Lassi Henriksson

SharePoint 2010:n integroiminen kertakirjautumisjärjestelmään

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

5.3.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Lassi Henriksson SharePoint 2010:n integroiminen kertakirjautumisjärjestelmään 49 sivua + 2 liitettä 5.3.2013
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Matti Puska

Opinnäytetyössä toteutettiin toimeksiantajayrityksen SharePoint-verkkoympäristön integroiminen jo olemassa olevaan kertakirjautumisjärjestelmään.

Projektin tarkoituksena oli parantaa käyttäjäkokemusta, ottaa kertakirjautuminen käyttöön, vähentää ylläpitokustannuksia sekä mahdollistaa yhteistyökumppaneiden turvallinen pääsy järjestelmään, jotta myös ulkopuoliset tahot pääsisivät käsiksi yrityksen sisäverkossa oleviin dokumentteihin.

Opinnäytetyössä keskityttiin CA SiteMinder Agent for SharePoint nimiseen tuotteeseen, jonka avulla toimeksiantajayrityksen nykyinen SharePoint-ympäristö liitettiin jo olemassa olevaan CA SiteMinder -pääsynhallintajärjestelmään.

Teoriaosuudessa käydään läpi tarvittavat terminologiat, käsitteet, tekniikat sekä käytetyt tuotteet ja ratkaisut. Käytännön osuudessa käsitellään tarvittavat määritykset SharePoint palvelimilla sekä asennetaan ja otetaan käyttöön CA SiteMinder Agent for SharePoint tuote.

Tulosten ja testausten perusteella kyseinen tuote päätettiin ottaa käyttöön yrityksen tuotantoympäristössä.

Avainsanat	SharePoint 2010, SiteMinder, kertakirjautuminen, SAML

Author(s) Title Number of Pages Date	Lassi Henriksson Integrating SharePoint 2010 into existing single sign-on infrastructure 49 pages + 2 appendices 5 March 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Communications and Data Networks
Instructor(s)	Matti Puska, Principal Lecturer

This thesis was commissioned by a company who wanted to integrate their current SharePoint environment into an existing single sign-on system.

The purpose of this project was to improve the user experience, enable single sign-on, reduce administrative costs and enable secure access to partners and customers, so that the external users could also access all the resources and documents located on the company intranet.

The project focused on a product named CA SiteMinder Agent for SharePoint for connecting the current SharePoint environment to an existing SiteMinder Web access management system. This thesis also maps out the capabilities of CA SiteMinder Agent for the SharePoint product.

The theoretical part of the thesis deals with terminologies, concepts, techniques and products needed in the project. The thesis also describes how CA SiteMinder Agent for SharePoint solution was installed, configured and taken into use in the virtual laboratory environment.

Based on the results, conclusions and customer requirements, the company decided to implement the solution and take it into production use.

Keywords	SharePoint 2010, SiteMinder, single sign-on, SAML

Sisällys

Lyhenteet

AD	*Active Directory*, Aktiivihakemisto, käyttäjätietokanta ja hakemistopalvelu.
Ekstranet	Yrityksen tai muun yhteisön ja asiakkaan tai yhteistyökumppanin välinen Internet-teknologiaa hyödyntävä suljettu verkkopalvelu.
HTTP	*Hypertext Transfer Protocol*, verkkoprotokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
IdP	*Identity provider*, identiteetintarjoaja joka luo, hallinnoi, ylläpitää ja välittää käyttäjätietoa tietoverkoissa.
Intranet	Tietoverkko, joka on eristetty tietyn ryhmän käyttöön.
OASIS	*Organization for the Advancement of Structured Information Standards*, voittoa tavoittelematon kansainvälinen järjestö, joka määrittelee ja ylläpitää verkkosovelluksissa käytettäviä XML-standardeja yhteensopivuuden edistämiseksi.
PowerShell	Microsoftin kehittelemä komentorivipohjainen skriptauskieli Windows-käyttöjärjestelmälle.
RP	*Relying Party*, palveluntarjoaja WS-Federation-rajapintaa käyttävissä verkkosovelluksissa. Tarjoaa ja välittää verkkopalveluita toisiin kokonaisuuksiin.
RST	*Request Security Token*, sisältää turvatunnistepyynnön, jonka avulla käyttäjä pyytää pääsyä verkkosovellukseen.
RSTR	*Request Security Token Response*, sisältää allekirjoitetun turvatunnistepyynnön sekä tarvittavan informaation käyttäjästä, jonka avulla käyttäjä voidaan todentaa verkkosovelluksessa.

SAML	*Security Assertion Markup Language*, XML-standardi käyttäjien tunnistamiseen ja valtuuttamiseen liittyvien tietojen jakamiseen tietoverkossa.
SP	*Service Provider*, palveluntarjoaja, joka tarjoaa ja välittää verkkopalveluita toisiin kokonaisuuksiin.
SSL	*Secure Socket Layer*, suojaustekniikka, joka mahdollistaa suojatun yhteyden luomisen käyttäjän ja palveluiden välille. Tekniikkaa käytetään myös tiedon suojaamiseen ja allekirjoittamiseen.
SSO	*Single Sign-On*, kertakirjautuminen, mahdollistaa käyttäjien pääsyn useisiin palveluihin vain yhdellä kirjautumisella.
STS	*Security Token Service*, identiteetintarjoaja WS-Federation-rajapintaa käyttävissä verkkosovelluksissa. Se luo, hallinnoi, ylläpitää ja välittää käyttäjätietoa tietoverkoissa.
URL	*Uniform Resource Locator*, www-sivujen osoitin. Merkkijono, jota käytetään osoittamaan verkossa sijaitsevia www-sivuja.
WAM	*Web Access Management*, mahdollistaa käyttäjien valtuuttamisen, todentamisen, hallinnoinnin, kirjaamisen ja kertakirjautumisen verkkosovelluksiin.
webSSO	*Web Single Sign-On*, toteutus, joka tarjoaa kertakirjautumisen Internet-selaimilla käytettäviin verkkosovelluksiin.
WS-Federation	*Web Services Federation Language*, XML-standardi käyttäjien tunnistamiseen ja valtuuttamiseen liittyvien tietojen jakamiseen tietoverkossa.
XML	*Extensible Markup Language*, merkintäkieli, jolla kuvataan tekstin rakennetta tai esitystapaa metainformaatiolla. Merkintäkielellä pyritään erottamaan tekstin looginen rakenne sisällöstä. XML-kieltä käytetään formaattina tiedonvälitykseen järjestelmien välillä.

1 Johdanto

Microsoft SharePoint tarjoaa verkkoympäristön, jolla voidaan toteuttaa räätälöityjä ratkaisuja www-sivustojen julkaisuun, ryhmätyöskentelyyn ja dokumentinhallintaan. SharePoint integroituu myös Microsoft Office -tuotteiden kanssa ja näin ollen laajentaa Office-tuotteiden käyttömahdollisuuksia. SharePoint-sivustoja on helppo muokata, ja sen monia toimintoja voidaan helposti laajentaa ja hyödyntää tarpeiden mukaan. SharePointin kasvanut suosio yritysten keskuudessa on lisännyt myös tarvetta sisällyttää se osaksi yrityksen kertakirjautumisjärjestelmää (Single Sign-On, SSO). Kertakirjautumisjärjestelmä mahdollistaa kyseiseen tietojärjestelmään liitettyjen palveluiden käyttämisen yhdellä käyttäjätunnuksella ja salasanalla.

Nykyään myös urakoitsijat, partnerit sekä asiakkaat tarvitsevat pääsyn yrityksen dokumentteihin, mutta sen toteuttaminen voi olla vaikeaa, jos käyttäjähakemistona toimii pelkkä Microsoftin aktiivihakemisto (Active Directory, AD). Aktiivihakemisto on yleisesti ottaen vain tietokanta, johon varastoidaan työntekijöiden käyttäjätunnukset ja monia muita perustietoja. Yhteistyökumppanit sijaitsevat usein myös täysin erillisissä käyttäjähakemistoissa, joten näiden hakemistojen ja käyttäjien yhdistäminen SharePoint-ympäristöön ei ole usein edes mahdollista. SharePoint 2010 mahdollisti ilmestyessään uusia tapoja todentaa käyttäjiä, ja se integroituu nyt myös huomattavasti paremmin yrityksen muihin järjestelmiin. Tässä työssä keskitytään uuteen väitetodennukseen (Claims Based Authentication) perustuvaan todennustapaan, jonka avulla toimeksiantajayrityksen nykyinen SharePoint-ympäristö integroidaan jo olemassa olevaan kertakirjautumisjärjestelmään. [18; 21.]

2 Tavoitteet ja työn rajaus

Työn tavoitteena on suunnitella ja toteuttaa toimeksiantajayrityksen nykyisen SharePoint-ympäristön integroimisen jo olemassa olevaan pääsynhallintajärjestelmään. Työn tarkoituksena on parantaa käyttäjäkokemusta, ottaa kertakirjautuminen käyttöön, vähentää ylläpitokustannuksia sekä mahdollistaa yhteistyökumppaneiden turvallinen pääsy järjestelmään. Yritys haluaa ensin julkaista nykyisen SharePoint-ympäristönsä vain ulkoisille käyttäjille, mutta palvelu tullaan ottamaan käyttöön myös sisäisille käyttäjille.

Yhteistyökumppanit sijaitsevat tällä hetkellä täysin erillisissä käyttäjähakemistoissa, joten tarkoituksena on, että kyseiset käyttäjähakemistot liitetään osaksi yrityksen CA SiteMinder -pääsynhallintajärjestelmää. Erillisestä käyttäjähakemistosta johtuen myöskään Office-asiakasintegraation (Office Client Integration) käyttö ei ole tällä hetkellä lainkaan mahdollista. Office-asiakasintegraatio mahdollistaa SharePoint-ympäristössä sijaitsevien dokumenttien muokkaamisen suoraan Microsoft Office -ohjelmistosta ilman erillistä dokumentin tallentamista. Työssä käytetty tuote CA SiteMinder Agent for SharePoint tukee kyseistä ominaisuutta, minkä lisäksi se integroituu täydellisesti SharePoint People Pickerin kanssa; se on palvelu jonka avulla käyttöoikeudet määritellään SharePoint-sivustoille. Käyttäjät voidaan myös helposti jakaa eri ryhmiin sekä rooleihin, joten käyttäjien näkymää ja pääsyä järjestelmään voidaan rajata esimerkiksi mihin toimipisteeseen tai organisaatioon kyseinen käyttäjä kuuluu. Aiemmin näiden ryhmien ja roolien luomiseksi vaadittiin valtavasti työtä eikä lopputulos ollut kuitenkaan sitä mitä alun perin lähdettiin hakemaan.

3 Käsitteet

3.1 Identiteetin- ja pääsynhallinta

Identiteetin- ja pääsynhallinta on käyttäjän tunnistamista yksiselitteisesti ja ilman epäilystä henkilön identiteetistä koko henkilön työssäolon elinkaaren ajan. [2.] Yleensä käyttäjänhallinta eli identiteetinhallinta on organisaatiossa keskitetty yhteen isoon identiteetinhallintajärjestelmään, joka toimii käyttäjätietojen päätallennuspaikkana. Siihen luodaan uudet käyttäjät sekä päivitetään muuttuneet tiedot, joista kaikki muut järjestelmät hakevat tietonsa käyttäjistä sekä käyttäjiin liittyvistä oikeuksista. Pääsynhallinnalla on tarkoitus varmistaa identiteetille pääsy ainoastaan niihin järjestelmiin sekä tietoon, jotka ovat käyttäjän työn kannalta välttämätöntä. [1; 2.]

3.2 Kertakirjautuminen

Kertakirjautuminen (Single Sign-On, SSO) mahdollistaa käyttäjien pääsyn useisiin palveluihin vain yhdellä kirjautumisella eli käyttäjän tarvitsee syöttää tunnuksensa vain kerran esimerkiksi töihin tullessaan, jonka jälkeen käyttäjällä on pääsy useampaan eri sovellukseen. Kertakirjautumisen päätarkoituksena on säästää kuluissa, joita syntyy

kun käyttäjät unohtavat salasanansa. Usein käyttäjillä on myös kymmeniä eri palveluita, joita he tarvitsevat työpäivänsä aikana, joka taas tarkoittaa kymmentä eri käyttäjänimeä sekä salasanaa. Näitä kaikkia tunnuksia on myös todella vaikea muistaa, joten useammat käyttäjät kirjoittavat tunnuksena erilliselle lapulle ja kiinnittävät sen näyttöpäätteeseensä. Tunnuksien kirjoittaminen paperille on kaikissa yrityksissä yleinen ongelma, josta päästään eroon käyttämällä kertakirjautumista. Kertakirjautuminen parantaa myös käyttäjäkokemusta, koska käyttäjien ei tarvitse enää muistaa kuin yksi käyttäjätunnus ja salasana. Esimerkkinä kertakirjautumisesta voitaisiin pitää käyttäjän kirjautumista omalle työasemalleen, jonka jälkeen hänellä on pääsy esimerkiksi sähköpostiohjelmaan ilman erillistä käyttäjätunnuksen ja salasanan syöttämistä. [1; 3.]

Web-kertakirjautumisella (Web Single Sing-On, webSSO) tarkoitetaan Internet-selaimella käytettäviä verkkosovelluksia ja palveluita, jotka ovat liitetty osaksi yrityksen kertakirjautumisjärjestelmää. Web-kertakirjautuminen on toteutettu yleisesti ottaen käyttäen suosituimpia federointitekniikoita SAML (Security Assertion Markup Language) tai WS-Federation (Web Services Federation Language), jotka taas ovat XML-standardeja käyttäjien tunnistamiseen ja valtuuttamiseen tietoverkoissa. Vaihtoehtoisesti web-kertakirjautuminen voidaan toteuttaa asentamalla erillinen agentti verkkosovelluksen edustapalvelimelle, joka taas on yhteydessä yrityksen keskitettyyn kertakirjautumisjärjestelmään. Käyttäjä ohjataan kirjautumispalvelimelle yrittäessään käyttää web-kertakirjautumisella suojattua verkkosovellusta tai palvelua. Onnistuneen sisäänkirjautumisen jälkeen käyttäjä ohjataan takaisin verkkosovellukseen ja käyttäjä päästetään sisään. Käyttäjällä on nyt pääsy kaikkiin niihin verkkosovelluksiin (ilman uudelleen kirjautumista), jotka ovat liitettynä osaksi yrityksen kertakirjautumisjärjestelmää. [4; 5.]

3.3 Yhteinen käyttäjäntunnistus

Yhteinen käyttäjäntunnistus eli federointi mahdollistaa organisaatioiden välisen järjestelmien käytön yhdellä käyttäjätunnuksella ja salasanalla. Kutsun kyseistä tekniikkaa tästä eteenpäin termillä federointi. Federoinnilla tarkoitetaan yhteenliittymää ja sanakirjasta katsottaessa se on joukko valtioita, jotka ovat yhdistyneet yhden hallinnon alle. [25.] Käyttäjille tämä merkitsee sitä, että yhdet tunnukset takaavat pääsyn esimerkiksi alihankkijoiden tai yhteistyökumppaneiden järjestelmiin. Yleisesti ottaen federointitekniikka on eduksi kaikissa niissä järjestelmissä ja menetelmissä, joissa verkkosovelluksen käyttäjät tulevat organisaation ulkopuolelta. Federoinnin johtoajatuksen mukaisesti

jokainen organisaatio vastaa itsenäisesti omien käyttäjiensä tunnistamisesta ja vastaavasti verkkosovelluksen palveluntarjoaja sovellusten käyttäjien asianmukaisesta valtuuttamisesta. Federointitekniikan käyttö alentaa ulkoisten palveluiden käyttöönottokynnystä sekä vähentää IT-kustannuksia kun käyttäjien ei tarvitse muistaa kuin yksi käyttäjätunnus ja salasana. Federointipalveluiden tekninen toteutus tehdään yleensä käyttäen SAML- tai WS-Federation XML-standardeja. [6.]

Identiteetintarjoaja (Identity Provider, IdP) on osapuoli joka luo, hallinnoi, ylläpitää sekä välittää käyttäjätietoja. Se myös todentaa käyttäjän ja luo todennustunnisteen eli tiedon, joka vahvistaa kyseisen käyttäjän aitouden palveluntarjoajalle. Identiteetintarjoaja joko todentaa käyttäjät suoraan käyttäjänimen ja salasanan perusteella tai tarkistamalla epäsuorasti joltain toiselta identiteetin tarjoajalta vastaanotetut tiedot käyttäjästä. Identiteetintarjoaja tunnetaan myös seuraavilla nimillä: SAML-viranomainen (SAML authority) ja luotettu identiteetin tarjoaja (Trusted Identity Provider). [13; 14.]

Palveluntarjoaja (Service Provider, SP) on partneri, joka tarjoaa verkkopalveluita esimerkiksi sisäverkon ulkopuolelta eri organisaatiosta. Palveluntarjoaja luottaa täysin identiteetintarjoajaan. Yleisesti ottaen kaikki informaatio käyttäjistä hallinnoidaan identiteetintarjoajan päässä, mutta useimmissa tapauksissa myös palveluntarjoaja hallinnoi omaa paikallista käyttäjähakemistoa, jotta käyttäjien pääsyä sovellukseen voidaan rajata. Palveluntarjoaja tunnetaan myös nimellä Relying Party, RP. [13; 14.]

Federointitekniikan käytöllä saavutetaan monia hyötyjä:

- Alustalla ei ole väliä eli tekniikkaa pystytään käyttämään millä tahansa järjestelmällä ja sovelluksella kunhan ne ovat noudattaneet esimerkiksi SAML- tai WS-Federation standardeja niiden implementoinnissa.

- Ei vaadi käyttäjätietojen ylläpitoa eikä synkronointia hakemistojen välillä.

- Parempi käyttäjäkokemus, koska se mahdollistaa kertakirjautumisen esimerkiksi johonkin ulkopuoliseen palveluun, joka ei sijaitse yrityksen omassa sisäverkossa.

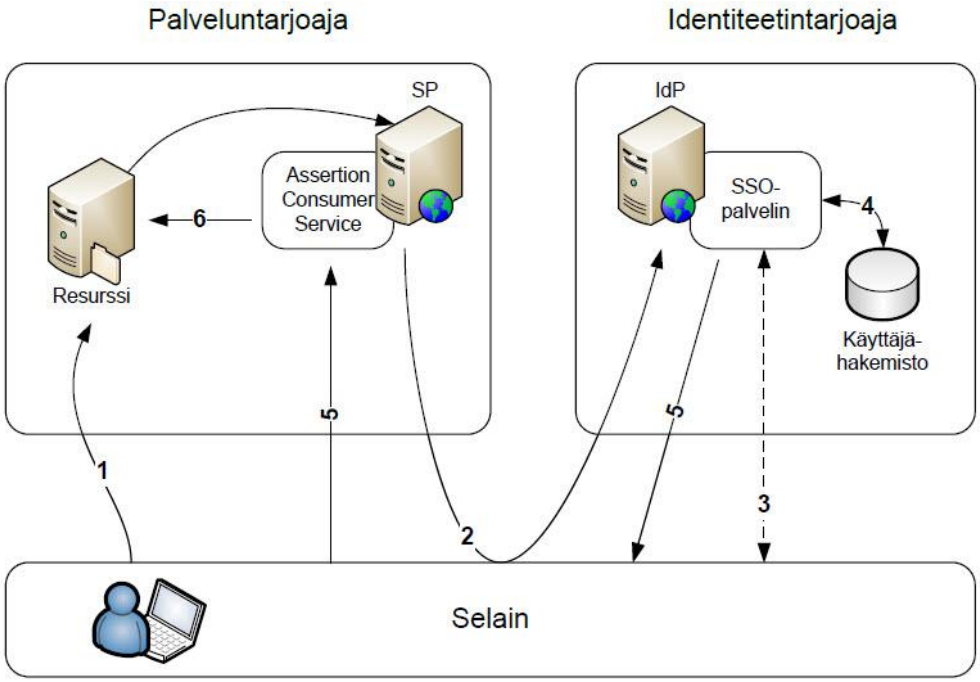
- Käyttö vähentää kustannuksia palveluntarjoajan päässä, koska käyttäjä pystyy kirjautumaan sisään useampaan ulkoiseen palveluun vain yhdellä kirjautumisella eli käyttäjätietojen hallinnointi tapahtuu identiteetintarjoajan päässä.

- Kaikki informaatio kuljetetaan XML-viesteissä mikä on informaatiopaketti joka sisältää yhden tai useamman tiedon käyttäjästä joltakin identiteetintarjoajalta. [5; 9.]

3.3.1 SAML

SAML (Security Assertion Markup Language) on OASIS (Organization for the Advancement of Structured Information Standards) Security Services Technical Committeen määrittelemä ja ylläpitämä XML-standardi käyttäjien tunnistamiseen ja valtuuttamiseen liittyvien tietojen jakamiseen tietoverkoissa. Sen pääasiallinen käyttötarkoitus on web-kertakirjautumisen toteuttaminen esimerkiksi Internet- ja intranetpalveluiden välille. [5; 9.]

Kuvassa 1 on esitetty esimerkki tilanteesta, jossa käyttäjä pyytää suojattua resurssia palveluntarjoajalta käyttäen SAML-rajapintaa.



Kuva 1. Esimerkki SAML-rajapintaa käyttävästä palvelusta.

Tapahtumat etenevät seuraavalla tavalla:

1. Käyttäjä pyytää suojattua resurssia palveluntarjoajalta (Service Provider, SP) eikä käyttäjä ei ole vielä kirjautunut sisään. Pyyntö ohjataan eteenpäin palveluntarjoajalle.

2. Palveluntarjoaja luo SAML-pyynnön (SAML AuthnRequest) ja ohjaa käyttäjän identiteetintarjoajalle (Identity Provider, IdP).

   ```
   <samlp:AuthnRequest></samlp:AuthnRequest>
   ```

3. Käyttäjällä ei ole voimassa olevaa istuntoa, joten hänet ohjataan kirjautumaan sisään järjestelmään.

4. Tiedot käyttäjästä haetaan suoraan järjestelmään liitetyistä käyttäjähakemistoista.

5. Identiteetintarjoaja luo allekirjoitetun SAML-vastauksen (SAML response) ja lähettää sen palveluntarjoajalle. SAML-vastaus sisältää kaikki ne tiedot käyttäjästä mitä palveluntarjoaja vaatii.

   ```
   <samlp:Response></samlp:Response>
   ```

6. Palveluntarjoaja muodostaa yhteyden ja päästää käyttäjän sisään sovellukseen. [19.]

3.3.2 WS-Security, WS-Trust ja WS-Federation

WS-Security (Web Services Security), WS-Trust ja WS-Federation (Web Services Federation Language) ovat standardeja, jotka määrittelevät federoinnin perusmallin. Ne kuuluvat kaikki samaan WS-*-perheeseen, ja niiden tarkoituksena on tuoda lisäsuojaa web-palveluihin.

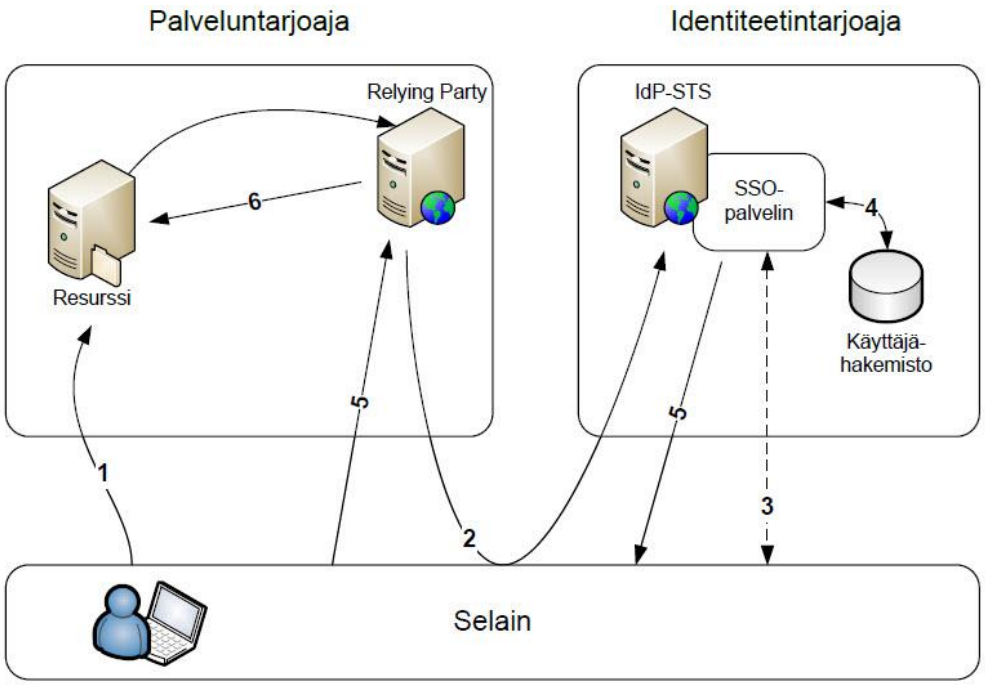
WS-Security määrittää, miten eheys ja luottamuksellisuus voidaan ottaa käyttöön useissa eri turvatunnisteissa. Sen pääpaino on XML-viestien allekirjoituksissa ja niiden

suojaamisessa. WS-Security on myös määritellyt, kuinka turvatunnisteita käytetään ja kuinka suojataan protokollat, jotka kuljettavat todennustunnisteita eli turvatunnisteita.

WS-Trust määrittelee palvelumallin eli turvatunnistepalvelun (Security Token Service, STS) ja protokollan, jota käytetään turvatunnisteiden pyytämiseen ja myöntämiseen. Turvatunnistepalvelu on ohjelmisto eli identiteetintarjoaja, joka on vastuussa turvatunnisteiden myöntämisestä sekä niiden muuntamisesta toiseen muotoon. Turvatunnistepalvelu muuntaa myönnetyt turvatunnisteet esimerkiksi SAML-viestiksi, jotka voidaan sitten jakaa kaikkien palveluntarjoajien (Relying Party, RP) kanssa. Määrittelyn tarkoituksena on saada ohjelmistoriippumaton protokolla, joka voi pyytää, myöntää, uusia, peruuttaa sekä validoida turvatunnisteita. Protokollan ydin on viestipari Request Security Token (RST), joka sisältää turvatunnistepyynnön, jonka avulla käyttäjä pyytää pääsyä johonkin verkkosovellukseen, ja Request Security Token Response (RSTR), joka sisältää allekirjoitetun turvatunnistepyynnön sekä tarvittavan informaation käyttäjästä, jonka avulla käyttäjä voidaan todentaa verkkosovelluksen päässä.

WS-Federation taas määrittää, miten turvatunnisteita siirretään eli kuljetusmekanismit. WS-Federation on IBM:n ja Microsoftin kehittelemä protokolla, joka on laajennus WS-Trust-määrittelyyn. WS-Federation rakentuu täysin turvatunnistepalvelumallin päälle, joka on määritetty WS-Trust määrittelyssä. WS-Federation-standardin periaate on sama kuin SAML-standardissa, mutta ne eivät ole kuitenkaan yhteensopivia. Protokolla kuljettaa kaiken informaation käyttäjistä väitteiden (Claims) sisällä ja niistä suosituin väitetyyppi on SAML-viesti. Tämä ei tarkoita sitä, että WS-Federation- ja SAML-standardit pystyisivät kommunikoimaan toistensa kanssa. Tuki SAML-rajapinnalle ymmärretään myös yleensä väärin. Yritykset väittävät ohjelmistojensa tukevan SAML-rajapintaa, mutta todellisuudessa ne tukevat SAML-viestejä eli väitteitä WS-Federation-rajapinnan sisällä. Tämä pätee myös tässä opinnäytetyssä käytetyssä ratkaisussa CA SiteMinder Agent for SharePoint. [8; 9; 10; 11; 12.]

Kuvassa 2 on esitetty esimerkki tilanteesta, jossa käyttäjä pyytää suojattua resurssia palveluntarjoajalta käyttäen WS-Federation-rajapintaa.



Kuva 2. Esimerkki WS-Federation-rajapintaa käyttävästä palvelusta.

Tapahtumat etenevät seuraavalla tavalla:

1. Käyttäjä pyytää suojattua resurssia palveluntarjoajalta (Relying Party, RP) eikä käyttäjä ole vielä kirjautunut sisään. Pyyntö ohjataan eteenpäin palveluntarjoajalle.

2. Palveluntarjoaja luo turvatunnistepyynnön (Request Security Token, RST) ja ohjaa käyttäjän identiteetintarjoajalle (Security Token Service, STS).

   ```
   <RequestedSecurityToken></RequestedSecurityToken>
   ```

3. Käyttäjällä ei ole voimassa olevaa istuntoa, joten hänet ohjataan kirjautumaan sisään järjestelmään.

4. Tiedot käyttäjästä haetaan suoraan järjestelmään liitetyistä käyttäjähakemistoista.

5. Identiteetintarjoaja luo allekirjoitetun turvatunnistevastauksen (Request Security Token Response, RSTR) ja lähettää sen palveluntarjoajalle. Turvatunnistevastaus sisältää kaikki ne tiedot (väitteet) käyttäjästä, joita palveluntarjoaja vaatii.

```
<RequestSecurityTokenResponse></RequestSecurityTokenResponse>
```

6. Palveluntarjoaja muodostaa yhteyden ja päästää käyttäjän sisään sovellukseen. [20.]

4 CA SiteMinder

4.1 Yleistä

CA SiteMinder on keskitetty pääsynhallintaratkaisu (Web Access Management, WAM), joka mahdollistaa käyttäjien valtuuttamisen (Authorization), todentamisen (Authentication), hallinnoinnin (Administration), kirjaamisen (Accounting) sekä kertakirjautumisen verkkosovelluksiin. SiteMinder tarjoaa keskitettyä käyttövaltuuspolitiikan hallintaa (Policy Management), joka skaalautuu helposti isoimpien yrityksien tarpeisiin. SiteMinder tarjoaa yksilöivän tavan todentaa käyttäjiä, seurata käyttäjiä sekä hallita käyttöoikeuksia, jonka jälkeen käyttäjillä on pääsy vain niihin resursseihin, joita he ovat valtuutettuja käyttämään.

Nykyään on sovelluksia, joita mahdollisesti käyttävät jopa miljoonat ihmiset ympäri maailman. Näihin kaikkiin sovelluksiin tarvitaan turvallinen pääsy sekä itse verkkosovellukset pitäisi saada suojattua. SiteMinder tekee tämän kaiken eli suojaa kaikki yrityksen verkkosovellukset ja portaalit sekä mahdollistaa kertakirjautumisen kaikkiin niihin sovelluksiin, jotka integroidaan SiteMinderin kanssa. Sovellukset voivat sijaita yrityksen sisä- tai ulkoverkossa. Verkkosovellukset integroidaan järjestelmään SiteMinder Web Agenteilla tai käyttäen yleisempiä federointitekniikoita kuten SAML ja WS-Federation. [17.]

4.2 SiteMinderin komponentit

SiteMinder koostuu seuraavista pääkomponenteista:

SiteMinder Policy Serverin tehtävänä on varmistaa, että kaikki siihen liitetyt Web Agentit eli verkkosovellukset pakotetaan käyttämään niitä sääntöjä ja käyttövaltuuspolitiikkoja, jotka ovat kyseiselle sovellukselle määriteltynä (kuva 3).

SiteMinder Web Agent on komponentti, joka asennetaan verkkosovelluksen edustapalvelimelle tai itse sovellukseen. Web Agent suojaa kaiken liikenteen palvelimelta eli kun käyttäjät pyytävät pääsyä sovellukseen, Web Agent päättää kenellä on pääsy sovellukseen ja mitkä oikeudet käyttäjä saa. Kaikki käyttövaltuuspolitiikat ovat määriteltynä Policy Serverillä, johon Web Agent on yhteydessä (kuva 3).

SiteMinder Policy Store on keskitetty tietokanta, johon kaikki Policy Serverit ovat yhteydessä. Se toimii päätallennuspaikkana kaikille käyttövaltuuspolitiikoille, suojatuille resursseille ja säännöille, jotka ovat eri sovelluksille määriteltynä (kuva 3).

SiteMinder Administrative UI on Internet-selaimella käytettävä hallintaliittymä SiteMinder-ympäristön hallintaan ja konfigurointiin. Hallintaliittymän kautta tehdään kaikki SiteMinder-ympäristön määritykset (kuva 3). [22.]

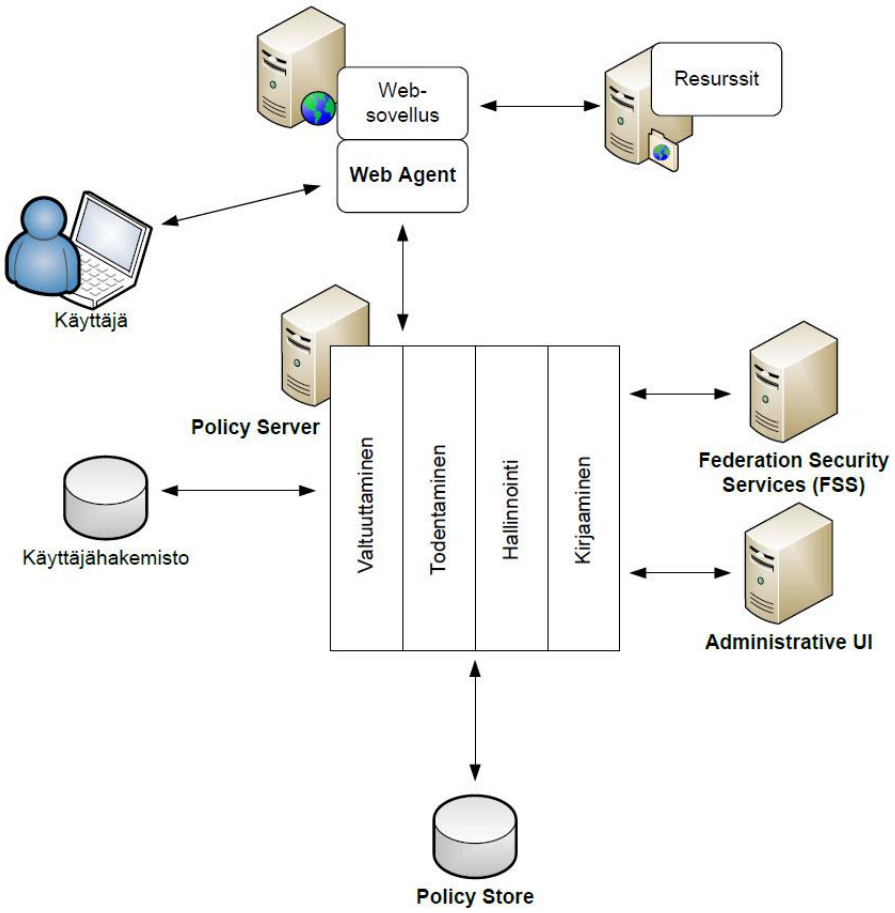
Käyttäjähakemistot (ei SiteMinder-komponentti), jotka ovat liitettynä SiteMinder Policy Serveriin. Tiedot käyttäjistä haetaan Policy Serveriin liitetyistä käyttäjähakemistoista (kuva 3).

SiteMinder Federation Security Services (FSS) on erillinen SiteMinder-laajennus, joka tukee yleisempiä käytössä olevia federointitekniikoita (kuva 3). Federointipalveluiden tekninen toteutus tehdään yleensä käyttäen SAML- tai WS-Federation-standardeja. SiteMinder tukee taulukon 1 mukaisia federointitekniikoita.

Taulukko 1. Tuetut federointitekniikat ja roolit SiteMinder-ympäristössä.

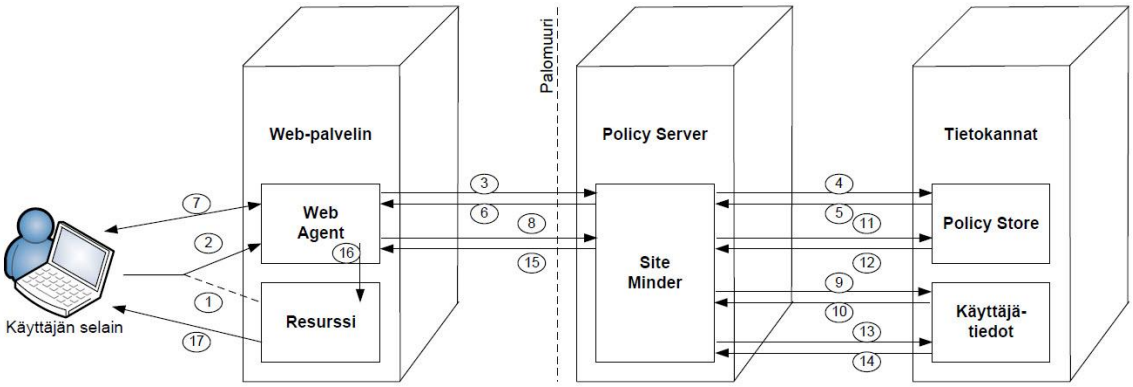
Protokolla	**Myöntää/luo SAML-assertioita**	**Vastaanottaa SAML-assertioita**
SAML 1.0/1.1	Producer	Consumer
SAML 2.0	Identity Provider (IdP)	Service Provider (SP)
WS-Federation (Legacy)	Account Partner (AP)	Resource Partner (RP)
WS-Federation (Partnership)	Identity Provider (IP)	Resource Partner (RP)

Kuvassa 3 on esitetty SiteMinder-ympäristön pääkomponentit ja se, miten komponentit ovat yhteydessä toisiinsa.



Kuva 3. CA SiteMinder pääkomponentit.

Kuvassa 4 on esitetty esimerkki tilanteesta, jossa käyttäjä pyytää suojattua resurssia eli yrittää päästä SiteMinder Web Agentilla suojattuun verkkosovellukseen.



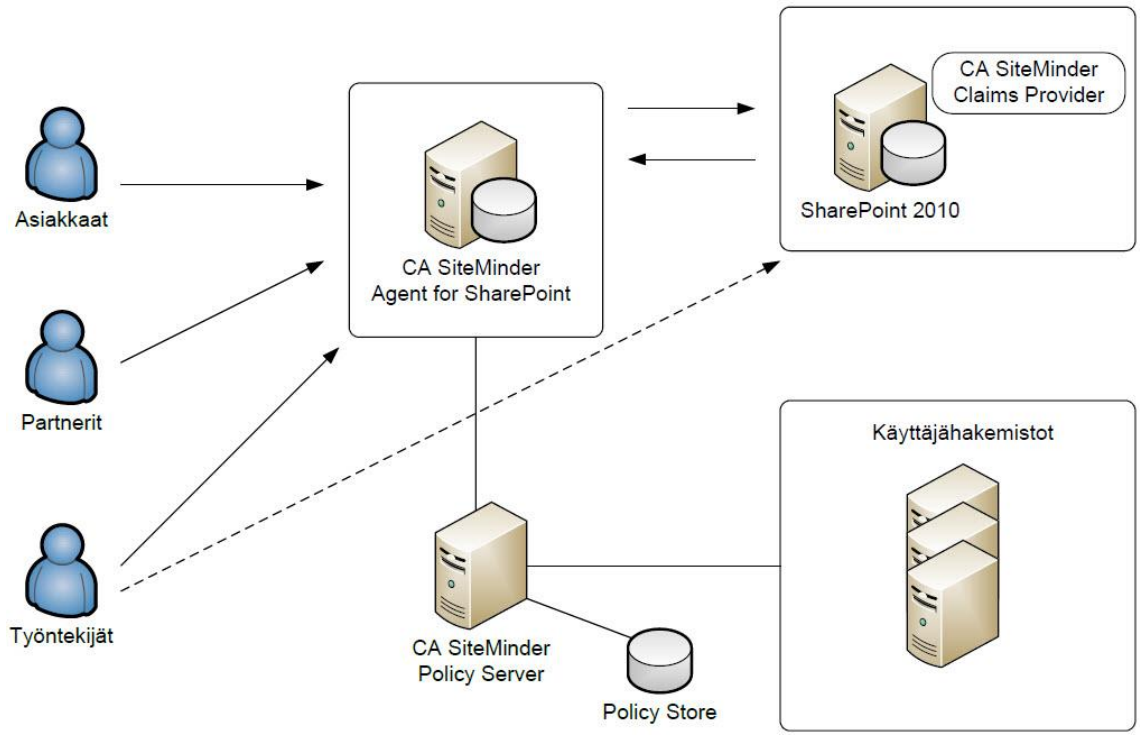
Kuva 4. CA SiteMinderin toimintaperiaate.

Tapahtumat etenevät seuraavalla tavalla:

Käyttäjä pyytää suojattua resurssia (1) ja Web Agent keskeyttää pyynnön (2). Web Agent kysyy Policy Serveriltä ”onko kyseinen resurssi suojattu?” (3), jonka jälkeen Policy Server hakee määritetyt käyttövaltuuspolitiikat ja säännöt Policy Storesta kyseiselle resurssille (4–5). Käyttäjällä ei ollut voimassa olevaa istuntoa, joten Policy Server pyytää käyttäjää kirjautumaan sisään järjestelmään (6–7). Web Agent kysyy Policy Serveriltä ”onko käyttäjä tunnistettu?” (8), jonka jälkeen Policy Server tarkistaa, löytyykö kyseinen käyttäjä Policy Serveriin liitetystä käyttäjähakemistosta (9–10). Tunnistuksen jälkeen Policy Server tarkistaa vielä, onko käyttäjällä oikeudet päästä kyseiseen resurssiin (11–12) ja noutaa samalla tarvittavat tiedot käyttäjästä (13–14). Policy Server lähettää tiedot käyttäjästä takaisin Web Agentille, jossa myös kerrotaan, että käyttäjällä on valtuudet päästä kyseiseen resurssiin (15). Web Agent prosessoi käyttäjän pyynnön ja käyttäjä päästetään sisään sovellukseen (16–17). [15; 16; 17.]

5 CA SiteMinder Agent for SharePoint

CA SiteMinder Agent for SharePoint 2010 on erillinen välityspalvelinratkaisu, jonka avulla yrityksen SharePoint 2010 -verkkoympäristö saadaan integroitua osaksi SiteMinder-pääsynhallintajärjestelmää. SharePoint Agent suojaa yrityksen kaikki resurssit ja dokumentit sekä mahdollistaa kertakirjautumisen käytön. Tällä mahdollistetaan myös yhteistyökumppaneiden turvallinen pääsy järjestelmään, koska kaikki liikenne SharePoint-palvelimille kulkee tämän välityspalvelimen kautta (kuva 5). SharePoint Agent todentaa kaikki käyttäjät SiteMinder Policy Serverin avulla, jotka pyytävät pääsyä SharePoint-sivustoihin. [21.]



Kuva 5. CA SiteMinder Agent for SharePoint pääkomponentit.

5.1 Agent for SharePoint pääkomponentit

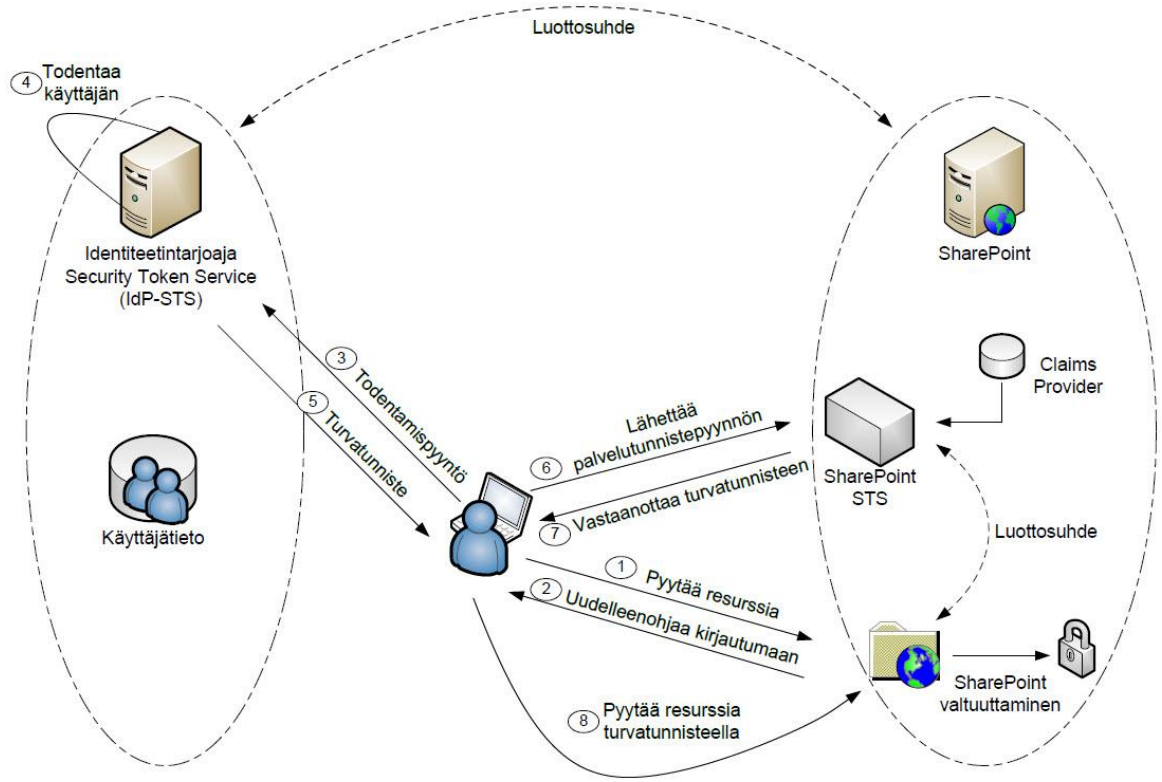
CA SiteMinder Agent for SharePoint on erillinen välityspalvelin joka pystytetään käyttäjien ja SharePoint-palvelimien väliin (kuva 5) eli toisin sanoen kaikki liikenne SharePoint-palvelimille kulkee tämän palvelimen läpi. SharePoint Agent kostuu useasta eri sovelluksesta eli itse välityspalvelin osuus on periaatteessa vain modifioitu versio CA:n tuotteesta SiteMinder Secure Proxy Server (SPS). Edustapalvelin osuus hoidetaan sisäänrakennetun Apache HTTP-palvelimen avulla, joka on avoimeen lähdekoodiin perustuva HTTP-palvelinohjelma. Kaikki liikenne palvelimelle suojataan SiteMinder Web Agentin avulla, joka on valmiiksi integroitu Apache HTTP-palvelimeen.

CA SiteMinder Claims Provider on komponentti joka asennetaan kaikille SharePoint-palvelimille (kuva 5). Sen avulla määritellään kaikki käyttöoikeudet SharePoint-sivustoille. Komponentin avulla SharePoint People Pickerillä voidaan määrittää käyttöoikeuksia käyttäjille, jotka löytyvät SiteMinder-ympäristöön liitetyistä käyttäjähakemistoista. Claims Provider on yhteydessä SharePoint Agent -palvelimella pyörivään Claims Search Web Service -sovellukseen, joka taas välittää käyttäjätietoa SiteMinder-ympäristöstä. [21.]

5.2 Väitteisiin pohjautuva todentamismenetelmä

Uuden SharePoint 2010-version myötä SharePoint tukee väitteisiin (Claims) perustuvaa todentamismenetelmää (Claims Based Authentication), joka käyttää WS-Federation-rajapintaa. Se on tunnistusmenetelmä, joka mahdollistaa ulkoisten käyttäjien todentamisen ja valtuuttamisen SharePoint-verkkosovelluksiin, jotka tulevat esimerkiksi joltain toiselta identiteetintarjoajalta (kuva 6). Aiemmin näiden käyttäjien tunnistaminen oli mahdollista vain SharePoint-ympäristöön liitettyjen käyttäjähakemistojen avulla, jotka sijaitsivat usein vain yrityksen sisäverkossa. [21.]

Kuvassa 6 on esitetty esimerkki tilanteesta jossa käyttäjä yrittää päästä väitetodennusta käyttävään SharePoint-verkkosovellukseen.



Kuva 6. SharePoint 2010 ja väitteisiin pohjautuva todentamismenetelmä.

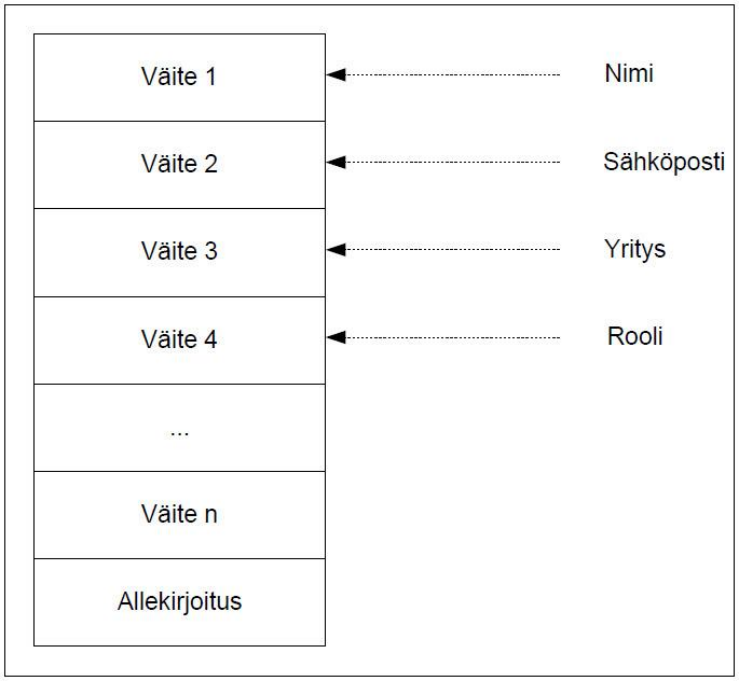
5.3 Väitteet

Väite (Claim) on tiedoksianto käyttäjästä eli jokin yksilöivä tunniste. Väitteet sisältävät tietoa käyttäjästä esimerkiksi etu- ja sukunimen sekä sähköpostiosoitteen. Väitteen sisälle voidaan asettaa oikeastaan mitä vain, kunhan se löytyy käyttäjähakemistosta kyseiseltä käyttäjältä. Väite voi myös sisältää jonkin rajoittavan tekijän käyttäjästä esimerkiksi, mihin organisaatioon kyseinen käyttäjä kuuluu, eli häneltä voidaan rajata käyttäjäoikeuksia johonkin sovellukseen organisaation perusteella.

5.4 Turvatunnisteet

Kaikki tarvittava informaatio kulkee turvatunnisteiden (Security Tokens) sisällä, jotka sisältävät yhden tai useamman väitteen käyttäjästä. Tunnisteita voidaan luoda eri muodoissa kuten SAML- tai WS-federation-rajapintaa käyttäen. Turvatunnisteet voidaan myös tarvittaessa allekirjoittaa SSL-varmenteella (Secure Socket Layer), jotta tunnisteiden sisällä oleva tieto saadaan suojattua (kuva 7). SSL-varmenne on suojaustekniikka, joka mahdollistaa suojatun yhteyden luomisen käyttäjän ja palveluiden välille, mutta tässä tapauksessa sitä käytetään turvatunnisteiden salaamiseen ja allekirjoittamiseen. Jokainen verkkosovellus joka vastaanottaa turvatunnisteita varmistaa niiden aitouden ennen kuin turvatunnisteiden sisällä olevia väitteitä käytetään mihinkään. [21.]

Kuvassa 7 on esitetty esimerkki turvatunnisteesta, jonka sisältämät väitteet käyttäjästä on allekirjoitettu SSL-varmenteella.



Kuva 7. Esimerkki turvatunnisteen sisällöstä.

5.5 Turvatunnistepalvelu

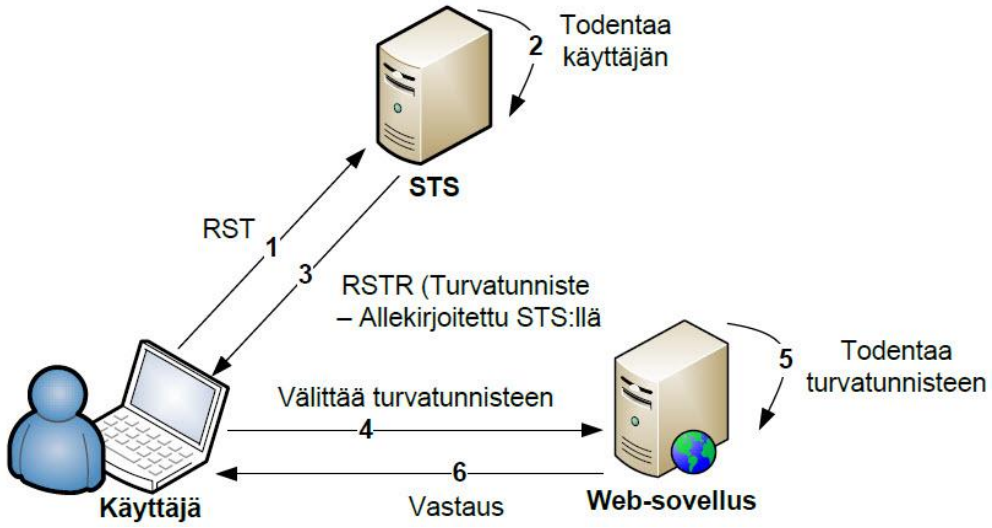
Turvatunnistepalvelu (Security Token Service, STS) on ohjelmistopohjainen identiteetintarjoaja, joka myöntää, välittää ja allekirjoittaa turvatunnisteita, jotka perustuvat WS-Trust ja WS-Federation määrityksiin. Muut palveluntarjoajat luottavat tämän palvelun luomiin turvatunnisteisiin.

Turvatunnistepalvelu käyttää seuraavanlaisia viestityyppejä:

RST (RequestSecurityToken) on viesti, joka sisältää todennuspyynnön. Pyyntö lähetetään identiteetintarjoajalle eli turvatunnistepalvelulle todennettavaksi. Pyyntö sisältää informaatiota käyttäjästä esimerkiksi käyttäjänimen ja salasanan.

RSTR (RequestSecurityTokenResponse) on vastausviesti, joka sisältää aiemmin lähetetyn RST-viestin turvatunnistepalvelun myöntämänä. Turvatunnistepalvelu vastaa RST-viestiin aina RSTR-viestillä jos käyttäjän todentaminen on onnistunut.

Kuvan 8 esimerkissä kuvataan käyttäjän todentaminen verkkosovellukseen turvatunnistepalvelun avulla.



Kuva 8. Turvatunnistepalvelun toimintaperiaate.

Tapahtumat etenevät seuraavalla tavalla:

1. Käyttäjä pyytää pääsyä verkkosovellukseen ja lähettää todentamispyynnön STS:lle RST-viestinä. RST-viesti sisältää esimerkiksi käyttäjän tunnukset, jotta STS pystyy todentamaan käyttäjän.

2. STS todentaa käyttäjän ja päättää, luodaanko käyttäjälle turvatunniste.

3. STS luo ja myöntää turvatunnisteen (esimerkiksi SAML 1.1 standardiin perustuvan tunnisteen) ja lähettää sen käyttäjälle RSTR viestinä.

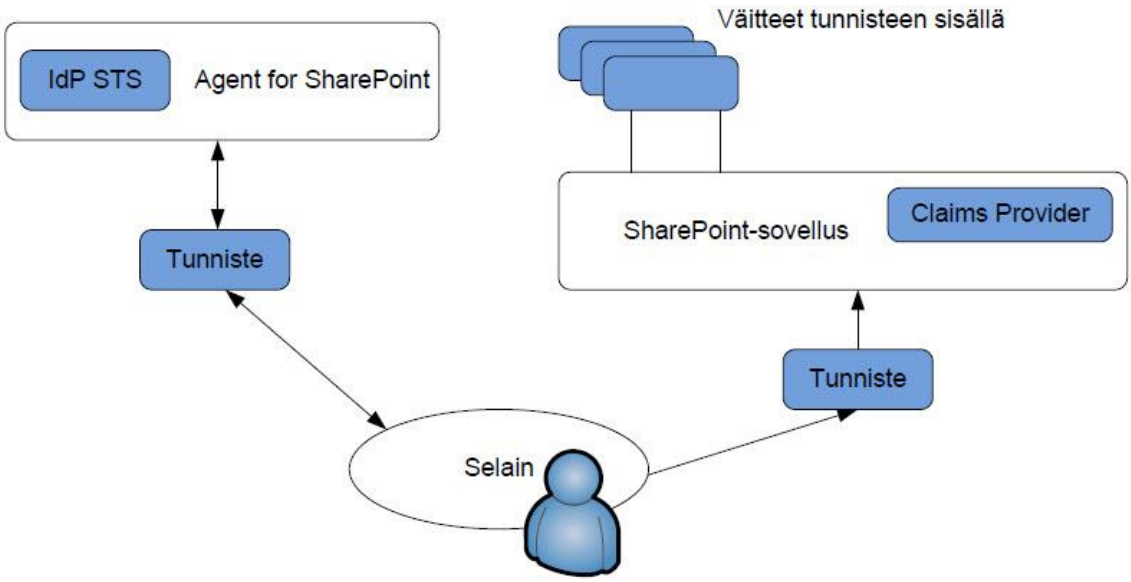
4. Käyttäjä vastaanottaa turvatunnisteen ja välittää sen verkkosovellukselle.

5. Verkkosovellus tarkistaa, että myönnetty turvatunniste on tullut luotettavalta identiteetintarjoajalta.

6. Verkkosovellus prosessoi käyttäjän pyynnön ja käyttäjä päästetään sisään sovellukseen. [23.]

Esimerkki federoinnista käyttäen väitetodennusta

SiteMinder Agent for SharePoint on ratkaisu, joka toimii yhtä aikaa identiteetintarjoajana sekä turvatunnistepalveluna, joten tulen kutsumaan kyseistä yhdistelmää nimellä IdP STS. Sen tarkoitus on todentaa käyttäjät, käsitellä väitteet ja muuntaa ne turvatunnisteiksi, joiden avulla SharePoint tunnistaa käyttäjät. Käyttäjän pyytäessä jotakin suojattua resurssia ohjaa SharePoint käyttäjän IdP-STS:lle todennettavaksi sekä pyytää lisätietoa käyttäjästä. IdP-STS:än täytyy kuitenkin pystyä todentamaan ensin käyttäjän henkilöllisyys, joten käyttäjä ohjataan kirjautumaan sisään esimerkiksi yrityksen kertakirjautumisjärjestelmään. Onnistuneen todentamisen jälkeen IdP-STS on kykenevä todentamaan käyttäjän olevan juuri se henkilö kuka hän väittää olevan. IdP-STS kerää kaiken tarvittavan tiedon käyttäjästä eli väitteet ja luo turvatunnisteen ja tiedot välitetään takaisin SharePoint-sovellukselle käyttäjän selaimen kautta (kuva 9). SharePoint tarkistaa käyttäjän turvatunnisteen ja päästää käyttäjän sisään sovellukseen. [21.]



Kuva 9. SiteMinder Agent for SharePoint toimintakaavio.

5.6 Vaatimukset CA SiteMinder Agent for SharePointille

CA SiteMinder Policy Server

SiteMinder Policy Serverin pitää täyttää seuraavat vaatimukset toimiakseen SharePoint Agentin kanssa:

- SiteMinder Policy Server v12.50
- SiteMinder Administrative UI v12.50
- SSL-varmenne turvatunnisteiden allekirjoittamiseen
- portit 44441, 44442, 44443 (kirjaaminen, todentaminen, valtuuttaminen)
- portti 44444 (yhteysvelhoa varten).

CA SiteMinder Agent for SharePoint

Asennettavan agentin minimiversio on 12.5.1, ja se vaatii minimissään 32-bittisen Java JDK version 1.6.0_30 tai sitä uudemman. Keskusmuistia tulee olla käytössä vähintään 256 MB eikä palvelimella saa olla mitään muuta HTTP-palvelinta asennettuna. Asennettava komponentti toimitetaan 32-bittisenä asennuspakettina, ja se on tuettu 32-bittisenä asennuksena kaikilla Microsoft Windows Server 2008 -versioilla (32- ja 64-bittinen).

Seuraavat portit täytyy olla avattuna CA SiteMinder Agent for SharePoint palvelimelle:

- portti 80 HTTP-pyynnöille (Apache HTTP-palvelin)
- portti 10080 HTTP-pyynnöille (Claims Search Web Service).

Microsoft SharePoint

SharePoint Agent on suunniteltu Microsoft SharePoint 2010:lle:

- Office-asiakasintegraatio (Office Client integration) vaatii vähintään Microsoft Office 2007 SP2:sen.
- Kaikki tarvittavat portit SharePoint-verkkosovelluksiin tulee olla avattuna.
- Kaikki Microsoft Windows Server ja SharePoint 2010 Service Pack päivitykset ovat tuettuja.
- Seuraavat SharePoint versiot ovat tuettuja: Foundation, Server ja Enterprise.
- SiteMinder Claims Provider toimitetaan 64-bittisenä asennuspakettina, ja se tukee samoja alustoja kuin SharePoint-palvelimet.
- SharePoint-verkkosovellukset toimivat vain väitetodentaminen (Claims Based Authentication) -tilassa. [21.]

6 CA SiteMinder Policy Serverin konfigurointi

Tässä luvussa käydään läpi tarvittavat muutokset SiteMinder Policy Serverin puolella. Käyn tarkemmin läpi vain kohdat, jotka ovat oleellisia tälle työlle. Oletuksena on, että CA SiteMinder -ympäristö on jo valmiiksi asennettu ja otettu käyttöön.

Kaikki objektit luodaan keskitetysti SiteMinder-hallintakäyttöliittymän (Administrative UI) avulla. Policy Server todentaa ja valtuuttaa käyttäjät, jotka pyytävät pääsyä SharePoint-ympäristön resursseihin. Kaikki asetukset tallennetaan keskitettyyn tietokantaan (Policy Store), johon Policy Server on yhteydessä.

6.1 SiteMinder-objektien määritys

Agent Object, jonka avulla suojattavat resurssit ja määritettävä SharePoint Agent yhdistetään toisiinsa. Luomisen jälkeen SharePoint Agent voidaan liittää suojaamaan haluttuja resursseja esimerkiksi SharePoint-sivustoja. Luodaan uusi Agent-objekti ja annetaan objektille nimi ”sharepointagent”

4.x Agent Object on tarkoitettu SharePoint Agent yhteysvelhoa (Connection Wizard) varten. Objektin avulla määritetään yhteysasetukset SharePoint Agent- ja Policy Server palvelimien välille. Luodaan uusi 4.x Agent-objekti nimeltä “sharepointagent-wizard”

Agent Configuration Object eli ACO:ssa määritellään kaikki parametrit, joilla vaikutetaan SharePoint Agentin toimintaan. SharePoint Agent on periaatteessa vain normaali SiteMinder Web Agent, joka on valmiiksi integroitu SharePoint Agentin mukana tulevaan Apache HTTP-palvelimeen. SiteMinder Policy Serverillä on jo valmiiksi määritelty ACO-objekti ”SharePoint2010DefaultSettings”, josta on tarkoitus kopioida kaikki perusasetukset määritettävälle Web Agentille. Kopioidaan kyseinen objekti ja luodaan uusi ACO-objekti nimeltä ”sharepointagent-aco”. Tämän jälkeen muokataan juuri luodun ACO-objektin parametria ”DefaulAgentName” ja määritetään sen arvoksi Agent-objektin nimi ”sharepointagent”. Nämä ovat minimivaatimukset, jotta SharePoint Agent suostuu käynnistymään. Kaikki muut asetukset tehdään myöhemmässä vaiheessa, kun lisätään uusia ominaisuuksia.

Policy Domain, joka on käytännössä vain jokin verkkosovellus joka on suojattu Web Agentilla. Verkkosovelluksen alle määritellään kaikki resurssit, käyttövaltuuspolitiikat, säännöt ja hakemistot, jotka Web Agentilla suojattuun verkkosovellukseen halutaan määritellä. Luodaan uusi Policy Domain -objekti ja annettaan sen nimeksi “SharePoint Agent”.

User Directory eli käyttäjähakemisto. Verkkosovelluksille voidaan määritellä yksi tai useampi käyttäjähakemisto, mistä halutut käyttäjät löytyvät. Testiympäristössä käyttäjähakemistona toimii Microsoftin aktiivihakemisto (Active Directory), joka on valmiiksi määriteltynä nimellä ”Userstore (AD)”. Määritetään kyseinen käyttäjähakemisto juuri luodulle Policy Domain -objektille ”SharePoint Agent”.

Realms eli ryhmä resursseja, joita Web Agentit suojaavat tai päästävät käyttäjät resursseihin ilman todennusta. Käyttäjän pyytäessä suojattua resurssia pyytää Web Agent ensin käyttäjää tunnistamaan itsensä, jonka jälkeen tiedot käyttäjästä välitetään eteenpäin verkkosovellukselle. Luodaan uusi resurssi ”/”, joka suojaa kaiken liikenteen SharePoint Agent palvelimelle. Määritellään myös aiemmin luotu Agent-objektin ”sharepointagent” suojaamaan kyseistä resurssia. SharePoint Agent palvelimella sijaitsee myös Claims Search Web Service -niminen palvelu, johon tarvitaan pääsy ilman todennusta ”/ClaimsWS/services/WSSharePointClaimsServiceImpl”. SharePoint käyttää kyseistä palvelua käyttöoikeuksien määrittämiseen yhdessä SharePoint People Pickerin kanssa.

AuthScheme on esimerkiksi jokin lomake tai tekniikka, jonka avulla käyttäjätiedot kerätään. Siihen voidaan määritellä esimerkiksi www-osoite, joka johtaa yrityksen kirjautumissivulle, jossa sitten käyttäjä syöttää tunnuksensa tai todentaa itsensä jollain muulla tavalla. Testiympäristössä on jo valmiiksi määriteltynä AuthScheme-objekti nimeltä ”HTLM-form auth. scheme”, joka johtaa keskitetylle kirjautumissivulle. Liitetään kyseinen AuthScheme-objekti aiemmin luodulle resurssille ”/”.

Rules eli säännöt, jotta SiteMinder Web Agent tietää, mitä tehdään, kun kyseistä resurssia kutsutaan. Luodaan uusi Rules-objekti eli sääntö ”*” resurssille “/”. Tämä sääntö suojaa kaiken liikenteen palvelimelle merkin ”/” jälkeen.

Policy eli käyttövaltuuspolitiikat, jossa määritellään kaikki mikä liittyy käyttäjien valtuuttamiseen. Objektiin voidaan lisätä yksittäisiä käyttäjiä, ryhmiä tai käyttäjähaaroja sekä

määrittää aiemmin luodut säännöt eri käyttäjäkunnille. Luodaan uusi Policy-objekti nimeltä ”Default Policies” ja liitetään käyttäjähaara ”OU=Sales,DC=contoso,DC=com” käyttäjähakemistosta ”Userstore (AD)” kyseiseen objektiin. Käyttäjähaarassa sijaitsevat kaikki Ekstranet-käyttäjät. Määritellään myös aiemmin luotu sääntö ”/*” käyttäjille, jotka sijaitsevat käyttäjähaarassa ”OU=Sales,DC=contoso,DC=com”. Tämän jälkeen kyseisillä käyttäjillä on pääsy kaikkiin SharePoint Agent -palvelimen resursseihin. Itse käyttäjien valtuutus tehdään kuitenkin SharePointin puolella.

6.2 Turvatunnisteiden salaaminen SSL-varmenteella

SharePoint Agent tarvitsee myös erillisen SSL-varmenteen, jotta turvatunnisteet voidaan salata, allekirjoittaa ja lähettää turvallisesti SiteMinder Policy Serverin ja SharePoint-palvelimien välillä. Tässä työssä käytetään hyväksi jo olemassa olevaa SSL-varmennetta nimeltä ”signingsps”.

7 SiteMinder Agent for SharePointin asennus ja käyttöönotto

Tämä luvussa käydään läpi CA SiteMinder Agent for SharePointin asennus sekä asetusten määrittäminen.

7.1 Asennus ja asetuksien määrittäminen

Asennus aloitetaan siirtämällä SharePoint Agentin asennuspaketit palvelimelle, jonka jälkeen käynnistetään asennusvelho nimeltä ”ca-spagent-12.5-win32.exe”. Määritetään SharePoint Agent asennettavaksi oletushakemistoon sekä valitaan käytettävä Java versio. Asennuksen jälkeen palvelin käynnistetään uudelleen.

7.2 Määritysvelho

Määritysvelhon avulla SharePoint Agent liitetään osaksi CA SiteMinder -ympäristöä sekä määritellään käytettävät portit Apache HTTP-palvelin- ja Claims Search Web Service palveluille. Rekisteröintiä eli liittämistä varten tarvitaan SiteMinder-objektien nimet, jotka määritettiin luvussa 6. Asetusten määrittäminen aloitetaan käynnistämällä Confi-

guration Wizard -määritysvelho (ca-spagent-config.cmd), jonka avulla SharePoint Agentin asetukset määritetään taulukon 2 mukaisesti. Onnistuneen rekisteröinnin jälkeen SharePoint Agent pystyy kommunikoimaan SiteMinder Policy Serverin kanssa.

Taulukko 2. Käytettävät määritysparametrit Configuration Wizard -määritysvelhoa varten.

SharePoint Agent	**Parametrit**
SiteMinder administrator name	siteminder
SiteMinder administrator password	*********
Trusted host name	sharepointagent
Host Configuration Object	sm-servers
Agent Configuration Object	sharepointagent-aco
IP address of the Policy Server where the host is registered	192.168.1.112
Host Configuration File name and location	..\proxy-engine\conf\defaultagent\SmHost.conf
Webagent Enable option	Yes
Apache Configuration	
Email address of the Agent for SharePoint administrator	admin@contoso.com
Fully qualified host name of the server	moss.extranet.contoso.com
Port number for HTTP requests	80
Port number for SSL requests	443
Claims WebService	
Port number for HTTP Claims WebService	10080
Port number for SSL Claims WebService	10443

Määritysten jälkeen käynnistetään SharePoint Agentin palvelut sekä varmistetaan palvelimen toimivuus.

Käynnistetään seuraavat Windows palvelut:

SiteMinder Agent for SharePoint niminen palvelu käynnistää sisäänrakennetun Apache HTTP-palvelimen ja SiteMinder Web Agentin. SiteMinder Agent for SharePoint Proxy Engine niminen palvelu taas käynnistää sisäänrakennetun välityspalvelimen.

Oletuksena kaikki liikenne palvelimelle (http://moss.extranet.contoso.com) ohjataan osoitteeseen (www.ca.com) SharePoint Agent -palvelimen läpi.

7.3 Yhteysvelho

SharePoint Connection Wizard -määritysvelhon avulla luodaan tarvittavat federointi-objektit (Federation Objects) SiteMinder Policy Serverin puolella eli määritellään SharePoint Agent -palvelin luotetuksi resurssikumppaniksi (Resource Partner). Resurssikumppaneiksi kutsutaan WS-Federation-rajapintaa käyttäviä verkkosovelluksia. SiteMinder Policy Server luo ja myöntää kaikki turvatunnisteet siihen liitetyille verkkosovelluksille eli palveluntarjoajille (Relying Party, RP). Kun käyttäjät pyytävät pääsyä johonkin suojattuun SharePoint-verkkosovellukseen ohjaa SharePoint käyttäjän tunnistautumaan luotetulle identiteetintarjoajalle eli SharePoint Agent -palvelimelle (IdP STS). Tämän jälkeen SharePoint Agent -palvelin kutsuu turvantunnisteiden myöntämiseen tarkoitettua palvelua SiteMinder Policy Serverillä, joka prosessoi pyynnön ja luo allekirjoitetun SAML-viestin (SAML assertion), joka muunnetaan lopuksi RSTR-viestiksi (RequestSecurityTokenResponse) eli turvatunnisteeksi. Myönnetty turvatunniste välitetään eteenpäin SharePoint Agent -palvelimelle, jonka avulla käyttäjä tunnistetaan SharePoint-verkkosovelluksessa.

Yhteysvelhon avulla määritetään myös käytettävät väitetyypit, eli tarvittavat tiedot käyttäjistä, jotka sitten liitetään haluttuihin käyttäjähakemisto attribuutteihin. Määritellyt väitetyypit lisätään turvatunnisteiden sisälle, joiden perusteella käyttäjät valtuutetaan SharePoint-verkkosovelluksessa. Määritetään myös ryhmille sekä rooleille omat väitetyyppinsä, jotta käyttöoikeuksien määrittäminen isommalle joukolle olisi helpompaa. Määrittäminen aloitetaan käynnistämällä SharePoint Connection Wizard -määritysvelho (caspconnect-12.5-win32.exe).

Määritysvelho tekee seuraavat asiat:

1. Luo uuden resurssikumppanin (Resource Partner) eli palveluntarjoajan SiteMinder Policy Serverille sekä määrittää käytettävät yhteysasetukset SharePoint Agentin ja Policy Serverin välille taulukon 3 mukaisesti.

2. Määrittää käytettävät väitetyypit eli tiedot käyttäjistä, jotka lisätään turvatunnisteiden sisälle.

3. Luo Windows PowerShell -skriptin, jonka avulla SharePoint Agentista määritetään luotettu identiteetin tarjoaja SharePoint-verkkosovelluksille. Windows

PowerShell on komentorivipohjainen skriptauskieli Microsoft Windows -käyttöjärjestelmille.

4. Kyseinen skripti suoritetaan myöhemmässä vaiheessa SharePointin keskitetty hallinta -palvelimella (Central Administration).

Taulukko 3. Käytettävät määritysparametrit Connection Wizard -määritysvelhoa varten.

Nimi	Parametrit
Policy Server Name	ps.contoso.com
Username	siteminder
Password	*********
Agent Name	sharepointagent-wizard
Shared Secret Key	*********
Select a domain	SharePoint Agent
Name	spagent
Authentication URL	http://moss.extranet.contoso.com/affwebservices/redirectjsp/redirect.jsp
SharePoint Realm	SiteMinderIDP
Skew Time	60
Validity Duration	4400
Signing Alias	signingsps
Protection Level	5
Enabled SignOut	No
Identifier Claim Names	useridentifier, userrole, smusergroups
Directory Attributes	sAMAccountName, employeeType, -

Määritysten jälkeen määritysvelho luo Windows PowerShell -skriptin nimeltä ”spagent.ps1”. Kyseistä skriptiä käytetään myöhemmässä vaiheessa SharePoint-palvelimien asetuksien määrittämisessä. Tässä vaiheessa tarkistetaan myös, että kyseinen palveluntarjoaja on luotu onnistuneesti SiteMinder Policy Serverillä (kuva 10). [21; 24.]

Kuva 10. Määritetty SiteMinder resurssikumppani.

8 SharePoint 2010:n ympäristön konfigurointi

Seuraavaksi määritellään tarvittavat asetukset SharePoint 2010 -palvelimilla. Kaikki määritykset tehdään SharePointin keskitetty hallinta -palvelimella.

8.1 Luotettu tunnistetietojen toimittaja

SharePoint 2010 tukee useita eri luotettuja identiteetin tarjoajia. Tässä luvussa määritellään uusi luotettu tunnistetietojen toimittaja eli SharePoint Agent -palvelin. Määritysten jälkeen SharePoint Agent -palvelin voi toimia luotettuna käyttäjätietojen välittäjänä yhdessä SiteMinder Policy Serverin kanssa SharePoint-verkkosovelluksille.

Turvatunnisteiden allekirjoittamiseen ja todentamiseen tarvitaan myös SSL-varmenne, joka on jo valmiiksi määriteltynä SiteMinder Policy Serverillä nimellä ”signingsps”. Kopioidaan kyseinen SSL-varmenne SharePointin keskitetty hallinta -palvelimelle. SharePoint Claims Provider tarvitsee kyseistä SSL-varmennetta turvatunnisteiden todentamiseen, jotka SiteMinder Policy Server luo, myöntää ja allekirjoittaa. Kopioidaan myös aiemmin luotu Windows PowerShell -skripti SharePoint Agent -palvelimelta, joka luotiin luvussa 7.3 ”Yhteysvelho”.

Windows PowerShell -skriptin muokkaaminen

Seuraavaksi lisätään käytettävät SSL-varmenteet, joita tarvitaan turvatunnisteiden todentamiseen. Koko ketju tarvitaan eli myös SSL-varmenteen myöntäjä. Testiympäristössä varmenteen myöntäjälle annetaan nimi ”ContosaCA” sekä itse käytettävälle varmenteelle ”SigningSPS”. Asetusten määrittäminen aloitetaan muokkaamalla aiemmin luotua Windows PowerShell -skriptiä, johon määritellään käytettävät SSL-varmenteet taulukon 4 mukaisesti.

Taulukko 4. Käytettävät SSL-varmenteet tunnistetietojen toimittajan määrittämiseen.

SSL-varmenne parametrit	**Sijainti ja nimi**
<full path to Root certificate file>	X:\ContosoCA.cer
<Trusted root authority name>	ContosoCA
<full path to Signing certificate file>	X:\signingsps.cer
<Trusted root authority name>	SigningSPS

Annetaan myös aiemmin määritetyille väitetyypeille helposti ymmärrettävät nimet, jotta saadaan parempi käsitys siitä mitä väite sisältää. Määritellään nimet käytettäville väitetyypeille taulukon 5 mukaisesti. Väitetyypit eli attribuutit yhdistetään myöhemmin virtuaalisiksi attribuuteiksi kohdassa ”SiteMinder Claims Provider”.

Taulukko 5. Käytettävät väitetyypit tunnistetietojen toimittajan määrittämiseen.

Väitetyyppi	**Nimi**
useridentifier	UserID
smusergroups	Group
userroles	Role

Määritetään vielä lisättävälle tunnistetietojen toimittajalle nimi, jonka täytyy olla sama kuin määritetty ”SharePoint Realm” -parametri osioissa ”Yhteysvelho”. Kyseinen nimi tulee näkymään SharePoint People Pickerissä luotettuna tunnistetietojen toimittajana. Määritellään myös kuvaus uudelle tunnistetietojen toimittajalle taulukon 6 mukaisesti.

Taulukko 6. Lisättävän tunnistetietojen toimittajan nimeäminen.

Tunnistetietojen toimittaja parametrit	**Nimi**
<Name of the trusted identity provider>	SiteMinderIDP
<Description for the Trusted Identity Provider>	SiteMinder Trusted IdP

Windows PowerShell skriptin suorittaminen

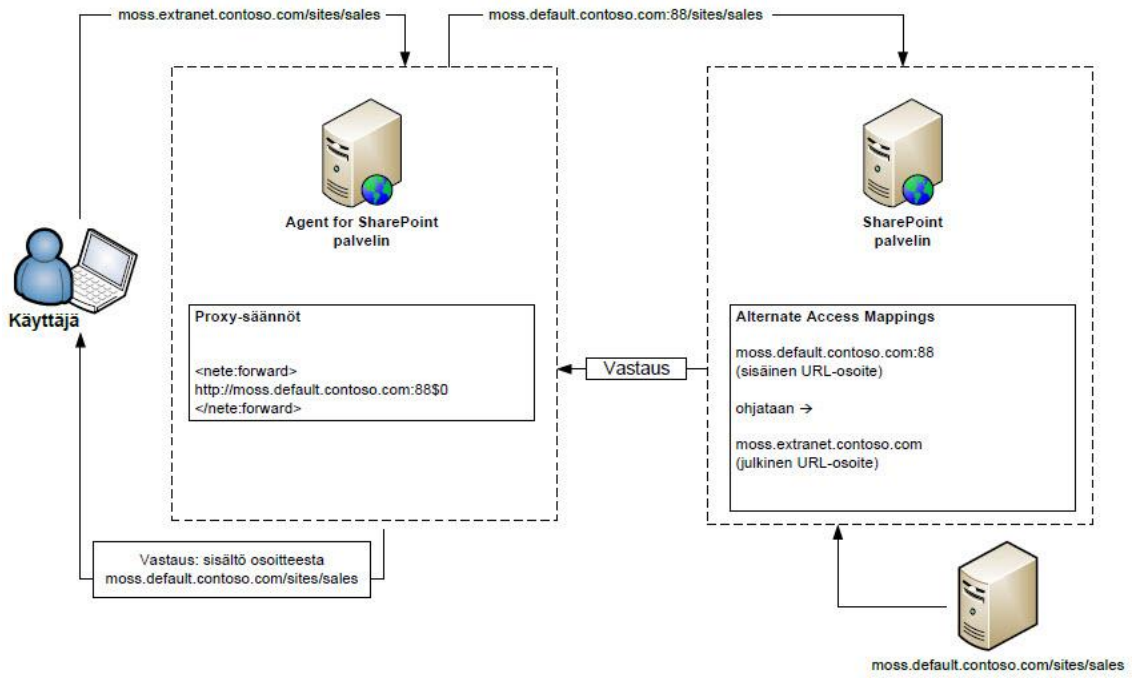
Määritysten jälkeen suoritetaan juuri muokattu Microsoft Windows PowerShell -skripti SharePointin keskitetty hallinta -palvelimella (katso liite 1). Uusi luotettu tunnistetietojen toimittaja on nyt rekisteröity, ja se on kaikkien SharePoint-verkkosovelluksien käytettävissä. Onnistuneen rekisteröinnin jälkeen tarkistetaan vielä uuden tunnistetietojen toimittajan määritykset suorittamalla komennon Get-SPTrustedIdentityTokenIssuer (katso liite 1). Tarkistetaan myös, että kaikki tarvittavat SSL-varmenteet löytyvät SharePointin keskitetty hallinta -palvelimelta” → ”Luottamussuhteenhallinta”. [21.]

8.2 Vaihtoehtoinen yhdistäminen käyttöä varten

Julkiset ja sisäiset URL-osoitteet

URL (Uniform Resource Locator) on merkkijono, jota käytetään osoittamaan verkossa sijaitsevia www-sivuja. SharePoint käyttää vaihtoehtoista yhdistämistä (Alternate Access Mappings) julkisten URL-osoitteiden ja sisäisten URL-osoitteiden vastaavuuden määrittämiseen SharePoint-verkkosovelluksissa, eli SharePoint Agent toimii välityspalvelimena, joka välittää pyyntöjä SharePoint-verkkosovelluksille käyttäen määritettyjä sääntöjä. Nämä säännöt välittävät liikennettä julkisesta URL-osoitteesta eli SharePoint Agent -palvelimelta suoraan SharePoint-verkkosovellusten sisäisiin URL-osoitteisiin (kuva 11). [21.]

Kuvan 11 esimerkissä kuvataan miten SharePoint Agent -palvelin välittää Ekstranet-käyttäjän liikenteen SharePoint-verkkosovellukseen.



Kuva 11. Kuinka liikenne välitetään sisäisille SharePoint-verkkosovelluksille.

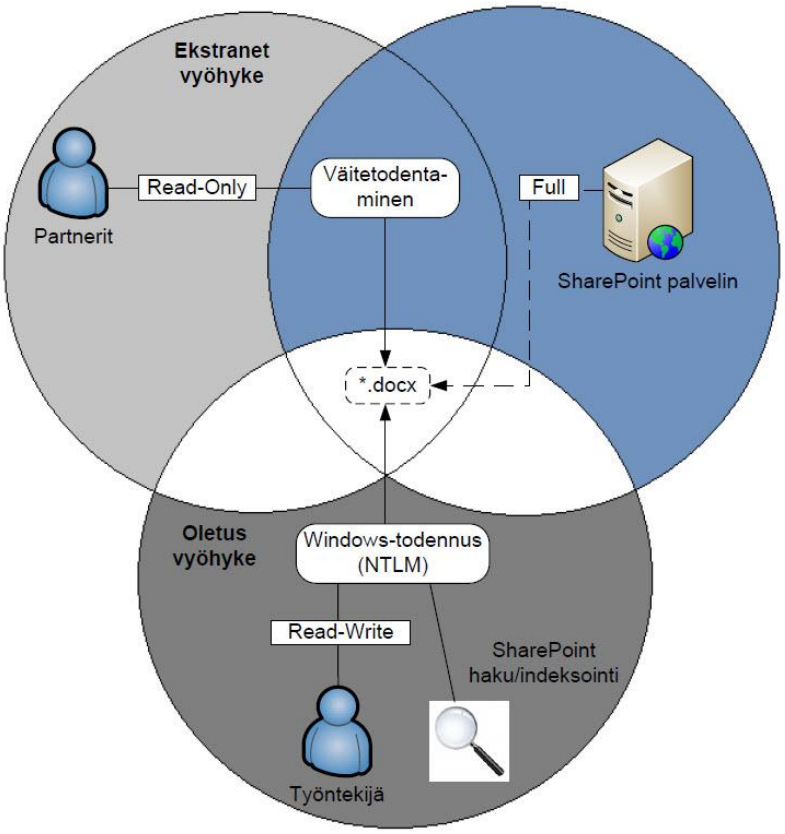
Vyöhykkeet

Jokainen SharePoint-verkkosovellus tukee viittä eri yhdistämisen kokoelmaa eli vyöhykettä kutakin URL-osoitetta kohden. Nämä viisi vyöhykettä ovat Oletus, Intranet, Ekstranet, Internet ja Oma. Kaikista SharePoint-verkkosovelluksista luodaan oma IIS (Internet Information Services) -sivusto eli verkkosovellus, jota ajetaan Microsoftin omassa HTTP-palvelin ratkaisussa. SharePoint-verkkosovellukset voidaan laajentaa käyttämään eri vyöhykkeitä, jota kutsutaan nimellä ”Laajenna WWW-sovellus toiseen IIS-sivustoon”. Laajentamisen jälkeen syntyy toinen IIS-verkkosovellus, mutta kumpaakin IIS-verkkosovellusta kohdellaan, ikään kuin ne olisivat yksi SharePoint-verkkosovellus. IIS on Microsoftin kehittämä ja käyttämä HTTP-palvelin-versio.

Kaikki verkkosovellukset ovat luonnin yhteydessä määritelty oletusvyöhykkeeseen, joten oletuksena käytetään aina Windows-todennusta, joka on integroitu Microsoftin aktiikivihakemiston kanssa. Julkiset URL-osoitteet on tarkoitettu urakoitsijoille, kumppaneille sekä asiakkaille, jotka tulevat organisaation ulkopuolelta.

Kullakin vyöhykkeellä voidaan käyttää eri todentamismenetelmiä, joten tarkoituksena on, että laajennetaan nykyistä sisäisille käyttäjille tarkoitettua SharePoint-verkkosovellusta Ekstranet-vyöhykkeellä. Uudelle vyöhykkeelle määritellään ulkoisille käyttäjille tarkoitettu julkinen URL-osoite moss.extranet.contoso.com. Tämä mahdollistaa väitetodennukseen perustuvan (Claims Based Authentication) todennustavan käytön, jota käytetään yhdessä SharePoint Agentin kanssa. [21.]

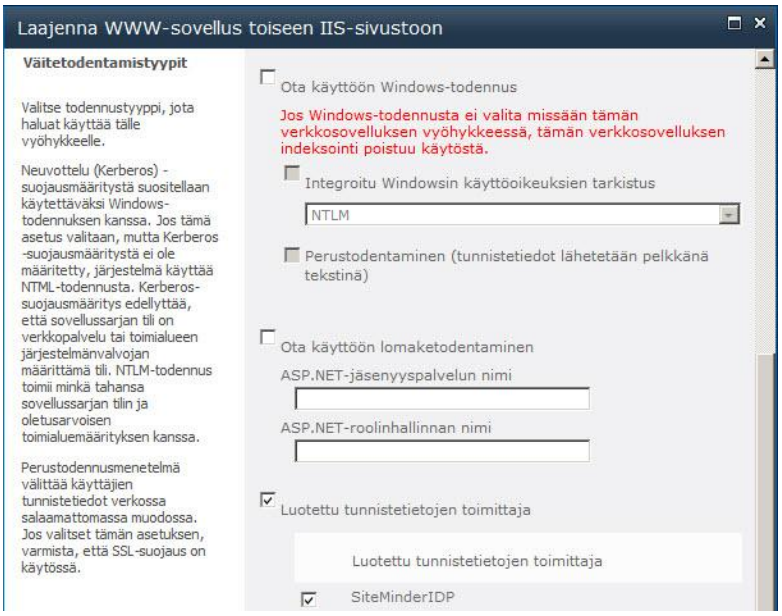
Kuvan 12 esimerkissä kuvataan, miten eri vyöhykkeillä voidaan määrittää eritasoiset käyttöoikeudet sekä käyttää useita eri todennusmenetelmiä samoihin resursseihin. Yksi vyöhykkeistä täytyy kuitenkin käyttää Windows-todennusta, jotta voidaan käyttää SharePointin haku/indeksointi ominaisuutta. [21.]



Kuva 12. Käyttöoikeuksien määrittäminen SharePoint-vyöhykkeille.

SharePoint-verkkosovelluksen laajentaminen uuteen vyöhykkeeseen

Testiympäristössä on jo olemassa oleva SharePoint-verkkosovellus ”Sales Department” osoitteessa http://moss.default.contoso.com/sites/sales, joka käyttää oletuksena Windows-todennusta. Laajennetaan kyseinen SharePoint-verkkosovellus Ekstranet-vyöhykkeeseen, johon kaikki ulkoiset käyttäjät tullaan ohjaamaan. Luodaan uusi IIS-sivusto ja annetaan sille nimi ”SharePoint Agent” sekä määritellään se ajettavaksi porttiin 88. Otetaan Windows-todennus pois päältä ja valitaan aiemmin luotu identiteetintarjoaja ”SiteMinderIDP” luotetuksi tunnistetietojen toimittajaksi (kuva 13) kyseiselle verkkosovellukselle. Lopuksi määritellään verkkosovelluksen vyöhyketyypiksi Ekstranet-vyöhyke.



Kuva 13. Uuden tunnistetietojen toimittajan määrittäminen SharePoint-verkkosovellukselle.

Julkisten ja sisäisten URL-osoitteiden määrittäminen

Seuraavaksi määritellään ulkoiset ja sisäiset URL-osoitteet juuri laajennetulle Ekstranet-vyöhykkeelle. Kyseiset asetukset määritellään SharePointin keskitetty hallinta -palvelimella kohdassa ”Määritä vaihtoehtoinen yhdistäminen käyttöä varten”. Ensimmäiseksi määritellään julkinen URL-osoite valitsemalla ”Muokkaa julkisia URL-osoitteita". Määritellään Ekstranet-vyöhykkeelle uusi julkinen URL-osoite http://moss.extranet.contoso.com, joka on tarkoitettu Ekstranet-käyttäjille. Tämän jälkeen luodaan vielä uusi sisäisen URL-osoite valitsemalla "Lisää sisäiset URL-osoitteet" ja määritellään Ekstranet-vyöhykkeelle uusi sisäisen URL-osoite http://moss.default.contoso.com:88.

Taulukko 7. Ekstranet-vyöhykkeen URL-osoitteet määritysten jälkeen.

Sisäinen URL-osoite	**Vyöhyke**	**Julkinen URL-osoite vyöhykkeelle**
http://moss.extranet.contoso.com	Ekstranet	http://moss.extranet.contoso.com
http://moss.default.contoso.com:88	Ekstranet	http://moss.extranet.contoso.com

SharePoint Agent -palvelimen määritykset

Seuraavaksi määritellään perussäännöt, kuinka SharePoint Agent -palvelin ohjaa liikenteen eteenpäin, kun palvelinta kutsutaan. Tämä tapahtuu muokkaamalla ”proxyrules.xml” määrittelytiedostoa.

Muokataan riviä ”<nete:forward>http://www.ca.com$0</nete:forward>” ja korvataan se SharePoint-ympäristön kuormantasaajan tai edustapalvelimen URL-osoitteella. Testiympäristössä käytetään aiemmin laajennettua SharePoint-verkkosovellusta, joten kaikki liikenne tullaan ohjaamaan kyseisen SharePoint-verkkosovelluksen sisäiseen URL-osoitteeseen. [21.]

<nete:forward>http://moss.default.contoso.com:88$0</nete:forward>

8.3 SiteMinder Claims Provider

SiteMinder Claims Provider on komponentti, joka integroituu SharePoint People Pickerin kanssa sekä mahdollistaa Ekstranet-käyttäjien käyttöoikeuksien määrittämisen SharePoint-verkkosovelluksissa. Claims Provider on yhteydessä SiteMinder Search Web Service nimiseen palveluun, joka on asennettu SharePoint Agent -palvelimella. Komponentti asennetaan SharePointin keskitetty hallinta -palvelimelle, jossa käyttöoikeudet eri SharePoint-verkkosovelluksille määritellään. Asennuksen jälkeen käyttäjiä voidaan hakea SharePoint People Pickerin avulla mistä tahansa hakemistosta, joka on liitettynä SiteMinder-ympäristöön.

Virtuaaliset attribuutit

Aiemmin luotujen väitetyyppien ja käyttäjähakemisto attribuuttien välille tarvitaan virtuaalinen linkki, jotta väitteiden sisällä kulkeva informaatio saadaan sidottua johonkin tiettyyn attribuutin arvoon. Määritysten jälkeen käyttäjiä, ryhmiä ja rooleja voidaan hakea väitteiden sisältämien arvojen perusteella ja näyttämään hakutulokset SharePoint People Pickerissä. SharePoint People Pickerissä nämä väitetyypit eli käyttäjähakemistoattribuuttien arvot on yleensä vaikea yhdistää oikeisiin käyttäjiin ja ryhmiin kuten taulukossa 8 on esitetty.

Taulukko 8. SharePoint People Picker näkymä ilman erikoisattribuuttia.

Käyttäjätieto	**Ryhmätieto**
sAMAccountName=usr1234	cn=grp1234,ou=groups,ou=sales,dc=contoso,dc=com

SharePoint Agent käyttää hyväksi virtuaalista erikoisattribuuttia, joka yhdistetään Microsoftin aktiivihakemiston näyttönimi-attribuuttiin ”displayName”. Määritysten jälkeen SharePoint People Picker osaa automaattisesti näyttää käyttäjän ja ryhmien nimet selkokielellä hakutuloksissa taulukon 9 mukaisesti.

Taulukko 9. SharePoint People Picker näkymä käyttäen erikoisattribuuttia.

Käyttäjätieto	**Ryhmätieto**
sAMAccountName=usr1234(John Smith)	cn=grp1234,ou=groups,ou=sales,dc=contoso,dc=com(Sales Managers)

Määritellään erikoisattribuutille virtuaalinen attribuutti SiteMinder Administrative UI:in avulla taulukon 10 mukaisesti. Yhdistetään se käyttäjähakemistoattribuuttiin ”displayName”.

Taulukko 10. Virtuaalinen erikoisattribuutti People Picker hakutuloksia varten.

Virtuaalisen attribuutin nimi	**Käyttäjähakemisto attribuutin nimi**
smuserdisplayname	displayName

Pakolliset väitteet (käyttäjätieto)

SharePoint Agent vaatii vähintään yhden väitteen käyttäjästä, jonka avulla hänet voidaan yksiselitteisesti tunnistaa. Liitetään jo aiemmin luotu väitetyyppi "useridentifier" käyttäjähakemisto attribuuttiin ”sAMAccountName” taulukon 11 mukaisesti. Tämä mahdollistaa käyttäjien hakemisen kyseisen attribuutin avulla, jonka jälkeen yksittäisille käyttäjille voidaan määrittää eritasoisia käyttöoikeuksia SharePoint People Pickerin avulla. Tämä on ainoa pakollinen väite, jonka avulla käyttäjät voidaan yksiselitteisesti tunnistaa.

Taulukko 11. Virtuaalinen attribuutti käyttäjiä varten.

Virtuaalisen attribuutin nimi	**Käyttäjähakemisto attribuutin nimi**
useridentifier	sAMAccountName

Määrityksiä voidaan helposti lisätä jälkeenpäin, jonka jälkeen käyttäjiä voidaan hakea esimerkiksi sähköpostiosoitteen avulla. SharePoint People Picker löytää tietoa vain määritettyjen väitteiden sekä määritettyjen virtuaalisten attribuuttien perusteella eli niiden sisältämien arvojen perusteella.

Valinnaiset väitteet (ryhmät ja roolit)

Ryhmille sekä rooleille voidaan määrittää myös virtuaaliset attribuutit. Ryhmät ja roolit mahdollistavat käyttöoikeuksien määrittämisen isommalle käyttäjäjoukolle SharePoint-verkkosovelluksiin yksittäisten käyttäjien sijaan. Voidaan esimerkiksi antaa vain lukuoikeudet kaikille niille käyttäjille, jotka kuuluvat johonkin tiettyyn ryhmään. Roolit taas yhdistetään johonkin tiettyyn käyttäjähakemisto attribuuttiin esimerkiksi ”employeeType”, joka sisältää arvon ”Sales Manager”. [21.]

Määritellään virtuaaliset attribuutit taulukon 12 mukaisesti, jotka aiemmin määritettiin käytettäviksi väitetyypeiksi.

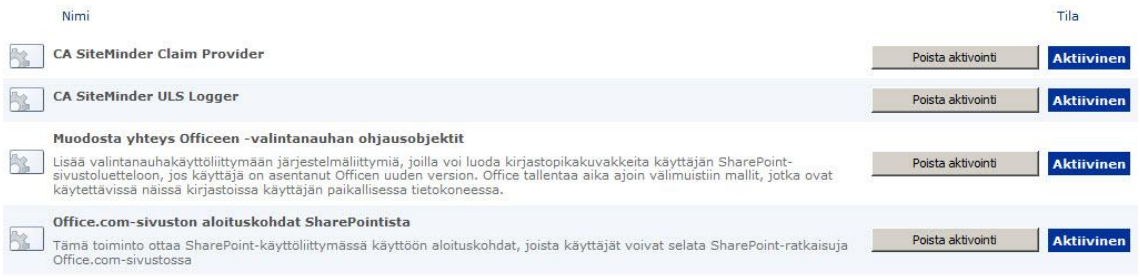
Taulukko 12. Virtuaaliset attribuutit ryhmiä ja rooleja varten.

Virtuaalisen attribuutin nimi	**Käyttäjähakemisto attribuutin nimi**
smusergroups	displayName
userroles	employeeType

8.3.1 SiteMinder Claims Providerin asennus

Asennus aloitetaan siirtämällä SharePoint Claims Providerin asennuspaketit SharePointin keskitetty hallinta -palvelimelle, jonka jälkeen käynnistetään asennusvelho nimeltä ” ca-spclaims-12.5-win64”. Määritetään SiteMinder Claims Provider asennettavaksi oletushakemistoon, jonka jälkeen palvelin käynnistetään uudelleen. Käynnistyksen jälkeen tarkistetaan, että SiteMinder Claims Provider on onnistuneesti asennettu

navigoimalla SharePointin keskitetty hallinta → ”Järjestelmän asetukset” → ”Klusterin hallinta” → ”Palvelinklusterin ominaisuuksien hallinta” (kuva 14). [21.]



Kuva 14. SiteMinder Claims Provider asennuksen tarkistaminen SharePoint-palvelimilla.

8.3.2 SiteMinder Claims Providerin käyttöönotto

SiteMinder Claims Providerin mukana toimitetaan käyttöönottoa varten tarkoitettu Windows PowerShell -skripti, jonka avulla juuri asennettu ”CASiteMinderClaimProvider” liitetään aiemmin luotuun tunnistetietojen toimittajaan ”SiteMinderIDP”. Otetaan uusi SiteMinder Claims Provider käyttöön suorittamalla alla oleva PowerShell-skripti (Update-SMTrustedIdentityTokenIssuer.ps1). [21.]

Update-SMTrustedIdentityTokenIssuer.ps1 -TrustedIdentityTokenIssuer "SiteMinderIDP"

8.3.3 SiteMinder Claims Search Web Servicen käyttöönotto

SiteMinder Claims Search Web Service on palvelu, joka on yhteydessä SiteMinder Claims Provideriin. Palvelu on asennettu SharePoint Agent -palvelimella, ja se välittää kaiken tarvittavan tiedon SiteMinder-ympäristöön liitetyistä käyttäjistä, ryhmistä sekä rooleista SharePoint People Pickerille. Kaikki informaatio välitetään väitteiden sisällä, jotka Claims Web Service vastaanottaa SiteMinder Policy Serveriltä. Palvelu otetaan käyttöön kaikissa niissä SharePoint-verkkosovelluksissa, jotka halutaan suojata SharePoint Agentilla. SharePointin keskitetty hallintasovellus tarvitsee myös kyseistä palvelua, jotta muutokset saadaan välitettyä kaikille samaan klusteriin liitetyille palvelimille. SiteMinder Claims Providerin mukana toimitetaan käyttöönottoa varten tarkoitettu Windows PowerShell -skripti (ADD-SMClaimSearchService.ps1), joka suoritetaan SharePointin keskitetty hallinta -palvelimella (katso liite 2). [21.]

SharePoint People Picker näkymä

SiteMinder Claims Provider tarjoaa vaihtoehtoja, miten SharePoint People Picker -hakutuloksien näkymää voidaan muokata. On siis mahdollista määrittää miten hakutulokset näytetään SharePoint People Pickerissä, kun käyttäjiä ja ryhmiä haetaan SiteMinder-ympäristöön liitetyistä käyttäjähakemistoista. SiteMinder Claims Provider tarjoaa kolmea eri vaihtoehtoa hakutuloksien muokkaamista varten taulukkojen 13–14 mukaisesti, jotta informaatio käyttäjistä olisi helpommin ymmärrettävässä muodossa.

Taulukko 13. Hakutulokset eli näkymä, SharePoint People Pickerissä (käyttäjätieto).

Asetus (UserName)	**Näkymä People Pickerissä**
UserNameFormat ValueOnly (oletus)	jsmith
UserNameFormat DisplaynameOnly	John Smith
UserNameFormat DisplaynameAppended	jsmith(John Smith)

Taulukko 14. Hakutulokset eli näkymä, SharePoint People Pickerissä (ryhmätieto).

Asetus (GroupName)	**Näkymä People Pickerissä**
GroupNameFormat ValueOnly (oletus)	CN=Sales,OU=Groups,OU=Sales,DC=contoso,DC=com
GroupNameFormat DisplaynameOnly	Sales
GroupNameFormat DisplaynameAppended	CN=Sales,OU=Groups,OU=Sales,DC=contoso,DC=com(Sales)

Määritellään vaihtoehto ”DisplaynameOnly” käyttöön molemmissa tapauksissa, joten hakutuloksissa näytetään käyttäjän ja ryhmän näyttönimiattribuutti (displayName). Muokataan People Picker -näkymää suorittamalla siihen tarkoitetut Windows PowerShell -skriptit (Set-SMClaimProviderConfiguration.ps1), joilla määritykset otetaan käyttöön. [21.]

Määritetään näyttönimiattribuutti käyttäjätiedolle:

.\Set-SMClaimProviderConfiguration.ps1 -UserNameFormat DisplaynameOnly

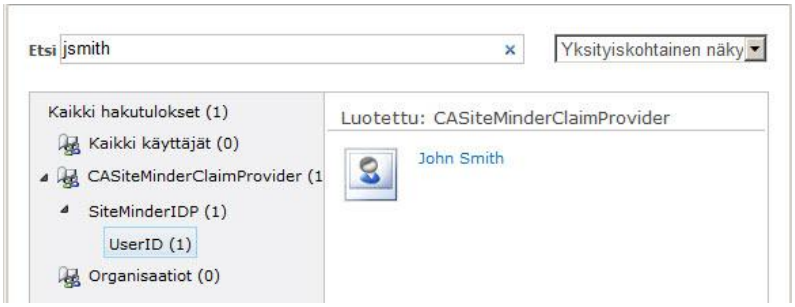
Määritetään näyttönimiattribuutti ryhmille:

.\Set-SMClaimProviderConfiguration.ps1 -GroupNameFormat DisplaynameOnly

SharePoint People Picker hakutoiminto

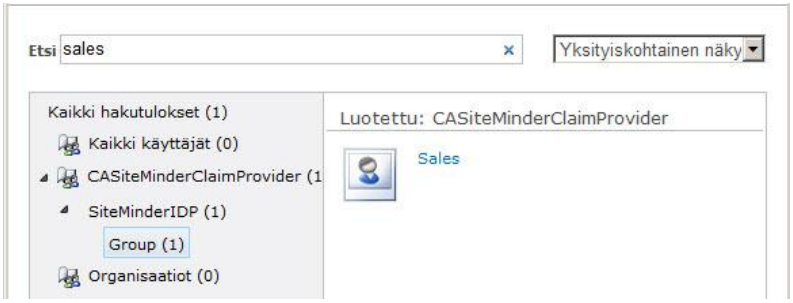
Kaikki tarvittavat määritykset on tehty ja SharePoint People Pickerin pitäisi löytää käyttäjät, ryhmät sekä roolit SiteMinder-ympäristöön liitetystä käyttäjähakemistoista. Testataan vielä toimivuus hakemalla käyttäjätietoa määritettyjen väitetyyppien avulla. Käyttöoikeuksien määrittäminen tapahtuu navigoimalla SharePointin keskitetty hallinta → Valitaan verkkosovellus ”SharePoint - Sales” ja painetaan ylävalikosta painike ”Käyttäjäkäytäntö”. Seuraavaksi valitaan ”Lisää käyttäjiä” ja valitaan vyöhykkeeksi ”Ekstranet”. Kohdassa ”Valitse käyttäjät” painetaan pientä kuvaketta nimeltä ”Selaa”. People Picker -näkymässä pitäisi löytyä aiemmin määritetty ”CASiteMinderClaimsProvider”, josta kaikki SiteMinder-käyttäjät löytyvät. Hakemiston alta pitäisi myös löytyä aiemmin luodut väitetyypit UserID, Group ja Role.

Haetaan käyttäjää ”John Smith” ja tarkistetaan, että kyseinen käyttäjä löytyy SharePoint People Pickerin avulla. Väitetyyppi ”UserID” on liitetty käyttäjähakemisto attribuuttiin ”sAMAaccountName”, joten etsitään käyttäjää väitetyypin arvolla ”jsmith”. People Pickerin pitäisi löytää ”John Smith” -niminen käyttäjä väitetyypin ”UserID” alta (kuva 15).



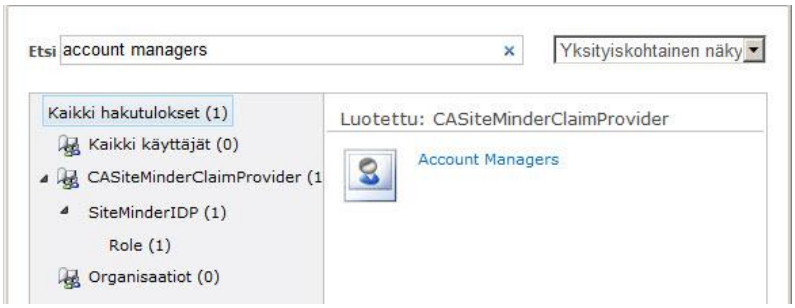
Kuva 15. Käyttäjätiedon hakeminen SharePoint People Pickerin avulla.

Seuraavaksi haetaan ryhmää nimeltä ”Sales” ja tarkastamme, että kyseinen ryhmä löytyy SharePoint People Pickerin avulla. Väitetyyppi ”Group” on liitetty käyttäjähakemisto attribuuttiin ”displayName”, joten etsitään ryhmää väitetyypin arvolla ”sales” (kuva 16).



Kuva 16. Ryhmätiedon hakeminen SharePoint People Pickerin avulla.

Testataan vielä roolihaku, joten haetaan roolia nimeltä ”Account Managers” ja tarkistetaan, että kyseinen rooli löytyy SharePoint People Pickerin avulla. Väitetyyppi ”Role” on liitetty käyttäjähakemisto attribuuttiin ”employeeType”, joten etsitään roolia väitetyypin arvolla ”account managers”. Ne käyttäjät, joiden ”employeeType” -kentän arvoksi hakemistossa on määriteltynä ”Account Managers”, kuuluvat tähän rooliin (kuva 17).



Kuva 17. Roolitiedon hakeminen SharePoint People Pickerin avulla.

8.4 Office-asiakasintegraatio

Office-asiakasintegraatio (Office Client Integration) mahdollistaa Microsoft Officen dokumenttien muokkaamisen suoraan SharePoint-verkkosovelluksesta ilman, että dokumenttia tallennetaan ensin esimerkiksi omalle koneelle. Kaikki käyttäjät voivat avata dokumentin muokattavaksi ja tallettaa muutokset suoraan SharePoint-verkkosovelluksessa sijaitseviin resursseihin.

Uusien HTTP-metodien määritys

Office-asiakasintegraatio tarvitsee toimiakseen uusia HTTP-metodeja, jotka määritetään SiteMinder Policy Serverillä. Normaalisti kertakirjautumisjärjestelmään liitetyissä

verkkosovelluksissa riittää, kun käytetään HTTP-metodeja eli operaatioita GET, POST, PUT. SharePoint Agent tarvitsee näiden lisäksi vielä kuusi uutta operaatiotyyppiä, jotta Office-asiakasintegraation käyttö olisi mahdollista. Uudet HTTP-metodit määritellään SiteMinder Administrative UI:in avulla. Olemassa olevaa agenttityyppiä muokataan ja lisätään taulukon 15 mukaiset operaatiotyypit ja tallennetaan asetukset.

Taulukko 15. Lisättävät HTTP-metodit Office-asiakasintegraatiota varten.

HTTP-metodit
PROPFIND
PROPPATCH
COPY
MOVE
LOCK
UNLOCK

Seuraavaksi otetaan uudet HTTP-metodit käyttöön eli lisätään ne alkuvaiheessa luotuun ”Protect all” -sääntöön ”SharePoint Agent” Policy Domain -objektin alle, joka suojaa kaikkia resursseja SharePoint Agent -palvelimella. Lisäksi tehdään vielä muutamat muutokset ACO-objektiin ”sharepointagent-aco”. Varmistetaan, että ”CssChecking” -parametri on asetettu arvoon “No”, koska SharePoint Agent toimii välityspalvelimena eikä asiakasintegraation käyttö ole mahdollista kyseisen tarkistuksen ollessa päällä. Sallitaan myös Office-asiakasintegraation käyttö osoitteessa http://moss.extranet.contoso.com asettamalla kyseisen arvon ”SPClientIntegration”-parametriin. Office-asiakasintegraatio on nyt määritetty ja otettu käyttöön. [21.]

9 Testaaminen

Agent for SharePoint on nyt asennettu sekä tarvittavat määrittelyt tehty. Sisäisille käyttäjille tarkoitettu SharePoint-verkkosovellus http://moss.default.contoso.com/sites/sales on laajennettu Ekstranet-vyöhykkeeseen, jonka osoitteeksi määriteltiin http://moss.extranet.contoso.com/sites/sales. Kyseinen SharePoint-verkkosovellus on myös suojattu SharePoint Agentilla, joka on liitettynä SiteMinder-kertakirjautumisjärjestelmään. Kaikki yrityksen Ekstranet-käyttäjät sijaitsevat käyttäjähaarassa: “OU=Sales,DC=contoso,DC=com”, johon on lisätty muutamia testikäyttäjiä testaamista varten. Ekstranet-käyttäjät tarvitsevat myös pääsyn kyseiseen verkkosovellukseen, joten määrittelemme ensin käyttöoikeudet ulkoisille Ekstranet-käyttäjille.

9.1 Ulkoisten Ekstranet-käyttäjien lisäys SharePoint-verkkosovellukseen

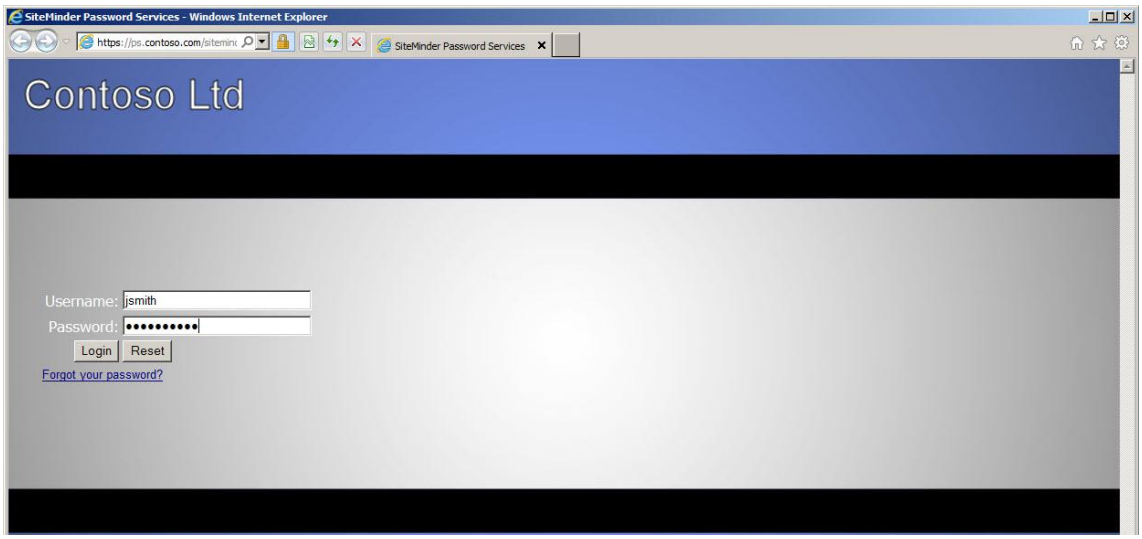
Käyttöoikeudet SharePoint-sivustoille määritetään SharePoint People Pickerin avulla, joten aloitetaan määritykset navigoimalla SharePointin keskitetty hallinta → Valitaan verkkosovellus ”SharePoint - Sales” ja painetaan ylävalikosta painike ”Käyttäjäkäytäntö”. Seuraavaksi valitaan ”Lisää käyttäjiä” ja valitaan vyöhykkeeksi ”Ekstranet”. Kohdassa ”Valitse käyttäjät” painetaan pientä kuvaketta nimeltä ”Selaa”.

Lisätään käyttäjä nimeltä ”John Smith”, joten etsitään kyseistä käyttäjää väitetyypin arvolla ”jsmith”. Valitaan kyseisen käyttäjä ja painetaan painiketta ”Lisää”. Määritetään kyseiselle käyttäjälle ”Full Control” -käyttöoikeudet ja tallennetaan määritykset. Käyttäjällä on nyt täydet oikeudet kyseiseen SharePoint-sivustoon (kuva 18).

Kuva 18. Määritetyt käyttöoikeudet yksittäisille käyttäjille Ekstranet-vyöhykkeellä.

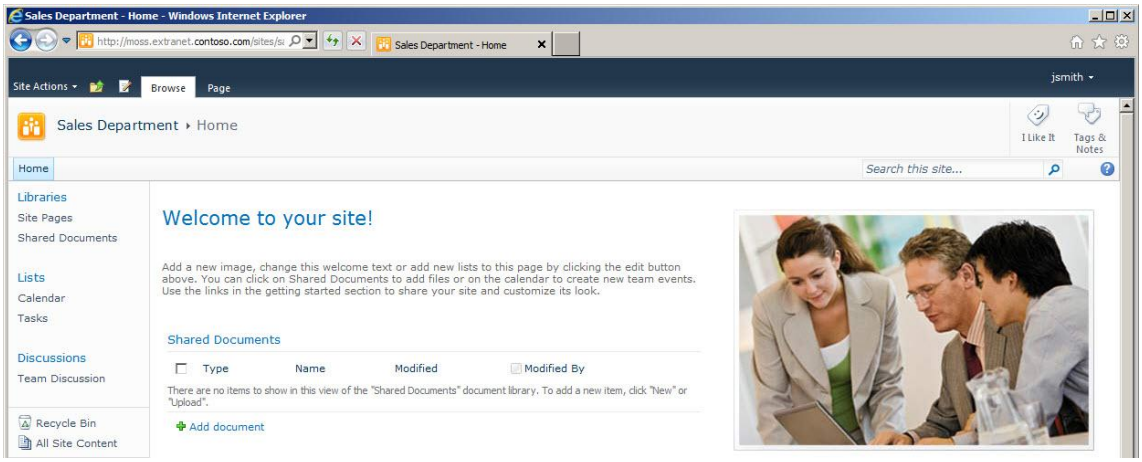
9.2 Kirjautuminen ja ominaisuuksien testaus

Seuraavaksi kirjaudutaan sisään Ekstranet-käyttäjille tarkoitettuun SharePoint-verkkosovellukseen osoitteessa http://moss.extranet.contoso.com/sites/sales. Jos käyttäjällä ei ole vielä voimassa olevaa istuntoa hänet ohjataan ensin kirjautumaan sisään järjestelmään (kuva 19).



Kuva 19. Keskitetty kirjautumissivu Web-kertakirjautumista varten.

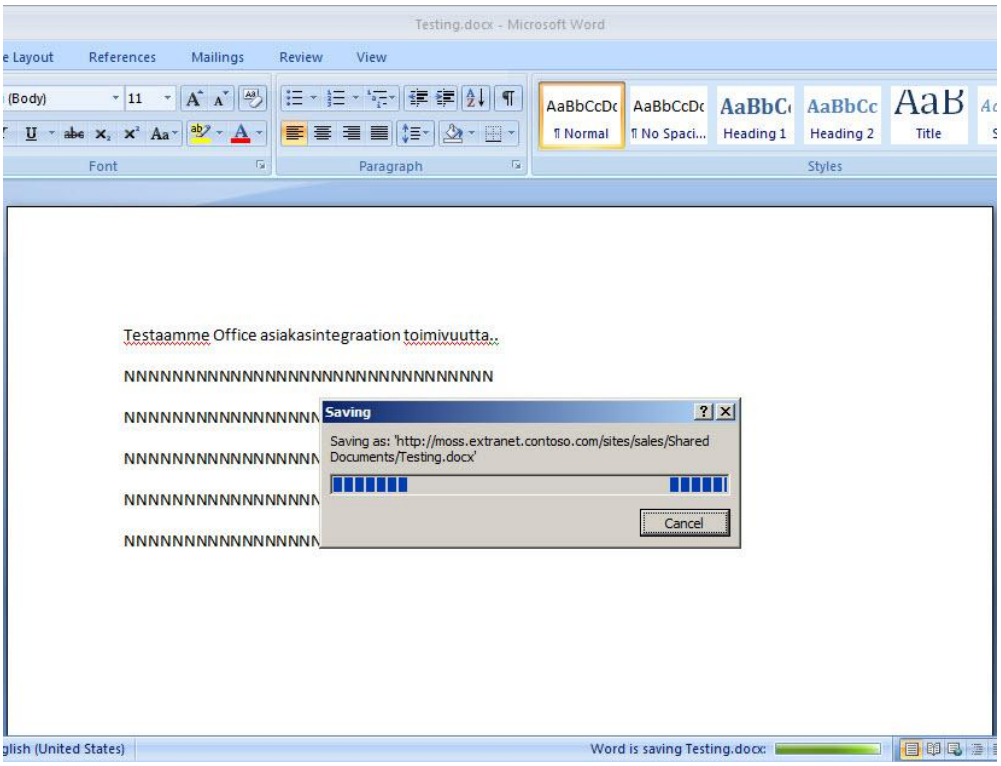
Onnistuneen tunnistuksen jälkeen käyttäjä päästetään sisään sovellukseen (kuva 20).



Kuva 20. SharePoint-verkkosovelluksen oletussivu.

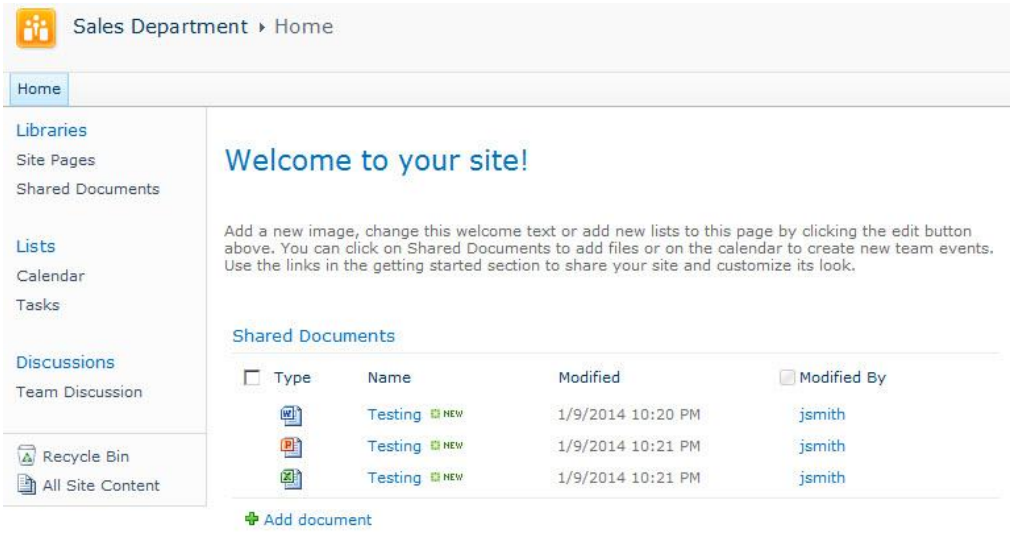
Seuraavaksi luodaan uusi Word-dokumentti testataksemme Office-asiakasintegraation toimivuutta. Luodaan Word-dokumentti ensin omalla koneella ja ladataan se Share-Point-sivuston ”Shared Documents” -kohdan alle. Valitaan juuri luotu Word-dokumentti ja avataan se muokkaamista varten valitsemalla ”Edit” (kuva 21). Word-dokumentti avautuu muokkaamista varten, jonka jälkeen muutokset voidaan tallentaa suoraan SharePoint-sivustolle. (kuva 22).

Kuva 21. Word-dokumentin avaaminen SharePoint-sivustolta.



Kuva 22. Muokatun Word-dokumentin tallentaminen suoraan SharePoint-palvelimelle.

Sama toistetaan myös Excel-tiedostolle ja PowerPoint-esitykselle. Kaikki tiedostot avattiin ”Edit” -toiminolla ja tehdyt muutokset tallennettiin suoraan SharePoint-sivustolle (kuvat 23).



Kuva 23. Muokatut Office tiedostot SharePoint-sivustolla.

9.3 Käyttöoikeuksien testaus (ryhmät ja roolit)

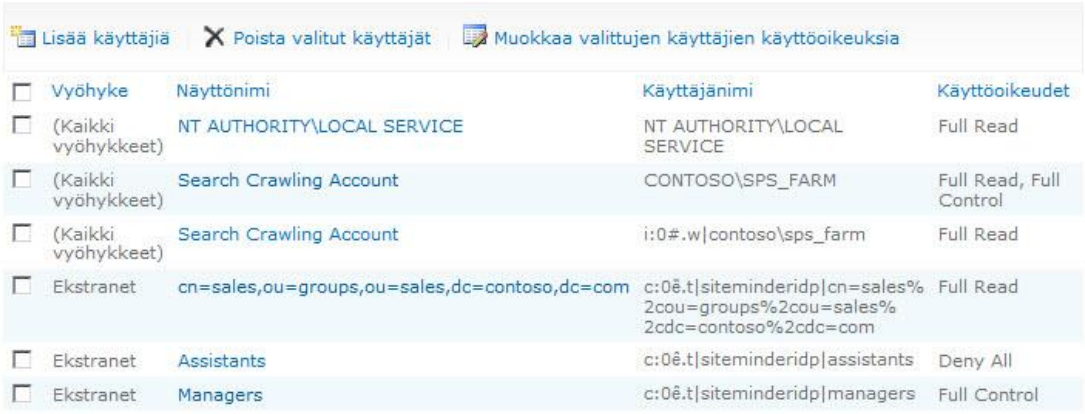
Seuraavaksi määritellään käyttöoikeuksia eri ryhmille ja rooleille eli asetetaan eritasoisia käyttöoikeuksia testaamista varten. Tarvittavat ryhmät ja roolit on määriteltynä testikäyttäjille taulukon 16 mukaisesti.

Taulukko 16. Käyttöoikeuksien määritys eri ryhmille ja rooleille.

Kokonimi	**Käyttäjänimi**	**Ryhmä**	**Rooli**
John Smith	jsmith	Sales (Full Read)	Managers (Full Control)
David Brown	dbrown	Sales (Full Read)	Assistants (Deny All)

Aloitetaan määritykset hakemalla People Pickerin avulla ryhmää nimeltä ”sales”. Valitaan kyseisen ryhmä ja painetaan painiketta ”Lisää”. Määritetään kyseiselle ryhmälle ”Full Read” -käyttöoikeudet ja tallennetaan määritykset. Kaikilla ryhmän jäsenillä on nyt vain lukuoikeudet määritettynä kyseiseen SharePoint-sivustoon.

Määritetään käyttöoikeudet myös roolien perusteella, joten haetaan roolia nimeltä ”Managers”. Valitaan kyseinen rooli ja painetaan painiketta ”Lisää”. Määritetään kyseiselle roolille ”Full Control” -käyttöoikeudet ja tallennetaan määritykset. Lisäksi estetään ”Assistants” roolin omaavilta Ekstranet-käyttäjiltä pääsy kokonaan kyseiseen SharePoint-sivustoon, vaikka hän kuuluisikin ryhmään nimeltä ”Sales” (kuva 24).



Vyöhyke	Näyttönimi	Käyttäjänimi	Käyttöoikeudet
(Kaikki vyöhykkeet)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read
(Kaikki vyöhykkeet)	Search Crawling Account	CONTOSO\SPS_FARM	Full Read, Full Control
(Kaikki vyöhykkeet)	Search Crawling Account	i:0#.w|contoso\sps_farm	Full Read
Ekstranet	cn=sales,ou=groups,ou=sales,dc=contoso,dc=com	c:0ê.t|siteminderidp|cn=sales%2cou=groups%2cou=sales%2cdc=contoso%2cdc=com	Full Read
Ekstranet	Assistants	c:0ê.t|siteminderidp|assistants	Deny All
Ekstranet	Managers	c:0ê.t|siteminderidp|managers	Full Control

Kuva 24. Määritetyt käyttöoikeudet ryhmille ja rooleille Ekstranet-vyöhykkeellä.

Testataan kirjautumista ensin käyttäjällä ”jsmith”. Kyseisellä käyttäjällä on vieläkin oikeus lisätä dokumentteja SharePoint-sivustolle, koska käyttäjälle on asetettu rooli nimeltä ”Managers” (Full Control), vaikka hän kuuluukin ryhmään nimeltä ”Sales” (Full-Read). Käyttäjällä ”dbrown” taas ei ole ollenkaan pääsyä kyseiselle SharePoint-sivustolle (kuva 25), vaikka hän kuuluu ryhmään nimeltä ”Sales” (Full-Read), koska käyttäjälle on asetettu rooli nimeltä ”Assistants” (Deny All).

Kuva 25. SharePoint -virheviesti.

10 Yhteenveto

Opinnäytetyössä integroitiin toimeksiantajayrityksen SharePoint-verkkoympäristö jo olemassa olevaan CA SiteMinder -pääsynhallintajärjestelmään ja käytiin laajasti läpi identiteetin- ja pääsynhallinnan eri osa-alueet. Tarkoituksena oli parantaa käyttäjäkokemusta, mahdollistaa kertakirjautuminen, mutta ehkä isoimpana asiana saada yrityksen asiakkaille ja kumppaneille myös turvallinen pääsy yrityksen sisäverkossa sijaitseviin resursseihin ja dokumentteihin.

Tätä toimeksiantoa tehdessä jouduin opiskelemaan melkein kaiken, mikä liittyy käyttäjien todentamiseen ja valtuuttamiseen SharePoint-verkkoympäristössä. Itse työssä käytetty tuote CA SiteMinder Agent for SharePoint oli myös hyvin monimutkainen asentaa ja määrittää, ehkä isoimpana ongelmana olivat määritettävien palveluiden määrä sekä puutteellinen ohjeistus. Tosin tuotehan on suhteellisen tuore, joten eiköhän se ohjeistus parane tässä matkan varrella. Olin myös yllättynyt siitä, mitä kaikkea Agent for SharePointin avulla voidaan tehdä ja miten saumattomasti se integroituu eri järjestelmiin ja palveluihin. Myös Office-asiakasintegraation käyttö toimi moitteettomasti, mikä oli myös niitä tärkeimpiä ominaisuuksia mitä toimeksiantajayritys tältä integroinnilta odotti.

Tuote teki kaiken, mitä siltä odotettiinkin, joten toimeksiantajayritys oli tyytyväinen lopputulokseen. Nykyinen SharePoint-verkkoympäristö saatiin liitettyä yrityksen jo olemassa olevaan kertakirjautumisjärjestelmään sekä mahdollistettiin asiakkaiden ja kumppaneiden turvallinen pääsy yrityksen sisäverkossa sijaitseviin resursseihin ja dokumentteihin.

Lähteet

1 Käsitteet ojennukseen. 2011. Verkkodokumentti. North Patrol. <http://viidestaso.wordpress.com/2011/04/29/kasitteet-ojennukseen-active-directory-ad-ldap-sso-ja-identiteetinhallinta/>. Päivitetty 29.4.2011. Luettu 7.3.2013.

2 Mitä on identiteetinhallinta. Verkkodokumentti. Propentus Oy. <http://www.propentus.com/fi/propentus_united_identity/mita_on_identiteetinhallinta.html>. Luettu 7.3.2013.

3 Single Sign On. 2006. Verkkodokumentti. Huntington Ventures. <http://www.authenticationworld.com/Single-Sign-On-Authentication/>. Päivitetty 2006. Luettu 8.3.2013.

4 Definition of Web Single Sign-On. Verkkodokumentti. Hitachi ID Systems. <http://hitachi-id.com/concepts/websso.html>. Luettu 15.3.2013.

5 Web Single Sign-On Systems. 2007. Verkkodokumentti. Washington University. <http://www.cse.wustl.edu/~jain/cse571-07/ftp/websso/>. Päivitetty Joulukuu 2007. Luettu 21.3.2013.

6 Federoinnin pika-opas (Yrityksen sisäisen julkaisu).

7 SOAP-protokolla. 2005. Verkkodokumentti. Jyväskylän yliopisto. <http://www.ad.jyu.fi/digdoc/TJTSD60_2005/soap/soap.xml>. Päivitetty 2005. Luettu 10.4.2013.

8 Web Services Federation Language. 2006. Verkkodokumentti. IBM. <http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf?S_TACT=105AGX04&S_CMP=LP>. Päivitetty Joulukuu 2006. Luettu 10.4.2013.

9 SAML Executive Overview. 2005. Verkkodokumentti. OASIS Open. <https://www.oasis-open.org/committees/download.php/11785/sstc-saml-exec-overview-2.0-draft-06.pdf>. Päivitetty 2005. Luettu 10.4.2013.

10 WS-Security. 2004. Verkkodokumentti. OASIS Open. <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf>. Päivitetty Maaliskuu 2004. Luettu 10.4.2013.

11 WS-Security. 2007. Verkkodokumentti. Microsoft. <http://msdn.microsoft.com/en-us/library/bb498017.aspx>. Päivitetty Toukokuu 2007. Luettu 10.4.2013.

12 WS-Trust and WS-Federation. Verkkodokumentti. empowerID. <http://www.empowerid.com/learningcenter/standards/ws-trust-fed>. Luettu 10.4.2013.

13 Identity provider and service provider roles. Verkkodokumentti. IBM. <http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.tivoli.fim.doc_6.2.1%2Fconcept%2FfederationproviderrolesSAML.html>. Luettu 17.4.2013.

14 Service Providers, Identity Providers & Security Token Services. Verkkodokumentti. empowerID. <http://www.empowerid.com/learningcenter/technologies/service-identity-providers>. Luettu 17.4.2013.

15 How Does SiteMinder Work. 2012. Verkkodokumentti. Blogspot. <http://itinfradiscussions.blogspot.fi/2012/02/how-siteminder-works.html>. Päivitetty Helmikuu 2012. Luettu 20.4.2013.

16 SharePoint 2010 claims based and mixed authentication. 2010. Verkkodokumentti. Blogspot. <http://karim-aziz.blogspot.com/2010/10/sharepoint-2010-claims-based-and-mixed.html>. Päivitetty Lokakuu 2010. Luettu 20.4.2013.

17 CA SiteMinder Implementation Guide. 2012. Verkkodokumentti. CA. <https://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_Files/PDF/siteminder_implementation_enu.pdf>. Päivitetty 2012. Luettu 20.4.2013.

18 Mikä on SharePoint. 2012. Verkkodokumentti. Itä-Suomen Yliopisto. <https://wiki.uef.fi/pages/viewpage.action?pageId=15008099>. Päivitetty 2012. Luettu 20.4.2013

19 SP-Initiated SSO--POST-POST. Verkkodokumentti. Ping Identity. <http://documentation.pingidentity.com/display/PF610/SP-Initiated+SSO--POST-POST>. Luettu 10.4.2013.

20 Passive Requestor Profile. Verkkodokumentti. Ping Identity. <http://documentation.pingidentity.com/display/PF610/Passive+Requestor+Profile>. Luettu 10.4.2013.

21 CA SiteMinder Agent for SharePoint. 2013. Verkkodokumentti. CA. <https://supportcontent.ca.com/cadocs/0/CA%20SiteMinder%20Agent%20for%20SharePoint%2012%2051-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?agent_for_sharepoint_guide.html>. Päivitetty 2013. Luettu 8.3.2013.

22 CA SiteMinder Policy Design Guide. 2011. Verkkodokumentti. CA. <https://support.ca.com/cadocs/0/CA%20SiteMinder%20r6%200%20SP6-

ENU/Bookshelf_Files/PDF/siteminder_ps_config_enu.pdf>. Päivitetty 2011. Luettu 8.3.2013.

23 Brokered Authentication: Security Token Service. 2005. Verkkodokumentti. Microsoft. <http://msdn.microsoft.com/en-us/library/ff650503.aspx>. Päivitetty 2005. Luettu 20.5.2013.

24 CA SiteMinder Legacy Federation Guide. 2013. Verkkodokumentti. CA. <https://enable.ca.com/support/?longURL=techinfo/siteminder12.51/casiteminder_federation_legacy_federation_guide_1251/documents/sm--12_51--siteminder_federation_legacy_federation_guide.pdf>. Päivitetty 2013. Luettu 20.5.2013.

25 Dictionary.com. 2009. Verkkodokumentti. Dictionary.com. <http://dictionary.reference.com/browse/federation>. Päivitetty 2009. Luettu 18.4.2013.

Liite 1. Luotetun tunnistetietojen toimittajan lisääminen

.\spagent.ps1

```
$rootcert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("X:\ContosoCA.cer")
New-SPTrustedRootAuthority -Name "ContosoCA" -Certificate $rootcert

$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("X:\signingsps.cer")
New-SPTrustedRootAuthority -Name "SigningSPS" -Certificate $cert

$map1 = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/claims/useridentifier" -IncomingClaimTypeDisplayName "UserID" -SameAsIncoming
$map2 = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/claims/smusergroups" -IncomingClaimTypeDisplayName "Group" –SameAsIncoming
$map3 = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/claims/userrole" -IncomingClaimTypeDisplayName "Role" -SameAsIncoming
$realm = "urn:SiteMinderIDP"
$signinurl = "http://moss.extranet.contoso.com/affwebservices/public/wsfeddispatcher"
$ap = New-SPTrustedIdentityTokenIssuer -Name "SiteMinderIDP" -Description "SiteMinder Trusted IdP" -realm $realm -ImportTrustCertificate $cert -ClaimsMappings $map1,$map2,$map2 -SignInUrl $signinurl -IdentifierClaim $map1.InputClaimType –UseWReply
```

Get-SPTrustedIdentityTokenIssuer

```
ProviderUri                 :http://moss.extranet.contoso.com/affwebservices/public/wsfeddispatcher
DefaultProviderRealm        :urn:SiteMinderIDP
ClaimTypes                  :http://schemas.xmlsoap.org/claims/useridentifier
                            :http://schemas.xmlsoap.org/claims/smusergroups
                            :http://schemas.xmlsoap.org/claims/userrole
HasClaimTypeInformation     :True
ClaimTypeInformation        :{UserID, Group, Role}
IdentityClaimTypeInformation :Microsoft.SharePoint.Administration.Claims.SPTrustedClaimTypeInformation
ClaimProviderName           :
UseWReplyParameter          :True
Description                 :SiteMinder Trusted IdP
SigningCertificate          :[Subject] CN=signing.sps.contoso.com
                            :[Issuer] CN=ContosoCA
Name                        :SiteMinderIDP
TypeName                    :Microsoft.SharePoint.Administration.Claims.SPTrustedLoginProvider
DisplayName                 :SiteMinderIDP
Status                      :Online
```

Liite 2. SiteMinder Claims Search Web Servicen lisääminen

SharePoint-verkkosovellus “Sales Department”:

.\ADD-SMClaimSearchService.ps1 -WebApplication http://moss.default.contoso.com:88 -claimSearchService http://moss.extranet.contoso.com:10080/ClaimsWS/services/WSSharePointClaimsServiceImpl

SharePointin keskitetty hallintasovellus:

.\ADD-SMClaimSearchService.ps1 -WebApplication http://moss:27681 -claimSearchService http://moss.extranet.contoso.com:10080/ClaimsWS/services/WSSharePointClaimsServiceImpl