Haaga-Helia
ammattikorkeakoulu Oy

Federaatio palveluna ja identiteettimallina Office 365:n kanssa

Antti Suutarla

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2018

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Antti Suutarla

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Federaatio palveluna ja identiteettimallina Office 365:n kanssa

Sivumäärä
35

Opinnäytetyön otsikko englanniksi
Federation as a service and as an identity model with Office 365

Tämä opinnäytetyö käsittelee federoitua, claim-pohjaista, identiteettimallia todentamisen ja valtuuttamisen yhteydessä, sekä federaatiopalvelua teknisenä komponenttina. Työssä avataan federoidun identiteetin perusajatusta yleismaailmallisin esimerkein tukien niin, että asiaa teknisesti tuntemattomankin on helppo lähestyä konseptia ja hahmottaa, mistä on kyse.

Käytännön teknisen toteutuksen kohteeksi on valittu useissa organisaatioissa suunnitteilla tai jo käytössä oleva Office 365 -palveluarkkitehtuuri. Työn teoria- ja pohdintaosuus nivoutuvat yhteen Office 365:n kanssa, kun työssä rakennetaan Microsoftin IT-infrastruktuuriratkaisuihin pohjautuva tekninen federaatiopalvelu sen yleisimmät toteutuksen hyvät käytännöt huomioiden. Toteutuksen yhteydessä hahmotetaan myös, kuinka käytetty todennus- ja valtuutustapa loppukäyttäjän näkökulmasta muuttuvat ja kuinka käyttäjä tästä esimerkiksi kertakirjautumisen kanssa hyötyy.

Työn tuloksena on valmis, teknisesti toteutettu palvelukomponentti, jonka kautta claim-pohjaista todennusta ja valtuutusta käytetään Office 365:n kanssa. Tuloksena myös lukijalla tulisi olla käsitys, kuinka aiemmin totutusta poikkeavasta toteutus- ja ajattelutavasta federoidussa autentikoinnissa on kyse, sekä kuinka sitä voisi sovellusteknisten mahdollisuuksien rajoissa hyödyntää muissakin toteutuksissa Office 365:n toimiessa vain yhtenä sovelluskohtaisena esimerkkinä.

Asiasanat
federaatio, identiteetti, federaatiopalvelu, office 365

Sisällys

1 Johdanto

Office 365 ohitti vuonna 2017 myynnissä määrällisesti ensimmäistä kertaa tavallisen, paikalliselta medialta käytettävän Office-tuoteperheen myynnin. (Fortune 2017.) Tämän ja muiden, niin kutsuttujen pilvi- ja SaaS-palveluiden yleistyessä ja mullistaessa tavallisten IT-palveluiden kenttää jatkuvasti, ovat niissä lukuisin eri tavoin palveleva federaatiopalvelu ja sen tarjoama federoitu identiteetti yksi infrastruktuuripalveluiden merkittävimmistä taustatekijöistä tänä päivänä. Tämän teknisen palvelukomponentin tarkoitus on mahdollistaa palvelukohtaisesti rajatun luottamusverkon sisällä yhden käyttäjäidentiteetin toiminta eri järjestelmien välillä, ja termi itsessään tarkoittaakin käyttäjän erillisten identiteettien kytkemistä toisiinsa. (Valtiovarainministeriö 2008, 39.) Federaatiopalvelun avulla voidaan tehdä loppukäyttäjälle näennäisesti merkityksettömän erillisen identiteetin olemassaolo näkymättömäksi niin, ettei tämän tarvitse lainkaan huolehtia identiteetin elinkaaren hallinnan yleisimmistä kulmakivistä, kuten esimerkiksi erillisestä tunnuksesta salasanoineen tai kesäloman aikana vanhentuneesta sellaisesta.

Microsoft-natiivissa IT-infrastruktuuriympäristössä federaatiopalvelu on luonnollisinta toteuttaa tätä varten tarjolla olevalla Windows-palvelinkäyttöjärjestelmäroolilla, joka tunnetaan nimellä Active Directory Federation Services. Nimensä mukaisesti palvelu yhdistyy paikalliseen aktiivihakemistoon, joka palvelee identiteetin – tunnistustietojen – tarjoajana. Vaikka palvelun käyttämä teknologia tai standardit eivät ole millään tavalla uusia, on monelle yritykselle ensimmäinen federaatiopalvelun potentiaalinen tarve tullut eteen vasta sitä merkittävästi hyödyntävän, yrityksille ja yhteisöille suunnatun Office 365 -palvelun myötä aivan viime vuosina. Tämän mukana on voitu hyödyntää täysin uusia tapoja virtaviivaistaa käyttäjäidentiteetin ja sen elinkaaren hallintaa tavoista, jotka aiemmin ovat rajoittuneet paikallisiin tai toisaalle kokonaan eriytyneisiin, usein vähemmän standardeihin pohjautuviin ratkaisuihin.

Tämän opinnäytetyön kohderyhmä ovat Office 365:n käyttöönottoa tai sen palveluarkkitehtuurin kehittämistä suunnittelevan organisaation IT:n ja tämän päätöksenteon ympärillä työskentelevät henkilöt. Suurin hyöty työstä on nähtävissä teknisen arkkitehtuurin ja ratkaisusuunnittelun parissa työskenteleville asiantuntijoille. Työn tavoite on tälle kohderyhmälle selvittää, mikä Office 365:n taustalle käyttöönotettavan federaatiopalvelun ja sen muodostaman luottamusverkon sisällä käytettävän identiteetin tarkoitus on, sekä kuinka federoitua identiteettiä itseään käsitellään todennuksen ja valtuutuksen kanssa. Tavoitteena on myös esittää, kuinka federaatiopalvelu voidaan teknisesti toteuttaa Office 365:n kanssa ja mitä toteutuksessa tulee huomioida. Esitetty ratkaisu- ja toteutustapa palvelusta

ovat toki vain yksi lukuisista erilaisista mahdollisuuksista toteuttaa vastaava palvelu, mutta tuotantokäyttöön lähes sellaisenaan täysin sopiva.

1.1 Työn rajaus

Samasta nimestään huolimatta yritys- ja yhteisökäyttöön tarkoitettu Office 365 eroaa tavalliselle kuluttajalle suunnitellusta, vastaavanlaisesta tuotepaketista merkittävästi. Siinä missä kuluttajaversio nojaa taustalla olevaan palveluarkkitehtuuriin lähes yksinomaan palvelun tilauksen ja lisensoinnin vahvistamisen puolesta, on yrityskäytössä taustalla valinnaisia, mutta huolellista suunnittelua vaativia palvelukokonaisuuksia. (Microsoft a.) Nämä kaikki nojaavat joko jollakin tavalla yhdistettyyn tai natiivisti samaan, federoituun, käyttäjäidentiteettiin, joista jälkimmäinen on tämän työn keskiössä. Mahdollisesti käyttöön otettavia palveluita kuten Exchange Online, Skype for Business tai Yammer ei kuvata sen tarkemmin erikseen. Näitä vastaavista pääteohjelmista puolestaan havainnollistetaan ainoastaan selainkäyttöiset versiot. Koko Office 365 -yritysalustan käyttöönotto itsessään vaatii myös ennalta pohdittavia, organisaatiokohtaisia rajauksia, joita työ ei käsittele. Koska hyödyistään huolimatta federaatiopalvelun käyttöönotto Office 365:n yhteydessä ei ole pakollista, odotetaan lukijalta perusymmärrystä organisaatioiden käyttöön suunnatun Office 365:n palveluarkkitehtuurista, sen yleisistä vaatimuksista ja Windows-palvelinkäyttöjärjestelmätekniikasta. Tällaisen tiedon voidaan kohderyhmältä odottaa löytyvän. Teknisesti federaatio Office 365:n kanssa on myös mahdollista toteuttaa lukuisilla muiden toimittajien kuin Microsoftin ratkaisuilla, mutta niitä työ ei käsittele.

1.2 Keskeisiä käsitteitä

Azure AD -hakemisto Office 365:n taustalla oleva (pilvi)käyttäjähakemisto. Organisaatiokohtainen ja nimeltään uniikki, erottava tekijä eri organisaatioiden välillä. Office 365- ja Azure AD -käyttäjähakemistoja voidaan käsitellä synonyymeinä ja niistä käytetään myös nimitystä **tenant**.

Claim Tunnistusseloste, jossa todennettu käyttäjäidentiteetti välitetään. Claim itsessään ei määrittele mihin käyttäjä voi tai ei voi päästä, se määrittelee todennetusti mitä käyttäjä on tai ei ole. On claimin vastaanottavan osapuolen tehtävä määritellä tämän perusteella, mihin käyttäjällä on – tai ei ole – valtuutus. Käytetään myös nimitystä **assertion**. Myös federoitu identiteetti rinnastetaan usein termiin claim-pohjainen autentikointi. (Roundtree 2013, 54-55.)

Claims provider Federaatiopalvelun luottama osapuoli, joka on lähde federoidun identiteetin muodostamiseen. Tämän opinnäytetyön puitteissa aktiivihakemisto – Active Directory Domain Services (AD DS). Tunnetaan myös käsitteellä **(claims) issuer** – taho, jonka tietojen pohjalta claim myönnetään. (Roundtree 2013, 55-56.)

Federaatio Luottamusverkosto, johon kuuluvien palveluntarjoajien ja tunnistajien kanssa käyttäjäidentiteetillä voidaan asioida turvallisesti ja saumattomasti kuin yhdessä ympäristössä. (Valtiovarainministeriö 2008, 61.)

Federaatiopalvelu Tekninen komponentti, joka tuottaa palvelualustan claims-pohjaiselle todennukselle. Tässä opinnäytetyössä **Active Directory Federation Services (AD FS)**.

Identity provider Osapuoli, joka vastaa käyttäjän tunnistamisesta ja tunnistusselosteen välittämisestä palveluntarjoajalla. Tämän työn puitteissa federaatiopalvelu; AD FS. Tunnetaan myös lyhenteellä **IdP**, tai voidaan käyttää termiä **STS; Security Token Service**. (Baler ym 2013, XXV.)

Kertakirjautuminen Kirjautuminen määrätyllä käyttäjätunnuksella palveluun niin, että käyttäjätunnus on autentikoitu vain kerran. Käytetään myös nimitystä **SSO; single sign-on**. (Valtiovarainministeriö 2008, 49.)

(Käyttäjä)identiteetti Joukko ominaisuuksia, jotka kuvaavat käyttäjää ja joiden avulla käyttäjä voidaan yksilöivästi tunnistaa. (Valtiovarainministeriö 2008, 39.)

SaaS eli **Software as a Service** on (pilvi)palvelutoimitusmalli, jossa sovellus tarjotaan käyttöön palveluna ilman organisaatiolle omistettua ja asennettua tuotantoympäristöä, jonka päällä sovellusta ajetaan.

SAML XML-pohjainen avoin protokolla, jota käytetään välittämään tunnistusväline (token) todennuksesta ja valtuutuksesta vastaavan luottamusverkoston sisällä. Lyhenne sanoista **Security Assertion Markup Language**.

(Security) Token Tunnistusväline, joka kuljettaa muodostetun claimin digitaalisesti allekirjoitettuna. Allekirjoituksella voidaan varmistua claimin alkuperästä ja eheydestä. (Roundtree 2013, 55.)

Service provider Palveluntuottaja tai -tarjoaja, jolle claimin sisältävä token välitetään valtuutusta varten. Termi tunnetaan AD FS:n yhteydessä myös nimellä **Relying Party** ja vastaavilla lyhenteillä **SP** tai **RP**. Service provider on tässä työssä Office 365. (Baler ym 2013, XXIV)

Todentaminen Varmistuminen identiteetin todenmukaisuudesta, oikeellisuudesta ja alkuperästä. Käytetään myös termiä **autentikointi**. (Valtiovarainministeriö 2008, 112.)

Valtuuttaminen Todennetulle käyttäjälle myönnetty lupa määrätyn tiedon käyttöön. Käytetään myös termiä **autorisointi**. (Valtiovarainministeriö 2008, 126.)

WS-Federation Osa WS-* -määrittelymallia, joka kirjautumisprotokollana keskittyy claimien ja tokenien käsittelyyn. Office 365 käyttää oletuksena WS-Federation -protokollaa. (Goodner M., Hondo, M., Nadalin, A., McIntosh, M., Schmidt D. 2007, Part 1.)

1.3 Työssä käytetyt tekniset määritykset

Työssä viitataan esimerkinomaisesti nimillä muun muassa paikallisiin toimialueratkaisuihin ja Office 365:n sekä Azure AD:n hakemistoihin eri yhteyksissä. Esimerkkien ja käytännön toteutuksen selkeyden vuoksi työssä esitettävissä ratkaisuissa on näille määritetty seuraavat nimet:

- Organisaation nimi: **Sikhmi & Co.**
- Paikallinen toimialue (aktiivihakemisto):
    - FQDN: **sikhmi.net**
    - NETBIOS-nimi: **SIKHMI**
- Julkinen DNS -nimi: **sikhmi.net**
- Office 365- / Azure AD -hakemisto: **sikhmi365.onmicrosoft.com**
- Federaatiopalvelun nimi: **fs.sikhmi.net**
- Federaatiopalvelun URL: **https://fs.sikhmi.net**

2 Federaatiopalvelun rooli ja federoitu identiteetti

Hämmennystä aiheuttavan terminologian sijaan federaatiopalvelun käsitettä ja toimintaa voidaan lähestyä kokonaan toisesta, yleismaailmallisemman näkökulman esimerkistä:

Olet lähdössä matkalle ja sinun täytyy päästä lentokoneeseen (**Office 365**). Et voi kävellä suoraan koneeseen sisään, vaan sinun täytyy kulkea lentokentän (**federaatiopalvelu**) läpi. Menet lentokentällä lipputiskille (**claims provider**), jossa sinulta kysytään passia identiteettisi varmistamiseksi **(todentaminen)**. Todennuksen onnistuttua saat virkailijalta henkilökohtaisen matkalippusi (**claim**), joka on varustettu nimetyn lentoyhtiön luottamin tunnuksin (**token**). Lippu oikeuttaa sinut määrätyn lentoyhtiön tietylle lennolle tiettyyn kohteeseen ja voit tämän portilla virkailijalle esittämällä (**valtuutus**) nousta kyytiin koneeseen (**service provider**). (Baler ym 2013, 3-4.)

Koko tapahtumaketjun täytyy tapahtua tässä järjestyksessä, ja jos yksikin osa tapahtumaketjusta epäonnistuu, et pääse lennolle. Jos esimerkin lentokenttä olisi kokonaisuudessaan yrityksen itsensä omistamaa, luottamaa ja hallinnoimaa toimialuetta, ei luottamusverkostoja ulkopuolisiin tahoihin – kuten kentällä operoiviin muiden lentoyhtiöiden toimijoihin – tarvitsisi rakentaa eikä niissä käytettyä erillistä identiteettiä tietoturvineen, elinkaarinen ja muine merkittävine tekijöineen ylläpitää. Aiemmin luottamusverkostoja rakennettaessa on jouduttu nojaamaan verkkoteknisesti ja tietoturvallisesti raskaisiin luottosuhteisiin kokonaisten toimialueiden välillä. Näissä usein koko organisaatio on määritelty tietyin ehdoin luottamaan toiseen vain sen takia, että näiden välillä on voitu käyttää yksittäisiä resursseja yksisuuntaisesti tai keskenään ristiin. Tätä ovat sanelleet ensisijaisesti vanhemmat autentikointiprotokollat, kuten Kerberos ja NTLM, joiden käyttö soveltuu yhä hyvin organisaation toimintaan sen omassa sisäverkossa pysyttäessä. (Baler ym 2013, XVIII; Ivey 2013; Roundtree 2013, 18-19.)

Toinen meille kaikille varmasti tuttu esimerkki on verkkopankkitunnuksilla kirjautuminen johonkin palveluun. Tässä luottamusverkosto syntyy siitä, että emme luovuta verkkopankin autentikointitietoja suoraan kolmannen osapuolen palveluun, vaan verkkopankille itselleen. Tällöin palvelun ja pankin välillä vallitsee luottamusverkosto, jossa palvelu luottaa verkkopankilta saamaansa tietoon käyttäjän identiteetistä. Palvelun tehtäväksi jää ainoastaan valtuuttaa käyttäjä määrättyyn tietoon pääsyyn tämän identiteetin perusteella.

SaaS- eli Software as a Service -malliset palvelut, kuten Office 365, ovat perinteisellä pelikentällä uusia tekijöitä. Näiden toiminnan ajatuksena on tuottaa sovelluksia käytettäväksi

palveluna ilman, että käyttäjäorganisaation itse tarvitsee tehdä mittavia investointeja rakentaakseen palvelun vaatimaa taustainfrastruktuuria. Palvelun käyttämä taustainfrastruktuuri on valmiina olemassa ja organisaatio itse maksaa sen käytöstä esimerkiksi käyttäjämäärän tai käyttökapasiteetin mukaan, myös ilman huolia infrastruktuurin vaatimasta ylläpidosta. (Microsoft Azure.) Näistä käytettäessä termiä pilvipalvelu syntyy usein mielikuva, että palvelun taustainfrastruktuuri on vain mystisesti jossakin. Tämä puolestaan saattaa herättää huolta siitä, missä ja miten tietoa säilytetään, kuka siihen pääsee käsiksi, miten tiedon saatavuuden voidaan häiriötilanteissa varautua ja niin edelleen. Nämä kysymykset ovat palveluntarjoajalle kohdistettuina oleellisia, mutta täytyy muistaa, että kyseessä on palvelutuotantomalli. (Grance & Mell 2011, 2-3.) Samat kysymykset tulisi selvittää yhtä lailla, jos organisaatiolla itsellään olisi esimerkiksi konesali huolehdittavanaan.

Federoitu identiteetti ja claim-pohjainen autentikointi saattavat kuulostaa taivaan lahjalta eri identiteetti- tai todennusmallien suunnittelussa, mutta näin ei aina automaattisesti ole. Esimerkiksi saman toimialueen sisällä toimiessa käyttäjillä on jo olemassa yksi yhteinen identiteettisäilö – aktiivihakemisto – sekä usein käytössään Windows-maailmasta tunnetut kirjautumisratkaisut, kuten Kerberos tai varmennepohjainen X.509-todennus yhdistettynä Integrated Windows Authentication -ominaisuuteen, jolloin erillistä identiteetin todennusta ei tarvitse tehdä. (Gregory 2014a; Baler ym 2013, 2-3.) Jos sen sijaan jokin Office 365:n alustasovellus, kuten SharePoint, asennetaan paikallista infrastruktuuria vasten, on usein mahdollista asettaa käyttöön claim-pohjainen todennus. Merkittävää lisähyötyä siitä ei tällaisessa käyttöskenaariossa kuitenkaan saada. Jos sen sijaan paikalliselle, organisaation sisäiselle toimialueelle asennettaisiin SharePoint, jota käyttäisivät myös ulkopuoliset tahot ilman mahdollisuutta toimialueen sisäiseen autentikointiin, olisivat hyödyt selkeästi nähtävät. Tällöin ei olisi tarvetta työläille ja raskaille toimialueiden välisille luottamussuhteille, joilla resursseja on tavanomaisesti valtuutettu. (Ivey 2013.) Kun yhtälöön lisätään se, että ulkopuolisten käyttäjien identiteetti voitaisiin hallita paikallisen toimialueen ulkopuolella ja samalla estää sisäisen toimialueen näkyvyys ulkopuolisille tahoille käytännössä kokonaan, olisivat hyödyt jo merkittäviä.

Tämä ajattelutapa käännettynä toisin päin on monien muiden pilvipalveluiden lisäksi myös Office 365:n lähtökohtaisia toiminta-ajatuksia: Lukuisat organisaatiot käyttävät samojen alustapalveluiden päälle rakennettuja samoja sovelluspalveluita mutta erillään toisistaan niin, että heillä ei ole yli organisaatiorajojen mitään näkyvyyttä. Näin ollen he ovat myös eristettyinä toistensa ympäristöistä. Esimerkiksi vastaavasta voitaisiin mieltää hotelli, jossa ei olisi yhteisiä käytäviä, tiloja tai palveluita, vaan jokaiselle käyttäjäorganisaatiolle kokonaan oma sisäänkäynti. Tästä olisi kyllä pääsy kaikille tarjolla oleviin palveluihin, mutta kaikista muista hotellin käyttäjäorganisaatioista erillään ja heille näkymättömästi.

Ajatusta voidaan jatkaa claim-pohjaisessa todennuksessa claimin itsensä sisältöön ja sen merkitykseen. Käyttäjäidentiteetille voidaan etukäteen määritellä claimina, mihin tällä on valtuutus. Federaatiopalvelun myöntämästä claimista voisi edellä mainittu hotelli päätellä esimerkiksi, ettei käyttäjällä ole valtuutusta hotellin ravintolapalveluihin. Käyttäjän ei tarvitsisi selvittää tätä hotellilla erikseen esitellen henkilöllisyystodistustaan ja hotellin varaustietojaan eri tahoille useaan otteeseen, vaan tämä olisi ennalta määrätty ja hotelli toimisi tämän, luottamusverkon kesken määräävän tekijän mukaan. Tällöin samainen SharePoint-käyttäjä ei edes näkisi sivustoa, johon hänellä ei ole valtuuksia ja välttyisi täten turhalta autentikoinnilta, joka ei autorisoinnin puolesta johtaisi mihinkään. Identiteetin valtuutus on kuitenkin sovelluksen vastuulla, se on vain claim-pohjaisesti autentikoidessa ennalta määrättyä identiteetin ja sen lähteen perusteella. (Baler ym 2013, 12.)

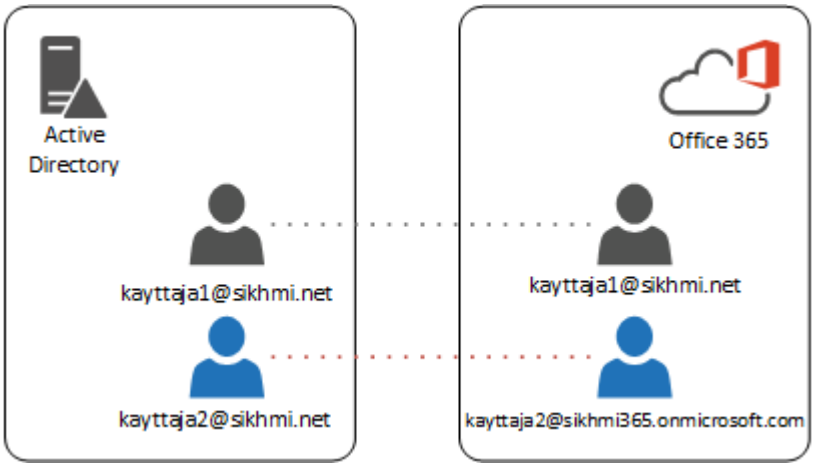
Tällaisten käyttöskenaarioiden ratkaisumalli rajoittuu kuitenkin myös alusta- ja sovellustukeen. Esimerkiksi sähköpostipalvelun paikallisesti asennettava toteutusvaihtoehto, Microsoft Exchange, ei tue federoitua autentikointia pääteohjelmista käsin, vaikka samat pääteohjelmat, kuten Outlook, voivat hyödyntää sitä natiivisti (Office 365:n) Exchange Online -alustan kanssa. (Redmond, T., Cunningham, P., Van Horenbeeck, M. & Hansen, S. 2018, Chapter 3.) Exchangen kohdalla sen historian painolastin ja niistä siirtymävaiheiden mukanaan tuomia syitä tarkemmin analysoimatta voi olla sovellusteknisesti todella raskasta, jopa mahdotonta, lisätä valmiiseen sovellukseen myöhemmin tuki claim-pohjaiselle autentikoinnille, jos sovelluksessa ei toiminnallisuutta tälle ole alkujaan olemassa. Koko sovellusteknisen toteutuksen, sen hyödyntämien identiteettilähteiden ja näiden monimuotoisuuden sekä sovelluksen käyttötarkoitusten lisäksi on siis syytä huomioida sovelluksen itsensä asettamat reunaehdot claim-pohjaisen todennuksen ja valtuutuksen käyttömahdollisuudelle ylipäätänsä. (Gregory 2014a; Roundtree 2013, 34-35.) Mikäli sovellus lähtökohtaisesti suunnitellaan tämä mielessä tai se tukee tätä muuten, voidaan siitä käyttää nimitystä claims-tietoinen (claims-aware).

Näillä muutamalla esimerkillä on havainnollistettavissa se, kuinka jopa yhden sovellustoimittajan saman tuoteperheen sovellusten paikallisesti ja SaaS-mallilla tarjottavien palveluiden erot voivat toteutusteknisesti erota merkittävästi toisistaan. Tämä työ ei kuitenkaan käsittele paikallisia toteutuksia palveluista näitä rinnastuksia enempää, sillä koko Office 365 on rakennettu alusta alkaen mallilla, jossa organisaatiokohtaisia luottamusverkostoja voidaan esteettä hyödyntää jokaisen palvelukomponentin kanssa ja siihen jopa rohkaistaan.

3 Identiteetti ja Office 365

Office 365:n kanssa voidaan käytännössä käyttää kolmea erilaista identiteettimallia. (Microsoft b.)

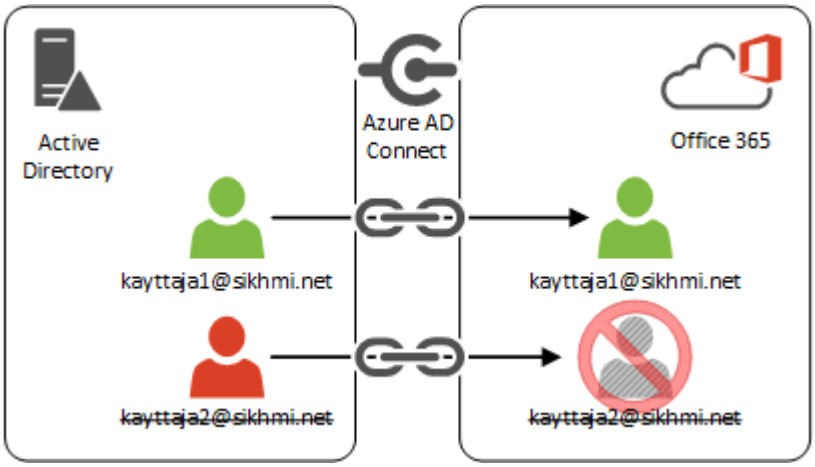
3.1 Pilvi-identiteetti



Kuva 1. Puhdas pilvi-identiteetti, jossa käyttäjätunnukset ovat toisistaan erillään

Pilvi-identiteetti on lähtökohtaisesti tunnistettavissa sen onmicrosoft.com -päätteestä (**sikhmi365.onmicrosoft.com**), jossa sitä ennen tuleva pääte on Office 365 -hakemiston uniikki nimi. (Microsoft d.) Jos organisaatio on lisännyt Office 365:n käyttöön oman julkisen toimialueensa nimen, kuten **sikhmi.net**, voidaan pilvi-identiteetille määritellä käyttöön myös tämä. Tällöin loppukäyttäjän tunnus paikallisessa käyttäjähakemistossa voi olla esimerkiksi **kayttaja1@sikhmi.net** ja Office 365:ssä samanmuotoinen. Tunnuksilla ei todellisuudessa ole kuitenkaan sen enempää yhteistä, vaan niitä tulee hallinnoida eri paikoista (Active Directory ja Office 365 Admin Portal) ja niillä on lähtökohtaisesti muun muassa eri salasana. Lisäksi salasanakäytännöt saattavat olla erilaisia, jolloin käyttäjällä on näennäisesti sama tunnus, mutta hänen tulee kuitenkin huolehtia näiden vaatimasta ylläpidosta erikseen. Jos tunnus ikään kuin naamioidaan tällä tavalla samannimiseksi, voi se aiheuttaa käyttäjälle sekaannusta, sillä hänelle itselle ei ole täysin selvää kumpaa tunnusta hän milloinkin käyttää. Oleellista on mainita myös, että autentikointi tapahtuu suoraan Azure AD:a vasten. (Microsoft b; Redmond ym 2018, Chapter 4.)

3.2 Synkronoitu identiteetti

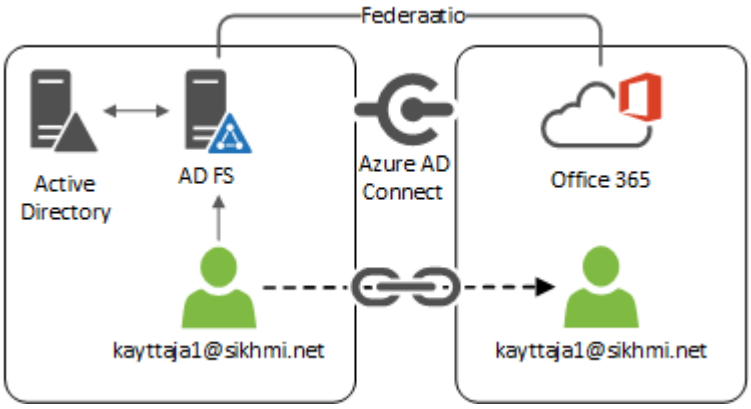


Kuva 2. Synkronoitu identiteetti, jossa paikallinen hakemisto on määräävä

Synkronoitu identiteetti nimensä mukaisesti synkronoidaan paikallisesta aktiivihakemistosta Office 365:n taustalla olevaan Azure AD -hakemistoon. Tällöin käyttäjätunnuksia ei tarvitse hallita useassa eri paikassa, vaan merkitsevä lähde identiteetin tiedoille on yksi ja sama. Käyttäjätunnuksen sisältämät tiedot pysyvät yhtenäisinä määrätyin aikavälein tapahtuvan hakemistosynkronoinnin myötä. Jos käyttäjätunnus poistetaan paikallisesta hakemistosta, poistuu se automaattisesti myös Office 365:stä. Synkronointiin voidaan sisällyttää myös käyttäjätunnuksen salasana (hash-muodossa), jolloin ei tarvitse hallita erillisiä salasanoja tunnukselle ja merkitsevä salasanakäytäntö on myös yhtenäinen paikallisen hakemiston kanssa.

Synkronoidulla identiteetillä ei kuitenkaan voida toteuttaa aitoa kertakirjautumista, eli käyttäjän tulee oletusarvoisesti aina palveluihin päästäkseen syöttää käyttäjätunnus ja salasana käsin. Synkronoitu identiteetti vaatii pohjalle Office 365 -hakemiston, johon käyttäjähakemisto synkronoidaan. Yhteen Azure AD -hakemistoon voidaan tuoda tietoja vain yhdestä synkronointipalvelusta. Synkronointi tehdään Microsoftin siihen varta vasten tarjoamalla Azure AD Connect -nimisellä työkalulla, jonka toimintaan ei kuitenkaan tässä perehdytä. Myös synkronoidulle identiteetille oleellista on, että autentikointi käyttäjätunnuksella tapahtuu suoraan Azure AD:a vasten. (Microsoft b; Redmond ym 2018, Chapter 4.)

3.3 Federoitu identiteetti



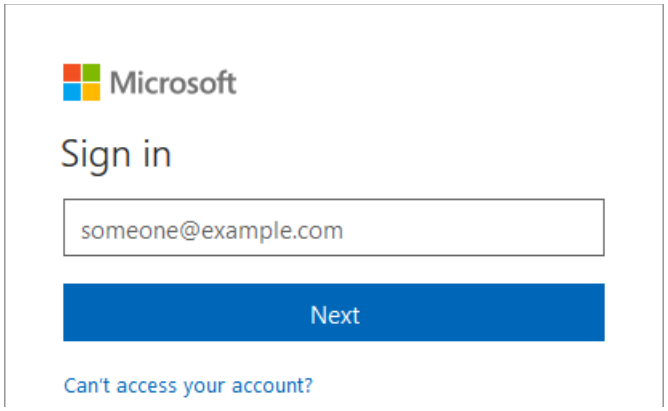
Kuva 3. Federoitu identiteetti

Federoitu identiteetti vaatii taustalleen identiteetin hakemistosynkronoinnin, sillä ainoastaan autentikointitapa muuttuu teknisesti, kun paikallisen federaatiopalvelun ja Office 365:n välille määritellään federaatio. Käyttäjätunnusta ja sen elinkaarta hallitaan paikallisessa hakemistossa kuten synkronoitua identiteettiä. Myös taustalle vaaditaan yhä hakemistosynkronointi, sillä on tärkeää huomioida, ettei federaatiopalvelu itse synkronoi mitään tietoja – se ei ole sen tehtävä. Sen sijaan paikalliselle toimialueelle konfiguroidun federaatiopalvelun ja Office 365:n välillä on nyt luottamusverkosta, jossa AD FS on identiteetin tarjoaja (**IdP**) ja Office 365 on palveluntarjoaja (**SP**). Toisin sanoen Office 365 luottaa AD FS:n paikallista aktiivihakemistoa vasten tekemään todennukseen, saaden tältä **claimin**, jonka pohjalta käyttäjä voidaan valtuuttaa käyttämään määrättyjä osia palvelusta. Koska autentikointi tapahtuu paikallisen toimialueen sisällä, voidaan käyttäjien päätelaiteasetuksia määritellä siten, ettei näiden tarvitse syöttää käyttäjätunnusta ja salasanaa mihinkään, vaan palveluihin päästään kertakirjautumisen avulla. (Microsoft b; Redmond ym 2018, Chapter 4; Roundtree 2013, 28-29.)

4 Federaatio ja Office 365

Oletustilanteessa käyttäjäidentiteetin toimialuetta ei ole määritelty Office 365:ssa federoiduksi, vaan käyttäjätunnuksella on @organisaatio.onmicrosoft.com -muotoinen pääte. (Microsoft c.) Vaikka Azure AD -tenantiin olisi lisätty toinen, organisaation oma toimialue joka olisi määritetty federoiduksi, käyttää Office 365 oletuksena WS-Federation passive -protokollaa. Tämä tarkoittaa käytännössä sitä, että käyttäjän täytyy saada sovellukselta, tässä tapauksessa Office 365:ltä, aloite autentikoinnin suorittamiseksi. (Goodner ym, 2007, Part 2.)

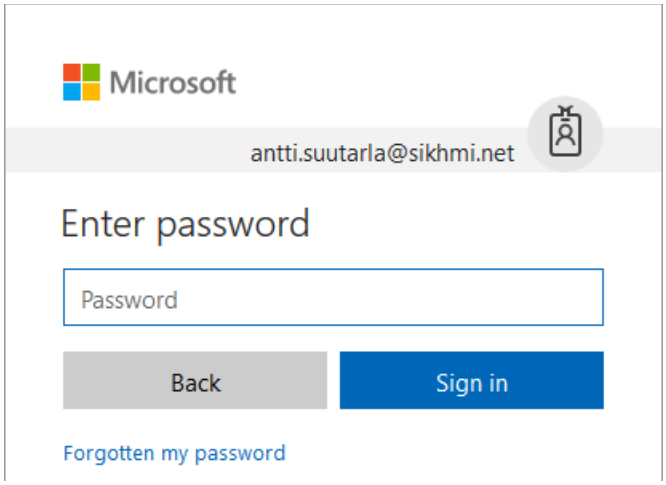
Päästäkseen Office 365 -portaaliin internetin kautta, käyttäjän tulee mennä selaimella osoitteeseen **https://login.microsoftonline.com**, jossa häneltä pyydetään sähköpostiosoitetta.



Kuva 4. Office 365 -portaaliin kirjautuminen.

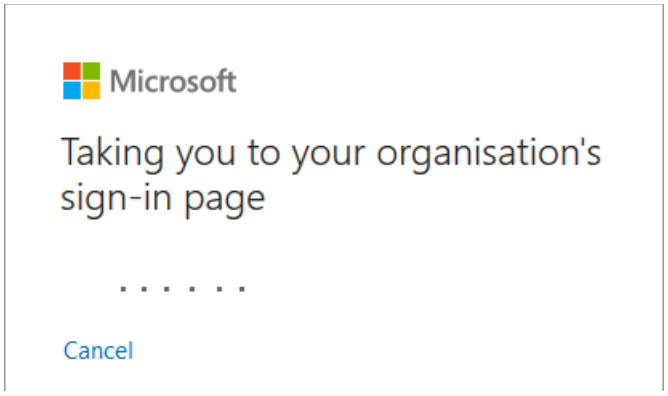
Kirjautumisessa tunnistetaan käyttäjätunnuksen toimialue, josta päätellään, onko se määritetty jollakin organisaatiolla federoiduksi ja jos näin on, mihin federaatiopalveluun käyttäjä tulee ohjata. Itse asiassa tähän voi syöttää täysin keksityn käyttäjätunnuksen ja yhdistää siihen esimerkiksi minkä tahansa tunnetun organisaation toimialueen päätteeksi, kuten asdsqwerty@nokia.com. Jos kyseinen toimialue on federoitu millään organisaatiolla jolla Office 365 on käytössä, ohjataan käyttäjä tämän federaatiopalveluun autentikoitumaan (edellyttäen että se on julkisen internetin yli tavoitettavissa). Näin satunnaisesti toimien käyttäjällä ei ole usein edellytyksiä suorittaa todennusta kyseisen toimialueen tunnuksilla, mutta hänen voi olla mielenkiinnosta täysin mahdollista päästä katsomaan, miltä jonkin organisaation federaatiopalvelu näyttää.

Käyttäjätunnuksen syöttäminen toimii siis toivottuna aloitteena autentikoinnille. Koska käyttäjän toimialue ei tässä tapauksessa ole määritetty federoiduksi, pyydetään käyttäjää autentikoimaan syöttämällä salasana erikseen – näin tapahtumaketju etenisi, jos käytössä olisi pilvi- tai synkronoitu identiteetti ja käyttäjä kirjautuisi tavanomaisesti selaimella.



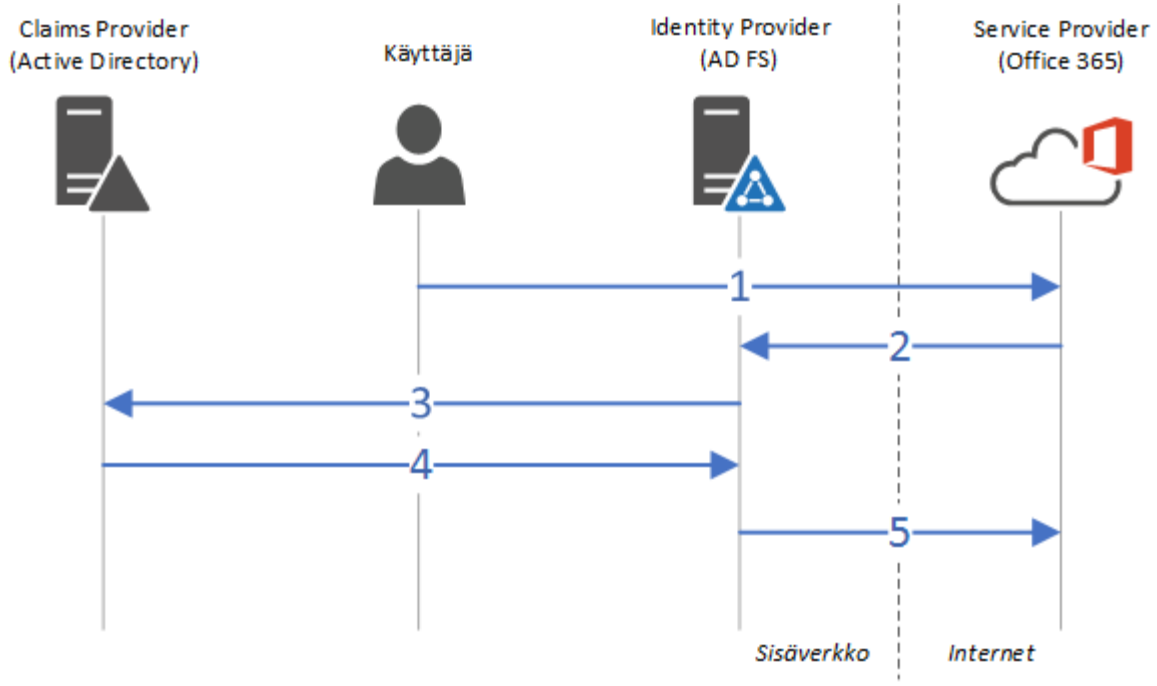
Kuva 5. Autentikointi pilvi-identiteetillä Azure AD:a vasten.

Jos käyttäjän toimialue asianmukaisesti kuitenkin tunnistetaan federoiduksi, häneltä ei pyydetä manuaalisesti syötettävää salasanaa, vaan hänet ohjataan organisaation määritettyyn federaatiopalveluun autentikoitavaksi.



Kuva 6. Federoitu identiteetti tunnistettu kirjautuessa.

Koska toteutettava ja toivottu lopputulos on kertakirjautuminen palveluun, ei käyttäjä missään vaiheessa syötä mitään tunnuksia mihinkään, vaan hetken kuluttua hän on todennuksen ja valtuutuksen onnistuttua päässyt palveluun. Koska tästä silmänräpäyksessä tapahtuvasta toiminnasta ei käyttäjälle näy varsinaisen federaatiopalvelun toiminta lainkaan, eikä näin ole tarkoituskaan, on tätä tapahtumaketjua syytä avata.



Kuva 7. Claim-pohjaisen autentikoinnin tapahtumaketju (Baler ym 2013, 20; Roundtree 2013, 57-59; Redmond ym 2018, Chapter 4, Figure 4-2; Bertocci 2016, Chapter 2, Figure 2-5.)

1. Käyttäjä menee Service Providerina toimivaan sovellukseen, Office 365:een.
2. Sovellus tunnistaa autentikoimattoman käyttäjän, ja sen että käyttäjäidentiteetti no-jaa federoituun todennukseen. Käyttäjä ohjataan todennettavaksi määrätyssä federaatiopalvelussa.
3. Federaatiopalvelu tekee varsinaisen todennuksen toimialueen sisällä määrättyä Claims Provideria – aktiivihakemistoa – vasten.
4. Claims Provider palauttaa todennetusta käyttäjäidentiteetistä tiedon federaatiopalvelulle.
5. Federaatiopalvelu toimittaa identiteetistä myönnetyn claimin token-muodossa sovellukselle, joka sen perusteella valtuuttaa käyttäjän sovellukseen.

Koska sovelluksen ja federaatiopalvelun välillä on kahdenkeskinen luottamusverkosto, kiteytyy koko federoidun identiteetin, claim-pohjaisen autentikoinnin, kertakirjautumisen ja federaatiopalvelun ajatus kolmeen ydinkohtaan:

- Käyttäjä suorittaa ylläolevista vaiheista ensimmäisen, kaikki muu tapahtuu ilman käyttäjältä vaadittua toimia ja käyttäjälle täysin näkymättömästi.
- Sovelluksessa ei hallita aktiivihakemistosta erillistä käyttäjäidentiteettiä.
- Sovellus ei ole tietoinen eikä sillä ole mitään yhteyttä federaatiopalvelun taustalla olevaan varsinaisena identiteettisäilönä toimivaan aktiivihakemistoon.

Toiminta-ajatuksen selkeyden vuoksi käsiteltiin esimerkkiä, jossa käyttäjän aloitteena toimii käyttäjätunnuksen syöttäminen, mutta käytännössä vaikkapa sähköpostia lukiessa

vaaditun aloitteen tekee sähköpostisovellus. Myös selainkäytössä käyttäjän kotiorganisaatio voidaan kertoa palvelulle suoraan osoitteessa niin, ettei käyttäjältä vaadita senkään osalta mitään aloitetta, mutta tähän tullaan käytännön esimerkkinä myöhemmin.

4.1 Claim ja tokenit

Yleinen kuvaus siitä, mitä claim on, määritellään näin:

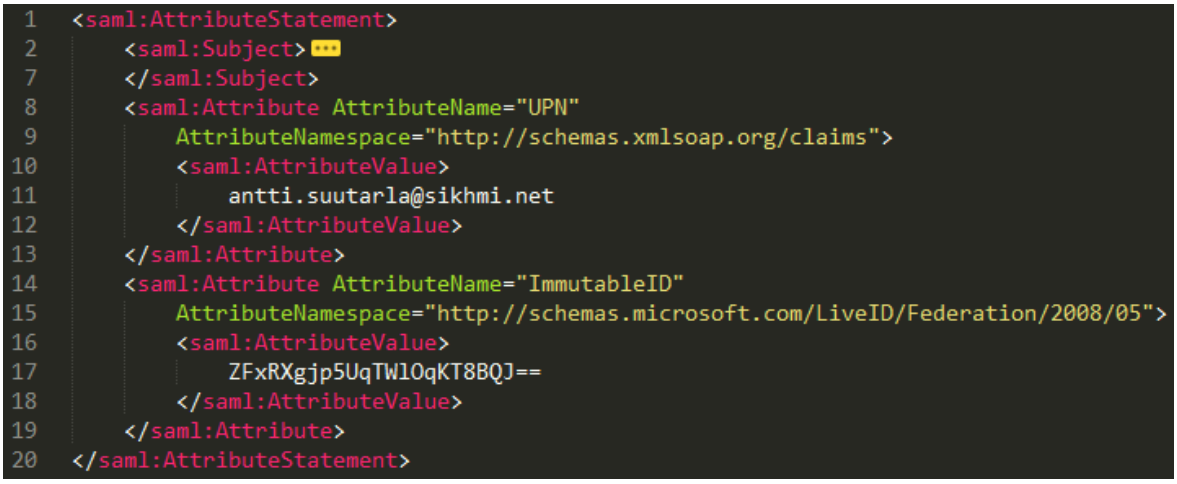
> [A claim is] a statement that one subject makes about itself or another subject. For example, the statement can be about a name, identity, key, group, privilege, or capability. Claims are issued by a provider, and they are given one or more values and then packaged in security tokens that are issued by a security token service (STS). They are also defined by a claim value type and, possibly, associated metadata. (Microsoft d.)

Jokaista claim-pohjaista todennusta käyttävää sovellusta kohden määritellään federaatiopalveluun claim-säännöt. Nämä säännöt muodostuvat sovelluksen vaatimuksista ja ne kertovat, mitä claimin tulee sisältää ja missä muodossa, jotta Service Provider voi yksilöivästi valtuuttaa käyttäjäidentiteetin. (Bertocci 2016, Chapter 2.) Esimerkiksi Office 365 käyttää oletuksena kahta claim-sääntöä.

Taulukko 1. Office 365:n oletuksena käyttämät claim-säännöt

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(store = "Active Directory", type = ("http://schemas.xmlsoap.org/claims/UPN", "http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"), query = "samAccountName={0};userPrincipalName,objectGUID;{1}", param = regexreplace(c.Value, "(?<domain>[^\\]+)\\(?<user>.+", "${user]"), param = c.Value);
c:[Type == "http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"] => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Value = c.Value, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1.nameid-format:unspecified");

Säännöt tehdään AD FS:lle niin kutsutuin claim rule language -ilmaisuin ja ne muodostavat tokenin mukana kulkevan claimin. Halutessaan sääntöjä voi tehdä ja kirjoittaa manuaalisesti, mutta yleisimpien sääntöjen hallintaan on AD FS:n kanssa helpottamassa graafinen käyttöliittymä, jonka valinnoin sääntöjä voi rakentaa tuntematta claim rule languagen logiikkaa. (Microsoft e.) Office 365:n käyttämät claim-säännöt muodostuvat automaattisesti myöhemmin käsiteltävän teknisen toteutusvaiheen yhteydessä, eli oletussääntöjä ei tarvitse käyttöönotossa manuaalisesti tehdä tai ylläpitää.

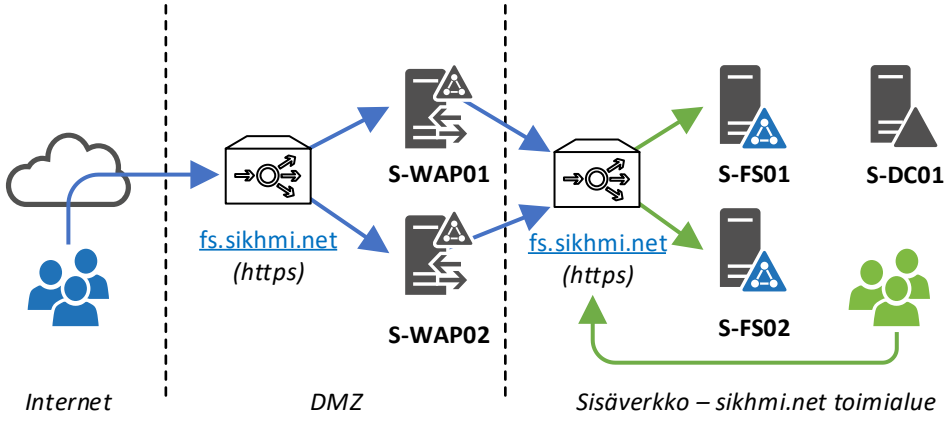


Kuva 8. Osa tokenista ja sen sisältämästä claimista (Goodner ym 2007, Appendix A.)

Useiden web-selainten liitännäisillä voi selainten debug-tilassa poimia web-liikenteestä tokeneja ja katsoa tarkemmin, mitä niiden claimit pitävät sisällään. Aivan kaikkea näistä ei SSL-salausta purkamatta näe, mutta sisällön hahmotusta varten tarpeeksi. Claimin oleellisimmasta osasta voimme nähdä kaksi määritystä, käyttäjän UPN ja ImmutableID (rivit 12-23), jotka Office 365 haluaa tietää identiteetistä. Näille on määritelty säännöissä myös esimerkiksi nimiavaruus (namespace), jolla tietueet Service Providerin toimesta tunnistetaan. Vaikka token itse kulkeekin SSL-suojattua yhteyttä pitkin, sitä itseään ei oletusarvoisesti salata erikseen, mutta teknisesti tämäkin on mahdollista. Token ei kuitenkaan koskaan kuljeta esimerkiksi käyttäjän salasanaa, koska sen tehtävä on ainoastaan valtuuttaa jo todennettu käyttäjäidentiteetti palveluun. Tokenin tapa näkyä web-liikenteessä vaihtelee hieman sen mukaan, onko käytössä SAML vai WS-Federation protokolla. Myös se, tuleeko aloite autentikoinnille ja autorisoinnille sovelluksen (SP) vai identiteetin tarjoajan (IdP) puolelta vaikuttaa siihen, kuinka pyyntö muodostaa claim ja token tapahtuu. (Gregory 2014b.)

5 Federaatiopalvelun toteutus

5.1 Infrastruktuurin määrittely ja vaatimukset



Kuva 9. Ylätason tekninen kuva AD FS -infrastruktuuriratkaisusta

Palvelun jatkuvuuden turvaaminen perustuu sen kahdentamiseen niin, että kussakin palvelussa käytössä olevasta palvelinroolista (Web Application Proxy eli WAP ja AD FS) on kaksi erillistä instanssia eri palvelimille asennettuina. Koska palvelua käytetään ainoastaan yhdellä ainoalla URL:lla (tässä tapauksessa **https://fs.sikhmi.net**), tulee kunkin kahden palvelinparin eteen sijoittaa instanssi kuormantasaajasta. Tämän tarkoitus on jakaa palvelinten käyttökuormaa tasaisesti, mutta sen lisäksi eritoten seurata palvelun teknistä tavoitettavuutta kullakin palvelimella. Mikäli palvelussa ilmenee häiriö, ei käyttäjiä ohjata kyseiselle palvelimelle häiriön aikana vaan heitä palvelee vastaava, kahdennettu palvelin. Palvelinkapasiteetin peilatun kahdennuksen yleiset hyvät käytännöt pätevät myös tässä, eli esimerkiksi palvelinten levykapasiteetin ei tulisi olla saman levyjärjestelmän varassa, sillä tällöin häiriö siinä voisi lamaannuttaa molemmat palvelimet ja koko palveluun tulisi odottamaton katko.

Koska palvelu toimii puhtaasti (ja ainoastaan) https-protokollalla, vaaditaan tätä varten SSL-salausvarmenne. Office 365:n kanssa varmenne tulee olla sellaiselta julkiselta myöntäjältä, johon yleisesti päätelaitteiden käyttöjärjestelmät luottavat, eikä tähän siten sovellu esimerkiksi toimialueen oma, sisäinen, varmennepalveluinfrastruktuuri. Lähtökohtainen edellytys on myös käyttää samaa – ei ainoastaan saman nimistä – varmennetta federaatiopalvelun jokaisella palvelimella, WAP-palvelimet mukaan lukien. Jos tarkoitus on käyttää varmennepohjaista todennusta AD FS:n kanssa esimerkiksi mobiilipäätelaitteilla, ei voida käyttää yleistä, niin kutsuttua wildcard-varmennetta, missä on yhden toimialueen kaikki alitoimialueet mukana (kuten ***.sikhmi.net**), ellei siinä ole vielä yhtä tasoa alemmas ulottuvaa nimeä mukana – tässä tapauksessa **certauth.fs.sikhmi.net**.

Web Application Proxy -palvelinten funktio on olla eräänlainen julkaisualusta varsinaiselle federaatiopalvelulle, eivätkä nämä palvelimet myönnä itse claimeja lainkaan, vaan ne ainoastaan välittävät pyynnöt niistä varsinaisille federaatiopalvelun omille palvelimille. Toisin kuin AD FS -palvelimet, eivät WAP-roolissa olevat palvelimet tarvitse mitään toimialueen sisäisiä palveluita eivätkä täten yhteyttä toimialueelle. Tämän vuoksi ne tulisi verkkoteknisesti sijoittaa DMZ:n kaltaiselle verkkoalueelle, jolloin yhteyttä toimialueella oleville federaatiopalvelimille ei tarvitse – ajatus tietoturvasta takaraivossa – avata suoraan internetistä. Palvelun kannalta voidaan myös tunnistaa internetistä (= WAP:n kautta) tulevat käyttäjät sisäverkon (= suoraan AD FS:lle tulevat käyttäjät) käyttäjistä ja määritellä eri toimintoja näille toimimaan eri tavoin, kuten esimerkiksi monivaiheisen tunnistautumisen pakollisuus internetistä tultaessa. Ainoa vaatimus WAP-palvelimille suojatun https-yhteyden lisäksi on löytää federaatiopalvelun edessä oleva kuormantasaaja sen nimellä – **fs.sikhmi.net** – ilman toimialueen nimipalvelun apua, mutta tämä ohjaus voidaan toteuttaa manuaalisesti palvelinkohtaisesti. Ulkoista, julkista, nimipalvelua ei tule käyttää, sillä julkinen IP-osoite palvelun URL:n takana on eri kuin sisäverkon kuormantasaajan IP-osoite, johon ohjaus halutaan tehdä. Kuormantasaaja ei saa purkaa sen kautta kulkevaa suojattua https-liikennettä vaikka se olisi näin mahdollista konfiguroida, sillä AD FS tunnistaa puretun ja uudelleen salatun liikenteen eikä pidä sitä oletuksena eheänä ja turvallisena.

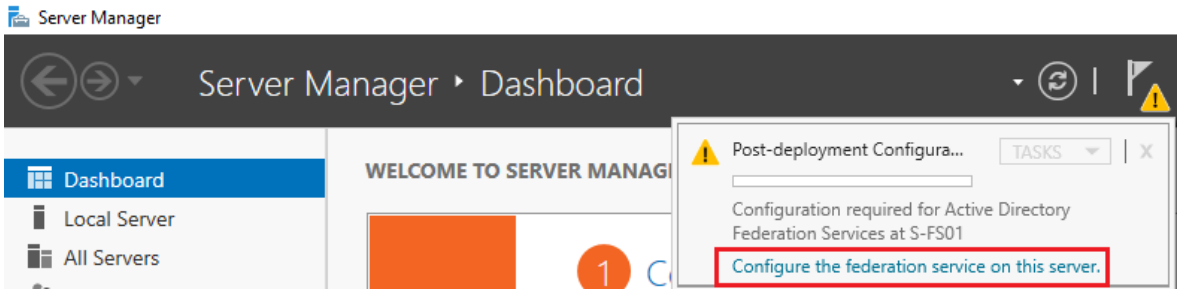
Käytettävät Windows Server -versiot tulisi olla niin uusia kuin saatavilla on. Tämän työn kirjoitushetkellä Windows Server 2008 R2 on yhä tuettu ja siihen kuuluva AD FS -versio 2.0 täysin käyttökelpoinen Office 365:n kanssa, mutta moni palvelun ylläpidollinen ja teknisesti määritettävä osa-alue on hankalammin, tai yksinkertaisesti vain kankeammin, toteutettavissa. Windows Server 2012 -käyttöjärjestelmä tarjoaa tästä ainoastaan hieman uudemman version, josta käytetään osin virallista versionumerointia 2.1. Windows Server 2012 R2 tuo mukanaan version 3.0, jossa on jo merkittävästi parannuksia aiempiin versioihin nähden. Työn esimerkeissä käytetään Windows Server 2016 -palvelinkäyttöjärjestelmää ja sen AD FS -versiota ”4.0”, joka tämän työn kirjoitushetkellä on uusin julkisesti saatavilla oleva julkaisu Windows Server -käyttöjärjestelmästä. Microsoft on ensisijaisesti luopunut nimeämästä AD FS:n versionumeroita erikseen, mutta nämä voidaan juoksevasti nimetä palvelinkäyttöjärjestelmäversion mukaan.

Palvelun määritykseen tarvitaan paikallisen toimialueen **Domain Admin** -tasoinen ylläpitotunnus, sekä Azure AD -hakemistoon **Global Administrator** -tasoinen tunnus.

5.2 AD FS -palvelinten asennus ja konfigurointi

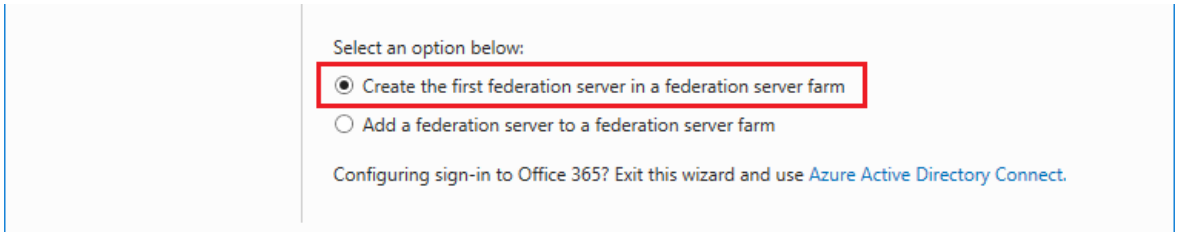
Molemmille palvelimille (tässä **S-FS01** ja **S-FS02**) lisätään Windows Server Managerin kautta **Active Directory Federation Services** roolipalvelu (ja sen riippuvuudet, mikäli asennus sellaisia ehdottaa). Roolipalvelun lisääminen ei vielä määritä itse palvelua lainkaan, vaan se tulee tehdä erikseen.

5.2.1 Ensimmäinen palvelin



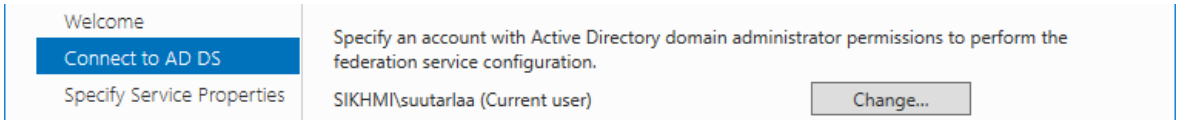
Kuva 10. Määritetään federaatiopalvelurooli

Roolin määrityksen ensimmäisellä sivulla valitaan, että ollaan määrittelemässä ensimmäistä palvelinta uutena perustettavaan federaatiopalvelufarmiin. Viittauksesta Office 365:n kanssa käytettävään kirjautumistapaan ei tule välittää.



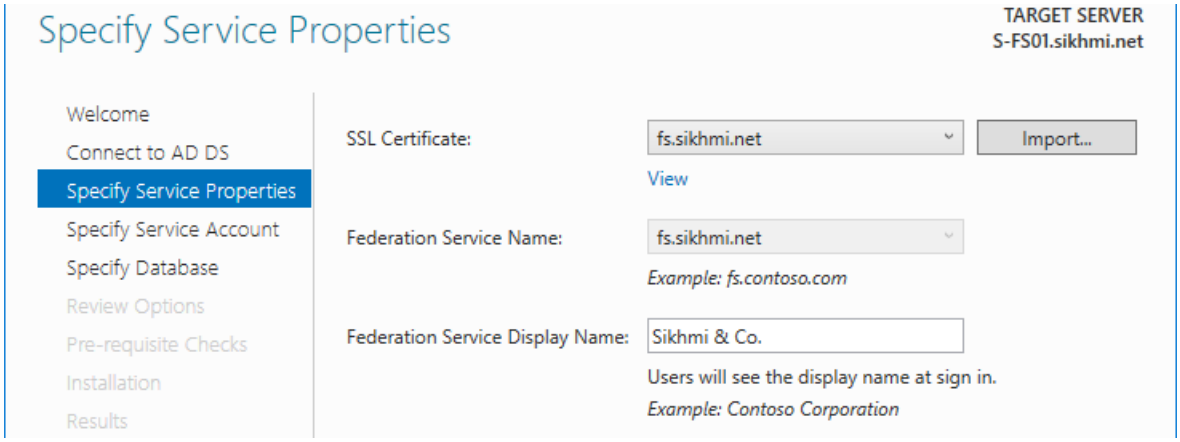
Kuva 11. Määritetään farmin ensimmäistä palvelinta

Seuraavalla sivulla pyydetään syöttämään toimialueen Domain Admin -tasoinen tunnus, jolla tarvittavat toimialuekohtaiset asennusmääritykset tehdään. Oletuksena ehdotetaan käyttäjätunnusta, jolla roolin määritysvelho on käynnistetty. Annettavan tunnuksen kanssa tulee huomioida, että sitä käytetään vain asennuksen aikana, ei palvelun itsensä kanssa.



Kuva 12. Määritetään asennuksen käyttämä ylläpitotunnus.

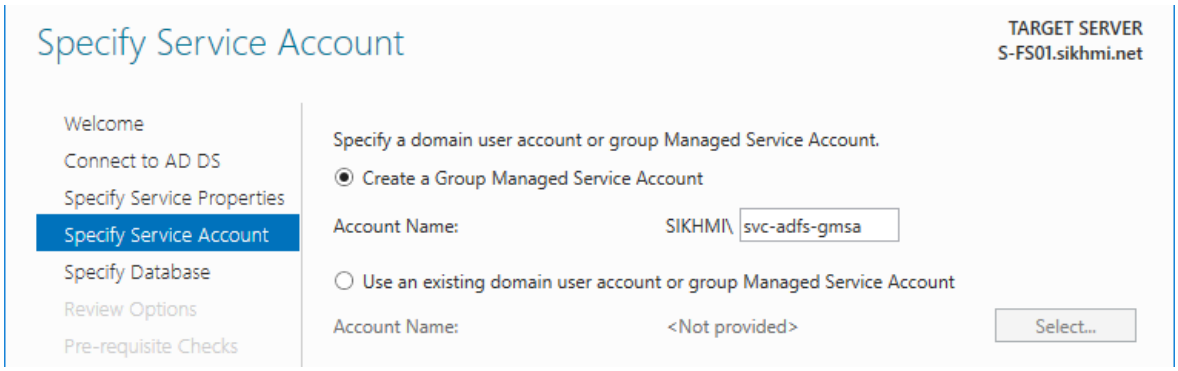
Asennusvelhon kolmannella sivulla määritellään palvelun itsensä asetuksia.



Kuva 13. Palvelumääritykset.

Tässä valitaan palvelun käyttöön tuleva julkinen varmenne, jonka tulee löytyä palvelimelta. Jos haluttu varmenne ei näy alasvetovalikossa, tulee varmistaa, että varmenne on nimenomaan palvelimen konevarmennesäilössä ja että myös sen yksityinen avain on käytettävissä. Palvelun nimeksi tulee määrittää osoite, johon myös valittu varmenne sopii. Tämän tulee olla tavoitettavissa oleva URL, wildcard-osoite (***.sikhmi.net**) ei siis kelpaa nimeksi. Varmenteeksi wildcard sen sijaan kelpaa (aiemmin mainituin ehdoin). Näyttönimeksi voidaan antaa esimerkiksi organisaatiota itseään kuvaava nimi – tämän kentän käyttö on hyvin vapaamuotoista.

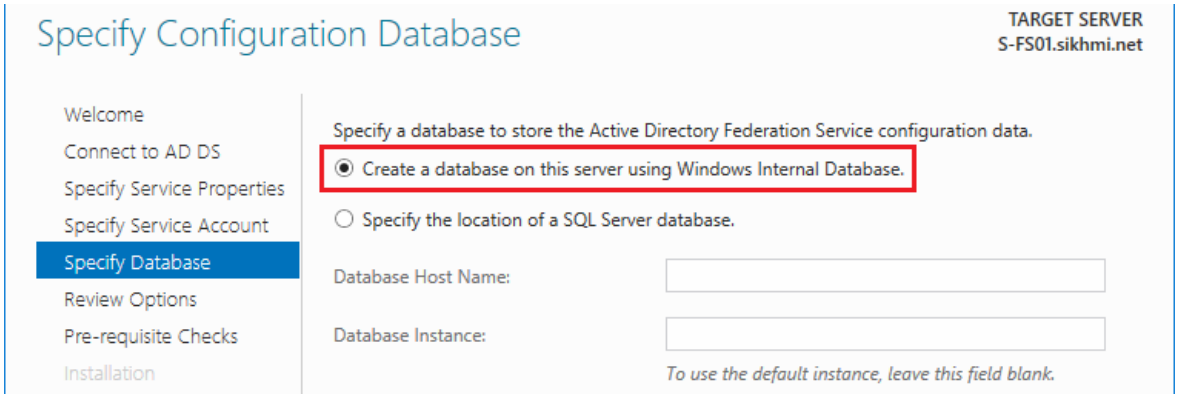
Seuraavalla sivulla määritetään palvelun käyttöön tuleva palvelutunnus. Tällä ajetaan itse palvelua, tämä luvitetaan palvelun käyttöön tulevaan tietokantaan ja tälle luvitetaan palvelun itse itselleen käyttöön myönnettävien varmenteiden hallinta.



Kuva 14. Määritetään palvelun käyttämä palvelutunnus

Tässä voidaan noudattaa toimialueen yleistä palvelutunnuskäytäntöä, mutta edellä mainituista seikoista johtuen tunnuksen muuttaminen myöhemmin on erittäin työlästä ja valinta

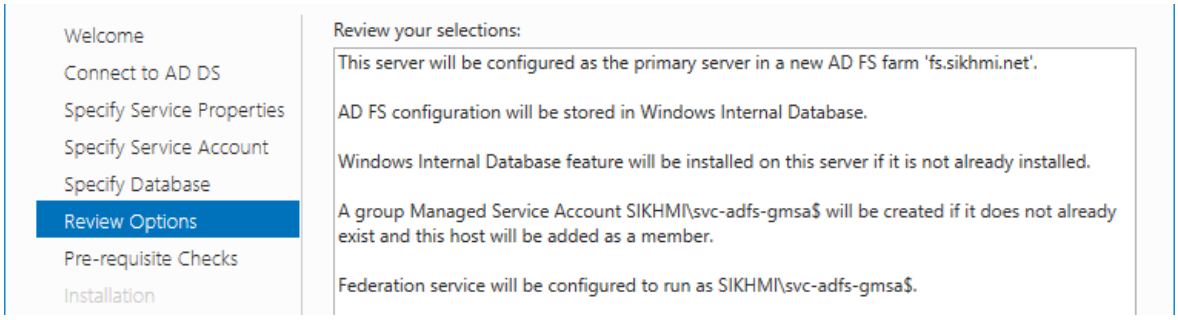
tähän tulisi perustaa niin, ettei päädyttäisi tilanteeseen, jossa tunnus jouduttaisiin vaihtamaan. Seuraavaksi valitaan palvelun käyttöön tulevan tietokannan tyyppi.



Kuva 15. Palvelun käyttämän tietokannan valinta

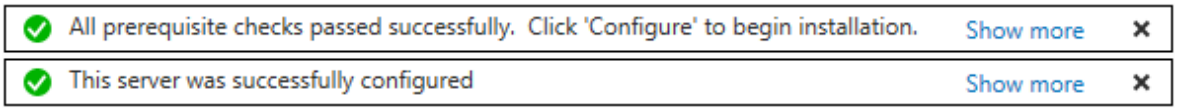
Windows Internal Database eli WID asentuu palvelimelle, johon palvelu itse tulee myös. Käyttämällä dedikoitua SQL-instanssia sisäisen tietokannan sijaan voidaan saada vielä hajautetumpaa vikasietoisuutta palvelun toimivuuteen, mutta toisaalta hajautettu SQL-farmi itsessään voi tulla kustannuksiltaan huomattavasti suuremmaksi kuin federaatiopalvelu itse. SQL-instanssin puolesta puhuvat sen muutamat hyödyt nimenomaan federaatiopalvelun näkökulmasta – varsinkin jos sellainen on muun, olemassa olevan, palvelininfrastruktuurin puolesta käytettävissä – mutta koska näitä ominaisuuksia ei voida merkittävästi hyödyntää Office 365:n kanssa ja koska on täysin tuettua myöhemmin vaihtaa käytettävää tietokantaa, päädymme nyt valitsemaan oletuksena tarjotun WID:n tietokannaksi. (Amirali 2013.) Tästä seuraa myös olennaisesti näkyvä muutos palvelun tekniseen hallintaan ja ylläpitoon, joka käsitellään palvelun testauksen todentamisessa.

Seuraava sivu näyttää koosteen aiemmin tehdyistä valinnoista ja kertoo määritykset, joilla palvelua ollaan asentamassa.



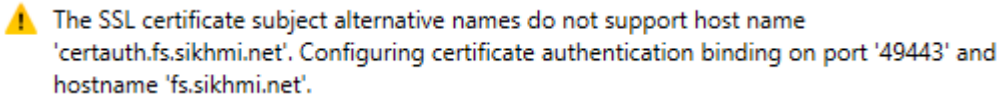
Kuva 16. Kooste palvelun määrityksistä

Tässä kohdassa voidaan vielä tarkistaa, että määritykset ovat oikein ja halutunlaiset. Jos ja kun niihin ollaan tyytyväisiä, tarkistetaan niiden edellytykset seuraavalla sivulla, jonka jälkeen viimeinen sivu ilmoittaa, että palvelu on asennettu onnistuneesti.



Kuva 17. Palvelu on määritelty onnistuneesti

Vaatimusten tarkastuksessa ja palvelun konfiguroinnin tuloksissa saattaa esiintyä huomautuksia erinäisistä asioista, mutta mikäli mitään varsinaista virhettä, kuten puuttuvat käyttöoikeudet tai määritetyn palvelutunnuksen alustuksen epäonnistuminen, ei ilmene, voit huoletta viimeistellä asetukset. Yksi huomautuksista voi olla edellä mainitun varmenteen vaatimuksista sen yhteensopivuus useamman alitoimialueen osoitteille.

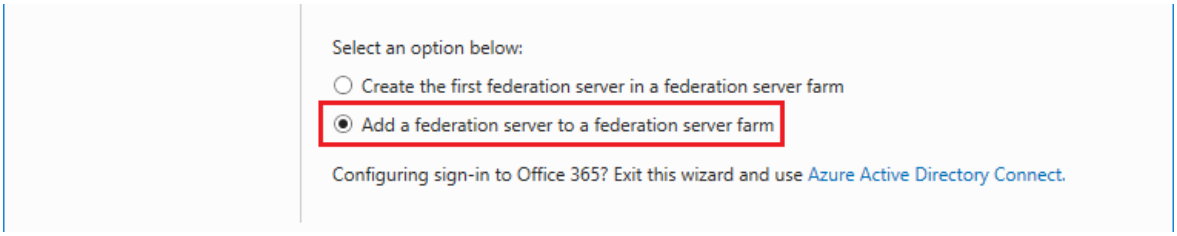


Kuva 18. Huomautus varmenteen toimintaominaisuuksien puuttumisesta

Jostakin syystä tästä ei ilmoiteta esivaatimuksien tarkastuksessa edes huomautuksena, vaan ilmoitus tulee vasta kun palvelu on määritelty, minkä vuoksi varmenteen toiminnallisuuden yhteensopivuudesta on hyvä varmistua etukäteen. Teknisesti SSL-varmenne on yksinkertaista vaihtaa myöhemmin, mutta jos varmenne on hankittu alun perin vääränlaisena, voi tästä syntyä yllättäviäkin kustannuksia varmenteen mahdollisista muista ominaisuuksista ja käyttökohteista riippuen.

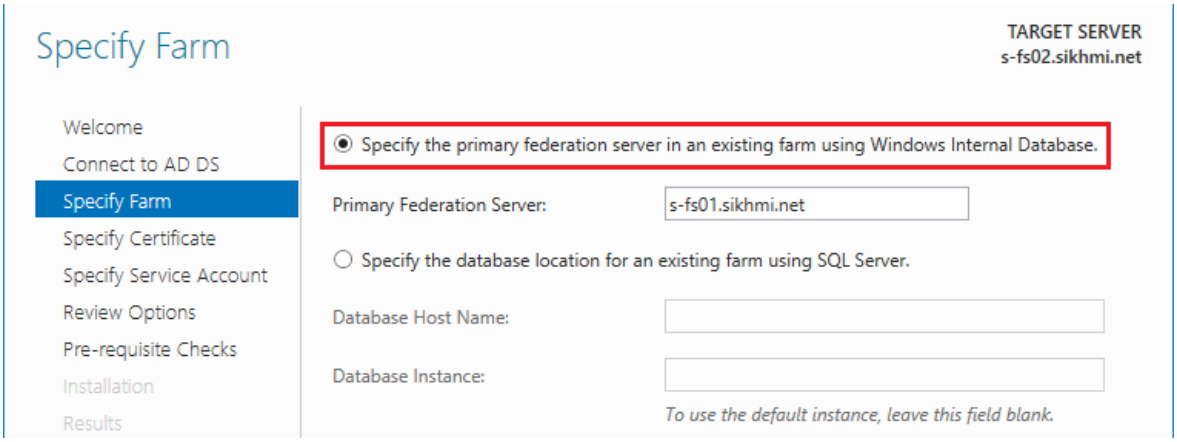
5.2.2 Toinen palvelin

Roolin määrityksen ensimmäisellä sivulla valitaan tällä kertaa, että ollaan lisäämässä uutta palvelinta olemassa olevaan farmiin.



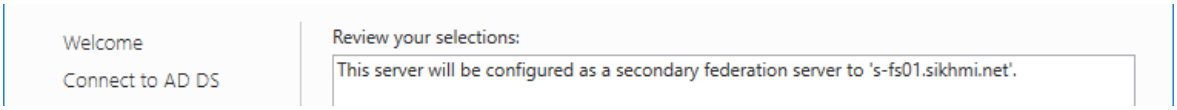
Kuva 19. Määritetään farmin toista palvelinta

Koska ensimmäinen palvelin määriteltiin käyttämään WID-tietokantaa, tapahtuu farmin tunnistus palvelinta siihen lisätessä sen mukaisesti (sillä tässä vaiheessa roolin määritystä palvelin ei tiedä, onko se toinen vai kahdeksas lisättävä palvelin).



Kuva 20. Palvelin lisätään farmiin perustuen farmissa käytetyn tietokannan tyyppiin

Avainsanana valinnassa näkyy tässä vaiheessa pyyntö kertoa farmin ensisijainen palvelin – SQL-tietokantaa käytettäessä farmin palvelimilla ei ole ensi- tai toissijaista roolia toisiinsa nähden, mutta tähän palataan vielä myöhemmin. Seuraavilla sivuilla palvelussa käytettävä varmenne ja palvelutunnus määritetään täysin samalla tavalla kuin ensimmäisenkin palvelimen kohdalla. Myös kooste määrittelyn tiedoista näytetään samalla tavalla, ainoastaan yhdellä pienellä erotuksella aiempaan nähden.



Kuva 21. Määritysten yhteenvedossa palvelin nimetään toissijaiseksi

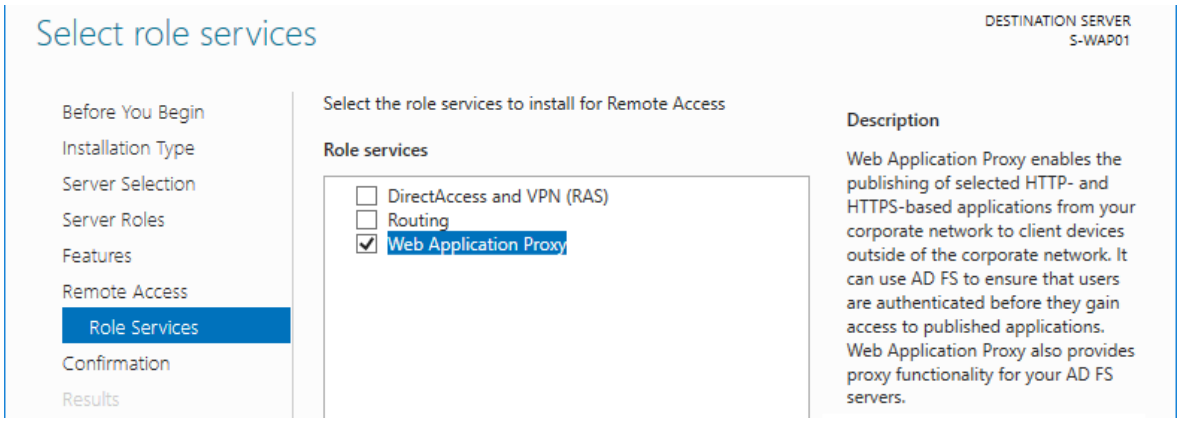
Muuten määrittelyn esitarkistukset ja niiden huomautukset kerrotaan samoin tavoin ja reunaehdoin kuin ensimmäisen palvelimen kohdalla, aivan kuten ilmoitus määrittelyn lopputulemasta ja sen onnistumisesta.

5.3 WAP-palvelinten asennus ja konfigurointi

WAP-roolissa toimivien palvelinten asennus ei eroa käytännössä lainkaan, oli kyseessä sitten ensimmäinen tai viides palvelin. Esivaatimuksista on syytä tarkentaa, että lähtökohtaisesti palvelimille asennettavan varmenteen tulee olla teknisesti yksi ja täysin sama varmenne kuin mitä federaatiopalvelimilla käytetään. Ei siis riitä, että varmenteessa on esimerkiksi kaikki samat nimet kuin mitä varsinaisilla federaatiopalvelimilla käytetyssä on, vaan varmenteen niin kutsutun sormenjäljen, thumbprintin, täytyy olla sama.

Toiseksi, ylätason toteutuskuvasta näkyy, että käyttäjät tulevat WAP-palvelimille ulkoisesta verkosta käsin ja heidät tulee ohjata sisäverkossa osoitteeseen, joka on samalla nimellä kuin ulkoverkon osoite mutta sisäverkon IP-osoitteella. Toisin sanoen WAP-palvelimet eivät saa selvittää **fs.sikhmi.net** nimeä julkisen nimipalvelun kautta, koska tällöin käyttäjät ohjattaisiin sieltä takaisin WAP-palvelimille itselleen. Myös jos palvelimia ei ole liitetty sisäverkon toimialueelle, eivät ne välttämättä voi hyödyntää sisäverkon erillisen nimipalvelun määrityksiä joita sisäverkon palvelimet muuten käyttäisivät. Näin ollen yksinkertaisin ratkaisu on lisätä federaatiopalvelun nimitietue, **fs.sikhmi.net**, sen sisäverkon IP-osoitteella palvelinten **hosts** -tiedostoon. Hosts-tiedoston käyttö nimenselvityksessä voi olla ensisilmäyksellä suuri punainen vaate monelle Windows-ylläpitäjälle, mutta esimerkiksi tarvetta käsin myöhemmin muuttaa tietuetta usealle eri palvelimelle ei ole ennakoitavissa.

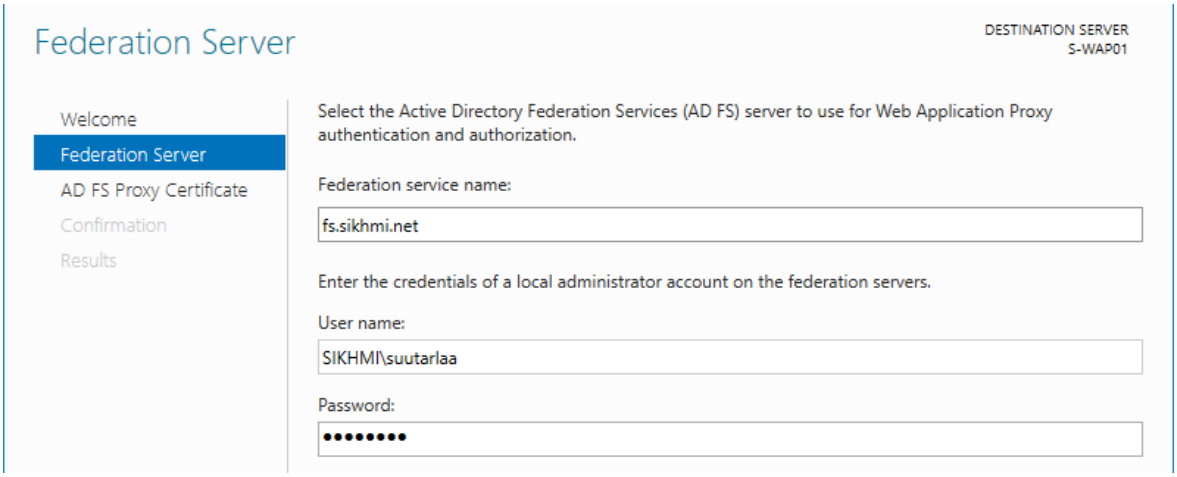
Kun esivaatimukset ovat tältä erää kunnossa, voidaan siirtyä asentamaan itse roolipalvelua, joka tällä kertaa löytyy hieman poikkeavasti.



Kuva 22. WAP-roolin asennus

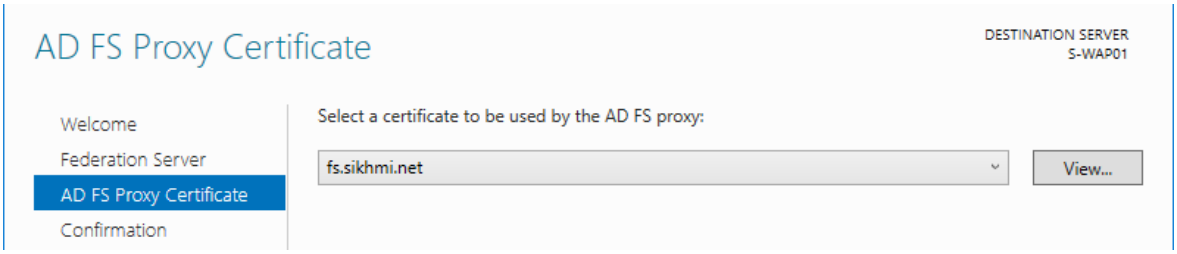
Varsinaiseksi palvelimelle asennettavaksi rooliksi tulee siis valita ”Remote Access”, jonka alta tulee asennusvelhon seuraavilla sivuilla valittavaksi kaivattu ”Web Application Proxy”. Myös asennusvelhon kuvaus kertoo, että roolipalvelun virka on toimia välityspalvelimena varsinaiselle AD FS:lle.

Roolipalvelun määrityksissä tulee kertoa palvelun nimi (**fs.sikhmi.net**, jonka tulee siis selvitä sisäverkon federaatiopalvelimille).



Kuva 23. WAP-roolin määritys

Myös käyttäjätunnukset, joilla on ylläpito-oikeudet varsinaisiin federaatiopalvelimiin, täytyy syöttää erikseen, sillä WAP-palvelimilla ei lähtökohtaisesti ole tietoa edes käytetyn toimialueen nimestä. Palvelun käyttämän nimen täytyy seuraavan sivun määrityksissä vastata WAP-palvelimille asennetun varmenteen nimeä. Myös konevarmennesäilön ja varmenteen yksityisen avaimen käytettävyyden tulee olla kunnossa, aivan kuten federaatiopalvelimillakin.

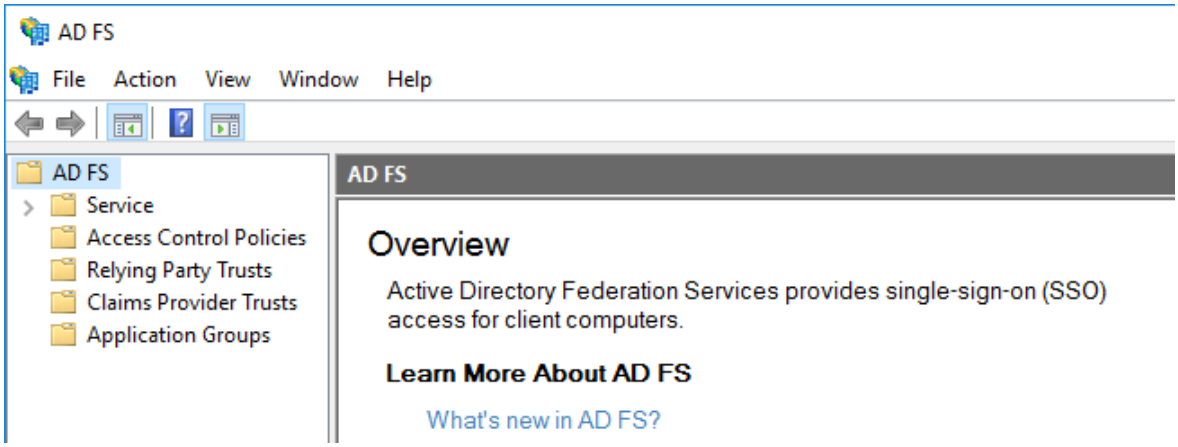


Kuva 24. WAP-palvelinten käyttämän varmenteen määritys

Seuraava sivu tiivistää määritysten muutamat valinnat yhteen, jonka jälkeen määritys on valmis. Kuten tässäkin nähtiin, on WAP-palvelinten määritys huomattavasti suoraviivaisempaa kuin federaatiopalvelun omien palvelinten.

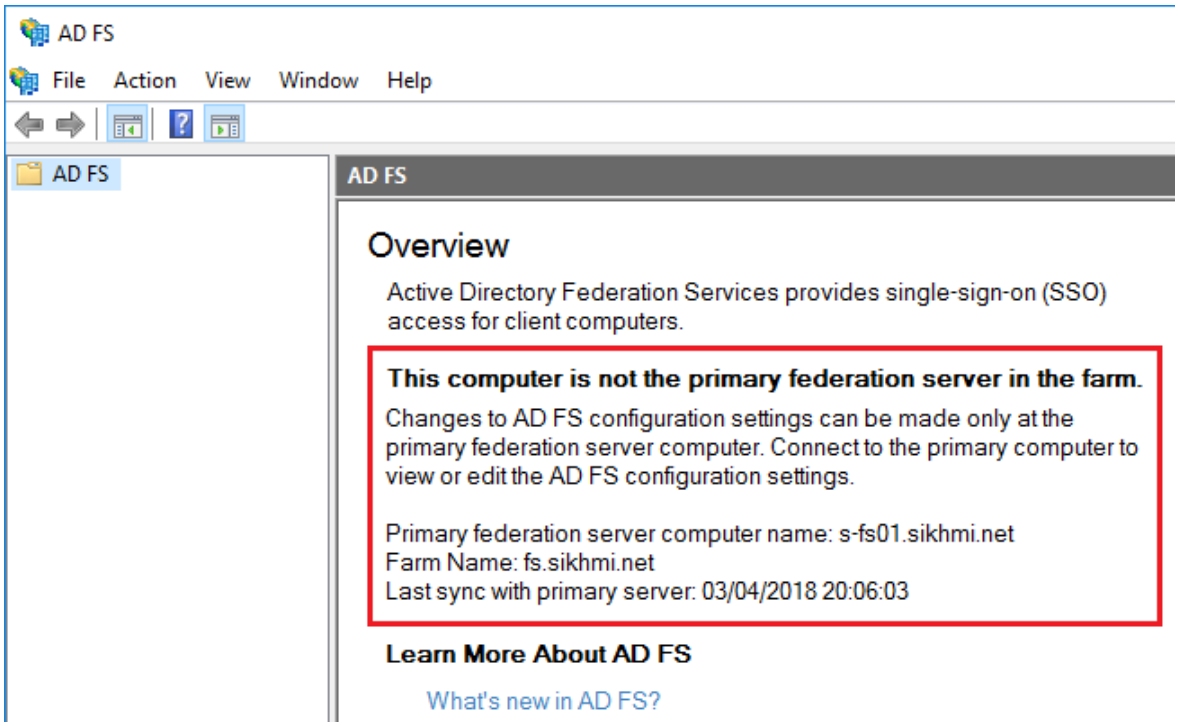
5.4 Federaatiopalvelun toimivuuden testaus

Ennen testausta on varmistettava, että aiemmin määritellyt nimipalveluohjaukset ovat kunnossa sekä sisä- että ulkoverkosta palveluun tultaessa. Tämän jälkeen voidaan todentaa palvelun toimivuus kolmea hyvin yksinkertaista tapaa käyttäen.



Kuva 25. AD FS hallintakonsoli

Ensisijaiselta AD FS -palvelimelta käsin varmistetaan, että **AD FS Management** hallintakonsoli aukeaa ja latautuu ilman virheilmoituksia. Tässä myös nähdään WID-tietokannan käytöstä SQL-kantaan verrattuna muodostuva käytännön ero.



Kuva 26. Toissijainen AD FS -palvelin

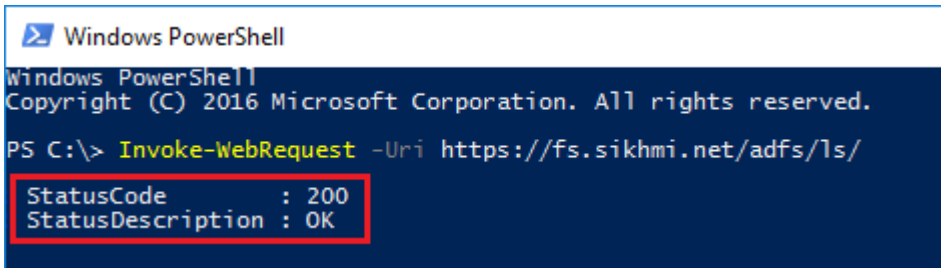
WID-tietokantaa käytettäessä saman farmin eri federaatiopalvelimien välillä on ensi- ja toissijaiset roolit, ja palvelua voidaan hallita ainoastaan ensisijaiselta palvelimelta käsin. Muut farmin palvelimet autentikoivat käyttäjiä, mutta peilaavat konfiguraatiomuutoksia palveluun itsensä ensisijaiselta palvelimelta ja kertovat, milloin ovat synkronoinnin viimeksi tehneet. (Amirali 2013.) Koska SQL-tietokantaa käytettäessä kaikilla farmin palvelimilla on yksi yhteinen, erillinen tietokantapalvelimensa, voidaan muutoksia konfiguraatioon tehdä miltä farmin palvelimelta käsin tahansa. Tässä tapauksessa halutaan varmistua palvelun toimivuudesta ensisijaiselta palvelimelta.

Toinen, erittäin oleellinen osa palvelun käyttöä ja sen tavoitettavuutta on palvelun itse itseään standardien mukaisesti kuvaileva metadata-tiedosto. Tiedosto pitää XML-muodossa sisällään palvelua koskevan konfiguraation, joka on myös julkisesti saatavilla. Palvelun konfiguraatiota muutettaessa tiedosto päivittää itse itseään, jolloin Relying Partyinä toimivat kolmannen osapuolen sovellukset osaavat päivittää itselleen tiedon federaatiopalvelun konfiguraatiomuutoksista. Koska AD FS:n metadatan URL on aina samassa muodossa (**https://<Palvelun URL>/FederationMetadata/2007-06/FederationMetadata.xml**), voimme varmistaa, että se on tavoitettavissa ja että se aukeaa.

Kuva 27. Federaatiopalvelun metadata

Huomaa, että Internet Explorer ei usein osaa avata tiedostoa tulkiten sitä oikein XML-formaatiksi, mutta jos osoite aukeaa ilman virheilmoitusta niin palvelun toiminta on siltä osin varmistettu. Huomaa myös testata osoite niin sisä- kuin ulkoverkosta, koska näistä siihen johtavat reitit kulkevat eri kautta.

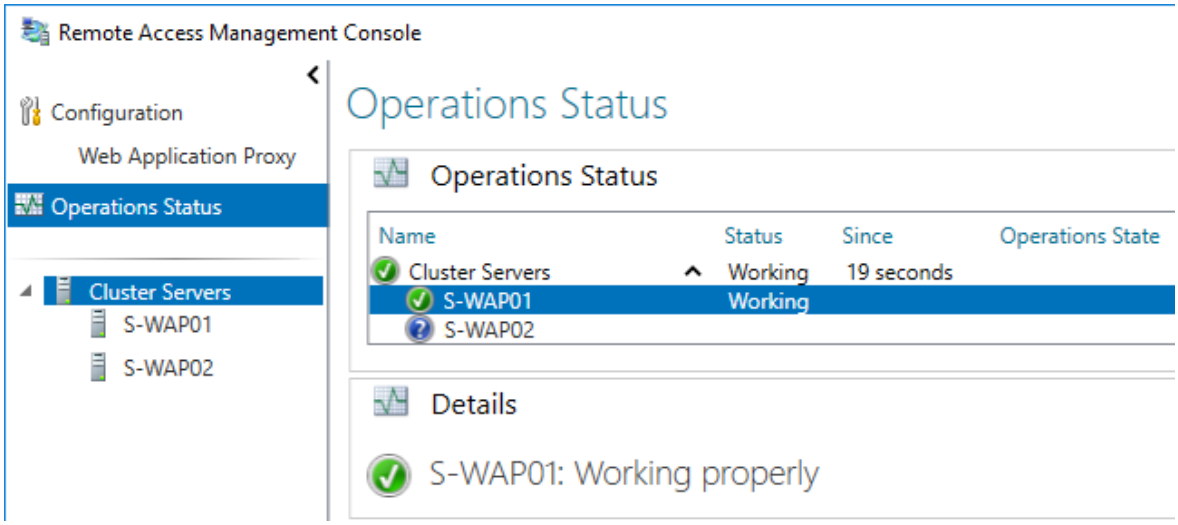
Kolmas keino on – esimerkiksi Windowsin sisäänrakennettua PowerShell-konsolia käyttäen – testata, että palvelun oletus-endpoint vastaa sille tehtyihin pyyntöihin. Koska oletusosoite on tässäkin aina sama (**https://<Palvelun URL>/adfs/ls/**) on testi helppo ajaa palvelua vasten, sisä- ja ulkoverkosta jälleen kerran erikseen. Testin haluttu tulema on HTTP-tilakoodi ”200 OK”.



Kuva 28. Oletus-endpointin tarkistus

Aiemmin on usein testaamiseen käytetty myös URL:ia, jolla viitataan Identity Providerin aloitteesta kirjautumiseen (”IdPInitiatedSignon”). Kyseinen kirjautumissivu on Windows Server 2016 AD FS:n versiosta alkaen oletuksena poissa käytöstä ja sen mahdollisessa käyttöönotossa tulisi testauksen ohella huomioida useita muita asioita, jonka vuoksi palvelun toiminta tulisi varmentaa muilla tavoin.

Mikäli palvelun toimivuuden kanssa saadaan eri tuloksia sisä- ja ulkoverkosta käsin, tulee WAP-roolipalvelinten toimivuus tarkistaa erikseen näiden Remote Access Management -hallintakonsolista.



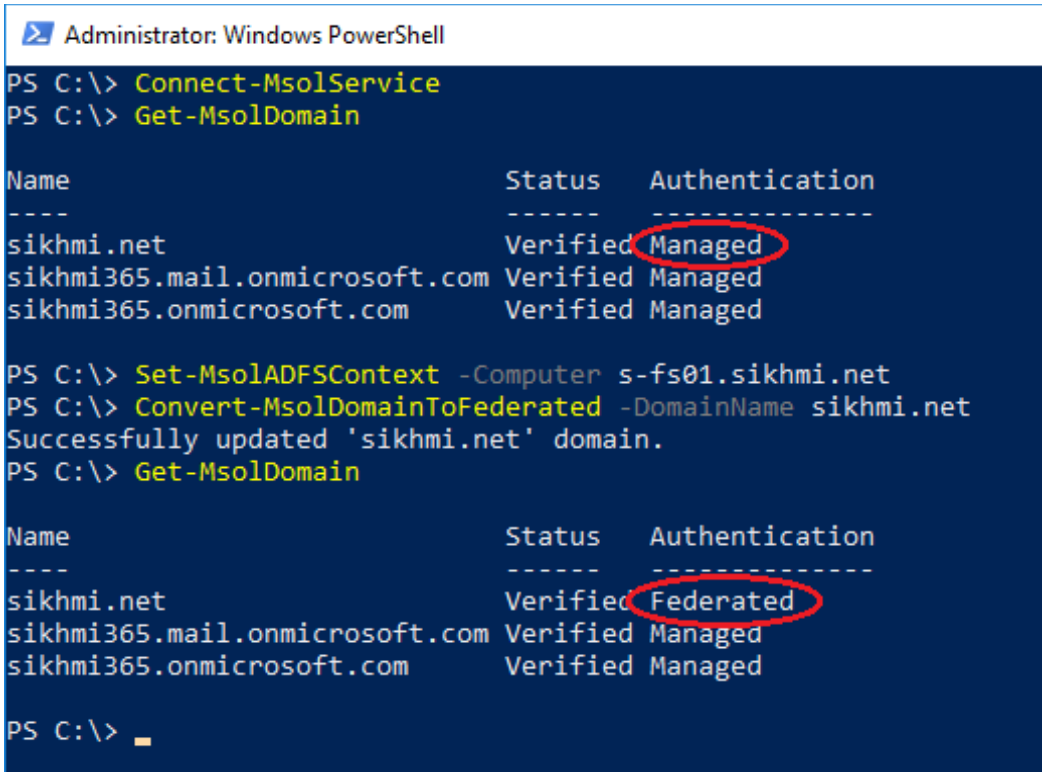
Kuva 29. WAP-palvelun status-näkymä

Koska WAP-palvelimet eivät tunnista muuta konfiguraatiota kuin federaatiopalvelun nimen ja sen kanssa käytetyn varmenteen, on niiden hallintakonsolin näkymä hyvin minimaalinen ja vailla säätömahdollisuuksia. Tarvittaessa palvelun roolinmääritysvelho voidaan ajaa uudestaan, mikäli jompikumpi edellisistä määrityksistä on muuttunut (teoriassa; palvelun nimeä ei tulisi muuttaa), mutta usein ongelmanselvitys kääntyy verkkotekniseen toteutukseen ja liikenteen kulkemiseen haluttua reittiä. Koska WAP-palvelu ei yksinään myönnä claimeja, ei palvelun näkökulmasta voi loogisesti syntyä tilannetta, jossa ulkover-

kosta palvelu toimisi ja sisäverkosta ei. Tällöin katse kääntyy taas verkkoliikenteen oikeaan reititykseen. Jos palvelun tilaa tarkastellaan hallintakonsolin cluster-näkymästä jossa nähdään kaikki federaatiofarmissa käytössä olevat WAP-palvelimet, on normaalia toiminnallisuutta etteivät palvelimet näe toistensa tilaa (toiset palvelimet näkyvät sinisen kysymysmerkin symbolilla ilmaistuna), sillä näiden välillä keskenään ei ole syytä olla siihen tarvittavia tietoliikenneyhteyksiä.

5.5 Federoidun autentikoinnin määrittäminen Office 365:een

Tavanomaisesti pilvi- tai synkronoitua identiteettiä käyttäen organisaation oma, julkinen DNS-nimi, on lisätty Office 365 -hakemistoon ja täten sitä käytetään UPN-suffixina, mutta lisättäessä sitä ei oletuksena määritetä federoiduksi, vaan se täytyy tehdä erikseen. Tämä tapahtuu MSOnline -nimisen PowerShell-moduulin avulla, eikä sitä voi tehdä Office 365 Admin Portalin kautta.



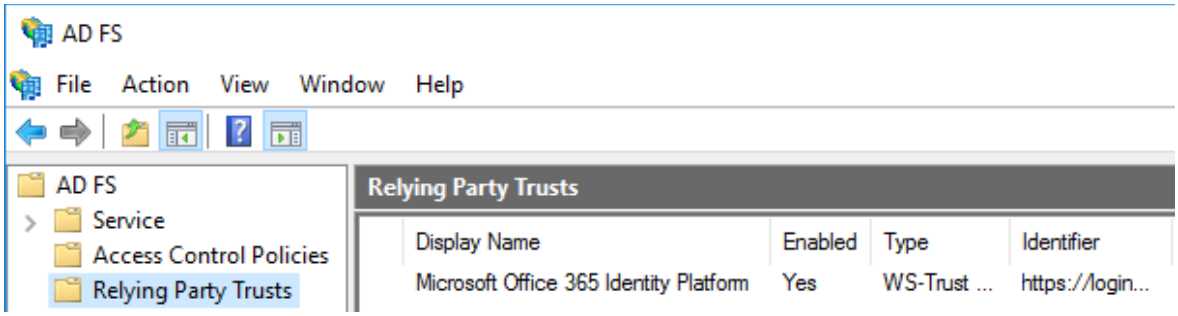
Kuva 30. Määritetään organisaation julkisesti käyttämän UPN-suffix federoiduksi

Yksi kerrallaan suoritetut komennot läpikäyden:

1. Otetaan yhteys Office 365 -palveluun. Pyyntö syöttää käyttäjätunnus ja sen salasana ylläpitoa varten tulee cmdletia suoritettaessa automaattisesti.
2. Tarkastetaan käytössä olevien toimialueiden nykytila ja voidaan todeta, että **sikhmi.net** on Managed-tilassa, eli autentikointi tehdään manuaalisesti.

3. Määritetään ensisijainen federaatiopalvelin, jota vasten muutos tehdään. Tämä komento tulee suorittaa vain, jos cmdletejä ajetaan joltakin muulta toimialueen palvelimelta kuin ensisijaiselta AD FS -palvelimelta.
4. Muutetaan toimialue **sikhmi.net** käyttämään federoitua autentikointia ja todetaan, että muutos onnistui.
5. Tarkastetaan uudestaan toimialueiden tila ja nähdään, että **sikhmi.net** toimialueen käyttämä autentikointitapa muuttui.

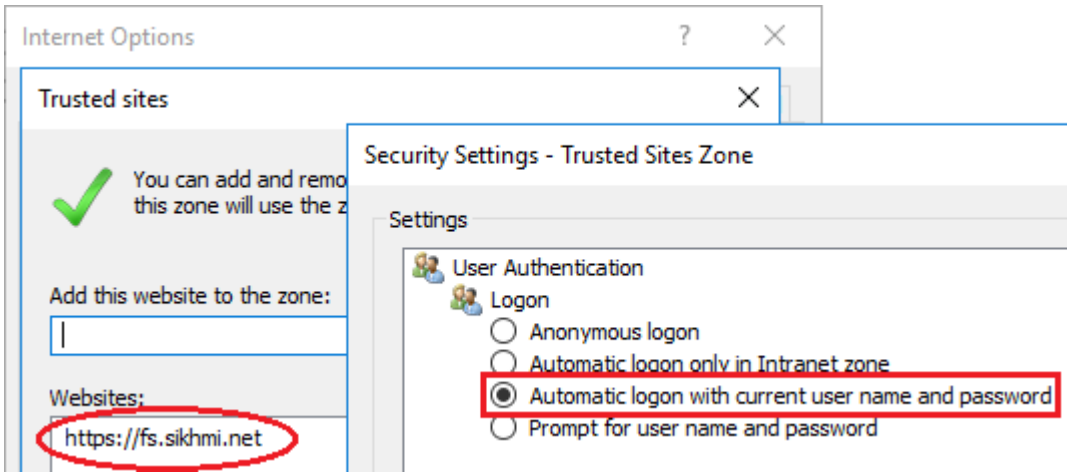
Välittömästi tämän jälkeen voimme myös nähdä (ensisijaiselta) federaatiopalvelimelta, että Microsoft Office 365 Identity Platform ilmestyi palveluun käyttöön listalle Relying Party -sovelluksista. Relying Party Trustia tarkemmin tutkimalla sieltä löytyy myös aiemmin tarkastellut claim-säännöt, joita Office 365 käyttää.



Kuva 31. Office 365 Relying Party Trustina AD FS:llä

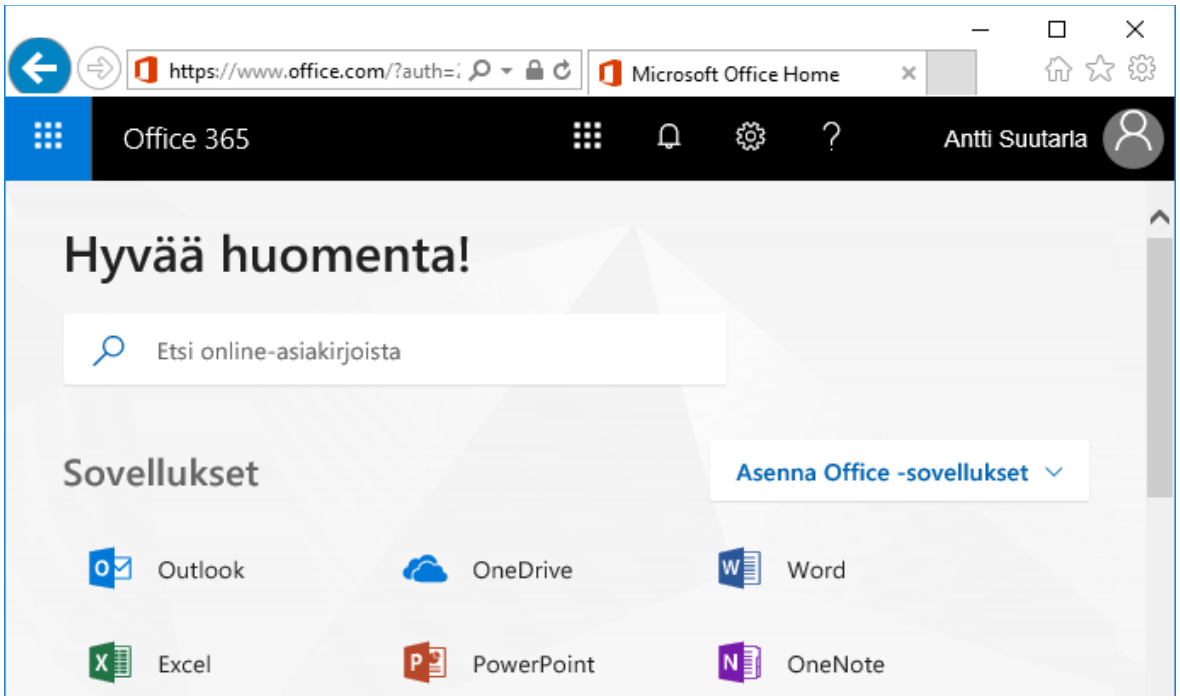
5.6 Kertakirjautumisen testaus käyttäjänä

Kaikkien edellä tehtyjen askelmerkkien jälkeen puuttuu enää yksi toimenpide, jonka jälkeen käyttäjillä toimii Office 365:n selainkäyttöisten sovellusten kertakirjautuminen: Käyttäjien selaimeen tulee määrittää federaatiopalvelun osoite (**https://fs.sikhmi.net**) joko sisäverkon tai luotetun vyöhykkeen sivustoksi ja automaattinen Windows-kirjautuminen tapahtumaan vastaavalla vyöhykkeellä. Tämän laajamittaiseen toteuttamiseen koko organisaation kattavasti on keskitettyjä tapoja, kuten Group Policyt, joilla voidaan huomioida myös eri selaimia, mutta näitä ei käsitellä tässä vaan testin nimissä vaaditut muutokset tehdään **sikhmi.net** toimialueelle liitetyn työaseman Internet Exploreriin manuaalisesti.



Kuva 31. Internet Explorerin kertakirjautumisen testaukseen käytetyt määritykset

Selaimessa Office 365:lle voidaan kertoa pelkkää kirjautumissivua URL:ssa käytettäessä kotiorganisaatio. Käyttämällä WS-Federation protokollan whr -parametria (kotiorganisaatio; home realm) testaukseen käytettävällä työasemalla, voidaan selaimeen syöttää osoitteeksi **https://login.microsoftonline.com/?whr=sikhmi.net**. Selain tekee taustalla muutaman uudelleenohjauksen (jotka on kuvattu aiemmin claim-pohjaisen autentikoinnin tapahtumaketjussa), joiden lopputuloksena käyttäjä toivotetaan tervetulleeksi Office 365 portaaliin – kertakirjautuneena vailla tunnuskyselyä ja federoidulla identiteetillä todennettuna.



Kuva 33. Kertakirjautuminen ja claim-pohjainen autentikointi Office 365 -portaaliin

6 Yhteenveto ja pohdinta

Opinnäytetyön tavoitteena oli selvittää, mikä on federoidun identiteetin merkitys ja kuinka tätä voidaan todentamisen ja valtuuttamisen yhteydessä määritellyn luottamusverkoston sisällä hyödyntää. Nimettynä käyttötapauksena ja samalla esimerkkisovelluksena tässä toimi Office 365, jonka kanssa claim-pohjainen autentikointi, autorisointi ja federoidulla identiteetillä kertakirjautuminen otettiin onnistuneesti käyttöön.

Federoidun identiteetin keskeisen toiminta-ajatuksen perusteella työn tulosta tai mahdollisia hyötyjä voi olla hankala loppukäyttäjän näkökulmaan asettuen nähdä. Näkisin tämän johtuvan ensisijaisesti siitä, että koko palvelukomponentin funktio on tehdä taustalla tapahtuvasta, loppukäyttäjälle käytännössä merkityksettömästä tapahtumaketjusta entistä näkymättömämpi. Samalla tästä tapahtumaketjusta kuitenkin muodostuu IT-infrastruktuurin ylläpidon, eheyden ja turvallisuuden kannalta yhtenäisempi, helpommin ja keskitetymmin hallittavissa oleva kokonaisuus. Monesta ylläpidollisesti työllistävästä ja loppukäyttäjälle käyttäjäkokemukseltaan epäkäytännöllisesti toimivasta sovelluksesta olisi vähemmän päänvaivaa, jos ne voitaisiin yhdistää keskitettyyn identiteettisäilöön. Tällöin myös autentikointi voisi tapahtua muualla kuin sovelluksessa itsessään, ja sovellus voisi keskittyä palvelemaan sitä mihin se on tarkoitettukin.

Tarjottavien palvelutuotantomallien muutos ohjaa organisaatioita tämän tyyppisten sovellusten suuntaan, mutta muutos ei tapahdu yhdessä yössä. Organisaatiot eivät välttämättä itse tunnista edes käyttävänsä palvelua, jonka toiminnaltaan voisi luokitella SaaS- tai pilvipalveluksi. Tällöin federoitu identiteetti ja federaatiopalvelu ovat lähes keskeisimmässä, mutta silti niin näkymättömässä roolissa käytön taustalla. Myös työn aiheen ajankohtaisuus tai sen (uutuus)arvo voitaisiin kyseenalaistaa sillä, että käytetty tekniikka on ollut olemassa jo toistakymmentä vuotta. Kuitenkaan moni IT-alan ammattilainen ei siihen välttämättä ole koskaan törmännyt tai tiennyt sitä voitavan hyödyntää. Näin, vaikka samainen käyttäjä olisi ehkä tietämättään vuosia käyttänyt jotakin sovellusta federoidulla autentikoinnilla ja identiteettimallilla.

Vaikka työssä tehty teoria- ja toteutusosuus täyttävät niille työssä annetut tavoitteet, ei tämä tarkoita, etteikö etenkin toteutusosassa olisi jatkokehitykselle tilaa. Tämä kattaa myös Office 365:n, mutta yksin jo federaatiopalvelun määrittelyssä laajempaan tai monimutkaisempaan käyttöön olisi toteutettavaa niin paljon, että sitä olisi johdonmukaisen kerronnan kannalta ollut hyvin vaikea sisällyttää työn rajaukseen. Tarvitsematta edes muuttaa federaatiopalvelun tämän työn tuloksen toiminnallisuuden edellytyksiä, voisi palveluun

jatkokehityksenä määritellä lisäksi vaikkapa monivaiheisen tunnistuksen määrätylle käyttäjäryhmälle tai tietylle sovellukselle. Palvelun voisi myös yhdistää esimerkiksi rinnakkaisorganisaatioyksikön identiteettisäilöön niin, että sen toiminnallisuus itse kääntyisikin Service Provideriksi toisaalta luottamusverkosta katsottuna. Hieman pienempi ja yleisempi muutos voisi olla esimerkiksi se, että organisaatiolla olisi useita julkisia nimiä käytössä sähköpostiosoitteissaan, sillä tämäkin vaatisi omat muutoksensa federaatiopalveluun.

Ammatillisessa kehityksessä tämä luo haasteensa siinä, että palvelu voidaan määrittää lähes niin monimutkaisesti toimivaksi kuin sitä keksitään hyödyntää. Tällöin siihen saadaan todella moninaisesti toimivia kokonaisratkaisuja luottamusverkkojen ja niiden sisältä käytettävien sovellusten välillä, mutta yhä teknisesti samoin reunaehdoin toimien. Myös työn ratkaisun palkitsevuus näkyy toteutuksen monimuotoisuudesta huolimatta yhä koko palvelun perusajatuksessa: Palveluista tehdään loppukäyttäjän kannalta niin suoraviivaisia ja käytännöllisiä kuin mahdollista, mutta samalla ne palvelevat sen ylläpitäjääkin hyödyillään.

Opinnäytetyön tekijälle työn kirjoittamisen vaikeutena sekä asioiden työssä esittämisessä olivat jatkuvasti esille nousevat, samat kysymykset, kuin mihin työ pyrkii teoriallaan ja toteutusratkaisullaan vastaamaan. Useaan otteeseen oli todella hankalaa koittaa selkokielisesti yrittää kertoa, mitä ratkaisulla oikeastaan voi hyötyä tai mikä sen virka olisi. Tässä oli kirjoittajana myös toistuvasti vältettävä sortumasta toistamaan itseään, missä mielestäni onnistuin etenevän kerronnan rajoissa pysyen. Työ on toistaiseksi pisin koskaan kirjoittamani teksti. Vaikka ammatillinen asiantuntemus aiheesta kertomista tukikin hyvin, tuntui työn rajaus ja etenkin siinä pysyminen välillä vaikealta. Lähes huomaamattaan asioista innostui välillä kirjoittamaan liiaksikin, vain palatakseen myöhemmin tiivistämään kohtia, jotka eivät työn rajauksen kannalta olleetkaan niin oleellisia.

Työn pohjaa korostavat ne lukuisat organisaatiot, joilla on voinut olla Office 365 käytössään vuosia ilman federoidun identiteetin hyödyntämistä tai edes tietoa sen tarjoamista mahdollisuuksista. Tällöin voin ainoastaan toivoa, että työ vastaa tulevaisuuteen katsoen kysymykseen, miksi federaatiopalvelua ja sen tarjoamaa identiteettimallia edes suunnitella harkitsevansa käyttöönotettavaksi. Omaa henkilökohtaista osaamistani työ on onnistuneesti kehittänyt kaventamalla kuilua tavasta, jolla dialogia palvelun toimintaperiaatteista ja sen tarjoamista mahdollisuuksista käydä – niin laaja-alaisesta huomioitavasta kokonaisuudesta kuin kyse monesti onkin.

6.1 Palaute

Opinnäytetyön teoria- ja toteutusosaltaan lähes valmis, mutta muuten viimeistelemätön versio annettiin tarkasteltavaksi kolmelle, hieman eri IT-palvelusektoreita edustavalla henkilölle kommentoitavaksi. Henkilöt valikoituivat yksilöinä heidän työnkuvan vuoksi. Heidän näkökulmat ovat henkilöiden omia, perustuvat puhtaasti henkilöiden ammatilliseen osaamiseen, eivätkä edusta heidän (opinnäytetyön kirjoitushetken) työnantajiensa näkökulmia. Työstä ei laadittu erillisiä tutkimuskysymyksiä eikä vastauksista analyysejä tarkemmin, vaan henkilöille annettiin vastattavaksi ainoastaan seuraava kysymys:

Näkisitkö tämän [opinnäyte]työn olevan itsellesi tai asiakkaallesi teknisenä yleiskäsityksenä ja toteutuskuvauksena niin selkeä, että tästä hahmottaisi mitä federaatiolla (teknisenä komponenttina ja identiteettimallina) tarkoitetaan, sekä kuinka työtä voisi hyödyntää myös Office 365:n lisäksi?

Tähän kysymykseen saatiin vastaukseksi seuraavanlaiset palautteet.

> Opinnäytetyösi on erittäin kattava dokumentti palveluiden yleiskäsityksen muodostamiseen ja tietämyksen syventämiseen. Tästä selviää erittäin hyvin eri toimintojen ja palveluiden riippuvuussuhteet keskenään, kokonaiskuvan hahmottaminen on tämän avulla helpompaa kuin esim. MS:n dokumentaatioista tulkiten. (Baljaskin 26.4.2018.)

> Työstä saa mielestäni selkeän kuvan AD FS federaation käytöstä Office 365:n identiteettimallina. Työtä voi myös mielestäni hyödyntää federaatiopalvelun teknisessä asennuksessa, koska työ pitää sisällään selkeän ohjeistuksen perusteluineen AD FS farmin tekniseen asennukseen. (Lamppu 27.4.2018.)

> Työ on hyvin jäsennelty ja se etenee loogisesti sekä sisältää kaiken oleellisen hyvin perusteltuna ja kuvattuna koskien O365-federaatiota ja sen käyttöönottoa. Voisin suositella kenelle tahansa tekniseksi ohjeistukseksi O365:n federaation käyttöönottoon. (Siitonen 27.4.2018.)

Lähteet

Amirali, J. 2013. FAQ on ADFS – Part 1. Luettavissa: https://blogs.technet.microsoft.com/askpfeplat/2013/07/22/faq-on-adfs-part-1/. Luettu: 8.3.2018.

Baler, D., Bertocci, V., Brown, K., Densmore, S., Pace, E. & Woloski, M. 2013. A Guide to Claims-Based Identity and Access Control – Second Edition. Microsoft patterns & practices.

Baljaskin, M. 26.4.2018. Komponenttivastaava, Office 365. Valtion tieto- ja viestintätekniikkakeskus Valtori. Sähköposti.

Bertocci, V. 2016. Modern Authentication with Azure Active Directory for Web Applications. Microsoft Press.

Goodner M., Hondo, M., Nadalin, A., McIntosh, M., Schmidt D. 2007. Understanding WS-Federation. Luettavissa: https://msdn.microsoft.com/en-us/library/bb498017.aspx. Luettu 13.3.2018.

Grance, T. & Mell, P. 2011. National Institute of Standards and Technology. The NIST Definition of Cloud Computing. Luettavissa: https://doi.org/10.6028/NIST.SP.800-145. Luettu: 19.4.2018.

Fortune 2017. Microsoft Office 365 Just Hit a Big Milestone. Luettavissa: http://fortune.com/2017/07/20/microsoft-office-365-earnings/. Luettu: 13.3.2018.

Gregory, D. 2014a. ADFS Deep Dive: Planning and Design Considerations. Luettavissa: https://blogs.technet.microsoft.com/askpfeplat/2014/11/23/adfs-deep-dive-planning-and-design-considerations/. Luettu: 10.3.2018.

Gregory, D. 2014b. ADFS Deep Dive: Comparing WS-Fed, SAML, and OAuth. Luettavissa: https://blogs.technet.microsoft.com/askpfeplat/2014/11/02/adfs-deep-dive-comparing-ws-fed-saml-and-oauth/. Luettu: 28.3.2018.

Ivey, S. 2013. An Introduction to AD FS We Can All Understand. Luettavissa: https://blogs.technet.microsoft.com/askidentity/2013/05/13/an-introduction-to-ad-fs-we-can-all-understand/. Luettu: 4.3.2018.

Lamppu, S. 27.4.2018. Senior Cloud Advisor. Nixu Cybersecurity. Sähköposti.

Microsoft a. Deployment planning checklist for Office 365. Luettavissa: https://support.office.com/en-us/article/deployment-planning-checklist-for-office-365-5fa4f6ef-35ad-4840-91c1-4834df3df5a0. Luettu 13.3.2018.

Microsoft b. Understanding Office 365 identity and Azure Active Directory. Luettavissa: https://support.office.com/en-us/article/understanding-office-365-identity-and-azure-active-directory-06a189e7-5ec6-4af2-94bf-a22ea225a7a9. Luettu: 1.3.2018.

Microsoft c. Domains FAQ - Office 365. Luettavissa: https://support.office.com/en-us/article/domains-faq-1272bad0-4bd4-4796-8005-67d6fb3afc5a. Luettu: 13.3.2018.

Microsoft d. Claims-based identity term definitions. Luettavissa: https://docs.microsoft.com/en-us/sharepoint/dev/general-development/claims-based-identity-term-definitions. Luettu: 29.3.2018.

Microsoft e. The Role of the Claim Rule Language. Luettavissa: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd807118(v=ws.10). Luettu: 5.4.2018

Microsoft Azure. What is SaaS? Software as a service. Luettavissa: https://azure.microsoft.com/en-us/overview/what-is-saas/. Luettu: 20.3.2018.

Redmond, T., Cunningham, P., Van Horenbeeck, M. & Hansen, S. 2018. Office 365 for IT Pros – Fourth Edition.

Roundtree, D. 2013. Federated Identity Primer. Elsevier. Oxford.

Siitonen, T. 27.4.2018. Senior Cloud Architect. Capgemini Finland. Sähköposti.

Valtiovarainministeriö 2008. Valtiohallinnon tietoturvasanasto. Edita. Helsinki. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229. Luettu: 5.3.2018.