LAUREA

Autentikoinnin mahdollisuudet, Case: Aton PDM -tuotteenhallintajärjestelmä

Laine, Janne

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Autentikoinnin mahdollisuudet, Case: Aton PDM -tuotteenhallintajärjestelmä

Janne Laine
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2010

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Tietojenkäsittely
Tietoverkot

Tiivistelmä

Janne Laine

Autentikoinnin mahdollisuudet, Case: Aton PDM -tuotteenhallintajärjestelmä

Vuosi 2010 Sivumäärä 34

Tämän opinnäytetyön tavoitteena oli löytää erilaisia tapoja järjestää tietojärjestelmäkäyttäjien autentikointi eli todentaminen Aton PDM -tuotteenhallintajärjestelmässä. Autentikoinnin tavoitteiksi määriteltiin käyttäjätunnusten ja salasanojen yhtenäistäminen eli olisi mahdollista kirjautua samoilla tunnuksilla työasemalle sekä Aton PDM -järjestelmään. Lisäksi käyttäjiä haluttiin jakaa eri ryhmiin kustannuspaikoittain, jotta järjestelmän käytön kustannuksia pystytään jakamaan selvemmin. Myös käyttäjien käyttäjätunnuksien aktiivisuudesta haluttiin lisätietoa, jotta tiedetään kuinka paljon Aton PDM:ää käytetään. Työn toimeksiantajana toimi Konecranes Standard Lifting Hämeenlinnasta.

Opinnäytetyön teoriaperusta muodostuu kolmesta eri asiasta. Alussa käydään läpi autentikoinnin eli todentamisen eri menetelmiä, ja niihin liittyviä tietoturva-asioita. Toisena asiana käsitellään Active Directory -hakemistopalvelua, joka on käytössä Konecranes Standard Liftingillä. Hakemistopalvelu ja sen protokollat liittyvät tärkeänä osana tietokantakäyttäjien autentikoinnin järjestämiseen. Kolmantena asiana nostetaan esille Oracle 10g -tietokanta, johon nojautuu myös Aton PDM -tuotteenhallintajärjestelmä. Oracle-tietokantaa käsitellään pääasiallisesti autentikoinnin kannalta.

Esiteltäviin lopputuloksiin saatiin neljä erilaista autentikointijärjestelmää, joita ovat Passlogix v-GO, Oracle identiteetin hallinta, Microsoftin identiteetin integrointipalvelin ja Windows-natiivi-autentikointisovitin. Edellä mainittujen tavoitteiden kokonaisvaltaista toteutumista on vaikea arvioida, koska esitettyjä tuloksia ei ole käytännössä testattu. Käytännön testaus tapahtuu siinä vaiheessa, kun teoriatasolla on saatu valikoitua paras vaihtoehto Konecranes Standard Liftingin ympäristöön soveltuvaksi. Teoriatasolla tuloksista voidaan kuitenkin sanoa, että ne ovat varteenotettavia vaihtoehtoja ja vastaavat kaikki ainakin käyttäjätunnusten ja salasanojen yhtenäistämisen haasteeseen. Active Directory -hakemistopalvelun kautta on myös mahdollista jakaa käyttäjiä erilaisiin ryhmiin, joten tietokantakäyttäjien jako kustannuspaikoille onnistuu sen kautta.

Asiasanat: autentikointi, käyttäjähallinta, käyttäjätietokanta, tuotteenhallintajärjestelmä, Oracle tietokanta, hakemistopalvelu

Laurea University of Applied Sciences
Laurea Leppävaara
Data processing
Information networks

Janne Laine

Abstract

Authentication's possibilities, Case: Aton PDM -product data management

Year 2010 Pages 34

This thesis aimed to find different ways of organizing the authentication of system users within the Aton PDM -product management system. The chief requirement for the authentication was unifying usernames and passwords so that an employee could sign in to his/her workstation and the Aton PDM -system using the same username/password-combination. In addition, it was requested that the users would be divided into different groups according to their positions in order to see more clearly how the cost of using the system was divided between different branches. There was also interest in how actively the users were in using Aton PDM. The thesis was commissioned by Konecranes Standard Lifting in Hämeenlinna.

The theoretical base of the thesis revolves around three points. First I will discuss different methods of authentication and data security issues related to them. After that I will look at Active Directory service that Konecranes Standard Lifting is using. The directory service and its protocols are closely related to organizing the authentication of system users. My final topic is the Oracle 10g -database that is the basis of, among others, Aton PDM -product management system. The discussion on Oracle -database is mainly from the authentication point of view.

In the end, four different authentication systems got included in the results. Those four are Passlogix v-GO, Oracle identity management, Microsoft identity integration server and Windows native authentication adapter. It's difficult to assess the realization of the abovementioned goals since the presented results have not yet been tested in practice. The testing will happen once the option best suited for Konecranes Standard Lifting has been chosen on a theoretical level. In theory, it can be said, though, that they are all viable options and fit the bill at least on the subject of unifying the usernames and passwords. The Active Directory service also allows the division of users into different groups and so it can be used to divide the database users according to their position.

Key words: authentication, user management, user database, product data management, Oracle database, directory services

Sisällys

1 Johdanto

Tämä opinnäytetyö on tehty Laurean Leppävaaran toimipisteen tietojenkäsittely-koulutusohjelman päättötyönä. Opinnäytetyön tekeminen aloitettiin syyskuussa 2009, ja se valmistui maaliskuussa 2010. Työn aihe on saatu Konecranes Standard Liftingiltä Hämeenlinnasta, mikä on toiminut myös työn toteutuspaikkana. Aihe-ehdotus oli etsiä erilaisia ratkaisuja Aton PDM -tuotteenhallintajärjestelmän autentikoinnin uudelleen järjestämiseen. Tämä kuulosti hyvältä opinnäytetyön aiheelta, joten siitä hetkestä alkoi kirjoittajan matka työn parissa.

1.1 Toimeksiantajan esittely

Työn toimeksiantaja on Konecranes Standard Lifting Oy. Konecranes Standard Lifting on osa Konecranes-konsernia. Konecranes Oy:n historia alkaa vuodesta 1910, jolloin KONE Oy perustettiin. Tuolloin KONE Oy oli erikoistunut sähkömoottoreiden korjaamiseen ja myöhemmin lähinnä hissien valmistamiseen. Konecranes Oy irtautui emoyhtiö KONE Oy:stä vuonna 1994. (Konecranes 2009b.)

Konecranes Oy on yksi maailman johtavista nostolaitteita (kuva 1) valmistavista yrityksistä, jonka liiketoiminta-alueet ovat raskasnostolaitteet, standardinostolaitteet ja kunnossapito. Yrityksen liiketoiminta on alkanut vuonna 1930, ja toimintaa on nyt 50 eri maassa. Konsernin pääkonttori sijaitsee Hyvinkäällä, ja toimipisteitä on yhteensä 500 maailmanlaajuisesti.

Asiakkaista mainittakoon erilaiset konepajat, sellu- ja paperiteollisuus sekä autoteollisuus. Konecranes Oy:n liikevaihto oli noin 2103 miljoonaa euroa vuonna 2008, ja työntekijöitä yrityksessä oli 9900. Suomessa Konecranes Standard Lifting sijaitsee Hämeenlinnassa ja toimipisteessä valmistetaan standardinostimia ja nostinten vaihteita. (Konecranes 2009c.)

Kuva 1: CXT 600 -nostin (Konecranes 2009a, 1)

1.2 Työn taustaa

Työn kirjoittajan taustalla on työskentely Konecranesin palveluksessa Hämeenlinnassa. Kirjoittaja on toiminut erilaisissa tuotannon tehtävissä monena kesänä. Sittemmin hän on ollut yhtäjaksoisesti Konecranesin IT-osastolla kesästä 2008 ja toiminut muun muassa toiminnanohjausjärjestelmän (iLMari) tukiryhmässä ja Helmi-projektissa, jonka aikana vaihdettiin kaikki Konecranesin työasemat uusiin.

Opinnäytetyön aihe on saatu Aton PDM -tuotteenhallintajärjestelmästä vastaavalta henkilöltä. Hänen mukaansa kyseisen järjestelmän käyttäjähallintaa tulisi uudistaa. Tarkemmin sanoen tulisi kartoittaa uusia mahdollisuuksia järjestelmän käyttäjien autentikointiin.

Opinnäytetyön teoriaperusta muodostuu kolmesta eri osa-alueesta. Aluksi käydään läpi autentikoinnin eli todentamisen eri menetelmiä ja niihin liittyviä tietoturva-asioita. Toisessa vaiheessa käsitellään Active Directory -hakemistopalvelua, joka on käytössä Konecranes Standard Liftingillä. Hakemistopalvelu ja sen protokollat liittyvät tärkeänä osana tietokantakäyttäjien autentikoinnin järjestämiseen. Kolmannessa vaiheessa nostetaan esille Oracle 10g -tietokanta, johon nojautuu myös Aton PDM -tuotteenhallintajärjestelmä. Oracle-tietokantaa käsitellään pääasiallisesti autentikoinnin kannalta.

1.2.1 Työssä käytettävät tutkimusmenetelmät

Opinnäytetyön päätutkimusmenetelmäksi sopii parhaiten tapaustutkimus, jossa luodaan kehittämisehdotuksia ja -ideoita yhteen tapaukseen (caseen). Tarkoitus on kehittää suppeasta aiheesta mahdollisimman paljon ideoita ja vastata kysymykseen, miten tehdä uusi rakenne toimintaprosessiin.

Toisena tutkimusotteena on konstruktiivinen tutkimusmenetelmä, joka on käytännönläheistä ongelmanratkaisua. Tämä tutkimusote ei kuitenkaan sovellu täysin työhön, koska tarkoitus ei ole testata tai arvioida ratkaisuja käytännössä. Joka tapauksessa kyseisestä tutkimusmenetelmästä löytyy vaiheita, jotka sopivat opinnäytetyöhön.

Opinnäytetyössäni tulen tekemään tapaustutkimuksen vaiheet samalla lailla, miten ne on esitetty Kehittämistyön menetelmät -kirjassa:

1. alustava kehittämistehtävä tai -ongelma
2. ilmiöön perehtyminen käytännössä ja teoriassa
3. kehittämistyön täsmennys
4. empiirisen aineiston keruu ja analysointi eri menetelmillä
5. kehittämisehdotukset tai -mallit.

(Ojasalo K, Moilanen T & Ritalahti J 2009.)

Tässä työssä alustava kehittämistehtävä on Aton PDM -tuotteenhallintajärjestelmän käyttäjien autentikointiprosessin muuttaminen ylläpidon kannalta helpommaksi. Aluksi perehdytään tapaukseen käytännössä haastattelemalla järjestelmän ylläpitäjää. Teoriatietoa etsitään erilaisista lähteistä, enimmäkseen sähköisistä medioista, koska ne ovat parhaiten ajan tasalla ja niistä löytyy uusinta tietoa. Lisäksi yritetään löytää vastaavanlaisia tapauksia muualta, jotta saataisiin muiden kokemuksia kyseisestä tapauksesta. Koko prosessin ajan tarkennetaan, mitkä asiat ovat tärkeitä autentikoinnin ja Aton PDM -tuotteenhallintajärjestelmän kannalta. Kun analysoitua aineistoa on kerätty tarpeeksi, siitä rakennetaan erilaisia kehitysideoita, joiden avulla käyttäjien autentikointi olisi mahdollista toteuttaa.

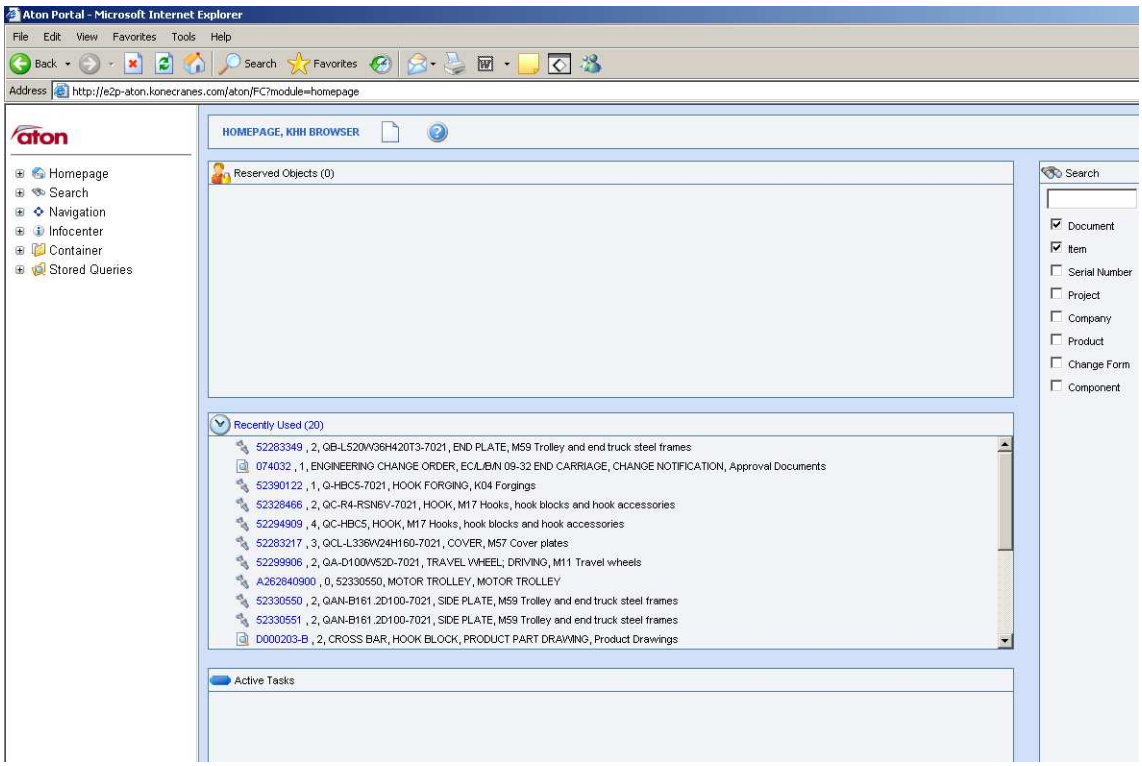
1.2.2 Aton PDM -tuotteenhallintajärjestelmä

Konecranes Standard Liftingillä on käytössä porilaisen ohjelmistoyrityksen Modultek Oy:n kehittämä Aton PDM (Product Data Management) -tuotteenhallintajärjestelmä. Aton PDM on Oracle-pohjainen tietokanta, joka perustuu Java-ohjelmointiin. Konecranesilla Aton PDM:ää käytetään selaimessa toimivan Aton Portal -käyttöliittymän (kuva 2) kautta.

Aton PDM:ää voidaan kutsua tietopankiksi, josta löytyy muun muassa:

- nimikkeet
- tuotteet
- nimikkeistä koostuvat tuoterakenteet
- dokumentit
- projektit
- asiakastiedot.

Aton PDM:n avulla pystytään hallitsemaan keskitetysti nimikkeitä, mikä mahdollistaa myös nimikkeiden perustamisen ja koodauksen, nimikkeiden vertailun sekä vaihtoehtoisten komponenttien käytön. Järjestelmässä valitaan tuotteen ja tuotekonfiguraatioiden rakenne, jolloin saadaan muodostettua erilaisten nostinten osaluettelot. Dokumenttien hallinnassa voidaan tallentaa erilaisia dokumentaatioita muun muassa muistioita ja piirustuksia.
Konecranes Standard Liftingissä Aton PDM:ää käyttää päivittäin noin 500 käyttäjää ja satunnaisesti toiset 500 käyttäjää. (Modultek 2009a; Modultek 2009b.)



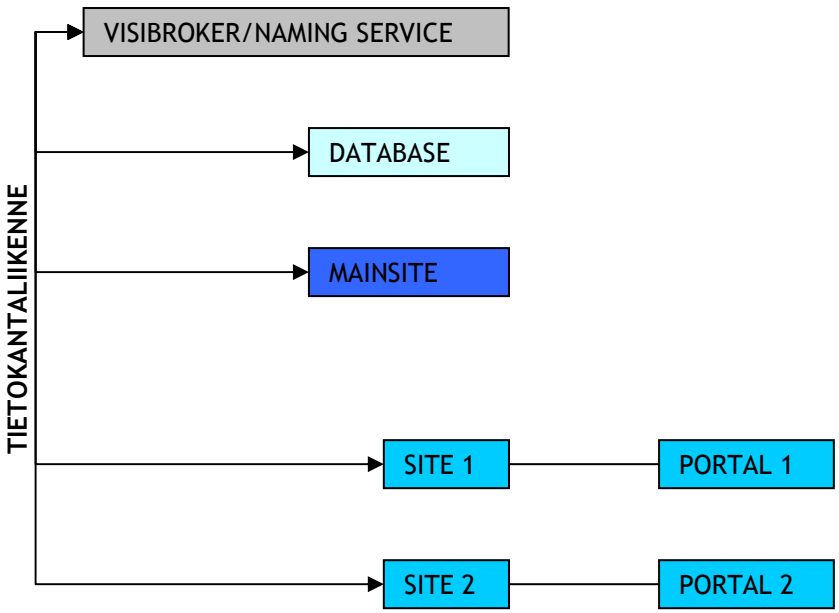
Kuva 2: Aton PDM -tuotteenhallintajärjestelmän käyttöliittymä (Konecranes 2010)

1.2.3 Aton PDM -tuotteenhallintajärjestelmän rakenne

Aton PDM -tuotteenhallintajärjestelmä (kuva 3) koostuu Oracle-tietokannasta (Database), erilaisten palvelimien palveluista (Site Services) ja viestinviejästä (Visibroker/Naming Service). Tietokanta pitää sisällään käyttäjien autentikoinnin, oikeushallinnan ja ohjelmalogiikan. Ohjelmalogiikka kuvaa, miten tietoja käsitellään, jotta järjestelmä pystyy tuottamaan siltä vaaditut palvelut. (Mikkola 2006, 20.) Lisäksi tietokanta sisältää metatietoa eli kuvailevaa ja määrittävää tietoa kaikista tietokannan tietovarannoista. (Aton PDM -järjestelmävastaavan haastattelu.)

Site Services -osioon kuuluu pääpalvelin (MAINSITE), jonka kautta kaikki liikenne kulkee Oracle-tietokannalle ja takaisin. Sen lisäksi on olemassa muutamia tiedosto- ja sovelluspalvelimia, joiden on tarkoitus tarjota palveluitaan paikallisesti. Tiedostopalvelimella säilytetään tiedostoja ja sovelluspalvelimen avulla pystytään käynnistämään Aton Portal -käyttöliittymä, jolla Aton PDM:ää käytetään. (Aton PDM -järjestelmävastaavan haastattelu.)

Viestinviejä (Visibroker/Naming Service) toimii eri palvelimien (Site) välillä. Kaikki käskyt, jotka menevät tietokantaan tai palvelimelta palvelimelle, kulkevat viestinviejän kautta. Aton PDM -tuotteenhallintajärjestelmään ei kuulu muita komponentteja Konecranesin ympäristössä. Se on periaatteessa täysin itsenäinen järjestelmä, vaikka sillä tosin onkin integraatioita muihin järjestelmiin, kuten myyjien käyttämään Markman -ohjelmistoon. (Aton PDM -järjestelmävastaavan haastattelu.)



Kuva 3: Aton PDM -tuotteenhallintajärjestelmän rakenne

1.2.4 Autentikoinnin alkutilanne

Alkutilanteessa Aton PDM -tietokannan käyttäjien autentikointi tapahtuu Oracle-tietokannassa itsessään. Tietokannassa käytetään henkilökohtaista käyttäjätunnusta ja salasanaa, jotka on määritelty tietokantaan sisäisiksi. Näin ollen jokaista käyttäjätunnusta hallitaan yksittäisesti, joten käyttäjähallinta on tällä hetkellä ylläpidolle työlästä. Konecranesilla myös uskotaan tietokantakäyttäjien määrän kasvavan tulevaisuudessa. Tämän takia autentikoinnissa on kehitystarpeita, joita käydään läpi tarkemmin työn tavoitteissa.

1.3 Työn tavoitteet

Tavoitteista mainittakoon käyttäjätunnusten ja salasanojen yhtenäistäminen eli olisi mahdollista kirjautua samoilla tunnuksilla työasemalle sekä Aton PDM -järjestelmään. Salasanojen yhtenäistäminen tarkoittaa sitä, että käyttäjä syöttää saman käyttäjätunnus-salasana -yhdistelmän kirjautuessaan työasemalle ja Aton PDM -järjestelmään. Vielä parempi vaihtoehto on, että käyttäjän autentikointiin riittäisi yksi kirjautuminen työasemalle. Sen jälkeen käyttäjä voisi käyttää myös Aton PDM -järjestelmää ilman uudelleen kirjautumista. Tämä on kuitenkin haasteellista toteuttaa. Jos käyttäjien autentikointiin riittäisi kirjautuminen työasemalle, niin käyttäjätunnusten uudelleen luonti ja nollaus siirtyisivät Aton PDM -järjestelmätuelta ulkoistettuun tietotekniikkatukeen. Tämä vapauttaisi aikaa Aton PDM -järjestelmätuelle normaaliin kehitystyöhön. Silti käyttäjien hallinnan tulisi myös jatkossa onnistua Aton PDM:n kautta, jos järjestelmätuella tulee siihen tarvetta.

Lisäksi käyttäjiä halutaan jakaa eri ryhmiin kustannuspaikoittain, jotta järjestelmän käytön kustannuksia pystytään jakamaan selvemmin. Myös käyttäjien käyttäjätunnuksien aktiivisuudesta halutaan lisäinformaatiota, jotta tiedetään kuinka paljon Aton PDM:ää käytetään. Näitä kehitystarpeita varten etsitään uutta autentikointijärjestelmää.

1.3.1 Aiheen rajaus

Työssä on tarkoitus tehdä vaatimusmäärittely toteuttamisprojektille eli toisin sanoen esittää erilaisia vaihtoehtoja autentikoinnin järjestämiseen. Autentikoinnin mahdollisuuksia tutkitaan järjestelmänhallinnan ja -ylläpidon näkökulmasta, ei niinkään käyttäjän kannalta. Työssä ei tulla tekemään eri vaihtoehtojen testausta käytännössä, vaan se tehdään sitten, kun löydetään teoriassa mahdollisimman sopiva vaihtoehto autentikoinnin järjestämiseen Konecranesin ympäristössä. Myöskään ratkaisuehdotusten aiheuttamia kustannuksia ei työssä käydä läpi, koska se ei ole työn kannalta oleellisin asia. Kustannuksia kartoitetaan siinä vaiheessa, kun päätetään, mihin suuntaan käyttäjähallintaa lähdetään viemään.

2 Autentikointi

Käyttäjähallinnassa on kyse yrityksessä sovituista kokonaisvaltaisista käytännöistä, jotka koskevat niin liiketoiminnan prosesseja, toimintatapoja kuin teknologioitakin. Käyttäjähallinnassa tärkeä osa on autentikointi, joka tarkoittaa käyttäjän todentamista. Tietojärjestelmissä autentikointi on toiminto, jonka avulla käyttäjä todistaa henkilöllisyytensä järjestelmälle. Autentikointi on kuitenkin eri asia kuin käyttäjän tunnistaminen, koska tunnistamisessa selvitetään käyttäjän henkilöllisyys, eikä tyydytä pelkästään väitetyn henkilöllisyyden varmentamiseen. Tietojärjestelmissä autentikointi on lajiteltu kolmeen eri arkkitehtuuriin.

Ensimmäinen ja yleisin arkkitehtuuri on, että käyttäjä tietää käyttäjätunnuksen ja salasanan, jonka hän syöttää autentikointia suorittavalle palvelimelle. Palvelin vertaa tietoja tietokannan muistissa oleviin yksittäisen käyttäjän tietoihin ja päästää käyttäjän järjestelmään tietojen ollessa yhteneväiset. Arkkitehtuurin ongelmat liittyvät salasanaan, jota tulisi vaihtaa tarpeeksi usein. Salasanan pitäisi olla muutamaa merkkiä pitempi ja vaikeasti arvattavissa, mutta silti se täytyisi muistaa ilman muistilappua. Salasanaa ei myöskään tulisi kertoa kenellekään, joka voisi käyttää sitä väärin. (Anderson 2003; Jäppinen 2002, 11–13.)

Käyttäjällä on -arkkitehtuurissa käyttäjä omistaa jotain, mikä mahdollistaa autentikoinnin. Se voi olla esimerkiksi sirukortti tai älykortti, joka sisältää käyttäjän tunnisteen. Kortit sisältävät varmenteita, joiden avulla kortin käyttäjä todennetaan. Tunnisteeseen on mahdollista lisätä salasana, jolloin menetelmästä tulee varmempi tietoturvan kannalta. Se voi olla PIN-koodi, joka on voimassa tietyn ajan ja syötettävä lukulaitteelle, joka on kytketty tietokoneeseen kiinni. Käyttäjällä on -arkkitehtuuri perustuu julkisen avaimen infrastruktuuriin (Public Key Infrastructure, PKI), joka on luotu julkisten avainten ja varmenteiden hallintaan. Julkisen avaimen infrastruktuuri toimii niin, että kaksi osapuolta luottaa kolmanteen osapuoleen, jota kutsutaan varmentajaksi. Varmentaja taas yhdistää julkisen avaimen ja sen haltijan. Tällöin puhutaan henkilövarmenteesta, joka sitoo henkilön julkisen avaimen sitä käyttävään henkilöön. (Viestintävirasto 2009a; Jäppinen 2002, 16–18.)

Käyttäjä on -arkkitehtuuri tarkoittaa biometristä tunnistusmenetelmää. Biometrisistä tunnistustavoista esimerkkejä ovat ääni, verkkokalvo, sormenjälki ja käsiala. Myös käyttäytymiseen perustuvia menetelmiä voidaan käyttää, joista esimerkkejä ovat puheentunnistus, allekirjoitus ja näppäimien painallus. Kaikkien näiden ominaisuuksien tutkiminen vaatii aina autentikointijärjestelmään asennettavan lisälaitteen, jonka avulla nämä ominaisuudet voidaan muuntaa järjestelmän ymmärtämään muotoon. Joka tapauksessa käyttäjän biometriikka täytyy olla tallennettuna tietokantaan, jotta tunnistus voidaan tehdä. Tämän arkkitehtuurin hyvä puoli on, että biometriikkaa on vaikea väärentää ja niinpä onkin todennäköistä, että

tulevaisuudessa tämän kaltainen autentikointimenetelmä tulee yleistymään myös yritysten tavallisissa toiminnoissa. (Jäppinen 2002, 13–16.)

2.1 Autentikointimallit

Yrityksen tietojärjestelmissä voi olla käytössä erilaisia autentikointimalleja. Näitä ovat järjestelmäkohtainen autentikointi, keskitetty autentikointi ja Single-Sign-On (SSO) eli kertakirjautuminen. Autentikointimallilla kuvataan tapaa, jolla käyttäjä käyttää kirjautumistietojaan. Käyttäjän kirjautumistiedot ovat useimmiten käyttäjätunnus ja salasana.

2.1.1 Järjestelmäkohtainen autentikointi

Järjestelmäkohtainen autentikointi tarkoittaa sitä, että jokaisella järjestelmällä on oma toimintamekanismi käyttäjän autentikointiin. Tämä aiheuttaa ongelmia käyttäjälle, koska hänen tulee muistaa monen eri järjestelmän käyttäjätunnus-salasana -yhdistelmä. Jos taas käyttäjä käyttää samoja tunnuksia eri järjestelmissä muistaakseen ne, niin tällöin käytöstä muodostuu tietoturvariski. Eri käyttäjätunnus-salasana -yhdistelmä jokaisessa järjestelmässä lisää tietoturvallisuutta, koska yhden yhdistelmän joutuminen vääriin käsiin ei aiheuta uhkaa muissa järjestelmissä. Myös järjestelmien ylläpidon kannalta malli on työläs, koska jokaista käyttäjää on hallittava järjestelmäkohtaisesti. Tämä syö ylläpidolta tarpeellisia resursseja järjestelmien kehittämisestä, minkä tulisi olla jatkuvaa toimintaa. (Anderson 2003.)

2.1.2 Keskitetty autentikointi

Keskitetyllä autentikoinnilla tarkoitetaan sitä, että järjestelmät käyttävät yhtä autentikoinnin suorittavaa palvelinta. Tosin käyttäjän on silti aina kirjautuessaan järjestelmään annettava käyttäjätunnus-salasana -yhdistelmä, mutta se voi olla sama jokaisessa järjestelmässä. Toisin sanoen käyttäjän ei tarvitse muistaa kuin yksi käyttäjätunnus-salasana -yhdistelmä. Tämä aiheuttaa suuremman tietoturvariskin, koska yhdistelmän joutuessa vääriin käsiin, ovat kaikki järjestelmät vaarassa. Järjestelmien ylläpidon kannalta keskitetty malli on helpompi, koska ylläpidon ei tarvitse hallita kuin yhtä autentikointia suorittavaa palvelinta. (Anderson 2003)

2.1.3 Single Sign-On eli kertakirjautuminen

Käyttäjät pitävät työläänä sitä, että tarvitsee erikseen kirjautua jokaiseen järjestelmään. Tätä pulmaa varten on kehitetty Single Sign-On eli kertakirjautuminen. Kertakirjautuminen tarkoittaa sitä, että käyttäjän ei tarvitse kuin kerran kirjautua työasemalleen, niin samalla käyttäjätunnus-salasana -yhdistelmällä hän kirjautuu myös muihin järjestelmiin. Käyttäjän ei

siis tarvitse tämän jälkeen syöttää kirjautumistietojaan uudestaan käyttäessään erilaisia ohjelmistoja. Kertakirjautumisen mahdollistamiseksi on kehitetty turvallinen Kerberos -autentikointiprotokolla, josta kerrotaan tarkemmin kappaleessa 3.1.1. (Anderson 2003.)

2.2 Tietoturva

Kansallista tietoturvapäivää vietetään vuosittain helmikuussa. Tämä kertoo siitä, että tietoturvasta on tullut tärkeä asia nyky-yhteiskunnassa. Teemapäivän tavoitteena on edistää turvallista Internetin käyttöä lähinnä nuorien parissa, jotka käyttävät tietoyhteiskunnan palveluja enemmän kuin ennen. Tietoturva käsitteellä tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Myös yritysten on tunnistettava tietoturvauhat ja pyrittävä suojautumaan niiltä yksinkertaisten tietoturvasuositusten avulla. (Viestintävirasto 2009b.)

2.2.1 Tietoturvariskit autentikoinnissa

Autentikointi on usein kaksiosainen tapahtuma, jossa käyttäjä ensin tunnistetaan käyttäjätunnuksen avulla ja sen jälkeen todennetaan salasanan tai biometrisen tunnisteen avulla. Näitä syötettyjä tietoja vertaillaan tietokannassa oleviin tietoihin, mikä joko hyväksyy tai hylkää käyttäjän.

Jotain mitä käyttäjä tietää -autentikointimenetelmällä tietoturvariskit liittyvät yleensä käyttäjän välinpitämättömyyteen. Tähän sopii hyvin termi ”stupid user”, joka tarkoittaa sitä, että käyttäjä omalla käytöksellään aiheuttaa turhaa tietoturvauhkaa yritysten järjestelmille. Käyttäjä saattaa kertoa oman henkilökohtaisen salasanansa muille työkavereille, käyttäjä käyttää liian lyhyttä salasanaa tai sitten hän on kirjoittanut sen muistilapulle, joka on hyvin helppo havaita tai jopa varastaa. On tutkittu, että jopa 86 prosenttia salasanoista on helppo selvittää niin sanotun sanakirjahyökkäyksen avulla, jossa hyökkääjä yrittää selvittää salasanan koettamalla sanakirjan sanoja erillisen ohjelman avulla. (Jäppinen 2002, 11–13.)

Jotain mitä käyttäjällä on -autentikointimenetelmä on edeltäjäänsä varmempi menetelmä, mutta siihenkin liittyy joitakin tietoturvariskejä. Ongelma tässä menetelmässä on, että lukulaite tunnistaa ainoastaan käyttäjän antaman kortin tai poletin eikä sen kantajaa. Joten varastetulla tai kopioidulla kulkukortilla on mahdollista päästä sisään järjestelmiin. (Jäppinen 2002, 16–18.)

Käyttäjä on -menetelmässä vaikeuksia aiheuttavat biometrisen informaation luonnolliset muutokset kuten hiusten kasvattaminen, silmälasit tai sormien hikoilu, jotka vaikeuttavat tunnistusta. Biometrisessä tunnistuksessa on olemassa myös niin sanottu ”harmaa alue” eli, jos sormenjälki on melkein varmasti oikea, niin hylätäänkö vai hyväksytäänkö se. Tässä asiassa on

hyvä ottaa huomioon se mihin käyttäjä on pyrkimässä (vrt. toimistotarvikevarasto tai palvelinhuone). Myös tässä autentikointimenetelmässä on mahdollista varastaa käyttäjän tietoja, esimerkiksi ottaa toisesta henkilöstä kuva ja esittää sitä omanaan järjestelmälle. Järjestelmän autentikoinnissa verrataan vain kuvia, eikä sitä onko kuvan lähettäjä oikea. Sähköisestä dokumentista voidaan kopioida henkilön allekirjoitus tai sormenjälkitunnistuksessa voidaan yrittää väärentää sormenjälkidata sormenjäljen sijaan. Sormenjäljen varastamisessa on vielä se huono puoli oikealle käyttäjälle, että hän ei voi muuttaa sormenjälkeään toisenlaiseksi, vaan se on varastettu lopullisesti. (Jäppinen 2002, 13–16.)

3 Active Directory -hakemistopalvelu

Konecranes Standard Liftingillä on käytössä Microsoft Windows Server 2003, jossa hakemistopalveluna toimii Active Directory (AD). Active Directory on käyttäjätietokanta ja hakemistopalvelu, jonka avulla hallitaan verkon resursseja. Hakemistopalveluun voidaan tallentaa tietoja käytetystä järjestelmäympäristöstä ja sen komponenteista, kuten käyttäjistä, ryhmistä ja laitteista. Näitä tallennettuja tietoja pystytään muokkaamaan halutulla tavalla. Lisäksi AD toimii eri järjestelmien integraatiopisteenä eli yhteisenä alustana ja yhdistää ylläpitotehtäviä.

Active Directory:n rakenne perustuu X.500 -hakemistopalvelun standardiin (Weider 1992). Hakemistopalvelussa tieto tallennetaan puumaiseen rakenteeseen, jossa on kahdenlaisia objekteja, säiliöviä ja ei-säiliöviä. Ei-säiliövässä objektissa ei ole sisällä muita objekteja, kun taas säiliövän objektin sisällä voi olla muita objekteja. Loogisesti hakemistopalvelu rakentuu kolmeen eri tasoon, jotka ovat toimialueet (domain), puut (tree) ja metsät (forest). Tasot yhdistetään toisiinsa luottosuhteiden avulla. Luottosuhteet ovat transitiivisia, eli jos A luottaa B:hen ja B luottaa C:hen, niin myös A luottaa C:hen. (Kivimäki 2004; TechNoxx 2010.)

Tasoista ylimpänä on metsä, joka kuvaa jokaisen objektin ominaisuuksia ja sääntöjä hakemistossa. Metsätason alla on puurakenne, joka sisältää erilaisia toimialueita. Kaikista alimmaisena on toimialue, jonka ympärille rakenne perustuu. Toimialueella määritellään käyttäjä- ja tietokonetilit. Toimialueille annetaan NetBios -nimi, joka noudattaa Internetin nimipalvelujärjestelmää (Domain Name System, DNS) nimeämismenetelmää. Nimeämismenetelmä muuttaa Internetin käyttämät numeeriset osoitteet helpommin muistettaviksi nimiksi. Tästä syystä Active Directory vaatii toiminnassa olevan DNS-palvelun. (Kivimäki 2004; TechNoxx 2010.)

3.1 Autentikointi Active Directoryn kautta

Toimialueiden väliset transitiiviset luottamussuhteet muodostavat perustan Active Directory

-hakemistopalvelun autentikointiarkkitehtuurille. Luottamussuhteiden avulla pystytään määrittelemään objektien ja subjektien toimialueiden välistä liikennettä. Jos käyttäjä on kirjautunut toimialueelle A ja hänet on todennettu oikeaksi käyttäjäksi, niin hänellä on pääsy myös B ja C toimialueille. (Microsoft Corporation 2003.)

Active Directory -hakemistopalvelu tukee useita autentikointimenetelmiä, joiden avulla voidaan todentaa käyttäjiä ja tietokoneita. Yksi näistä autentikointimenetelmistä on Kerberos 5 -protokolla. Tässä menetelmässä tarvittavat salausavaimet tallennetaan keskitetyn ohjauspalvelimen tietokantaan, jotta autentikoinnista saadaan hallittava. Lisäksi tämä takaa, että autentikoinnin ominaisuuksia voidaan helposti monipuolistaa ja parantaa sen toimintaympäristöä kehityksen mukana. Active Directory mahdollistaa myös vahvemman autentikoinnin eli biometriikan käytön. Biometriikan käyttö tosin vaatii Active Directory -ympäristöön tiettyjä laajennuksia sekä yleensä joitakin lisälaitteita kuten kortinlukijan. (Microsoft Corporation 2003.)

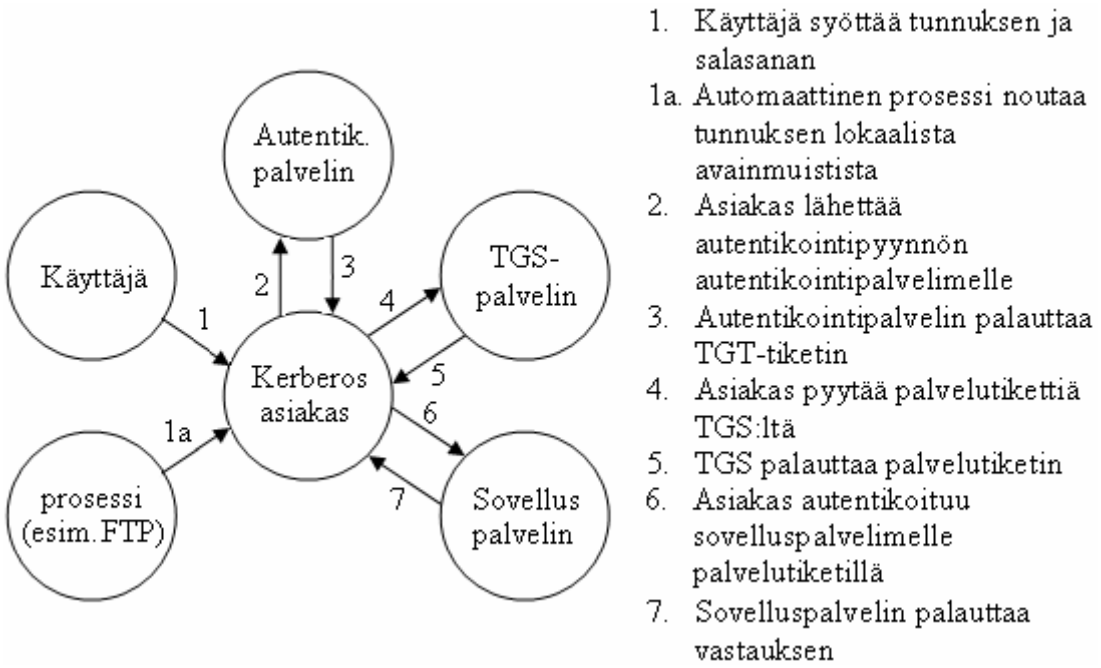
3.1.1 Kerberos 5 -protokolla

Kerberos -todennusprotokolla on kehitetty 1980-luvun loppupuolella Massachusettsin teknillisessä korkeakoulussa (Massachusetts Institute of Technology, MIT) Athena-projektin seurauksena. Athena-projektin tarkoituksena oli parantaa verkkopalvelujen tietoturvaa ja salausta. Protokolla on saanut nimensä Kreikan mytologiasta tunnetusta kolmipäisestä vahtikoirasta nimeltään Kerberos. Nykyään käytössä olevassa LDAPv3 verkkoprotokollassa on käytössä SASL-tunnistus (Simple Authentication and Security Layer, SASL). Se on autentikointimalli, joka käyttää autentikointimetodinaan juuri Kerberosta.

Tällä hetkellä viimeisin versio on Kerberos 5 -protokolla, jonka tarkoituksena on luoda turvallinen kertakirjautumiseen perustuva autentikointimenetelmä, jossa verkkoliikenne salataan. Kerberos toimii myös nykyään oletuksena Windows XP -käyttöjärjestelmän tunnistusprotokollana. Konecranesilla on käytössä Windows XP -käyttöjärjestelmä, joten se on yksi syy, miksi protokollan toimintaa käsitellään työssä.

Kerberos 5 -protokollan toiminta perustuu keskitettyyn tietokantaan, joka sisältää symmetrisiä salausavaimia. Käytännössä tämä tarkoittaa järjestelmän ja käyttäjän välistä jaettua salasanaa. Keskitettyyn tietokantaan on tallennettu tietoa muun muassa salasanojen toiminta-ajoista sekä siitä, koska käyttäjä on viimeksi vaihtanut salasanaa. Active Directory -hakemistopalvelu ympäristössä keskitetyn tietokannan korvaa toimialueen ohjauspalvelin (Domain Controller, DC). DC sisältää myös autentikointipalvelimen (Authentication Server), joka autentikoi asiakkaan ja antaa tälle lipunmyöntölipun (Ticket Granting Ticket, TGT), jonka avulla asiakas pyytää palvelukohtaisia tikettejä. Samaan ohjauspalvelimeen kuuluu vielä

TGS-verkkopalvelu (Ticket Granting Server), joka antaa asiakkaille palvelutikettejä eli palvelu vain myöntää varsinaiseen kohdepalveluun oikeuttavan lipun. (Learn Networking 2008.)
Alla olevassa kuvassa Ville Kinnunen on kuvannut omassa opinnäytetyössään hyvin Kerberos -protokollan toimintaa.



Kuva 4: Kerberos -protokollan toiminta (Kinnunen 2006, 41)

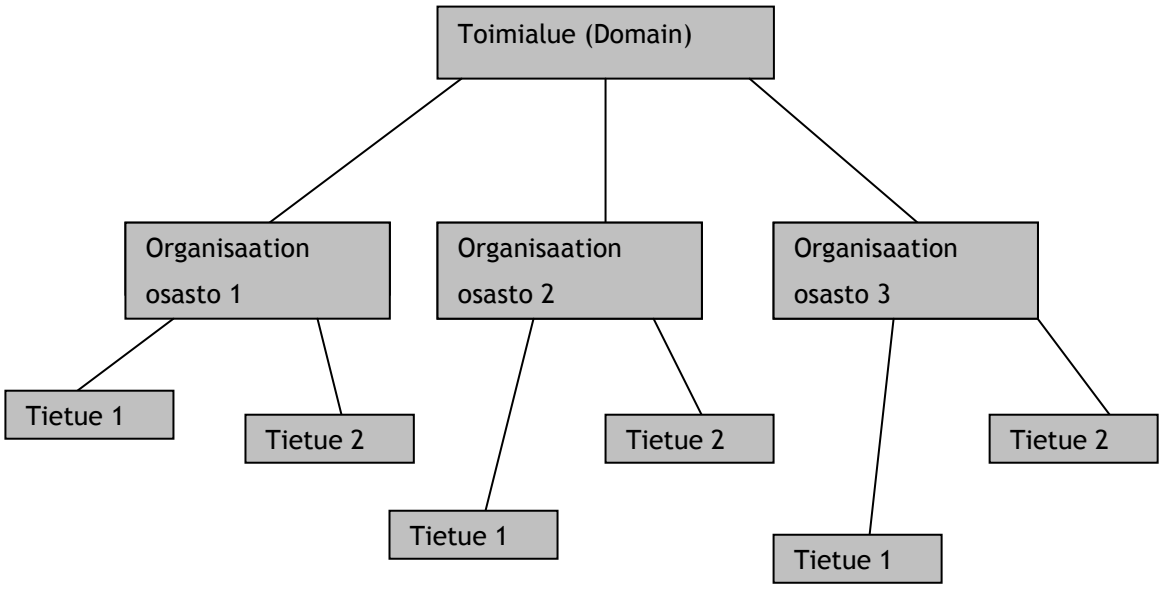
3.2 LDAP - kevennetty verkkoprotokolla

Active Directory on hakemistopalvelu ja LDAP (Lightweight Directory Access Protocol) on hakemistopalveluja varten kehitetty verkkoprotokolla, joka liittyy olennaisena osana keskitettyyn käyttäjähallintaan. Verkkoprotokolla on käytäntö, joka määrittelee laitteiden tai ohjelmien väliset yhteydet tietoverkoissa. LDAP:in ensimmäinen versio on kehitetty Michiganin yliopistossa vuonna 1993 ja nykyään käytetään LDAPv3:sta, joka on kolmas versio protokollasta. Protokolla on syrjäyttänyt monimutkaisemman X.500-standardin, joka kehitettiin vuonna 1988. Kevennetty verkkoprotokolla tulee siitä, että se on yksinkertaisempi kuin edeltäjänsä ja tarjoaa vain tärkeimmät X.500:n toiminnot. Lisäksi protokolla toimii suoraan TCP/IP:n (Transmission Control Protocol/Internet Protocol) päällä.

3.2.1 LDAP:in osat ja hierarkia

Mark Wilcox kertoo kirjassaan, että LDAP koostuu tietomuodosta, protokollasta ja API:sta (Application Programming Interface) eli ohjelmointirajapinnasta. (Wilcox 1999) Tietomuoto on malli, miten hakemistotietoa voidaan tallentaa LDAP-palvelimelle ja hakea sieltä. Tieto-

muoto on tehty monipuoliseksi sitä varten, että se palvelisi mahdollisimman monia alustoja globaalisti.
Protokolla määrittelee, miten käyttäjät ja palvelimet keskustelevat keskenään. Yhteys LDAP-palvelimen ja käyttäjän kanssa voidaan kuvata kolmeen eri vaiheeseen, jotka ovat yhteys palvelimelle, operaatioiden toteuttaminen ja yhteyden sulkeminen. Jos protokolla määrittelee käyttäjän ja LDAP-palvelimen välisiä yhteyksiä, niin API-ohjelmointirajapinta esittää, miten muut ohjelmistot voivat olla yhteydessä LDAP-palvelimeen. LDAP-hierarkia on puumainen rakenne, mikä on esitetty kuvassa 5. (Wilcox 1999.)



Kuva 5: Yksinkertainen LDAP-hierarkia

3.2.2 LDAP -protokollan mallit

LDAP voidaan jakaa neljään eri malliin, jotka ovat tietomalli, nimeämismalli, toimintamalli ja tietoturvamalli. Lyhyesti voidaan sanoa, että tietomalli on sitä varten, että tiedetään millaista tietoa hakemistoon voidaan tallentaa. Hakemiston tietueet nimetään nimeämismallin mukaan ja tietoturvamalli käsittelee sitä, miten hakemisto suojataan luvattomalta käytöltä. Tämän työn kannalta tärkein osa on toimintamalli, joka määrittelee kuinka hakemiston resursseja ylläpidetään. (IBM 2004, 27–55.)

LDAP:in toimintamalli sisältää kolme autentikointioperaatiota. Ensimmäinen operaatio (bind) suorittaa käyttäjän tunnistautumisen ja yhteyden avaamisen LDAP-palvelimelle. LDAP-palvelin vertaa annettua käyttäjätunnusta ja salasanaa omasta henkilökohtaisesta tietueesta löytyvään tietoon ja tämän täytyy täsmätä, jotta operaatio onnistuu. Toinen operaatio (unbind)

sulkee käyttäjän yhteyden palvelimeen. Ja kolmannella operaatiolla (abandon) käyttäjä voi keskeyttää käynnissä olevan istunnon. (IBM 2004, 27–55.)

Seuraavassa esitetään malli (Kuisma 2006, 12), miltä yhteyden avaaminen ja käyttäjätunnuksen (laineja) tunnistautuminen näyttäisi Java-kielellä ohjelmoituna:

LDAPConnection ldap=new LDAPConnection(); ***luodaan viite objektiin***

ldap.connect("ldap.somewhere.com",389); ***avataan yhteys***

ldap.authenticate(uid=laineja, ou=opiskelijat,

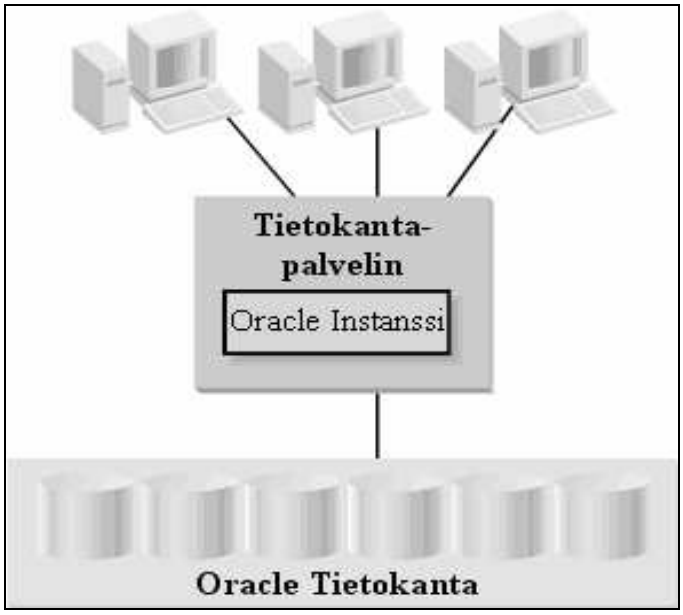
o=inf.ammattikorkeakoulu.fi, "jaanus"); ***suoritetaan autentikointi***

4 Oracle 10g -tietokanta

Konecranesilla käytössä oleva Aton PDM-tietopankki on Oracle 10g -tietokanta. Oracle 10g -tietokanta on relaatiotietokanta eli tietokantaan voidaan liittää yksi tai useampia valideja relaatioita. Tämä ominaisuus mahdollistaa laajennettujen tietokantaoperaatioiden käytön tavanomaisten tietokantojen lisäys-, poisto- ja hakutoimintojen lisäksi. Tietokantaoperaatioista lisäys tarkoittaa rivien lisäämistä tietokantaan SQL-komennolla, kun taas poisto-operaatio poistaa rivejä tietokannasta. Hakutoimintojen avulla pystytään hakemaan tietokannasta tietoa määritetyillä hakuehdoilla. Lisäksi relaatiotietokannan laajennettuja ominaisuuksia ovat valinta, projektio ja yhdiste. Valinta on tietokantaoperaatio, jolla lähtötaulusta muodostetaan tulostaulu riveistä, jotka täyttävät annetun ehdon. Kun taas projektio on operaatio, jolla annetuista lähtötaulun sarakkeista muodostetaan tulostaulu poistaen siitä mahdolliset toistuvat rivit. Viimeisenä on yhdiste, jossa kaksi samanrakenteista lähtötaulua yhdistetään siten, että tulostauluun otetaan mukaan kummankin lähtötaulun rivit, kuitenkin siten, ettei sama rivi toistu. (Nykänen 1996; Helsingin Yliopisto 1996.)

Oracle-tietokannassa tiedot on tallennettu loogisesti taulualueisiin ja fyysisesti tiedostoihin. Taulualueilla voi olla erilaisia lohkoja, kun taas tiedostot muodostuvat erikokoisista tietoblokeista. Kumpaakin aluetta Oracle hallinnoi hallintapalvelimen avulla sen tiedon mukaan, mikä on talletettu systeemitaulualueelle. Hallintapalvelin koostuu Oracle-tietokannasta ja instanssista. Instanssi taas koostuu muistirakenteista ja käyttöjärjestelmän prosesseista. Tietokantaan liitetään yleensä vain yksi instanssi, jonka kanssa käyttäjä kommunikoi eli lähettää pyynnön, jonka perusteella instanssi välittää pyynnön mukaiset tiedot käyttäjälle.

Oracle 10g -tietokanta käyttää Oracle Net -nimistä verkkorajapintaa, joka toimii TCP/IP-protokollan päällä. Tämä mahdollistaa asiakas-palvelin arkkitehtuurin (kuva 6), johon Oraclen tietokantojen toiminta perustuu. Asiakkaan halutessa tietokantaan, Oracle-kuuntelija vastaanottaa pyynnön ja muodostaa yhteyden asiakkaan ja tietokannan välillä. Tämän jälkeen asiakas ja instanssi ovat yhteydessä toisiinsa ilman kuuntelijan apua. (Greenwald, Stackowiak, Stern 2004, 31.)



Kuva 6: Oraclen tietokanta-arkkitehtuuri (Greenwald, Stackowiak, Stern 2004, 32)

4.1 Autentikointi eri tasoilla Oracle-tietokannassa

Oracle-tietokannoissa on kolme tietoturvan hallinnan tasoa. Ensimmäinen taso on tietokantataso, jossa tietoturvamäärityksillä asetetaan käyttäjälle rajoituksia tietokannan käytön suhteen. Käyttöjärjestelmätaso koskee oikeastaan vain järjestelmän ylläpitäjiä, koska tasolla jaetaan oikeuksia tietokantaan liittyviin tiedostoihin, joihin yleensä tavallisella tietokantakäyttäjällä ei ole oikeuksia. Kolmannella tasolla eli tietoliikennetasolla tietoturvan hallintaan käytetään Oracle Net -verkkorajapintaa, jonka avulla voidaan toteuttaa erilaisia autentikointimenetelmiä. Kaikilla näillä kolmella tasolla voidaan suorittaa myös käyttäjän autentikointi. (Greenwald, Stackowiak, Stern 2004.)

4.2 Autentikointi tietokantatasolla

Käyttäjä siis voidaan määritellä Oracle-tietokantaan kaikille kolmelle edellä mainitulle tasolle. Autentikointi toteutetaan jokaisella tasolla hieman toisistaan poikkeamilla tavoilla. Tällä hetkellä Konecranesilla Aton PDM -tuotteenhallintajärjestelmän käyttäjien autentikointi suo-

ritetaan tietokantatasolla, jossa käyttäjä on määritelty tietokannan lokaaliksi käyttäjäksi. Käyttäjän autentikointi tapahtuu käyttäjätunnus-salasana -menetelmällä ja autentikoinnin suorittaa tietokanta itsessään. Oracle-tietokannassa on olemassa sisäinen hallintajärjestelmä, joka valvoo, että salasana on vähintään neljän merkin pituinen ja eri kuin käyttäjätunnus. Tämä estää heikoimpien salasanojen käytön Oracle-tietokannoissa. (Greenwald, Stackowiak, Stern 2004.)

4.3 Autentikointi käyttöjärjestelmätasolla

Oracle-tietokantakäyttäjän autentikointi on mahdollista suorittaa myös käyttöjärjestelmätasolla, jolloin käyttäjä määritellään tietokannassa ulkoiseksi käyttäjäksi. Päästäkseen tietokantaan, käyttäjän on kirjauduttava lokaaliin eli paikalliseen käyttöjärjestelmään, jonka päällä tietokanta toimii. Käyttöjärjestelmätasolla autentikointi voidaan järjestää myös niin, että tietokanta luottaa muihinkin kuin lokaaliin käyttöjärjestelmään. Tämä on tosin tietoturvan kannalta huono tapa, sillä mihin tahansa verkosta löytyvään käyttöjärjestelmään kirjautunut käyttäjä pääsee vapaasti tietokantaan, koska tietokanta luottaa myös kyseisen käyttöjärjestelmän suorittamaan autentikointiin. (Kinnunen 2006, 52.)

4.4 Autentikointi tietoliikennetasolla

Tietoliikennetasolla on mahdollista määritellä käyttäjä ulkoiseksi, jolloin autentikointi suoritetaan samalla tavalla kuin edellisellä tasolla. Tietoliikennetason autentikointi voidaan suorittaa myös määrittelemällä käyttäjä tietokantaan globaaliksi käyttäjäksi, jolloin hänelle muodostuu oma käyttäjätili Oracle Internet Directory (OID) -hakemistopalveluun. OID on LDAPv3-pohjainen hakemistopalvelu, joka parantaa skaalautuvuutta, saatavuutta ja turvallisuutta Oracle-tietokannoissa. Käyttäjän kirjautuessa tietokantaan, autentikointi siirtyy tietokannan puolelta hakemistopalvelun puolelle, joka suorittaa autentikoinnin määritetyllä autentikointimenetelmällä. (Kinnunen 2006, 52.)

5 Opinnäytetyön tulokset

Tässä kappaleessa käsitellään tutkimustyön tuloksia eli ratkaisuehdotuksia Aton PDM -tuotteenhallintajärjestelmän tietokantakäyttäjien autentikoinnin järjestämiseen. Tuloksissa käydään läpi neljä erilaista ratkaisua, joita ovat Passlogix v-GO, Oracle identiteetin hallinta, Microsoftin identiteetin integrointipalvelin ja Windows-natiivi autentikointisovitin. Jokaisen ratkaisun kohdalla kerrotaan minkälaiseen käyttöön ne soveltuvat ja mikä on niiden toimintaperiaate.

5.1 Passlogix v-GO

Passlogix v-GO on kaupallinen kertakirjautumisympäristö, joka on suunniteltu yrityksen käyttöoikeuksien hallintaan. Passlogix v-GO tarjoaa vahvan tunnistuksen mahdollisuuden, jolloin käyttöön otetaan esimerkiksi sirukortti ja sen pin-koodi. Tunnistuksen vahvistaminen on mahdollista myös pitkillä, kryptisillä Windows-salasanoilla, johon v-GO tarvittaessa taipuu. Suomessa v-GO -teknologiaa käyttää omissa järjestelmissään muun muassa Oracle Corporation ja IBM Corporation.

Passlogix v-GO:n etuja ovat salasanojen vaihtoon liittyvien tukipyyntöjen väheneminen, koska salasanoja ei ole niin paljon käytössä ja käyttäjällä on mahdollisuus asettaa itselleen uusi salasana. Tämä säästää huomattavasti aikaa käyttäjätuelta, ja vapauttaa resursseja muihin tukitoimintoihin. Myös käyttäjiltä säästyy aikaa, koska heidän ei tarvitse odottaa uuden salasanan luomista, vaan he voivat tehdä sen itse. Käyttäjän ei myöskään tarvitse muistaa montaa salasanaa, jolloin niitä ei tarvitse kirjoittaa muistilappuihin. Tämä lisää automaattisesti yrityksen tietoturvaa. (Raxco 2007, 1-4.)

5.1.1 Passlogix v-GO:n toimintaperiaate

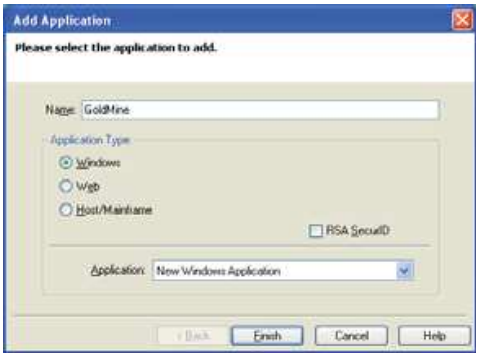
Passlogix v-GO:n toimintaperiaate perustuu siis käyttäjän kertakirjautumiseen, joka usein on Windows-logon. Tämän jälkeen kirjautuessaan Aton PDM -tuotteenhallintajärjestelmään, v-GO antaa oikean käyttäjätunnuksen ja salasanan automaattisesti. V-GO ratkaisua voidaan hallita keskitetysti olemassa olevilla työasemilla ja sen hallintatiedot siirtyvät keskitetyn hakemistopalvelun kautta. Tällaisia keskitettyjä hakemistoja ovat esimerkiksi Active Directory (AD), Lightweight Directory Access Protocol (LDAP) tai Oracle, joista on kerrottu tarkemmin työn aikaisemmissa luvuissa. (Raxco 2007, 1-4.)

Salasanan resetointi itsepalveluna voidaan toteuttaa Passlogix v-GO SSPR (Self Service Password Reset) palvelun avulla. Käyttäjä voi vaihtaa salasanansa Windows-logon ikkunasta, kun hänen henkilöllisyytensä on ensin varmistettu kysymysmenetelmää käyttäen. Passlogix v-GO sisältää erillisiä moduuleita, joiden avulla pystytään hallitsemaan jaettuja työasemia, käyttämään vahvaa tunnistamista tai toimittamaan uudet salasanat käyttäjälle turvallisesti. (Raxco 2007, 4.)

Passlogix v-GO:n käyttöönotto tapahtuu Goldmine-ohjelmistolla, joka on tavallinen Windows-sovellus. Järjestelmän ylläpitäjä lisää v-GO:n kertakirjautumisen piiriin ja sen jälkeen tieto siirtyy työasemilla oleville v-GO -clienteille keskitetyn hakemiston kautta. (Raxco 2007.)

Seuraavassa on esitetty (kuvat 7-11) Passlogix v-GO:n käyttöönotto:

1. Järjestelmän ylläpitäjä avaa v-GO hallintakonsolin ja Goldmine-ohjelmiston.

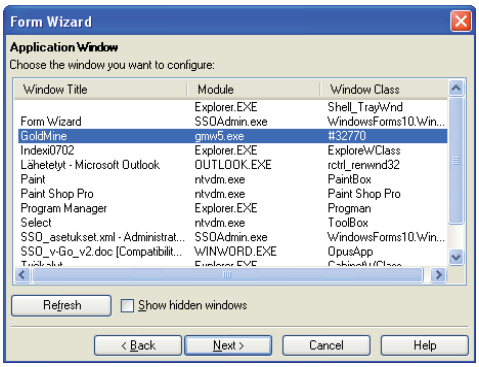


Kuva 7: Sovelluksen lisäys (Raxco 2007, 5)

2. Järjestelmän ylläpitäjä määrittää logon-toiminnon.

Kuva 8: Logon-toiminnon valinta (Raxco 2007, 5)

3. V-GO näyttää aktiiviset ikkunat ja järjestelmän ylläpitäjä valitsee Goldmine-ikkunan.

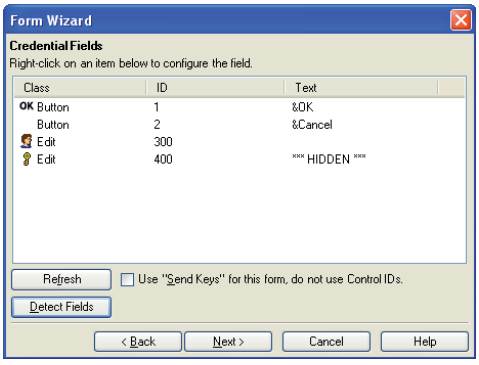


Kuva 9: Goldmine-ohjelmiston valinta (Raxco 2007, 5)

4. V-GO tunnistaa logon-ikkunan kentät ja näyttää käyttäjätunnuskentän ja salasanakentän.

Kuva 10: Goldmine-ohjelmisto (Raxco 2007, 5)

5. Järjestelmän ylläpitäjä valitsee Seuraava ja Lopetus. Määrittely on valmis.



Kuva 11: Kertakirjautumisen määrittelyn lopetus (Raxco 2007, 5)

6. Järjestelmän ylläpitäjä jakaa määritykset työasemille keskitetyn hakemistopalvelun (esim. AD) kautta.

7. Käyttäjän täytyy ensimmäisellä kirjautumiskerralla syöttää käyttäjätunnus ja salasana Goldmineen, mutta sen jälkeen v-GO huolehtii kirjautumisesta.

Tällaisen ratkaisun käyttöönotto sopii paremmin yrityksen kokonaisvaltaiseen käyttäjien käyttöoikeuksien hallintaan, kuin pelkästään yhden järjestelmän (Aton PDM) käyttäjien autentikoinnin järjestämiseen.

5.2 Oracle identiteetin hallinta

Oraclella on oma identiteetin hallinta (Oracle Identity Management, OIM), joka on kehitetty käyttäjien oikeuksien hallintaan. OIM (kuva 12) koostuu kahdesta komponentista, jotka ovat Oracle Advanced Security Option (ASO) ja Oracle Directory Integration Platform (DIP). Komponenteista ASO:a on mahdollista käyttää käyttäjien autentikointiin ja DIP:a käyttäjätunnusten hallinnointiin. DIP-komponentti vaatii yhden lisenssin ja ASO-komponentti tarvitsee jokaista tietokantapalvelinta kohden yhden lisenssin. (Oracle 2004.)

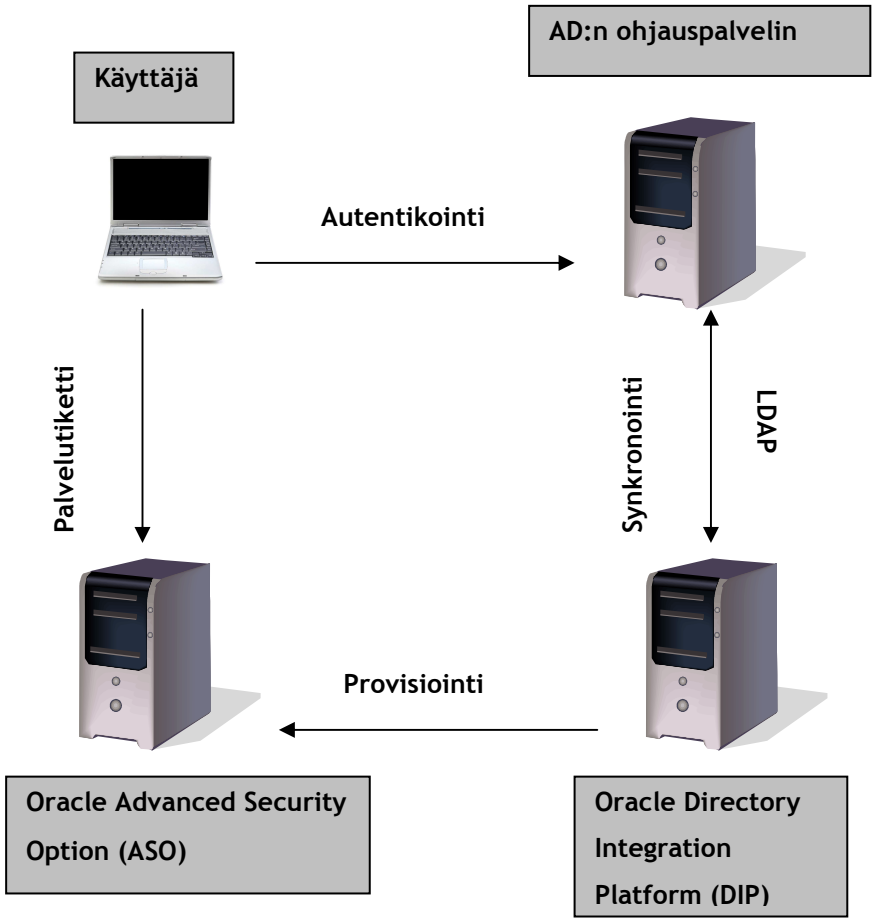
5.2.1 DIP-komponentin toimintaperiaate

DIP-komponentissa käytetään hakemistopalvelua nimeltään Oracle Internet Directory (OID). OID-hakemistopalvelun käyttäjä määritellään aina globaaliksi tietokannassa. OID-hakemistopalvelun ja Active Directoryn synkronoidessaan keskenään, hakemistopalveluissa olevat käyttäjätiedot yhtenevät. DIP-komponentissa on myös synkronointipalvelu, joka varmistaa, että Active Directoryyn tehdyt muutokset siirtyvät OID-hakemistopalveluun ja toisinpäin. OID-hakemistopalvelussa oleva provisiointipalvelu eli käyttäjätietojen hallintapalvelu välittää käyttäjiin liittyvät muutokset tietokantaan. Näin ollen Aton PDM -tietokannan käyttäjätunnusten luonti ja hallinta on mahdollista Active Directoryn kautta. (Oracle 2004.)

5.2.2 ASO-komponentin toimintaperiaate

ASO-komponentin avulla voidaan suorittaa Konecranesin tietokantakäyttäjien autentikointi käyttämällä Kerberos -protokollaa. Aton PDM -tuotteenhallintajärjestelmän käyttäjä voidaan määritellä tietokantaan ulkoiseksi, jolloin autentikointi tapahtuu tietoliikennetasolla toimivalla ASO:lla. Käyttäjän kirjautuessa toimialueelle, hänet autentikoidaan Active Directoryn ohjauspalvelimella. Käyttäjätunnus muodostetaan tietokannassa Active Directory -hakemistopalvelun käyttäjätunnuksesta ja toimialueen nimestä, joiden väliin lisätään ”@”-merkki (esim. *käyttäjätunnus*@*toimialue*-DOMAIN.NET).

Käytettäessä Kerberosta autentikoinnin menetelmänä, tietokantapalvelin pyytää asiakasohjelmalta palvelutikettiä. Asiakasohjelmalla tarkoitetaan sovellusta, mikä toimii käyttöliittymänä, kun halutaan olla yhteydessä palvelimeen. Asiakasohjelma hakee palvelutiketin toimialueen ohjauspalvelimelta ja lähettää sen tietokantapalvelimelle, joka purkaa sen säilytykseen salaisen avaimen avulla. Palvelimen todetessa palvelintiketin olevan asetetut vaatimukset täyttävä, se luottaa siihen, että käyttäjä on aito. Lopuksi tietokannasta tarkastetaan, että käyttäjällä on oikeuksia Aton PDM -tietokantaan ja näin ollessa, hänet päästetään sisään. Jos käyttäjän oikeudet eivät riitä, häntä ei päästetä tietokantaan. (Oracle 2004.)



Kuva 12: Oracle identiteetin hallinta

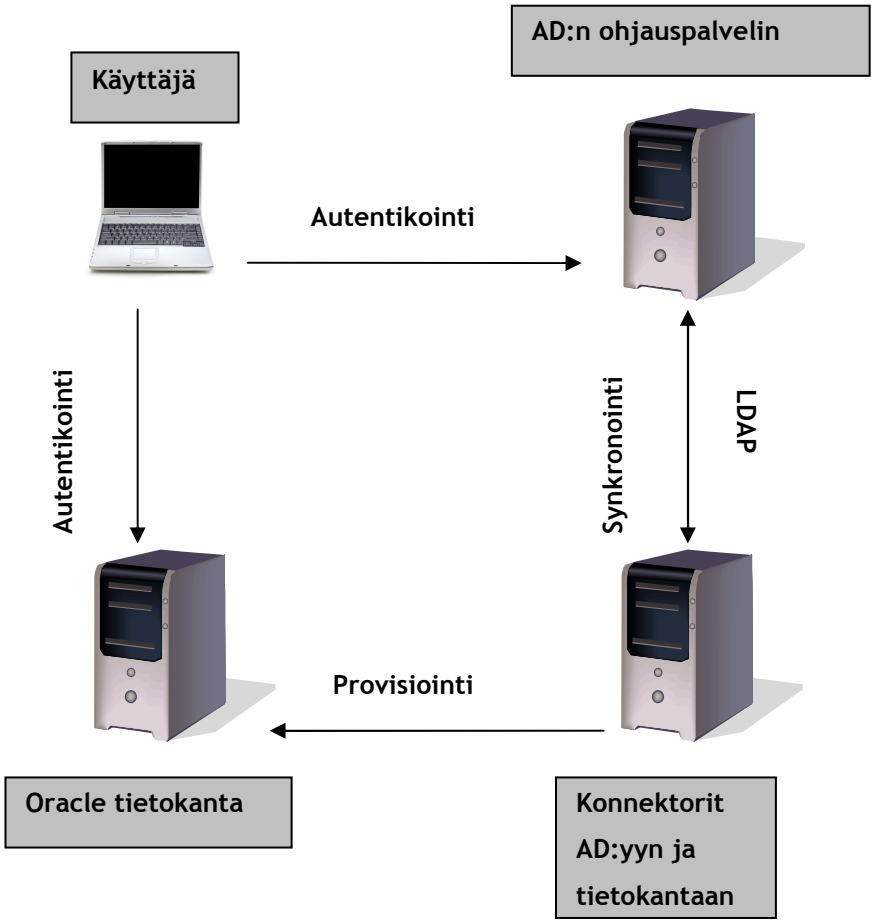
5.3 Microsoftin identiteetin integrointipalvelin

Microsoftin identiteetin integrointipalvelin (kuva 13) on Microsoft Corporationin tarjoama palvelu. Microsoftin identiteetin integrointipalvelimen (Microsoft Identity Integration Server, MIIS) avulla pystytään ylläpito keskittämään yhteen paikkaan. MIIS-palvelimelta keskitetty tieto toistetaan muihin järjestelmiin konnektorien eli liittimien ja porttien avulla. Integroin-

tipalvelin myös päivittää käyttäjään tapahtuvat muutokset kaikkiin ympäristönsä osiin. Palvelin tarvitsee tietojen tallennukseen Microsoft SQL -palvelimen ja se toimii Windows Server 2003 -käyttöjärjestelmän päällä, mikä on käytössä myös Konecranesilla. (Microsoft 2006.)

5.3.1 Microsoftin identiteetin integrointipalvelimen toimintaperiaate

Identiteetin integrointipalvelin toimii aika lailla samoin kuin Oraclen identiteetin hallinta, jota käsiteltiin aiemmin kappaleessa 5.2. Tässä tapauksessa MIIS-palvelin synkronoi itsensä Active Directory -hakemistopalvelun kanssa käyttäen LDAP -verkkoprotokollaa rajapintana. Jos tietokantakäyttäjän salasana muuttuu hakemistopalvelussa, se muuttuu myös MIIS-palvelimella. Tämän työn tekee konnektori, joka muodostaa ylläpitäjän tunnuksilla yhteyden Aton PDM:n tietokantaan ja muokkaa käyttäjän tietoja SQL-lauseilla. Näin salasanat pysyvät yhteneväisinä Aton PDM:n tietokannassa ja Active Directory -hakemistopalvelussa. Käytettäessä integrointipalvelinta, on Aton PDM -tietokannan käyttäjä määriteltävä sisäiseksi käyttäjäksi, jolloin autentikointi tapahtuu tietokannassa. MIIS-malli ei perustu Single Sign-On:iin eli kertakirjautumiseen vaan salasanojen synkronointiin. (Microsoft 2006.)



Kuva 13: Microsoftin identiteetin integrointipalvelin

5.4 Windows-natiivi-autentikointisovitin

Aton PDM -tuotteenhallintajärjestelmän tietokantaan ja asiakasohjelmiin asennetaan Windows-natiivi-autentikointisovitin (Windows Native Authentication Adapter, WNA), joka toimii Windows-alustalla ajettavissa Oraclen tietokannoissa. Aton PDM on juuri tällainen Windows-alustalla toimiva tietokanta. Autentikointisovitin mahdollistaa Oracle-tietokannan käsittelyn Active Directoryn -hakemistopalvelun objektina. WNA:n käyttöön ei tarvita erillistä lisenssiä, joten siitä ei synny lisäkustannuksia. (Keh 2004.)

5.4.1 WNA:n toimintaperiaate

WNA:n toimintaperiaate perustuu siihen, että luodaan Aton PDM -tietokanta yhdeksi objektiksi Active Directory -hakemistopalveluun. Tietokanta käyttäytyy samoin kuin mikä muu tahansa hakemistopalvelun objekti. Näin tietokannan käyttäjätunnuksia päästään hallinnoimaan Active Directory -tasolta ja määrittelemään halutut käyttöoikeudet. Tietokantakäyttäjän autentikointi tapahtuu Kerberos-protokollan avulla, kun hän lähettää pyynnön päästä tietokantaan. Toisin sanoen tietokantaan kohdistuva yhteydenmuodostus käännetään Active Directoryn objektiin kohdistuvaksi pyynnöksi. Active Directory -hakemistopalveluun voidaan luoda muitakin objekteja kuin itse tietokanta, kuten nimen selvitykseen tarkoitettu objekti. Kyseiseen objektiin pystytään tallentamaan tietokantojen kuuntelijoiden yhteystietoja. Tietokannan kuuntelijalla tarkoitetaan palvelimella olevaa prosessia, jonka vastuulla on kuunnella tulevia työasemien yhteyspyyntöjä ja hallita liikennettä palvelimeen. Joka kerta, kun työasema pyytää istuntoa palvelimen kanssa, kuuntelija vastaanottaa varsinaisen pyynnön. Jos työaseman tiedot vastaavat kuuntelijan tietoja, kuuntelija myöntää yhteyden palvelimeen. (Keh 2004.)

6 Loppuyhteenveto

Tässä luvussa käydään läpi työn tulosten sopivuutta alkutavoitteisiin nähden ja esitellään kirjoittajan oma valinta autentikoinnin suorittamiseksi. Lisäksi arvioidaan koko opinnäytetyöprosessia omiin kokemuksiin nojautuen.

6.1 Tulosten sopivuus ja tuloksellisuus

Alkutavoitteisiin oli merkitty käyttäjätunnusten ja salasanojen yhtenäistäminen. Tämä tarkoittaa sitä, että tietojärjestelmien käyttäjät pystyvät kirjautumaan esimerkiksi työasemalleen ja Aton PDM -tuotteenhallintajärjestelmään yhdellä ja samalla käyttäjätunnuksella ja salasanalla. Käyttäjien ryhmittelyn perusteena oli, että saadaan käyttäjät jaettua eri kustannuspaikoille ja sen kautta pystytään jakamaan kustannuksia järjestelmän käytön mukaan. Myös Aton PDM -tietokantakäyttäjien aktiivisuuden seuraaminen oli merkitty alustaviin tavoit-

teisiin. Tämä sen vuoksi, että nähdään millaiseksi järjestelmää tulee kehittää tulevaisuudessa.

Edellä mainittujen tavoitteiden kokonaisvaltaista toteutumista on vaikea arvioida, koska esitettyjä tuloksia ei ole käytännössä testattu. Käytännön testaus tapahtuu siinä vaiheessa, kun teoriatasolla on saatu valikoitua paras vaihtoehto Konecranes Standard Liftingin ympäristöön soveltuvaksi. Teoriatasolla tuloksista voidaan sanoa, että ne ovat varteenotettavia vaihtoehtoja ja vastaavat ainakin käyttäjätunnusten ja salasanojen yhtenäistämisen eli kertakirjautumisen haasteeseen. Microsoftin identiteetin integrointipalvelin perustuu kertakirjautumisen sijaan salasanojen synkronointiin.

Active Directory -hakemistopalvelu on tärkeä osa käyttäjähallintaa ja sen takia myös osa autentikointia. Tuloksissa kaikissa vaihtoehdoissa on hakemistopalvelulla jokin rooli käyttäjien autentikoinnissa. AD:n kautta on myös mahdollista jakaa käyttäjiä erilaisiin ryhmiin, joten tietokantakäyttäjien jako kustannuspaikoille onnistuu AD:n kautta.

6.2 Tulosten analysointi

Konecranes Oy on yksi maailman johtavista nostolaitevalmistajista. Niinpä tuloksia kartoitettaessa, on hyvä muistaa, että yritys tarvitsee ympärilleen ennalta hyväksi havaitut kumppanit toimiakseen. Tuloksia analysoitaessa voidaan sanoa, että niiden jokaisen takaa löytyy luotettava kaupallinen toimija. Microsoft tarjoaa omaa identiteetin integrointipalvelinta ja Windows-natiivi-autentikointisovitinta. Oraclelta taas löytyy oma identiteetin hallinta. Lisäksi Passlogix v-Go -ratkaisua myyvät muun muassa Oracle, IBM ja Sun, jotka ovat kaikki luotettavia ja suuria teknologiataloja. Voidaankin sanoa, että kaikki ratkaisuehdotukset ovat vahvoja ja luotettavia vaihtoehtoja.

Tuloksia arvioidessa on lähtökohta ollut se, että ne sopivat Konecranesin tietojärjestelmäinfrastruktuuriin. Konecranesissa käytössä olevien työasemien käyttöjärjestelmä, Aton PDM -tuotteenhallintajärjestelmän Oracle-tietokanta versio ja hakemistopalvelu ovat olleet tiedossa työtä tehdessä. Tämän takia on voitu sulkea tuloksista ne pois, jotka eivät sovi näihin järjestelmiin. Tämän tuloksena on lopulliseen kartoitukseen otettu neljä erilaista vaihtoehtoa tietokantakäyttäjien autentikoinnin järjestämiseen.

6.3 Oma valintani autentikoinnin suorittamiseksi

Oma valintani autentikoinnin suorittamiseksi on Oraclen identiteetin hallinta ja tarkemmin sanottuna nimenomaan autentikointiin tarkoitettu ASO-komponentti (Advanced Security Option). Autentikointi tapahtuu Active Directoryn ohjauspalvelimella käyttäjän kirjautuessa toi-

mialueelle. Autentikointimenetelmänä toimii Kerberos 5 -todennusprotokolla. ASO:n toimintaperiaatteesta on kerrottu paremmin luvussa 5.2.2.

Teoriatasolla Oraclen identiteetin hallinta tuntui sopivan parhaiten Konecranes Standard Liftingin infrastruktuuriin. Windows XP ja Oracle-tietokanta (versio 10g) ovat ASO:n kanssa yhteensopivia. Lisäksi Konecranesilla on käytössä Active Directory -hakemistopalvelu, jonka ohjauspalvelimeen ASO:n toiminta nojautuu. Yleisesti ottaen Oraclen tuotteet ovat sopeutuvia eri järjestelmiin ja sopivat monimuotoisiin tietotekniikkainfrastruktuureihin.

6.4 Opinnäytetyöprosessin arviointi

Opinnäytetyön tekeminen alkoi syyskuussa 2009, jolloin ei ollut vielä tiedossa mitä kaikkea on edessäpäin. Nyt kun työ on valmis maaliskuussa 2010, on hyvä käydä läpi mitä kaikkea työntekoon on liittynyt ja mitä työn kirjoittaja on tuntenut työtä tehdessään.

Työn aihe-ehdotuksen kirjoittaja sai tuotteenhallintajärjestelmä-asiantuntijalta ja se käsitteli asioita, jotka olivat täysin tuntemattomia työn kirjoittajalle. Ainoastaan Aton PDM -terminä oli jokseenkin tuttu. Alussa kirjoittajaa auttoivat sellaiset kirjat kuin Opinnäytetyöopas ammattikorkeakouluille (Hakala 2004) ja Kehittämistyön menetelmät (Ojasalo, Moilanen & Ritalahti 2009). Kirjoista selviää, minkälainen on opinnäytetyön tekemisen prosessi ja mitä ongelmia ja vaikeuksia sen tekoon liittyy. Lisäksi saa apua siihen, miten projektia kannattaa viedä eteenpäin ja millaisin eri työvaihein. Myös muutama palaveri työn toimeksiantajan kanssa teki työnkuvasta selvemmän.

Aina kun alku on ohitettu, niin sen jälkeen on helpompaa. Tällainen huomio on syntynyt työtä tehdessä, ja se varmasti pätee moneen eri asiaan. Asiat yleensä selkeytyvät ja vaikka monesti tunteekin epävarmuutta omia huomioita kohtaan, niin silti työ etenee pienin askelin eteenpäin. Epävarmuus työnteossa syntyy siitä, että ei olla omilla vahvuusalueilla, koska aihe ja siihen liittyvät termit eivät ole tuttuja. Niinpä asioista täytyy ottaa selvää erilaisten lähteiden avulla.

Pohdittaessa opinnäytetyön koko prosessia, kyseessä ei missään tapauksessa ole ylitsepääsemätön este, mutta se vaatii itsekuria ja aikaa. Näillä kahdella substantiivilla pääsee kunnialla maaliin asti. Lopulta jokaisen tulisi tuntea onnellisuutta ja ylpeyttä valmiista työstään, eikä helpotuskaan välttämättä ole väärä tunne.

Lähteet

Anderson, P. 2003. Authentication Models Explained: A backround to single-sign-on issues for the University of Edinburgh. Viitattu 11.12.2009.
http://www.ucs.ed.ac.uk/ucsinfo/cttees/citc/work/authdirwg/explain.pdf

Aton PDM -järjestelmävastaavan haastattelu. 2010.

Greenwald, R., Stackowiak, R. & Stern, J. 2004. Oracle Essentials: Oracle database 10g. Viitattu 25.1.2010.
http://books.google.fi/books?id=7QFaZ5zYHRYC&dq=oracle+essentials&printsec=frontcover&source=bl&ots=WUsB7p5ccx&sig=oUuENh2AKGh7x6OknG2ufwHJSQE&hl=fi&ei=u-YpS760Ocrz-Qad56j8BQ&sa=X&oi=book_result&ct=result&resnum=5&ved=0CCMQ6AEwBA#v=onepage&q=&f=false

Hakala, J. 2004. Opinnäyteopas ammattikorkeakouluille. Tampere: Tammer-Paino Oy.

Helsingin Yliopisto. 1996. Relaatiotietokantatermit. Viitattu 25.1.2010.
http://www.cs.helsinki.fi/u/laine/relaatiosanasto/v1996/rssuom_termit.html

Huotari, J. 2008. Oracle-perusteet. Viitattu 13.1.2010.
http://student.labranet.jamk.fi/~huojo/opetus/IIO30200/Oracle-pk.pdf

IBM. 2004. Understanding LDAP Design and Implementation. Viitattu 5.1.2010.
http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf

Jäppinen, P. 2002. 010627000 Tietoturvan perusteet: Tietokoneen turva. Viitattu 26.10.2009.
http://www2.it.lut.fi/kurssit/02-03/010627000/tkone.pdf

Keh, A. 2004. Oracle Corporation. Using Oracle with Microsoft Active Directory.
Viitattu 4.1.2010.
http://www.oracle.com/technology/tech/windows/wp/Oracle_with_Active_Directory_TWP.pdf

Kinnunen, V. 2006. Tietokantakäyttäjän autentikoinnin ja auktorisoinnin hallinnointi Active Directory -ympäristössä. Viitattu 25.1.2010.
https://oa.doria.fi/bitstream/handle/10024/30340/TMP.objres.189.pdf?sequence=1

Kivimäki, J. 2004. Active Directory Verkonhallinta. IT Press.

Konecranes. 2009a. Brand manual. Kuva otettu 21.1.2010.
http://brandmanual.konecranes.com/linked/en/guidelines_indcranes.pdf

Konecranes. 2009b. Historia. Viitattu 27.1.2010.
http://www.konecranes.fi/portal/fin/tietoa_meista/historia

Konecranes. 2009c. Yleisesittely. Viitattu 25.1.2010.
http://www.konecranes.fi/portal/fin/tietoa_meista/yleisesittely/

Konecranes. 2010. Aton Portal. Kuva otettu 21.1.2010.

Kuisma, T. 2006. LDAP ja käyttäjähallinta. Viitattu 25.1.2010.
http://www.mit.jyu.fi/opetus/opinnayte/LuK/LDAP/KuismaTiinaKandidaatintutkielma.pdf

Learn Networking. 2008. How Kerberos Authentication Works. Viitattu 3.12.2009.
http://learn-networking.com/network-security/how-kerberos-authentication-works

Microsoft Corporation. 2003. Windows Server 2003 Technical Reference - Technologies Collections - Windows Security Collection - Logon and Authentication Technologies. Viitattu 20.11.2009. http://technet.microsoft.com/en-us/library/cc780455(WS.10).aspx

Microsoft Corporation. 2006. Microsoft Identity Integration Server 2003 (MIIS 2003) Technical Library. Viitattu 14.1.2010.
http://technet.microsoft.com/fi-fi/library/cc720621(en-us,WS.10).aspx

Mikkola, T. & Virkki, O. 2006. Tieto tietojärjestelmässä. Viitattu 5.2.2010.
http://myy.helia.fi/~ict1td003/johdanto/mats/ICT03d_tieto_tietojarjestelmassa.pdf

Modultek. 2009a. Aton PDM. Viitattu 25.1.2010.
http://www.modultek.com/sivu.aspx?taso=1&id=95

Modultek. 2009b. Aton PDM - Toiminnot ja ominaisuudet. Viitattu 25.1.2010.
http://www.modultek.com/sivu.aspx?taso=2&id=142

Nykänen, O. 1996. Ohjelmistotekniikan seminaariesitelmä. Viitattu 27.11.2009.
http://www.mit.jyu.fi/opiskelu/seminaarit/ohjelmistotekniikka/aopast/#Heading13

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Porvoo: WSOY

Oracle Corporation. 2004. Oracle Identity Management: Integration with Windows. Viitattu 9.12.2009.
http://www.oracle.com/technology/tech/windows/wp/ow2004/Oracle_ID_mgmt_Windows.pdf

Raxco Finland Oy. 2007. Raxco Indexi. Viitattu 13.12.2009.
http://www.raxco.fi/doc_images/Indexi2_07.pdf

TechNoxx. 2010. Active Directory. Viitattu 25.1.2010.
http://www.technoxx.com/active-directory.html

Viestintävirasto. 2009a. Julkisen avaimen infrastruktuuri. Viitattu 11.1.2010.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki.html

Viestintävirasto. 2009b. Tietoturvakoulu. Viitattu 14.12.2009.
http://www.tietoturvakoulu.fi/

Weider, C. 1992. Technical Overwiew of X.500, RFC 1309. Saatavissa:
http://www.ietf.org/rfc/rfc1309.txt?number=1309

Wilcox, M. 1999. Implementing LDAP. Wrox Press.

Kuvaluettelo

Lyhenteet

AD	Active Directory
API	Application Programming Interface
ASO	Advanced Security Option
DC	Domain Controller
DIP	Directory Integration Platform
DNS	Domain Name System
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MIIS	Microsoft Identity Integration Server
MIT	Massachusetts Institute of Technology
OID	Oracle Internet Directory
OIM	Oracle Identity Management
PDM	Product Data Management
PKI	Public Key Infrastructure
SASL	Simple Authentication and Security Layer
SSO	Single Sign-On
SSPR	Self Service Password Reset
TCP	Transmission Control Protocol
TGS	Ticket Granting Server
TGT	Ticket Granting Ticket
WNA	Windows Native Authentication Adapter