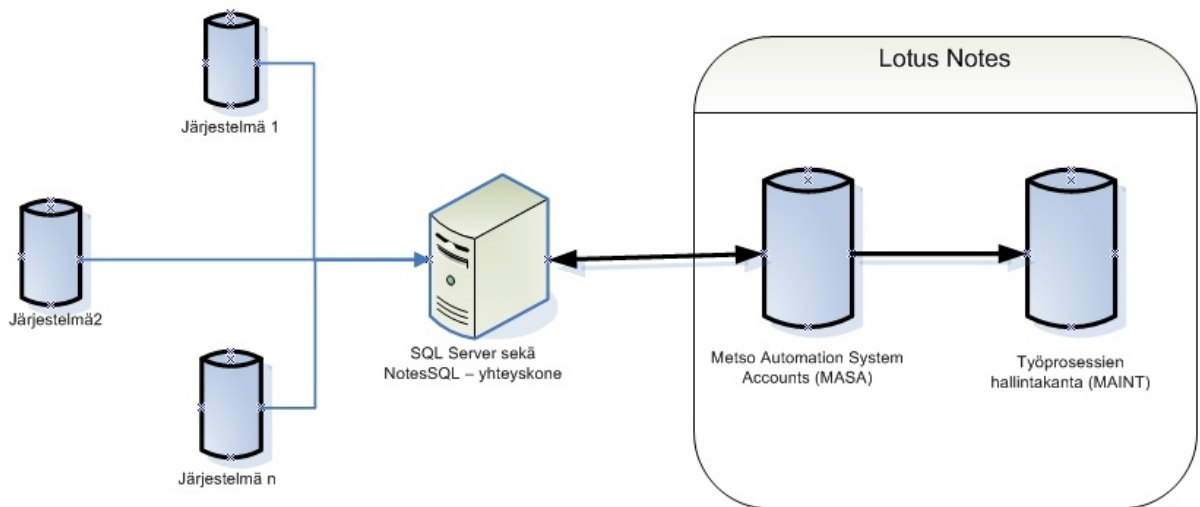
Tämän jälkeen tietohallinto tarkistaa lomakkeen oikeellisuuden ja hyväksynnän jälkeen pyyntö kirjautuu työn alla olevaksi. Vaiheen tarkoituksena on varmistaa, että pyyntö on järkevä.

Tietohallinnon hyväksynnän jälkeen kunkin järjestelmän pääkäyttäjälle lähtee sähköpostiviesti tunnuspyynnön toteuttamisesta. Tarvittaessa pääkäyttäjä kysyy esimiehlä lisätietoja. Pääkäyttäjä luo pyydetyn tunnuksen järjestelmään ja kuittaa tunnuspyynnön toteutetuksi käyttäjätunnussovellukseen. Toteutuksen kuittauksesta kirjautuu sovellukseen toteuttajan nimi sekä luontiajankohta. Kuittauksen jälkeen pyyntö tallentuu järjestelmään suoritetuksi.

Käyttäjätunnussovellus hakee tiedot kustakin järjestelmästä kerran vuorokaudessa, joten seuraavassa haussa luotu tunnus tulee näkyviin myös sovelluksen tietokantapuolelle. Tämä takaa sen, että tietokannassa on oikea tieto siitä mitä tunnuksia kussakin järjestelmässä on eikä vain tietoa pääkäyttäjän kuittauksesta. Toisaalta kuittautustietokin on näkyvissä sovelluksen työprosessia ohjaavalla puolella.

5.4 Sovelluksen osat

Tässä kappaleessa esitellään sovelluksen eri osat sekä niiden toiminta. Kuviossa 4 esitetään sovelluksen osat graafisessa muodossa.



Kuvio 4 Sovelluksen osat

5.4.1 Järjestelmät

Järjestelmät ovat liiketoiminnan tai sen tukitoimintojen kannalta välttämättömiä sovelluksia, joissa kullakin käyttäjällä on henkilökohtainen tunnus kirjautumista varten. Ne toimivat kukin oman tietokantatuotteensa tai hakemistonsa päällä ja niihin kuhunkin kirjaudutaan erikseen. Käytössä olevia tietokantatuotteita ovat mm. Oracle, SQL Server sekä Informix.

Käyttöönottoaiheessa käyttäjätunnussovelluksen piiriin kuuluvat SOX-auditoitavat järjestelmät sekä tietoturvan kannalta tärkeimmät järjestelmät. Niiden määrä tulee jatkossa kasvamaan, mutta aluksi on tärkeää saada sovellus toimintakuntoon ja koekäyttää sitä muutamilla järjestelmillä. Käyttöönottoaiheen järjestelmät ovat:

- Active Directory (verkkotunnukset)
- Aton (product data management)
- Eflow (sähköinen laskujen käsittely)
- Flexim (kulunvalvonta)
- Lean (toiminnanohjausjärjestelmä)
- Lotus Notes (sähköposti / työryhmäohjelmisto)
- SAP (taloushallinto)
- TietoPersona HR (henkilöstöhallintajärjestelmä)

5.4.2 SQL Server

Palvelimelle on asennettu SQL Server -tietokanta, jossa varsinainen tieto käyttäjätunnuksista kootaan ja säilytetään vuorokauden ajan. SQL Serverillä on kaksi ajastettua DTS-pakettia (data transformation services), jotka ajetaan kerran vuorokaudessa yöaikaan. Paketit kokoavat tarvittavat tiedot

kaikista järjestelmistä mukaan lukien Notesin MASA-kannan, jossa ajan- tasainen tieto käyttäjätunnuksista esitetään. DTS on SQL Serverin tarjoama ominaisuus, jonka avulla voidaan siirtää tietoa paketteina tietokantojen tai muiden tietovarastojen välillä.

Tietojen kerääminen eri järjestelmistä on jaettu kahteen erilliseen pakettiin, koska se on ylläpidollisesti järkevämpää ja virhetilanteiden selvittely helpottuu. Paketit tyhjentävät ensin käyttämänsä taulut SQL Serveriltä, jotta uuden tiedon haku niihin on mahdollista. Ensimmäinen paketti hakee henkilöstöhallintajärjestelmästä käyttäjien perustiedot kuten nimen, henkilönumeron, kustannuspaikan sekä esimiehen nimen. Toinen paketti kerää tiedot muista järjestelmistä sekä edellisen vuorokauden tiedot Notesin MASA-kannasta ja suorittaa tarvittavat vertailut. Vertaamalla järjestelmien uusia tietoja MASA-kannan edellisen vuorokauden tietoihin voidaan joukosta haarukoida sekä uudet että poistuneet tunnukset ja esimerkiksi henkilöiden muuttuneet kustannuspaikkatiedot.

Kun tarvittavat vertailut on suoritettu ja uusi tieto käyttäjistä koottu, se siirretään Notesiin MASA-kantaan. Vertailut ja tiedon keruu suoritetaan SQL Serverissä, koska sen ominaisuudet ovat tähän työhön huomattavasti Notesia parempia ja toteutus nopeampaa. Kerätty tieto kuitenkin siirretään Notesiin esittämistä varten. SQL Serverillä vertailussa käytettävään logiikkaan en sen monimutkaisuuden takia perehtynyt, joten sitä ei tarkemmin tässä työssä esitellä.

5.4.3 NotesSQL

Notesin tietokannat eivät ole relaatiotietokantoja. Ne ovat varsin omanlaisiaan tietokantoja, jotka eivät oikein sovi suoraan mihinkään kategori- aan. Ne ovat Notes-kantoja.

Relaatiotietokannat rakentuvat tauluista, joissa voi olla useita sarakkeita, attribuutteja. Jokainen attribuutti voi sisältää vain samaa tietotyyppiä olevia arvoja. Notes tietokantojen rakenne ja ajattelumalli on hyvin erilainen. Se on lähinnä hierarkkinen. Tietokannassa on dokumentteja (Notes). Dokumentti voi sisältää useita kenttiä (fields), joiden tietotyypit voivat olla erilaisia. Relatioajattelu ei sovellu Notes-kantojen toteutuksessa.

Notes dokumentit esitetään käyttäjille näkymissä. Näkymiin voidaan valita dokumentteja eri valintakriteerien mukaan. Kriteerinä voidaan käyttää minkä tahansa kentän sisältämää tietoa ja järjestää dokumentit kentän arvojen mukaisesti. Tämä mahdollistaa tietojen esittämisen eri lailla eri käyttötarkoitusten mukaan.

Notes-kannoilla ja relaatiomallilla on kuitenkin myös yhteisiä piirteitä. Helpottaakseen tiedon hakemista Notes-kannoista on IBM tehnyt NotesSQL-tuotteen. Se on ODBC-ajuri Notesille. Sen avulla on mahdollista

käsitellä Notes-kantaa ODBC-rajapinnan kautta kuin relaatiotietokantaa. NotesSQL:n avulla päästään tekemään kyselyjä ja päivittämään tietoja SQL-lausekkeiden avulla myös Notes-kantoihin. NotesSQL siis mahdollistaa sen, että SQL Server pystyy hakemaan tiedot myös Notes-kannasta ja palauttamaan uuden prosessoidun tiedon esittämistä varten Notesiin.

Kun Notes-kantoja käsitellään NotesSQL:n kautta, saadaan ne näyttämään relaatiokannoilta. Tällöin Notesin dokumentti vastaa relaatiomallin taulua ja kentät vastaavat taulun kenttiä. NotesSQL vaatii, että samalle koneelle täytyy asentaa myös Notes-client. Sekä Notes-client että NotesSQL on asennettu samalle palvelimelle kuin SQL Serverkin.

5.4.4 Käyttäjätunnustietokanta (MASA)

Käyttäjätunnustietokanta nimettiin MASA:ksi. Se on lyhenne sanoista Metso Automation System Accounts. MASA on Notes-kanta, johon tuodaan ajantasainen käyttäjätunnustieto SQL Serverin tietokannasta. Kanta ei ole täysin reaaliaikainen, vaan siitä nähdään edellisen yön tilanne. Päivän aikana järjestelmiin tehtävät muutokset tulevat näkyviin MASA:aan seuraavana yönä.

MASA on käyttäjätunnussovelluksen pääkanta. Sen kautta esitetään SQL Serverin keräämä tieto käyttäjistä ja tunnuksista. Se toimii myös käyttöliittymänä tunnuspyyntöjen tekemistä varten.

Jokaisesta käyttäjästä luodaan MASA-kantaan henkilökortti, joka sisältää henkilöstöhallintajärjestelmästä haetut tiedot kyseisestä käyttäjästä. Yhteistyökumppaneiden tiedot kirjataan suoraan MASA:an, koska heidän tietojiaan ei haluta ylläpitää Metson henkilöstöhallintajärjestelmässä. Kumppaneilla ei ole henkilönumeroa, joten heille annetaan juokseva numerosarja, joka toimii heidän yksilöivänä tietonaan. Kumppanitietojen ylläpidosta huolehtii nimetty henkilö Metso Automationin henkilöstöhallinnossa.

Jokaisen järjestelmän jokaisesta käyttäjätunnuksesta luodaan MASA-kantaan järjestelmäkortti. Se sisältää tiedon järjestelmästä, kyseisen käyttäjätunnuksen, sen luomispäivämäärän, käyttäjän nimen, sähköpostiosoitteen ja henkilönumeron. Jokainen järjestelmäkortti yhdistetään tiettyyn henkilökorttiin. Yksi järjestelmäkortti siis kuvaa yhtä yksittäistä käyttäjätunnusta jossakin järjestelmässä.

Henkilökortin ja järjestelmäkorttien välisenä avaimena toimii käyttäjän henkilönumero. Jokaisesta tietylle henkilölle kuuluvasta järjestelmäkortista löytyy sama henkilönumero kuin hänen henkilökortistaan. Käyttäjän ja tunnusten yhdistäminen tapahtuu varsinaisesti SQL Serverin DTS-paketin vertailu vaiheessa. Siellä yhdistämisavaimena käytetään henkilönumeroa niiden järjestelmien kohdalla, joista se löytyy ja sähköpostiosoitetta lo-

puissa. MASA-kanta kuitenkin käyttää tietojen yhdistämisessä ainoastaan henkilönnumeroa.

MASA-kannan käyttäjille näkyvät ainoastaan henkilökortit. Käytännössä henkilökortti on kannan päänäkymän rivi, joka sisältää tietyn käyttäjän tiedot (kuvio 5).

Name	InternetAddress	Notes	Name	Location	pid	Validity	Category	Contact	CostCenter
A.CLO	do.10@metsopartners.com	CLO 10M-HI/Automation/Partners	CLO		1037		Partner		
A.CLO	do.ad@metsopartners.com	CLO A/HI/Automation/Partners	CLO A/HI		1038		Partner		
Aalto Arno	arno.aalto@metso.com	Arno A Aalto/TRE/Automation/METSO	Tampere	601705	Valid	Employee	Pekka Paakkila	3105300 Logistics Manager	
Aalto Pentti	pentti.aalto@metso.com	Pentti Aalto/HI/Automation/METSO	Helsinki	701084	Valid	Employee	Eero Eskola	3104222 Machining, Heavy	
Aaltonen Arno Kristina	kristina.aaltonen@metso.com	Kristina Aaltonen/TRE/Automation/METSO	Tampere	601230	Valid	Employee	Jukka Neki	3350110 PPS-ryhmä asenn	
Aaltonen Petri Juhani	petri.aaltonen@metso.com	Petri Aaltonen/TRE/Automation/METSO	Rauma	601003	Valid	Employee	Aki Ala-Jaala	3105116 Paper Service, Paa	
Aaltonen Riitta Leena	riitta.aaltonen@metso.com	Riitta Aaltonen/HI/Automation/METSO	Helsinki	709550	Valid	Employee	Veli-Pekka	3104702 Method Developer	
Aaltonen Vesa	vesa.aaltonen@metsopartners.com	Vesa Aaltonen/TRE/Automation/Partners		11243		Partner	Heli Karala	3109901 PIG Measurement	
Aarnio Timo	timo.aarnio@metsopartners.com	Timo Aarnio/HI/Automation/Partners		1126		Partner			
Aattosaari Meija Johanna	meija.aattosaari@metso.com	Meija Aattosaari/TRE/Automation/METSO	Helsinki	601031	Valid	Employee	Jari Leppälampi	3107212 Performance service	
Abdelkader Souaya	soouya.abdel-ade@metso.com	Souaya Abdel-ade/HI/Automation/METSO	Bordeaux	1136	Valid	Employee			
Abanov Arkady	arkady.abanov@metsopartners.com	Arkady Abanov/TRE/Automation/Partners	Petrozavodsk	1033	Valid	Partner RTD	Pekka Kangasniemi	3108301 RTD projects	
Adnanov Anita	anita.adnanov@metso.com	Anita Adnanov/HI/Automation/METSO	Helsinki	601130	Valid	Employee	Arne Beng Svanbo	3101748 Helsinki	
Ahberg Aino	aino.ahberg@metsopartners.com	Aino Ahberg/TRE/Automation/Partners	Tampere	1034	Valid	Partner RTD	Heli Karala	3109901 PIG Measurement	
Ahberg Maarit	maarit.ahberg@metso.com	Maarit Ahberg/TRE/Automation/METSO	Tampere	1490	Valid	Employee			
Ahlstedt Jukka	jukka.ahlstedt@metso.com	Jukka Ahlstedt/TRE/Automation/METSO	Helsinki	705047	Valid	Employee	Tuomo Paakkonen	3104752 Machining, High pres	
Ahlstrand Mikka	mikka.ahlstrand@metsopartners.com	Mikka Ahlstrand/TRE/Automation/Partners		1151		Partner			
Aho Eetu Antero	eetu.aho@metso.com	Eetu Aho/HI/Automation/METSO	Helsinki	679010	Valid	Employee	Mika Salonen	3104001 Business Developm	
Aho Ilmari	ilmari.aho@metso.com	Ilmari Aho/HI/Automation/METSO	Helsinki	679516	Expired	Employee	Markku Markkinen	3104210 Tap Works I	
Ahokangas Tuomo	tuomo.ahokangas@metsopartners.com	Tuomo Ahokangas/TRE/Automation/Partners	Tampere	1128	Valid	Partner Project	Jarmo Kata	3105201 Projects/PM NE	
Ahola Tuomo	tuomo.ahola@metsopartners.com	Tuomo Ahola/TRE/Automation/METSO	Rauma	1192	Valid	Partner			
Ahonen Kristina	kristina.ahonen@metso.com	Kristina Ahonen/TRE/Automation/METSO	Tampere	601571	Valid	Employee	Pekka Ahonen	3105703 Applic. & Product S.	
Ahonen Markku Valtteri	markku.ahonen@metso.com	Markku Ahonen/HI/Automation/METSO	Helsinki	675019	Valid	Employee	Timo Sahlborg	3104301 PP Projects	
Ahonen Mikko	mikko.ahonen@metso.com	Mikko Ahonen/HI/Automation/METSO	Helsinki	670016	Valid	Employee	Timo Sahlborg	3104301 PP Projects	
Ahonen Risto	risto.ahonen@metso.com	Risto Ahonen/HI/Automation/METSO	Helsinki	675018	Valid	Employee	Ismo Penttinen	3105126 Engineering Systems	

Kuvio 5 MASA-kannan päänäkymä

Avatun henkilökortin (kuvio 6) kautta nähdään käyttäjän henkilötietojen lisäksi hänelle kuuluvat käyttäjätunnukset sekä Notes-ryhmät, joihin hän kuuluu. Käyttäjätunnus- ja Notes-tiedot ovat näkyvissä omilla välilehdillä.

Partner: **Tuomo Seppänen/TRE/Automation/METSO** tuomo.seppanen@metso.com
 Metso Costcenter: 3108300 IT Intrapalvelut, PAS Common, Location: Tampere Alue A
 Id Irvia Oy/HELSINKI

Person | Accounts | Notes | Miscellaneous | Administration | Edit History

Person Information to use in any relations to any systems. **Valid**
 Tässä olevaa henkilön informaatiota käytetään kaikissa yhteyksissä.
 This person information is not found form TPFR and all editable information must maintain here! Tälle henkilölle ei löydy perustietoja TPFR:stä, joten näkyvässä informaatiota on ylläpidettävä tässä.

Partner
 Other

HR Information

Name: Seppänen Tuomo
 Personnel ID: 11256
 Title:
 Location: City: Tampere
 Office:
 Alue A
 41140 Tampere
 Date of arrival: 24.10.2005

Notes and AD names and information
 FullName: Tuomo Seppänen/TRE/Automation/METSO
 Address: tuomo.seppanen@metso.com
 RAS:VPN GIA

Authors of this document
 Managers:
 Other Editors:
 Assistants:

MA Contact

Metso contact/Supervisor:
 Comment:

Partner Contact Information:
 Contact Email:
 Contact Phone:
 Comment:

Partner Info from MA Contacts:
 Country: Finland (FIN)
 1246050643
 MetsoPartnersID 201055

Metso Hierarchy and CostCenter Information:
 CostCenter: 3108300
 Name of CostCenter: 3108300 IT Intrapalvelut
 Department (level1): 11 Tietohallinto
 Department (level2): 11 Tietohallinto
 Department (level3): 11 - Tietohallinto
 Business Line/Unit: PAS Common
 Company: 601

Kuvio 6 Avattu henkilökortti

Accounts-välilehti sisältää käyttäjätunnustietojen lisäksi painikkeet, joiden kautta kyseiselle henkilölle voidaan joko tilata uusia tunnuksia, muuttaa vanhoja tai poistaa olemassa olevia (Kuvio 7).

Partner: **Tuomo Seppänen/TRE/Automation/METSO** tuomo.seppanen@metso.com
 Metso Costcenter: 3108300 IT Infopalvelut, PAS Common, Location: Tampere Alue A
 Ici Invia Oy/ HELSINKI

Person | Accounts | Notes | Miscellaneous | Administration | Edit History

System Accounts

Remarks: #

These buttons create Service Request to MAINT to add new accounts, change and remove accounts for this person.

[New accounts](#) [Change accounts](#) [Remove accounts](#)

Some systemaccounts for user:il256

e-mail name	Hino	System	User	Status	effective	expiration	Remarks
adm.tuomo.seppanen	il256	Metso AD		Valid	11.04.2002		
tuomo.o.seppanen	il256	Metso AD		Valid	28.10.2005		
tuomo.seppanen	il256	Lean PAS		Expired	14.09.2003	29.09.2004	
tuomo.seppanen	il256	Metso AD		Valid	25.09.2002		
tuomo.seppanen	il256	Notes Domino		Valid	11.11.2005		
tuomo.seppanen	il256	Person.Partner		Valid			RAS:VPN GIA

Kuvio 7 Accounts-sivulehti

Notesissa on helppoa tehdä näkymiä, joissa olemassa olevia tietoja voidaan ryhmitellä halutulla tavalla. MASA-kannassa onkin luotuna erilaisia näkymiä eri kohderyhmiä varten. Kannan päänäkymässä henkilökortit on järjestetty käyttäjän sukunimen mukaan aakkosjärjestykseen, jolloin kohdehenkilön löytäminen on helppoa. Ylläpitoa varten on luotu näkymä, josta nähdään yhdellä silmäyksellä, kuinka monta käyttäjätunnusta kussakin järjestelmässä on. Sama näkymä jakautuu alaspäin divisioonaa ja kustannuspaikkatasolle asti, jolloin voidaan helposti nähdä, ketkä tietyn kustannuspaikan henkilöt omaavat tunnukset tiettyyn järjestelmään. Tämä on myös esimiesten kannalta hyödyllinen näkymä, koska joidenkin järjestelmien tunnuksista aiheutuu sisäisiä kuluja.

5.4.5 Työprosessien hallintakanta (MAINT)

Tunnusten luonnin työprosessi hoidetaan erillisessä MAINT-kannassa. MAINT on myös Notes-kanta. Metsossa on jo aiemmin ollut käytössä MINT-kanta, jolla hoidetaan työ- ja vianselvityspyynnöt sekä Metso IT:n että ulkoistettujen kumppaneiden kanssa. Kanta on suunniteltu korvaamaan aiemmin sähköpostitse ja puhelimitse kulkeneet pyynnöt, joiden hallinta alkoi olla hankalaa. MINT on työprosessien hallintaan suunniteltu työkalu. Sen toimintaa pystytään muuttamaan määrittelyjen avulla monipuolisesti.

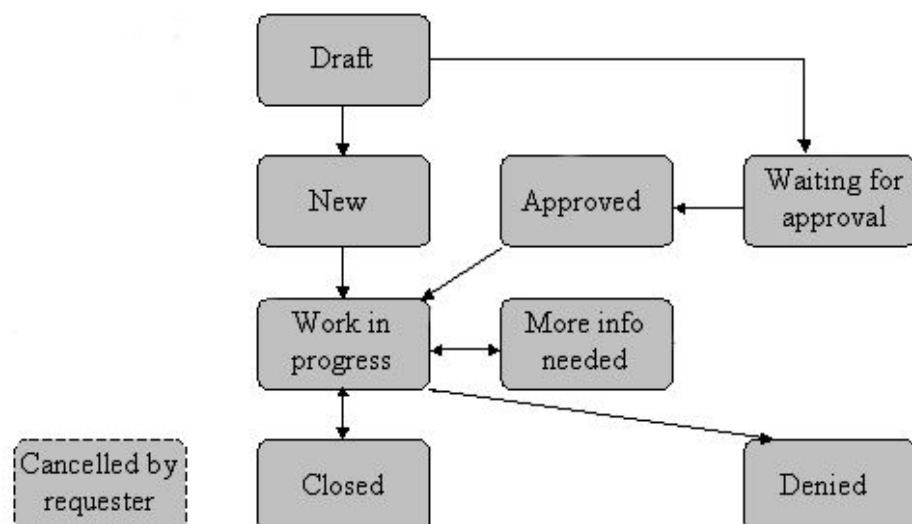
MAINT-kannan pohja kopioitiin suoraan MINT-kannasta. Tästä johtuu myös nimi. MINT:iin lisättiin väliin a-kirjain kuvaamaan Automationia. MAINT-kannan alkumäärityksissä saatiin apua Metso IT:ltä. MINT:ssa

on paljon ominaisuuksia, joita käyttäjätunnussovelluksessa ei tarvittu. Tästä syystä niitä ei myöskään kuvata tässä työssä.

Lähtökohtana on, että ennen kuin käyttäjälle voi tilata tunnuksia, hänen tietonsa täytyy löytyä MASA-kannasta. Jos käyttäjä on Metson oma työntekijä, siirtyvät hänen tietonsa henkilöstöhallintajärjestelmästä MASA:aan. Jos hän on yhteistyökumppani, hänen tietonsa täytetään suoraan MASA:an.

Tunnuspyynnöt tehdään hakemalla MASA-kannasta kyseinen henkilö ja valitsemalla hänen kohdaltaan accounts-välilehdeltä sopiva toimenpide, uusi tunnus, muutos tai poisto (kuvio 7). Kun pyyntö on tehty, kirjautuu siitä uusi työ MAINT:iin. Mikäli samalle henkilölle pyydetään muutoksia useisiin järjestelmiin kerralla, kirjautuu kustakin omasta työstä. MAINT-kannassa voidaan järjestelmäkohtaisesti määrittellä, mitä vaihteita työpyynnöllä on sekä kenelle työt siirtyvät toteutettaviksi. Liiketoiminnan kannalta kriittisiin järjestelmiin voidaan lisätä hyväksymisvaihe, jolloin työ siirtyy Waiting for approval -tilaan. Pääasiassa lähdetään kuitenkin siitä, että esimiehen tehdessä tilauksen se on automaattisesti hyväksytty. Hyväksymisvaihetta ei alkuvaiheessa oteta käyttöön mihinkään järjestelmään.

Kun MASA-kannasta tehty työpyyntö avautuu MAINT-kantaan, on se tilassa new (kuvio 8). New-tilassa työlle ei ole vielä määrätty suorittajaa. Tietohallinto tarkistaa New-tilassa olevat työt ja hyväksyessään valitsee työlle suorittajan järjestelmäkohtaisesti ennalta määritetystä nimilistasta. Suorittajat ovat järjestelmien pääkäyttäjät. Tällöin työ siirtyy Work in progress -tilaan ja suorittajalle lähtee sähköpostiviesti.



Kuvio 8 Työpyyntöjen tilat

Kun työpyyntö on suoritettu, lähettää toteuttaja tilanteesta ja järjestelmästä riippuen käyttäjätunnuksen ja salasanan joko esimiehelle tai suoraan käyttäjälle salatulla sähköpostiviestillä tai tekstiviestillä kännykkään. Tämän

jälkeen toteuttaja käy MAINT-kannassa kuittaamassa työn tehdyksi ja se siirtyy closed-tilaan. Työn suorittajan on myös mahdollista pyytää lisätietoa, jolloin työ siirtyy väliaikaisesti More info needed -tilaan ja pyynnön tekijälle lähtee sähköposti, jossa pyydetään tarkentavia tietoja. Kun hän kirjaa lisätiedot avoimeen työhön, se siirtyy takaisin Work in progress -tilaan.

Maint-kantaan on mahdollista tehdä työpyyntöjä myös suoraan. Tätä tapaa voi tietohallinto käyttää itse, mutta sitä ei markkinoida käyttäjille. Tällöin on myös mahdollista tallentaa kesken jäänyt pyyntö draft-tilaan ja jatkaa se valmiiksi myöhemmässä vaiheessa.

6 Käyttöönotto

Sovellus otettiin käyttöön rajoitetusti 1.1.2006. Toistaiseksi sovellus on ainoastaan tietohallinnon omassa testikäytössä. Pääosa toiminnallisuuksista on käytössä. Tunnuspyynnöt tulevat vielä tässä vaiheessa esimiehiltä sähköpostitse, mutta ne kirjataan tietohallinnon toimesta sovellukseen. 1.1.2006 alkaen kaikkien sovelluksen piirissä olevien järjestelmien tunnuspyynnöt siis löytyvät käyttäjätunnussovelluksesta ja järjestelmiin luodut käyttäjätunnukset tulevat automaattisesti sovellukseen näkyviin.

Kun henkilöstöhallintajärjestelmään lisätään uusi henkilö tai siirretään vanha expired-tilaan, tulee testikäytön aikana ilmoitus muutoksesta tietohallinnon henkilöille. Tämä viesti tullaan varsinaisen käyttöönoton yhteydessä ohjaamaan kyseisen henkilön esimiehelle. Viestissä on mukana linkki henkilön tunnustietoihin. Esimiehen tulee tällöin joko tilata tarvittavat tunnukset tai poistaa käyttäjän kaikki tunnukset.

Kun sovellusta otettiin käyttöön, syntyi oheistuotteena hyödyllinen lista tunnuksista, jotka eivät täsmänneet talossa työskenteleviin henkilöihin. Pääasiassa kyseessä oli talosta poistuneiden henkilöiden eri järjestelmissä olevia lukittuja tunnuksia. Nämä ovat kertyneet, koska järjestelmien pääkäyttäjät eivät aina ole saaneet tietoa käyttäjän poistumisesta. Nämä tunnukset saatiin näin ollen kerralla siivottua eri järjestelmistä. Tämä siivous oli yksi tärkeä osa sovelluksen käyttöönottoa.

Henkilöstöhallintoa ja järjestelmien pääkäyttäjiä on tiedotettu sovelluksen kehityksestä. Sovelluksen toiminta on käyty läpi henkilöstöhallinnon kanssa ja he ovat toimintamallin hyväksyneet. Seuraavaksi sovelluksen toiminta käydään läpi pääkäyttäjien kanssa ja heidät koulutetaan sovellukseen sekä uuteen toimintatapaan. Tämän jälkeen tiedotetaan esimiehille toimintamallin muutoksesta ja ohjeistetaan heidät sovelluksen käyttöön. Tämän hetken arviona sovellus saadaan täysimittaisesti käyttöön Metso Automationilla Tampereella helmikuun aikana.

7 Sovelluksen jatkokehitys

Sovellus saadaan pian täysmittaisesti käyttöön, mutta se tulee todennäköisesti muuttumaan melko paljon ensimmäisen vuoden aikana. Tulevia muutoksia on jo tiedossa. Muutkin Metso Automationin toimistot Suomessa on tarkoitus saada sovellukseen mukaan. Ensimmäiseksi on kuitenkin tarkoitus saada se toimimaan suunnitellusti Tampereella.

Muiden toimistojen mukaan tuleminen jossain vaiheessa tietää uusien järjestelmien tuloa sovelluksen piiriin. Uusia järjestelmiä on tulossa mukaan, myös Tampereella. Nämä tullaan lisäämään vähitellen, kun sovellus on saatu käyttöön.

Tällä hetkellä sovelluksesta lähtee sähköposteja turhan paljon eri työvaiheissa. Jos useampiin järjestelmiin tehdään tunnuspyyntöjä kerralla, lähtee pyynnön tekijälle jokaisesta järjestelmästä oma viestinsä. Lisäksi aina, kun jonkin pyynnön työtila MAINT-kannassa muuttuu, tulee tästä ilmoitus pyytäjälle. Näin pyytäjä pysyy hyvin ajan tasalla tunnusten toteuttamisessa, mutta tästä generoituu turhan paljon sähköpostia. Tämä johtuu MAINT-kannan pohjana käytetystä MINT-kannan toiminnallisuudesta. Sähköpostien lähetysasetuksia ei ole vielä käyty täysin läpi ja ne tullaan tarkastamaan, kun kiireellisemmät asiat on saatu kuntoon.

Kun käyttäjätunnussovelluksesta on nyt puhuttu liiketoiminnan puolellakin, on käynyt ilmi, että uuden käyttäjän tullessa tai vanhan poistuessa pitäisi tieto asiasta saada toimitettua useampaan kohteeseen. Esimerkiksi talon sisäinen postitus ja puhelinvaihde haluaisivat tiedon asiasta. Tällä hetkellä he saavat tiedon usein kuulopuheiden perusteella tai joutuvat itse kyselemään asian.

Tarkoitus on saada integroitua käyttäjätunnussovellukseen myös tiedon lähettäminen käyttäjän tulosta tai poistumisesta tarvittaville kolmansille osapuolille. Näissä tilanteissa ei tarvita kuin sähköpostin lähetys tiedosta tiettyihin osoitteisiin.

Testikäytön aikana havaittiin, että tunnuspyyntöjä saattaa kertyä yllättävänkin paljon kerralla. Tällöin olisi käyttöä ominaisuudelle, jolla voisi suorittaa MAINT-kannassa saman toimenpiteen usealle työpyynnölle kerralla. Jos esimerkiksi tunnuksien poistopyyntöjä kertyy samalle pääkäyttäjälle useita, hän voisi poistaa tunnuksset, valita kaikki poistoja koskevat työpyynnöt ja siirtää ne kerralla closed-tilaan.

Työpyyntöjen sulkemisen helpottamista on suunniteltu myös siten, ettei toteuttajan välttämättä tarvitsisi ollenkaan käydä kuittaamassa työtä suoritetuksi MAINT-kannassa. Kun tunnus luodaan järjestelmään, siirtyy siitä tieto seuraavana yönä MASA-kantaan. Tunnuksen siirtyminen voisi myös automaattisesti sulkea työn MAINT-kannasta. Tunnuksen luonnin ajan-

kohta saadaan näin selville vuorokauden tarkkuudella, mikä saattaisi olla riittävää. Lisäksi osaan järjestelmistä kirjautuu tieto, kuka tunnuksen on luonut ja sekin saataisiin siten automaattisesti kaivettua SQL-paketeilla. Toistaiseksi on hieman epäselvää, riittävätkö nämä tiedot SOX:in kannalta ja asiaa täytyy vielä selvittää.

Sovellukseen on suunniteltu myös kustannustietojen tuomista. Ainakin niiden järjestelmien osalta, joiden tunnuksista syntyy kuukausittaisia kuluja, voidaan tiedot tuoda sovellukseen. Näin ne saadaan näkyviin esimiehille. Kun saadaan selkeästi ilmaistua liiketoimintapuolelle myös tietojärjestelmistä aiheutuvat kulut konkreettisesti, saadaan ylimääräiset tunnuukset karsittua tehokkaasti pois.

Vaikka alustavassa vaatimusmäärittelyssä roolipohjaiset oletusoikeudet rajattiin pois, mietitään tällä hetkellä olisiko sellaisia mahdollista toteuttaa. Mukaan on tulossa, ja on jo tällä hetkellä, järjestelmiä, joissa roolipohjaisista määrittelyistä olisi huomattavaa hyötyä. Tämä kuitenkin vaatii paljon selvittelyä.

Tällä hetkellä myös konsernitason käyttäjätunnussovellus on uudelleen viereillä. Hankkeen toteutus kuitenkin ottaa oman aikansa ja tällä hetkellä selvitetään mahdollisia toteutusmalleja.

8 Työn arviointi

Alun perin työni piti liittyä Metso-konsernin keskitettyyn käyttäjätunnusten hallintaan, mutta projektin viivästyttyä Metso Automation päätti toteuttaa oman sovelluksensa. Tämän jälkeen tarkoitus oli tehdä vaatimusmäärittely Metso Automationiin sovellusta varten. Toteutuksen kuitenkin käynnistyttyä nopealla aikataululla SOX-auditoinnin takia, muuttui aiheeni vielä kerran lopulliseen muotoonsa. Tämä oli itselleni hyvä asia, sillä näin sain olla mukana myös sovelluksen toteutusvaiheessa. Näiden muutosten takia työn tekemiseen kuitenkin kului aikaa suunniteltua enemmän.

Erityisen tyytyväinen olen siihen, että sain olla mukana vaikuttamassa sovelluksen vaatimusmäärittelyyn sekä mietittäessä toteutustapoja. Tämä oli minulle tärkeää, koska sovellus tulee jatkossa olemaan myös oman työni apuna. Varsinaisen toteuttamisen tekivät Metso Automationin tietotekniikkahenkilöt ja ulkopuolinen konsultti. Testivaiheessa olin kuitenkin taas mukana ottamassa sovellusta käyttöön.

Objektiivisen lähdemateriaalin löytäminen aiheesta osoittautui yllättävän hankalaksi. En löytänyt aihetta käsittelevää kirjallisuutta käytännössä ollenkaan ja suurin osa verkkomateriaalista oli hyvin markkinointipainotteista. Suuremmilta ohjelmistovalmistajilta löytyi kuitenkin myös aihetta laajemmin käsitteleviä verkkodokumentteja. Näitä tutkittuani päädyin käyttämään työn pääaineistona Microsoftin "Identity and access management series" -dokumenttia. Tämä tuntui kokonaisuutena parhaalta löytämäältäni aineistolta.

Haasteellisinta tutkintotyössäni oli yrittää tehdä kuvausta järjestelmästä, joka kehittyi koko ajan. Ominaisuuksien määrä kasvoi ja toteutus muuttui jatkuvasti ja tulee edelleen muuttumaan vaikka sovellus onkin jo otettu käyttöön. Testikäytön alkaessa tilanne kuitenkin rauhoittui sen verran, että sain työni viimeistelyä.

Lopullisen aiheen valintaan olen tyytyväinen, sillä keskitetty käyttäjätunnusten hallinta on ajankohtainen ja myös työtehtävieni kannalta mielenkiintoinen aihe. Pääsin tutustumaan suuren yrityksen tietojärjestelmäprojektin toteutukseen alusta loppuun. Tärkeänä pidän myös sitä, että tekniikan lisäksi pääsin tutustumaan myös yrityksen toimintatapoihin. Käyttäjätunnusten hallinnassa, kuten monessa muussakin asiassa yrityksissä, pelkän tekniikan toimiminen ei riitä vaan myös prosessien täytyy olla kunnossa ja niitä on noudatettava. Toivon pääseväni jatkossa hyödyntämään työn tekemisessä kertynyttä osaamistani.

9 LÄHTEET

Metso Corporation 2005.[online] [viitattu 1.9.2005].

www.metso.com

Microsoft Identity and access management series 2004. [online] [viitattu 23.10.2005].

<http://www.microsoft.com/technet/security/topics/identitymanagement/identitymanagement/default.aspx>

Lindh, Merja, Järvenpää, Maija 2004. Sarbanes-Oxley luo mallia –miten kehitys vaikuttaa eurooppalaisiin käytäntöihin?. [online] [viitattu 24.10.2005].

http://www.pwc.com/fi/fin/ins-sol/publ/aviisori_current_issue/404_sarbane.html

Lehmus, Raimo. Microsoft Oy, Senior consultant. Identity Management lyhyesti. Esitelmä. Metso Automation 19.1.2005. Tampere.

10 Liitteet

Liite 1: Toteutuneen prosessin kuvaus

