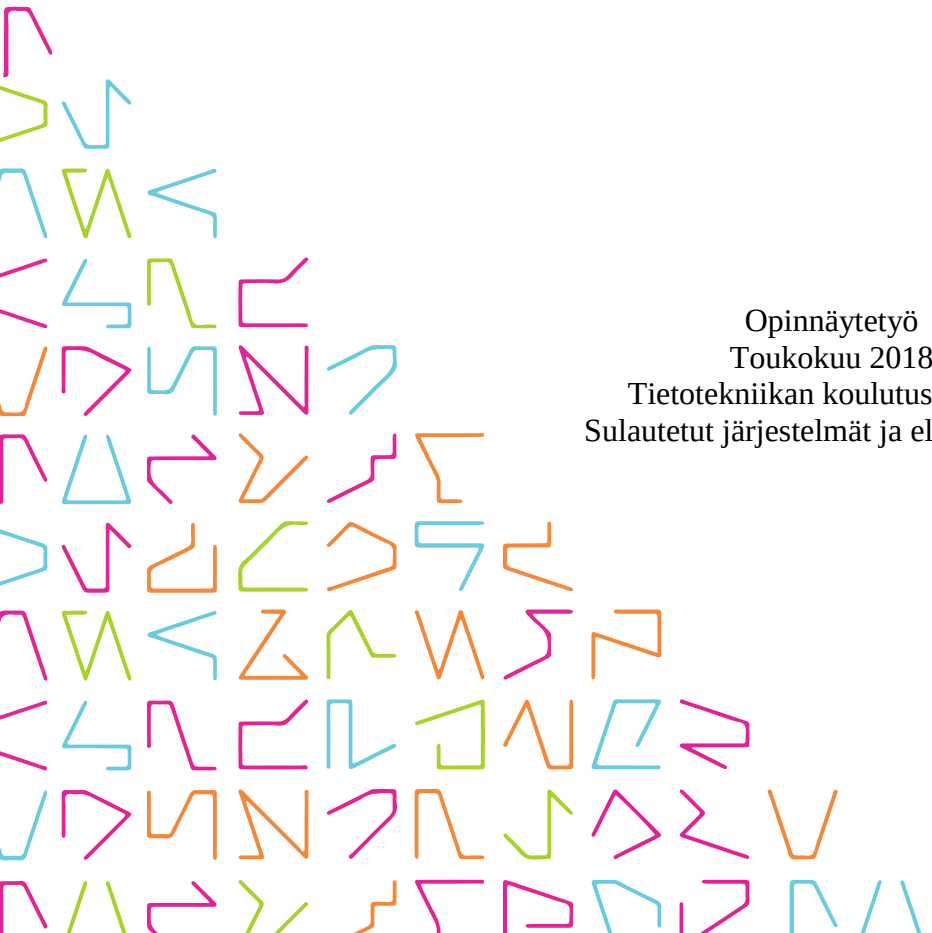
TAMPEREEN
AMMATTIKORKEAKOULU

SUOMI.FI-TUNNISTUKSEN KÄYTTÖÖNOTTO

Matti Huida



Opinnäytetyö
Toukokuu 2018
Tietotekniikan koulutusohjelma
Sulautetut järjestelmät ja elektroniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Sulautetut järjestelmät ja elektroniikka

HUIDA, MATTI:
Suomi.fi-tunnistuksen käyttöönotto

Opinnäytetyö 31 sivua, joista liitteitä 5 sivua
Toukokuu 2018

Tämän opinnäytetyön tarkoituksena on olla Suomi.fi-tunnistuksen käyttöönotto-ohje vahvaa tunnistautumista vaativille asiointipalveluille. Työn toimeksiantaja on Visma Consulting Oy, ja se on tehty helpottamaan vahvan tunnistautumisen käyttöönottoa projekteissa. Työn tarkoituksena on kuvata vahva tunnistautuminen, miten tehdään tunnistautumispyyntö ja kuinka tunnistuspalvelulta saadaan ja käytetään käyttäjästä haluttua tietoa.

Palvelun suojaaminen vahvalla tunnistautumisella vaatii rekisteröitymisen Suomi.fi-tunnistautumiseen. Rekisteröityminen tapahtuu luomalla palvelusta metadata-tiedosto, joka lähetetään Suomi.fi-tunnistautumiseen. Se kuvaa palvelun, sen käyttämät osoitteet ja mitä tietoja palvelu tarvitsee tunnistetusta käyttäjästä.

Kun palvelin saa kutsun suojattuun resurssiin, tarkistaa se ensin omasta istunnostaan, onko käyttäjä tunnistettu. Mikäli tietoa ei löydy, lähetetään käyttäjän selain tunnistuspalveluun, missä käyttäjä tunnistautuu.

Käyttöönotto-ohjeessa oletetaan, että Apache-palvelinta käytetään palvelinohjelmistona, Shibboleth-ohjelmistoa SAML-implementaationa ja että web-palvelin toimii välityspalvelimena, joka lähettää tiedot AJP-protokollalla.

Asiasanat: shibboleth, esuomi, suomi.fi-tunnistus, vahva autentikaatio

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Embedded Systems and Electronics

HUIDA, MATTI:
Implementing Suomi.fi e-Identification

Bachelor's thesis 31 pages, appendices 5 pages
August 2015

The purpose of this thesis is to act as an implentation guide for Suomi.fi e-Identification for services that require strong authentication. The assignment was received from Visma Consulting Oy, and it has been made to ease the implementation of strong authentication in projects. The purpose is to describe strong authentication, how authentication request is made, and how to get and use the data we want about the user from the identity provider.

Securing a service with strong authentication requires registering with the Suomi.fi e-Identification. Registration is made by creating a metadata file and sending it to Suomi.fi e-Identification. The metadata describes the service, what addresses it uses and what information the service requires from the authenticated user.

When the server receives a request to the resource that requires authentication, it first checks its own session for authentication info. If none is present, then the users browser is redirected to the identity provider for authentication

The implementation guide assumes the web server uses Apache application, Shibboleth as the SAML implementation and that the web server acts as a proxy for the application, sending the data using AJP protocol..

Key words: shibboleth, esuomi, suomi.fi-authentication, strong authentication

SISÄLLYS

LYHENTEET JA TERMIT

XML	Extensible Markup Language, merkintäkielistandardi
SAML	Security Assertion Markup Language, XML-standardi käyttäjien tunnistamiseen liittyvien tietojen jakamiseen
IdP	Identity Provider, tunnistuspalvelu joka ylläpitää ja tarjoaa käyttäjien tunnistamiseen liittyvää informaatiota
SP	Service Provider, asiointipalvelu, joka pyytää käyttäjiensä tunnistustietoa tunnistuspalvelulta
SSO	Single sign-on, kertakirjautuminen, useisiin palveluihin tunnistautuminen yhdellä kirjautumisella
KaPA-laki	Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016)
Apache	HTTP-palvelinohjelma
Shibboleth	SAMLiin pohjautuva avoimen lähdekoodin IdP- ja SP-implementaatio.
AJP	Apache JServ Protocol, protokolla jonka avulla välitetään tietoa web-palvelimelta sovellus-palvelimelle

1 JOHDANTO

Julkisella sektorilla on velvollisuus ja oikeus käyttää yhteisiä sähköisen asioinnin tukipalveluita. Visma Consulting Oy on toimittajana useille julkisen sektorin palveluille, joten tulevaisuudessa tulee useampia projekteja, jotka vaativat vahvaa tunnistautumista Suomi.fi-tunnistautumisen kautta. Tämän työn tarkoituksena on selventää, mitä tunnistautumistapahtumassa tapahtuu ja miten palvelu konfiguroidaan käyttämään vahvaa tunnistautumista. Työssä esitetään vaadittu dokumentaatio ja konfiguraatiotiedostot kohta kohdalta.

Tunnistautuminen tapahtuu lähettämällä tunnistautumispyyntö tunnistuspalveluun. Tunnistuspalvelu ohjaa käyttäjän tunnistautumisvälineeseen, esimerkiksi verkkopankkitunnistus tai mobiilitunnistus. Kun käyttäjä on tunnistettu, palauttaa tunnistuspalvelu käyttäjästä pyydetyt tiedot tunnistusta pyytävälle palvelulle. (Tekninen rajapintakuvaus 2018.)

Koska työ on tehty Visma Consulting Oy:lle, on käyttöönotossa käytetty Visman käyttämiä sovellusratkaisuja. Web-palvelinohjelmistona on Apachen HTTP-palvelin ja SAML-implementaationa käytetään Shibboleth-ohjelmistoa.

2 SUOMI.FI-TUNNISTUS

Suomi.fi-tunnistusta käytetään Suomen ja EU-kansalaisten tietoturvalliseen tunnistamiseen käyttäen eri tunnistusvälineitä. Se on tarkoitettu valtion hallintoviranomaisten, virastojen ja laitosten, liikelaitoksien, kunnallisien viranomaisten, tuomioistuinten ja muiden lainkäyttöelinten käyttöön. Julkisen sektorin organisaatioilla on velvollisuus tai oikeus käyttää Suomi.fi-tunnistusta palveluissa, joissa edellytetään käyttäjän vahvaa tunnistautumista. Nämä velvollisuudet tai oikeudet kuvataan laissa hallinnon yhteisistä sähköisen asioinnin tukipalveluista. Suomi.fi-tunnistuksen testiympäristö on kaikille avoin. (Suomi.fi-tunnistus, n.d.)

Palveluntarjoajalle tunnistautumisen ja käyttäjän identiteetin hallinnan siirtäminen ulkoiselle luotetulle palvelulle poistaa käyttäjän tunnistuksen kehittämistarpeen palvelusta. Yhtenäinen kertakirjautuminen mahdollistaa myös saman kertakirjautumisen sisältävien palveluiden välillä helpomman siirtymisen, sillä käyttäjän ei tarvitse tunnistautua jokaiseen palveluun erikseen.

Suomi.fi-tunnistuksen käyttöönotto vaatii asiointipalvelulta rekisteröimisen Suomi.fi-tunnistukseen, web-palvelinohjelmiston konfiguroinnin käyttämään SAML-standardin suojausta sekä SAML-implementaation asennuksen ja konfiguroinnin.

2.1 Metadatan tiedot

Suomi.fi-tunnistukseen liitytään hakemalla tarvittava tietolupa ja lähettämällä palvelun metadata-tiedosto tunnistuspalveluun, missä se lisätään tunnistusjärjestelmän palveluihin (Tekninen rajapintakuvaus 2018).

Palvelun tietolupa voi olla suppea, keskilaaja tai laaja. Tämä tietoluvan laajuus vaikuttaa siihen, mitä tietoja tunnistetusta käyttäjästä voidaan välittää asiointipalvelulle. Suppealla tietoluvalla käyttäjästä saadaan vain nimitiedot sekä henkilötunnus ja sähköinen asiointitunnus. Keskilaaja tietolupa sisältää suppean lisäksi myös osoite- ja sähköpostitiedot. Myös tieto turvakiellosta kuuluu keskilaajaan tietolupaan. Mikäli käyttäjällä on turvakielto, ei käyttäjän osoitetietoja välitetä. Laajimpaan tietolupaan kuuluu alempien lisäksi

myös tieto, onko käyttäjä Suomen kansalainen. (Tunnistetusta käyttäjästä välitettävät tiedot 2017.)

Metadata on SAML 2.0 -standardin mukainen XML-tiedosto, jolla kuvataan palvelun perustiedot tunnistavalle järjestelmälle. Osa metadatan kentistä ja attribuuteista on palvelun täyttämiä. Näiden lisäksi metadata sisältää kenttiä ja attribuutteja, joiden arvot tunnistuspalvelu määrää. Näiden kenttien ja attribuuttien arvot saa Suomi.fi-palvelusta. Liitteessä 1 on kokonainen esimerkkimetadata-tiedosto, jonka palvelulle muokattavat kentät esitellään alla. (Asiointipalvelun metadatatiedot 2018.)

Metadata-tiedosto koostuu EntityDescriptor-kentästä, johon sisältyy SPSSODescriptor-, Organization- ja ContactPerson-kentät. SPSSODescriptor-kenttä sisältää palvelua kuvailevia tietoja, Organization-kenttä palvelua tarjoavan organisaation tietoja ja ContactPerson-kenttä sisältää palvelun yhteyshenkilöiden yhteystiedot. (Asiointipalvelun metadatatiedot 2018.)

2.1.1 Palvelun täyttämät tiedot

Metadata-tiedoston EntityDescriptorin-kentän entityID-attribuutti yksilöi tunnistusta pyytävän palvelun. EntityID:n pitää olla asiointipalvelun verkkotunnuksen alainen URL, mutta sen ei tarvitse ohjata millekään verkkosivulle (Asiointipalvelun metadatatiedot 2018). Alla oleva esimerkki kuvaa esimerkki.fi-verkkotunnuksen alla olevaa palvelua ja tunnistusta pyytävä asiointipalvelu sidotaan sen polkuun /shibboleth. (Asiointipalvelun metadatatiedot 2018.)

```
<md:EntityDescriptor
  xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:ds=http://www.w3.org/2000/09/xmldsig#
  xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
  entityID="https://esimerkki.fi/shibboleth">
```

X509Certificate-kenttään tulee julkinen avain, jota vastaavalla yksityisellä avaimella allekirjoitetaan Suomi.fi-tunnistukselle lähtevät sanomat. Tämän avulla tunnistus varmistaa

pyynnön tulevan oikealta palvelulta. Tuotantoympäristössä varmenteen hyväksytyt myöntäjätahot ovat VRK, VeriSign, Thawte, Symantec ja Entrust, mutta testiympäristössä suositellaan itseallekirjoitettuja varmenteita. (Asiointipalvelun metadatatiedot 2018.)

Palvelun osoitteet, joihin tunnistuspalvelu ottaa yhteyttä, on kuvattu AssertionConsumerService- ja SingleLogoutService-kenttien Location-attribuutissa. AssertionConsumerService-kenttä sisältää osoitteen, johon tunnistuspalvelu lähettää tunnistautumisen tiedot. SingleLogoutService-kenttä kuvaa osoitteen, johon tunnistuspalvelu voi ottaa yhteyttä halutessaan invalidoida käyttäjän tunnistusistunnon. (Asiointipalvelun metadatatiedot 2018.)

Alla olevassa esimerkissä on sidottu tunnistustiedot vastaanottavaosoite sekä uloskirjautumisosoite. Osoitteet on määritelty Shibbolethissa, ja ne esitellään Shibbolethin konfiguraation kuvaavassa kappaleessa. Binding-attribuutti kertoo, mitä HTTP-protokollan metodia käytetään.

```
<md:SingleLogoutService
      Location="https://esimerkki.fi/Shibboleth.sso/SLO/POST"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
   <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
     Location="https://esimerkki.fi/Shibboleth.sso/SAML2/POST" index="1" />
```

UIInfo-kentän sisällä olevat kentät määrittävät käyttäjälle näkyviä tietoja palvelusta. ServiceName-kenttä sisältää asiointipalvelun nimen. Organization-kentän sisällä olevat kentät sisältävät organisaation nimen, näyttönimen ja verkko-osoitteen. Näistä tiedoista on toimitettava suomen-, ruotsin- ja englanninkielinen versio. Näiden lisäksi ContactPerson-kentässä voidaan määrittää asiointipalvelun yhteyshenkilöt. Palvelulla pitää olla vähintään yksi tekninen yhteyshenkilö. (Asiointipalvelun metadatatiedot 2018.)

Kaikissa itsetuottamissa tiedoissa pitää ottaa huomioon mahdolliset tunnistuspalvelun asettamat rajoitukset tiedoille, kuten Description-kentän maksimimerkkimäärä 255 (Asiointipalvelun metadatatiedot 2018).

2.1.2 Palvelun valitsemat kentät

Palvelun valitsemat kentät eroavat itse tuotetuista kentistä siten, että palvelun valitsemissa kentissä ja attribuuteissa arvot ovat Suomi.fi-tunnistuksen määräämiä. Näistä valitaan palveluun sopivat ja sen tarvitsemat arvot.

EntityAttributes-kenttä sisältää asiointipalvelun määrittelemän tunnistusvälineiden varmuustason. Taso voi olla korkea http://ftn.ficora.fi/2017/loa3 tai korotettu http://ftn.ficora.fi/2017/loa2. Mikäli halutaan korotettu taso, pitää se olla määriteltynä korkean tason kanssa. Näiden lisäksi voidaan myös määritellä mahdollinen Katso-väline. Taulukossa 1 on kuvattu hyväksytyt tunnistusvälineet ja millä tunnisteella niihin viitataan metadatassa. (Asiointipalvelun metadatatiedot 2018.)

Taulukko 1. Hyväksytyt tunnistusvälineet (Asiointipalvelun metadatatiedot 2018)

Arvo	Selite
http://ftn.ficora.fi/2017/loa3	korkea, fLOA3
http://ftn.ficora.fi/2017/loa2	korotettu, fLOA2
urn:oid:1.2.246.517.3002.110.1	verkkopankkitunnus
urn:oid:1.2.246.517.3002.110.2	varmennekortti
urn:oid:1.2.246.517.3002.110.3	mobiilivarmenne
urn:oid:1.2.246.517.3002.110.5	KatsoOTP
urn:oid:1.2.246.517.3002.110.6	KatsoPWD
urn:oid:1.2.246.517.3002.110.998	EIDAS-testitunnistaja, joka käytössä ainoastaan asiakastestiympäristössä
urn:oid:1.2.246.517.3002.110.999	testitunnistusväline, joka käytössä ainoastaan asiakastestiympäristössä

Tunnistetusta käyttäjästä halutut tiedot määritellään AttributeConsumingService-kentän sisään RequestedAttribute-kenttinä, joiden attribuuttien tiedot ovat saatavilla Suomi.fi-tunnistuksesta. Tunnistetusta käyttäjästä välitettävien tietojen saaminen riippuu käytetystä tunnistusvälineestä ja palvelun tietoluvan laajuudesta. Nämä tiedot on kuvattu taulukossa 2. (Tunnistetusta käyttäjästä välitettävät tiedot 2017.)

Taulukko 2. Tunnistetusta käyttäjästä välitettävät attribuutit (Tunnistetusta käyttäjästä välitettävät tiedot 2017)

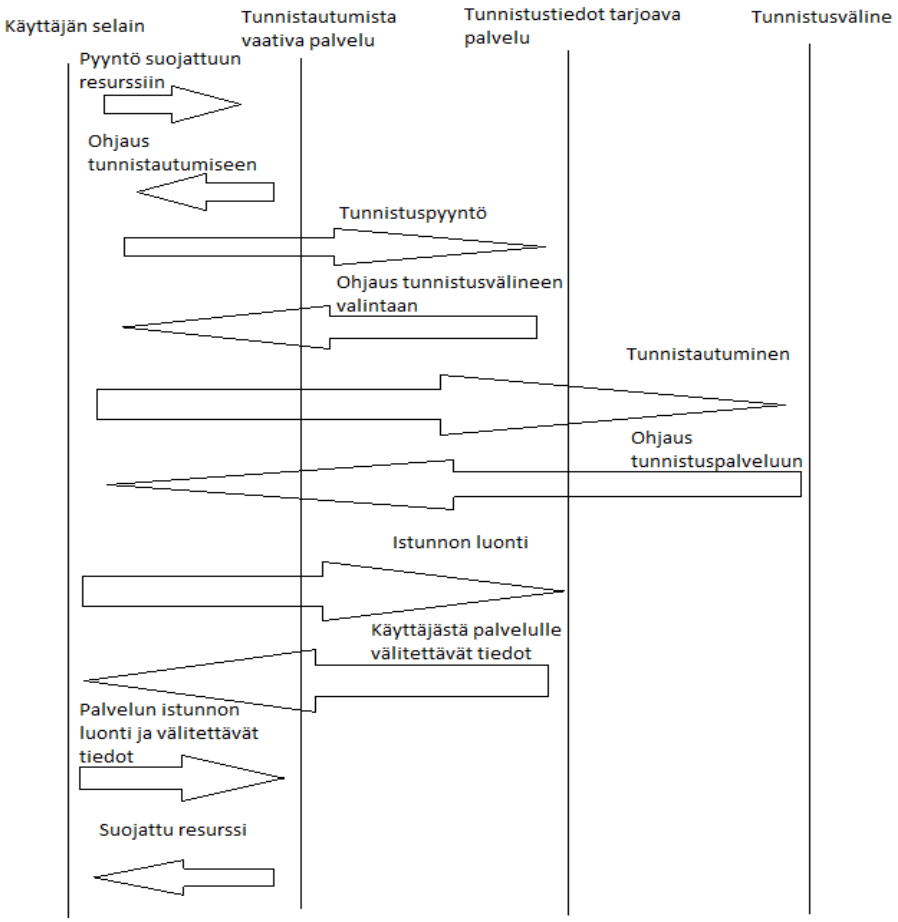
Tieto	**Kuvaus**	**OID & FriendlyName**
Sähköinen asiointitunnus	Sähköinen asiointitunnus,	urn:oid:1.2.246.22 electronicIdentificationNumber
Henkilötunnus, hetu	Henkilötunnus, joka yksilöi tunnistetun käyttäjän.	urn:oid:1.2.246.21 nationalIdentificationNumber
Katso ID	Katso-tunnisteeseen liitetty käyttäjätunnus, joka yksilöi tunnistetun käyttäjän.	urn:oid:1.2.246.517.3003.113.4 kid
Nimi, common name	Henkilön nimi muodossa sukunimi + kaikki etunimet. Jos kyseessä Katso-tunnistaja, palautetaan Katso-tunnisteeseen liitetty nimitieto.	urn:oid:2.5.4.3 cn
Koko nimi	Henkilön koko nimi muodossa ”Kutsumanimi Sukunimi”. Jos Väestötietojärjestelmään ei ole rekisteröity kutsumanimeä, on sen tilalla ensimmäinen etunimi (sama sääntö kuin kutsumanimessä).	urn:oid:2.16.840.1.113730.3.1.241 displayName
Kutsumanimi	Kutsumanimi tai ensimmäinen etunimi jos Väestötietojärjestelmään ei ole rekisteröity kutsumanimeä.	urn:oid:2.5.4.42 givenName
Sukunimi	Henkilön sukunimi.	urn:oid:2.5.4.4 sn
Etunimet	Henkilön kaikki etunimet.	http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName FirstName
Kotikunnan kuntanumero	Henkilön kotikunnan kuntanumero.	urn:oid:1.2.246.517.2002.2.18 KotikuntaKuntanumero
Kotikunta suomeksi	Henkilön kotikunnan suomenkielinen nimi.	urn:oid:1.2.246.517.2002.2.19 KotikuntaKuntaS
Kotikunta ruotsiksi	Henkilön kotikunnan ruotsinkielinen nimi.	urn:oid:1.2.246.517.2002.2.20 KotikuntaKuntaR

Vakinainen kotimainen lähiosoite, katuosoite suomeksi	Vakinaisen kotimaisen lähiosoitteen suomenkielinen kadunnimi, katunumero ja huoneistotunniste.	urn:oid:1.2.246.517.2002.2.4 VakinainenKotimainenLahiosoiteS
Vakinainen kotimainen lähiosoite, katuosoite ruotsiksi	Vakinaisen kotimaisen lähiosoitteen ruotsinkielinen kadunnimi, katunumero ja huoneistotunniste.	urn:oid:1.2.246.517.2002.2.5 VakinainenKotimainenLahiosoiteR
Vakinainen kotimainen lähiosoite, postinumero	Vakinaisen kotimaisen lähiosoitteen postinumero.	urn:oid:1.2.246.517.2002.2.6 VakinainenKotimainenLahiosoitePostinumero
Vakinainen kotimainen lähiosoite, postitoimipaikka suomeksi	Vakinaisen kotimaisen lähiosoitteen suomenkielinen postitoimipaikka. Muoto 0-50 merkkiä.	urn:oid:1.2.246.517.2002.2.7 VakinainenKotimainenLahiosoitePostitoimipaikkaS
Vakinainen kotimainen lähiosoite, postitoimipaikka ruotsiksi	Vakinaisen kotimaisen lähiosoitteen ruotsinkielinen postitoimipaikka.	urn:oid:1.2.246.517.2002.2.8 VakinainenKotimainenLahiosoitePostitoimipaikkaR
Vakinainen ulkomainen lähiosoite, katuosoite	Vakinaisen ulkomaisen osoitteen lähiosoite siten kuin henkilö on sen ilmoittanut väestötietojärjestelmään.	urn:oid:1.2.246.517.2002.2.11 VakinainenUlkomainenLahiosoite
Vakinainen ulkomainen lähiosoite, paikkakunta ja valtio suomeksi	Vakinaisen ulkomaisen lähiosoitteen postinumero, paikkakunta ja valtio. Valtio on erotettu pilkulla paikkakunnasta ja postinumerosta. Valtion nimi suomeksi. Elementissä on tietoa, kun henkilön ilmoittama asuinvaltion koodi löytyy ISO3166-koodistosta.	urn:oid:1.2.246.517.2002.2.12 VakinainenUlkomainenLahiosoitePaikkakuntaJaValtioS
Vakinainen ulkomainen lähiosoite, paikkakunta ja valtio ruotsiksi	Vakinaisen ulkomaisen lähiosoitteen postinumero, paikkakunta ja valtio. Valtio on erotettu pilkulla paikkakunnasta ja postinumerosta. Valtion nimi ruotsiksi. Elementissä on tietoa, kun henkilön ilmoittama asuinvaltion koodi löytyy ISO3166-koodistosta.	urn:oid:1.2.246.517.2002.2.13 VakinainenUlkomainenLahiosoitePaikkakuntaJaValtioR

Vakinainen ulkomainen lähiosoite, paikkakunta ja valtio selväkielinen	Vakinaisen ulkomaisen lähiosoitteen postinumero, paikkakunta ja valtio siinä tapauksessa, ettei asuinvaltio löydy ISO3166-koodistosta.	urn:oid:1.2.246.517.2002.2.14 VakinainenUlkomainenLahiosoitePaikkakuntaJaValtioSelvakielinen
Vakinainen ulkomainen lähiosoite, valtiokoodi	Vakinaisen ulkomaisen osoitteen valtiokoodi.	urn:oid:1.2.246.517.2002.2.15 VakinainenUlkomainenLahiosoiteValtiokoodi
Sähköpostiosoite	Sähköpostiosoite, jonka kansalainen ilmoittanut väestötietojärjestelmään.	urn:oid:0.9.2342.19200300.100.1.3 mail
Turvakielto	Turvakielto olemassa, kun arvo on 1. Jos kansalaisella on turvakielto, ei osoitetietoja välitetä tunnistustapahtuman yhteydessä.	urn:oid:1.2.246.517.2002.2.27 TurvakieltoTieto
Suomen kansalaisuus	Tieto siitä, onko Suomen kansalainen.	urn:oid:1.2.246.517.2002.2.26 SuomenKansalaisuusTietokoodi

3 TUNNISTAUTUMINEN

Tunnistautumistapahtuma syntyy, kun käyttäjä pyytää palveluntarjoajalta tunnistuksen vaativaa resurssia. Tällöin palveluntarjoaja tutkiin ensin omasta istuntotiedostaan, onko käyttäjä jo valtuutettu lataamaan kyseinen resurssi. Mikäli auktorisointitietoja ei löydy, ohjataan käyttäjän selain tunnistuspalveluun. Tämä tarkistaa, onko käyttäjällä tunnistettu istunto. Jos käyttäjällä on aktiivinen tunnistautumisistunto, palautetaan palveluntarjoajalle tunnistautumisvastaus. Mikäli istuntoa ei löydy, ohjataan käyttäjä tunnistautumaan yhteen määritellyistä tunnistautumisvälineistä. Tunnistautumisen jälkeen ohjataan käyttäjän selain takaisin tunnistuspalveluun, joka luo istunnon tunnistetulle käyttäjälle. Tunnistetun käyttäjän selain ohjataan palveluntarjoajalle käyttäjästä välitettävien tietojen kanssa. Tunnistuksessa tietojen välittämiseen käytetään SAML 2.0 -standardia. (Tekninen rajapintakuvaus 2018.)



KUVA 1. Tunnistautumistapahtuma

3.1 Tunnistuspyyntö

Kun asiointipalvelulla ei ole omassa istunnossaan käyttäjän tunnistetietoja, lähettää se pyynnön sille määritellylle tunnistuspalvelulle käyttäjän tunnistamista varten. Tunnistautumispyynnössä määritellään asiointipalvelun osoite, johon tunnistetun käyttäjän tiedot lähetetään, tunnistuspalvelun osoite, tunnistuspyynnön identifioiva tunniste, tunnistuspyynnön aikaleima, käytetty protokolla ja sen protokollan versio. Tunnistuspyynnössä voidaan myös lähettää tunnistusvälinepyyntö. Alla on esimerkki tunnistuspyynnöstä. Tunnistuspyynnön kentät on määritelty Shibbolethin konfiguraatiossa kappaleessa 4.1 (Tekninen rajapintakuvaus 2018.)

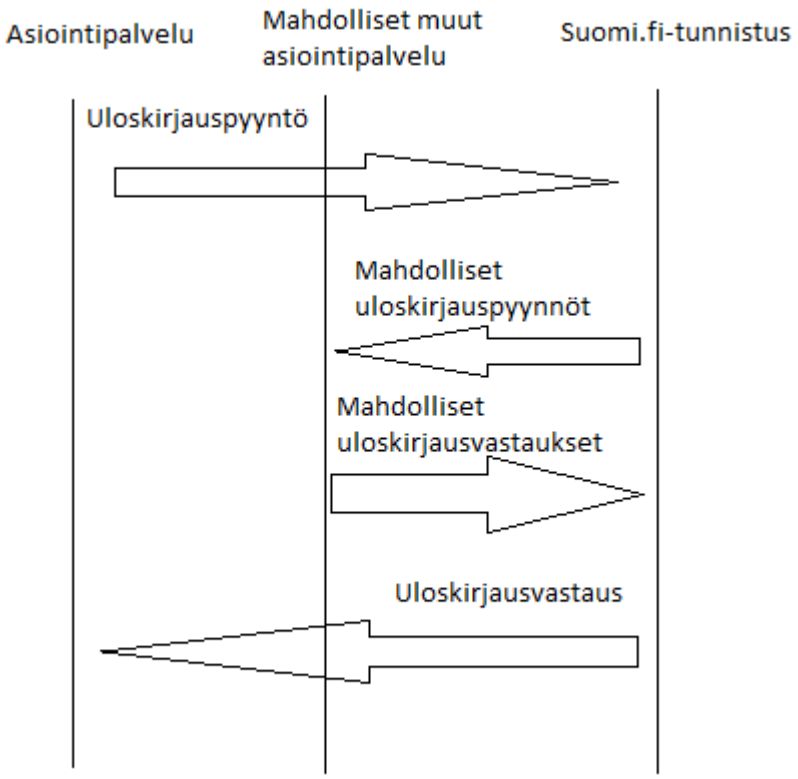
```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
        AssertionConsumerServiceURL="https://esimerkki.fi/Shibboleth.sso/SAML2/POST"
        Destination="https://testi.apro.tunnistus.fi/idp/profile/SAML2/Redirect/SSO"
        ID="_6e321c23b3929a5f2a0f09b9bd6d712a"
        IssueInstant="2018-05-13T18:43:16Z"
        ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Version="2.0">
 <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  https://esimerkki.fi/shibboleth
 </saml2:Issuer>
 <saml2p:Extensions>
  <vetuma xmlns="urn:vetuma:SAML:2.0:extensions">
   <LG>fi</LG>
  </vetuma>
 </saml2p:Extensions>
 <saml2p:NameIDPolicy AllowCreate="true"
          Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />
 <saml2p:RequestedAuthnContext
          Comparison="exact" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   urn:oid:1.2.246.517.3002.110.1
  </saml2:AuthnContextClassRef>
  <saml2:AuthnContextClassRefxmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   urn:oid:1.2.246.517.3002.110.3
  </saml2:AuthnContextClassRef>
```

```
 </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

Esimerkissä oleva Extensions-kenttä määrittelee vetuma-elementin, jonka arvona on ISO 639-1 -standardin mukainen kielikoodi. Tuetut kielet ovat suomi, ruotsi ja englanti. Tämä kenttä ei ole pakollinen. (Tekninen rajapintakuvaus 2018.)

3.2 Uloskirjauspyyntö

Suomi.fi-tunnistus voi lähettää uloskirjauspyynnön asiointipalvelulle, tai asiointipalvelu voi lähettää uloskirjauspyynnön Suomi.fi-tunnistukselle. Mikäli kertauloskirjaus on käytössä, pyytää tunnistuspalvelu muita asiointipalveluja kirjaamaan käyttäjän ulos. Kuva 2 havainnollistaa asiaa. (Tekninen rajapintakuvaus 2018.)



Kuva 2. Uloskirjaustapahtuma

4 PALVELUN KONFIGUROINTI

Tämä käyttöönotto-ohje kuvailee palvelua, jota tarjoillaan käyttäen Apache HTTP-palvelinta, sekä Shibbolethia SAML-implementaationa. Apacheen on myös asennettava mod_shib-moduuli, joka toimii Shibbolethin web-palvelimen puolen implementaationa. Tämän lisäksi oletetaan tunnistusta vaativan palvelun lukevan portistaan AJP-protokollan mukaista dataa.

4.1 Shibboleth

Shibbolethin konfiguraatio on XML-muodossa oleva shibboleth2.xml-tiedosto. Tähän tiedostoon kuvataan suojattavat palvelut yksitellen, ja määritellään näille palvelukohtaiset konfiguraatiot. Liitteenä 2 on kuvattuna yhden palvelun Shibboleth-konfiguraatio kokonaisena, ja nämä esitellään kohta kohdalta alla.

ApplicationOverride-kentässä kuvataan palvelun tietoja ja se on juurielementti kaikille tuleville kentille, jos toisin ei ole mainittu. EntityId-attribuutti kertoo palvelun Shibbolethin sisällä yksilöivän nimen. Mikäli Shibbolethiin on määritelty useita palveluita, tulee jokaisella olla yksilöivä EntityId. AttributePrefix-attribuuttiin määritetään, minkä etuliitteen Shibboleth lisää käyttäjästä välitettäviin tietoihin. Alla olevassa esimerkissä tiedot välitetään käyttäen AJP-protokollaa, joten tietoihin liitettään AJP_-etuliite. Tällöin Apache-palvelin välittää ne eteenpäin poistaen etuliitteen. Signing-attribuutti kontrolloi ulospäin lähtevien viestien allekirjoitusta. Encryption-attribuutti kontrolloi ulospäin lähtevien viestien salausta. (NativeSPApplication 2016.)

```
<ApplicationOverride id="esimerkki" entityID="https://esimerkki.fi/shibboleth" signing="true" encryption="false" attributePrefix="AJP_">
```

Sessions-kentässä kuvaillaan eri tunnistautumisistunnot ja niiden attribuutit. Lifetime-attribuutti kertoo istunnon maksimielinajan, timeout, kuinka kauan istunnossa saa olla pyyntöjen välisenä aikana. Molemmat arvot ovat sekunteina. Esimerkissä istunto voi olla enintään kaksi tuntia, ja pyyntöjen välillä saa olla enintään 32 minuuttia. CheckAddress-attribuutti on arvolla false, sillä sen oletusarvo on true. Jos checkAddress-attribuutti on arvolla

true, lisää tunnistuspalvelu tunnistusvastaukseen käyttäjän osoitteen. Asiointipalvelu varmistaa, että tämä osoite on sama kuin palvelua käyttävä selain. Tämä voi olla hyödyllinen turvallisuuden kannalta, mutta esimerkiksi osoitteenmuunnos ja välityspalvelimet tekevät osoitteen tarkistuksesta yleisen virhelähteen. HandlerURL-attribuutti kertoo, minkä polun taakse Shibboleth luo omat palvelunsa. (NativeSPSessions 2017.)

```
<Sessions lifetime="7200" timeout="1920" checkAddress="false" cookieProps="https" relayState="ss:mem" handlerSSL="true" handlerURL="/Shibboleth.sso">
```

Sessions-kentän lapsielementissä Logout-kentässä määritellään, kuinka uloskirjaudutaan. Logout-kenttä on yksinkertaistettu uloskirjautumisen käsittelijä, joka asentaa uloskirjautumispalvelun automaattisesti suositeltuun polkuun /Logout. Esimerkissä tehdään paikallinen SAML2-uloskirjautuminen, eli uloskirjautuminen tapahtuu ilman tunnistuspalvelua. Asiointipalvelu voi aloittaa uloskirjautumisprosessin ohjaamalla käyttäjän selaimen määriteltyyn uloskirjautumispalvelun polkuun. (NativeSPServiceLogout 2010.)

```
<Logout>SAML2 Local</Logout
```

Sessions-kentän lapsielementissä SessionInitiator-kentässä määritellään tunnistautumissession aloittavan käsittelijän tiedot. Type-attribuutti kertoo, mitä protokollaa käytetään. Location-attribuutti kertoo, mistä polusta sisäänkirjautumiskäsittelijä löytyy. Tähän osoitteeseen ottamalla yhteyttä voidaan sisäänkirjautuminen aloittaa manuaalisesti. Palvelulla voi olla useita käsittelijöitä ja yksi näistä pitää merkata oletusarvoksi antamalla isDefault-attribuutille arvo true. Apachen konfiguraatiossa käytetty requireSession true arvo ohjaa tähän oletuskäsittelijään. Id-attribuutti on valinnainen kenttä, jolla voidaan antaa käsittelijälle nimi. Tähän nimeen voidaan viitata Apachen requireSession konfiguraatiossa. EntityId-attribuuttiin tulee tunnistuspalvelun tunniste, joka on esimerkissä Suomi.fi-tunnistuksen testiympäristön arvo. (NativeSPSessionInitiator 2016.)

SessionInitator-kentän sisäinen AuthnRequest-elementtiin kuvataan, minkälainen lähtevä tunnistuspyyntö on. Jos alla olevaa esimerkkiä vertaa tunnistuspyynnön esimerkkiin huomaa, että tiedot ovat yhtenevät. AssertionConsumerServiceUrl-attribuutti kertoo, mihin osoitteeseen tunnistuspalvelu lähettää tiedot käyttäjästä. Destination-attribuutti kertoo, mihin tunnistuspalvelun osoitteeseen käyttäjä ohjataan. Esimerkissä on Suomi.fi-tunnis-

tuksen testiympäristön osoite. AuthnRequestin attribuutit ID ja IssueInstant täytetään tunnistuspyynnön tekohetkellä, ja niille konfiguroitavat tiedot ovat vain tiedoston validointia varten. (Tekninen rajapintakuvaus 2018.)

```
<SessionInitiator type="SAML2" Location="/Login" isDefault="true" id="Example"
 entityID="https://testi.apro.tunnistus.fi/idp1">
 <saml2p:AuthnRequest ID="aaa" Version="2.0" IssueInstant="2012-01-01T00:00:00Z"
  AssertionConsumerServiceURL="https://esimerkki.fi/Shibboleth.sso/SAML2/POST"
  Destination="https://testi.apro.tunnistus.fi/idp/profile/SAML2/Redirect/SSO"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
  <saml2:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   https://esimerkki.fi/shibboleth
  </saml2:Issuer>
   <saml2p:Extensions>
     <vetuma xmlns="urn:vetuma:SAML:2.0:extensions">
      <LG>fi</LG>
     </vetuma>
   </saml2p:Extensions>
  <saml2p:NameIDPolicy AllowCreate="true"
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
 </saml2p:AuthnRequest>
</SessionInitiator>
```

Sessions-kentän sisäisissä AssertionConsumerService-kentissä kuvataan, mitä tunnistukseen liittyviä palveluita Shibboleth tarjoaa. Näihin sidontoihin tunnistuspalvelu lähettää pyyntöjä ja niiden polut sijaitsevat Sessions-kenttään määritellyn HandlerURL-attribuutin perässä. Asiointipalvelun metadatassa määritellyt osoitteet on sidottu näissä tiedoissa. (NativeSPAssertionConsumerService. 2018.)

```
<md:AssertionConsumerService Location="/SAML2/POST" index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        <md:AssertionConsumerService Location="/SAML2/POST-SimpleSign" index="2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"/>
        <md:AssertionConsumerService Location="/SAML2/Artifact" index="3" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>
        <md:AssertionConsumerService Location="/SAML2/ECP" index="4" Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"/>
```

```
        <md:AssertionConsumerService Location="/SAML/POST" index="5" Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"/>
        <md:AssertionConsumerService Location="/SAML/Artifact" index="6" Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"/>
```

Sessions-kentän sisäisissä Handler-kentissä kuvataan Shibbolethin omia palveluita, jotka tarjoavat hyödyllistä funktionaalisuutta. Näiden käsittelijöiden osoite määritellään Location-attribuutissa, ja kaikille käsittelijöille voidaan antaa acl-attribuutti joka määrittää, mistä osoitteista kyseiseen käsittelijään saa ottaa yhteyttä. Esimerkissä on kuvattu neljä käsittelijää. MetadataGenerator-käsittelijä luo esimerkkimetadatan Shibbolethin sisäänrakennettujen olettamusten ja asiointipalvelun konfiguraation pohjalta. Status-käsittelijä raportoi asiointipalvelun toiminnallisen tilanteen ja joitain konfigurointivalintoja. Informaatio tulee yksinkertaisena XML-dokumenttina. Status-käsittelijään määritelty acl-attribuutti sallii vain paikalliset yhteydet. Session-käsittelijä näyttää tiedot käyttäjän Shibboleth-istunnosta, kuten käyttäjästä välitetyt tiedot ja tunnistuksen aikaleiman. Mikäli Sessions-käsittelijälle annetaan showAttributeValues-attribuutille arvo true, näyttää se käyttäjästä välitettyjen tietojen arvon. Sessions-käyttäjälle voi myös antaa contentType-attribuutin arvon application/json, jolloin palautettu arvo tulee JSON muodossa. (NativeSpHandler 2017.)

```
<Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
<Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>
<Handler type="Session" Location="/Session" showAttributeValues="false"/>
```

Errors-kentässä kuvataan virhetilanteen tiedot. RedirectErrors-attribuutti kertoo, mihin käyttäjän selain uudelleenohjataan virhetilanteen sattuessa. Uudelleenohjauksen tapahtuessa tulee kyselyn mukana virheviesti pyynnön parametrina. SupportContact-attribuutti kertoo palvelun yhteystiedon virhetilanteessa. (NativeSpErrors 2016.)

```
<Errors supportContact="tuki@esimerkki.fi" redirectErrors="https://esimerkki.fi"/>
```

MetadataProvider-kenttä kuvaa tunnistuspalvelun tiedot. Type-attribuutti kertoo, minkälainen kuvaava tiedosto on. Arvo XML kertoo tiedoston olevan XML-formaatissa. Attribuutti uri kertoo, mistä osoitteesta tiedosto löytyy. ReloadInterval-attribuuttii määrittää, kuinka monen sekunnin välein tiedosto pitää tarkistaa muutoksien varalta. BackingFile-

Path-attribuutille annetaan polku, johon Shibboleth tallentaa paikallisen kopion tiedostosta. On pidettävä huoli, että Shibbolethilla on oikeus lukea ja kirjoittaa annettuun polkuun. (NativeSPMetadataProvider 2016.)

```
<MetadataProvider type="XML" uri="https://testi.apro.tunnistus.fi/static/metadata/idp-metadata.xml"
backingFilePath="/var/cache/shibboleth/idp-metadata.xml" reloadInterval="7200">
</MetadataProvider>
```

Kentässä AttributeExtractor kuvataan, mistä löytyy ohje tunnistuspalvelun lähettämien tietojen sisällyttämiseen istunnon ympäristömuuttujiin. Kappaleessa 4.1.1 on kuvattu attribuuttikartta. Type-attribuutti määrittää tiedoston formaatin, joka on esimerkissä XML. Path-attribuutti kertoo, mistä polusta attribuuttikartta löytyy. (NativeSPAttributeExtractor 2014.)

```
<AttributeExtractor type="XML" validate="true" path="esimerkki/attribute-map.xml"/>
```

CredentialResolver-kenttään määritellään palvelun käyttämä varmenne ja avain. Type-attribuutti arvolla File kertoo, että valtuutukset ovat tiedostomuodossa. Key- ja certificate-attribuutit kertovat avaimen ja varmenteen tiedostojen sijainnit. (NativeSPCredentialResolver 2012.)

```
<CredentialResolver type="File" key="esimerkki/sp-key.pem" certificate="esimerkki/sp-cert.pem"/>
```

Testiympäristöä varten voidaan luoda itse varmenne ja avain. Tähän on käytetty Shibbolethin mukana tulevaa keygen-ohjelmaa. Keygen:lle annetaan komentoriviltä -e lipulla asiointipalvelun entityId, lipulla -h määritetään palvelimen verkkonimi ja -o lipulla, mihin hakemistoon avain ja varmenne luodaan. Keygen-ohjelma löytyy Shibbolethin asennuskansiosta.

```
./keygen.sh -e esimerkki.fi/shibboleth -h esimerkki.fi -o esimerkki
```

4.1.1 Attribuuttikartta

Attribuuttikartta kertoo, miten tunnistetusta käyttäjästä välitettävät tiedot käsitellään asiointipalvelun hyödynnettävään muotoon. Attribute-kentän name-attribuutti on löydettävissä liitteen 1 metadatasta pyydettävän attribuutin nimenä. Id-attribuutti kertoo, minkä nimisenä tieto tallennetaan istuntoon. Tähän yhdistetään Sessions-kentässsä määritelty etuliite, joten tietojen mennessä AJP-porttiin olisi esimerkiksi tiedon SHIB_sn nimi muotoa AJP_SHIB_sn.

```
<Attributes
  xmlns="urn:mace:shibboleth:2.0:attribute-map"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:saml="unr:oasis:names:tc:SAML:2.0:assertion">
 <Attribute name="urn:oid:2.5.4.4" id="SHIB_sn"/>
 <Attribute name="urn:oid:2.5.4.42" id="SHIB_givenName"/>
 <Attribute name="urn:oid:1.2.246.21" id="SHIB_nationalIdentificationNumber"/>
 <Attribute name="urn:oid:1.2.246.517.2002.2.18" id="SHIB_KotikuntaKuntanumero"/>
 <Attribute name="urn:oid:1.2.246.517.2002.2.19" id="SHIB_KotikuntaKuntaS"/>
</Attributes>
```

4.2 Apache HTTP-palvelin

Alla olevassa esimerkissä Apache-palvelin toimii välityspalvelimena tunnistusta vaativalle sovelluspalvelimelle, jonka välityspalvelin löytää osoitteella applikaatio-palvelin ja sovellus käyttää porttia 8009. ProxyPass-rivit kertovat, että välityspalvelimen tulisi välittää kaikki muut pyynnöt AJP-protokollalla osoitteeseen applikaatio-palvelin:8009, paitsi /Shibboleth.sso-polun alla olevat resurssit. Näitä ei välitetä, sillä ne ovat Shibbolethin omien käsittelijöiden polkuja ja Shibboleth sijaitsee välityspalvelimella, eikä sovelluspalvelimella. Tämän lisäksi palvelimen tulisi toimia käänteisenä välityspalvelimena samaan osoitteeseen. (NativeSPApacheConfig 2017.)

Vahvan tunnistautumisen takana oleva polku sijoitetaan Location-kenttään. Sen sisälle määritellään autentikointityyppi shibboleth. Shibbolethille tehdään asetuspyyntöjä ShibRequestSetting-komennolla. ApplicationId-optiolla määritellään minkä kappaleessa 4.1 kuvatun ApplicationOverriden istuntoasetukset halutaan käyttöön. RequireSession-

optio true arvolla määrittää, että tunnistautumissessio pitää olla olemassa ja validi. ShibUseEnvironment arvolla On määrittää, että käyttäjän tiedot välitetään ympäristömuuttujina. Require valid-user kertoo, että kaikki tunnistetut käyttäjät ovat valtuutettuja. (NativeSPApacheConfig 2017.)

Shibbolethin käyttämät polut pitää reitittää erikseen Location-kentällä ja antaa tälle myös samat asetukset (NativeSPApacheConfig 2017).

```
ProxyPass /Shibboleth.sso !

ProxyPass / ajp://applikaatio-palvelin:8009/
ProxyPassReverse / ajp://applikaatio-palvelin:8009/

<Location /Shibboleth.sso>
    ShibRequestSetting applicationId esimerkki
    SetHandler shib
</Location>

<Location /suojattu_resurssi>
    AuthType shibboleth
    ShibRequestSetting applicationId esimerkki
    ShibRequestSetting requireSession true
    ShibUseEnvironment On
    Require valid-user
</Location>
```

4.3 Tietojen käyttö palvelussa

Välitetyt tiedot näkyvät istunnossa avain-arvo-pareina, joissa avain on kappaleessa 4.1 esitetyn attribuuttikartan id, ja arvo on tunnistuspalvelun lähettämä tieto. Ohjelmallinen tietojen käyttö on riippuvainen käytettävästä ohjelmointikielestä, arkkitehtuurista ja alustoista. Palvelun tulee lopettaa paikallinen selainistunto ennen uloskirjauspyynnön lähettämistä Suomi.fi-tunnistukselle (Tekninen rajapintakuvaus 2018).

5 POHDINTA

Käyttöönotto-ohjeen tarkoituksena oli helpottaa Suomi.fi-tunnistuksen käyttöönottoa vanhoissa ja uusissa projekteissa. Ohjeen teon aikana kerättyä tietoa on jo käytetty hyväksi useissa projekteissa, joissa vahvaa tunnistautumista on tarvittu. Kerättyä tietoa on myös käytetty kehityksen ohjaussapuna projekteissa, joihin vahva tunnistautuminen on tulossa myöhemmin.

Vahvan tunnistuksen käyttöönoton vaatimien dokumenttien lukeminen ja yhteensovittaminen oli aluksi hyvin monimutkaiselta tuntuva tehtävä, mutta kun käyttöönotto oli toteutettu muutamalle projektille, alkoi käyttöönotto selkeytymään. Tunnistuksen käyttöönotto on hyvin suoraviivainen prosessi, kun on selvitetty asiointipalvelun näkökulmasta, miten asiointipalvelu halutaan suojata ja mitä tunnistetusta käyttäjästä halutaan tietää.

Vahvaa tunnistautumista käyttävien projektien on huolehdittava tietoturvasta, sillä tunnistuksen mukana liikkuu henkilön yksilöiviä tietoja. Projektien on pidettävä huolta, että näitä tietoja ei pääse vuotamaan.

Ohjetta tullaan todennäköisesti jatkokehittämään Visman sisällä tarkemmin Visman sisäisiin ratkaisuihin sopivaksi.

LÄHTEET

Suomi.fi-tunnistus. n.d. Luettu 7.5.2018. Kansallisen palveluarkkitehtuurin viestintäkanava. https://esuomi.fi/palveluntarjoajille/tunnistus/

Asiointipalvelun metadatatiedot. 2018. Luettu 7.5.2018. Kansallisen palveluarkkitehtuurin viestintäkanava. https://esuomi.fi/palveluntarjoajille/tunnistus/tekninen-aineisto/asiointipalvelun-metadatatiedot/

Tunnistetusta käyttäjästä välitettävät tiedot. 2017. Luettu 7.5.2018. Kansallisen palveluarkkitehtuurin viestintäkanava. https://esuomi.fi/palveluntarjoajille/tunnistus/tekninen-aineisto/tunnistetusta-kayttajasta-valitettavat-attribuutit/

Tekninen rajapintakuvaus. 2018. Luettu 7.5.2018. Kansallisen palveluarkkitehtuurin viestintäkanava. https://esuomi.fi/palveluntarjoajille/tunnistus/tekninen-aineisto/tekninen-rajapintakuvaus/

NativeSPAssertionConsumerService. Rod Widdowson. 2018. Luettu 7.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAssertionConsumerService

NativeSPSessionInitiator. Scott Cantor. 2016. Luettu 7.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessionInitiator

NativeSPSessions. Scott Cantor. 2017. Luettu 7.5.2018. Shibboleth Consortium https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessions

NativeSPApacheConfig. Scott Cantor. 2017. Luettu 7.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig

NativeSPApplication. Alex Stuar. 2016. Luettu. 11.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplication

NativeSPServiceLogout. Scott Cantor. 2010. Luettu 11.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPServiceLogout

NativeSpHandler. Scott Cantor. 2017. Luettu 11.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPHandler

NativeSPErrors. Scott Cantor. 2016. Luettu 11.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPErrors

NativeSPMetadataProvider. Scott Cantor 2016. Luettu 12.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataProvider

NativeSPAttributeExtractor. Scott Cantor. 2014. Luettu 12.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeExtractor

NativeSPCredentialResolver. Scott Cantor. 2012. Luettu 13.5.2018. Shibboleth Consortium. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPCredentialResolver

Shib-keygen. Russ Allery. 2011. Luettu 13.5.2018. Debian GNU/Linux. http://manpages.ubuntu.com/manpages/bionic/man8/shib-keygen.8.html

LIITTEET

Liite 1. Asiointipalvelun metadata

```
<md:EntityDescriptor
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
    entityID="https://esimerkki.fi/shibboleth">
  <mdattr:EntityAttributes
         xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
    <saml:Attribute
         xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
         Name="FinnishAuthMethod"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml:AttributeValue
           xmlns:xs=”http://www.w3.org/2001/XMLSchema”
           xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
           xsi:type="xs:string">
        http://ftn.ficora.fi/2017/loa3
      </saml:AttributeValue>
    </saml:Attribute>
  </mdattr:EntityAttributes>
  <md:SPSSODescriptor
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
      urn:oasis:names:tc:SAML:1.1:protocol">
    <md:Extensions>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="fi">
          Esimerkki - suomi
        </mdui:DisplayName>
        <mdui:DisplayName xml:lang="sv">
          Esimerkki - ruotsi
        </mdui:DisplayName>
        <mdui:DisplayName xml:lang="en">
          Esimerkki - englanti
        </mdui:DisplayName>
        <mdui:Logo>
          https://esimerkki.fi/site-logo.png
        </mdui:Logo>
        <mdui:Description xml:lang="fi">
          Kuvaus - suomi
        </mdui:Description>
        <mdui:Description xml:lang="sv">
          Kuvaus - ruotsi
        </mdui:Description>
        <mdui:Description xml:lang="en">
          Kuvaus - englanti
        </mdui:Description>
        <mdui:PrivacyStatementURL xml:lang=”fi”>
          Rekisteriselosteen URL – suomi
```

```
    </mdui:PrivacyStatementURL>
    <mdui:PrivacyStatementURL xml:lang=”sv”>
      Rekisteriselosteen URL – ruotsi
    </mdui:PrivacyStatementURL>
    <mdui:PrivacyStatementURL xml:lang=”en”>
      Rekisteriselosteen URL – englanti
    </mdui:PrivacyStatementURL>
  </mdui:UIInfo>
</md:Extensions>
<md:KeyDescriptor>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>/* Julkinen Avain */</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService
    Location=”https://esimerkki.fi/Shibboleth.sso/SLO/POST”
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
<md:NameIDFormat>
  urn:oasis:names:tc:SAML:2.0:nameid-format:transient
</md:NameIDFormat>
<md:AssertionConsumerService
   Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   Location=”https://esimerkki.fi/Shibboleth.sso/SAML2/POST”
   index="1" />
<md:AttributeConsumingService
    index="1"
    isDefault="true">
  <md:ServiceName xml:lang="fi">
    Palvelun nimi - suomi
  </md:ServiceName>
  <md:ServiceName xml:lang="sv">
    Palvelun nimi - ruotsi
  </md:ServiceName>
  <md:ServiceName xml:lang="en">
    Palvelun nimi - englanti
  </md:ServiceName>
  <md:RequestedAttribute
     FriendlyName="givenName"
     Name="urn:oid:2.5.4.42"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
      FriendlyName="sn"
      Name="urn:oid:2.5.4.4"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
      FriendlyName="nationalIdentificationNumber"
      Name="urn:oid:1.2.246.21"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
  <md:RequestedAttribute
      FriendlyName="KotikuntaKuntanumero”
      Name="urn:oid:1.2.246.517.2002.2.18"
```

```
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
        <md:RequestedAttribute
            FriendlyName="KotikuntaKuntaS"
            Name="urn:oid:1.2.246.517.2002.2.19"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
      </md:AttributeConsumingService>
    </md:SPSSODescriptor>
    <md:Organization>
      <md:OrganizationName xml:lang="fi">
        Organisaatio - suomi
      </md:OrganizationName>
      <md:OrganizationName xml:lang="sv">
        Organisaatio - ruotsi
      </md:OrganizationName>
      <md:OrganizationName xml:lang="en">
        Organisaatio - englanti
      </md:OrganizationName>
      <md:OrganizationDisplayName xml:lang="fi">
        Organisaation näyttönimi - suomi
      </md:OrganizationDisplayName>
      <md:OrganizationDisplayName xml:lang="sv">
        Organisaation näyttönimi - ruotsi
      </md:OrganizationDisplayName>
      <md:OrganizationDisplayName xml:lang="en">
        Organisaation näyttönimi - englanti
      </md:OrganizationDisplayName>
      <md:OrganizationURL xml:lang="fi">
        Organisaation URL - suomi
      </md:OrganizationURL>
      <md:OrganizationURL xml:lang="sv">
        Organisaation URL - ruotsi
      </md:OrganizationURL>
      <md:OrganizationURL xml:lang="en">
        Organisaation URL - englanti
      </md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="administrative">
      <md:GivenName>Etunimi</md:GivenName>
      <md:SurName>Sukunimi</md:SurName>
      <md:EmailAddress>mailto:Etunimi.Sukunimi@esimerkki.fi</md:EmailAddress>
    </md:ContactPerson>
    <md:ContactPerson contactType="technical">
      <md:GivenName>Etunimi</md:GivenName>
      <md:SurName>Sukunimi</md:SurName>
      <md:EmailAddress>mailto:Etunimi.Sukunimi@esimerkki.fi</md:EmailAddress>
    </md:ContactPerson>
  </md:EntityDescriptor>
```

Liite 2. Shibbolethin konfiguraatio

```
<ApplicationOverride      id="esimerkki"      entityID=”https://esimerkki.fi/shibboleth”
  signing="true" encryption="false" attributePrefix="AJP_">

  <Sessions  lifetime="7200"  timeout="1920"  checkAddress="false"  cookieProps="https"
   relayState="ss:mem" handlerSSL="true" handlerURL="/Shibboleth.sso">

    <Logout asynchronous="false">SAML2 Local</Logout>

    <SessionInitiator                  type="SAML2"                  Location="/Login"
      isDefault="true"id="Example" entityID="https://testi.apro.tunnistus.fi/idp1">

      <saml2p:AuthnRequest  ID="aaa"  Version="2.0"  IssueInstant="2012-01-01T00:00:00Z"
AssertionConsumerServiceURL=”https://esimerkki.fi/Shibboleth.sso/SAML2/POST”      Desti-
nation=”https://testi.apro.tunnistus.fi/idp/profile/SAML2/Redirect/SSO”
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">

        <saml2:Issuer               xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
          https://esimerkki.fi/shibboleth
        </saml2:Issuer>

        <saml2p:Extensions>
          <vetuma xmlns="urn:vetuma:SAML:2.0:extensions">

            <LG>fi</LG>
          </vetuma>

        </saml2p:Extensions>

        <saml2p:NameIDPolicy                                        AllowCreate="true"
         Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>

      </saml2p:AuthnRequest>

  </SessionInitiator>

    <md:AssertionConsumerService                                  Location="/SAML2/POST"
        index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>

    <md:AssertionConsumerService                        Location="/SAML2/POST-SimpleSign"
      index="2" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"/>

    <md:AssertionConsumerService                               Location="/SAML2/Artifact"
      index="3" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"/>

    <md:AssertionConsumerService                                   Location="/SAML2/ECP"
      index="4" Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"/>

    <md:AssertionConsumerService                                   Location="/SAML/POST"
      index="5" Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"/>

    <md:AssertionConsumerService                                 Location="/SAML/Artifact"
      index="6" Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"/>
```

```
    <Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>

    <Handler type="Status" Location="/Status" acl="127.0.0.1 ::1"/>

    <Handler type="Session" Location="/Session" showAttributeValues="false"/>

    <Handler type="DiscoveryFeed" Location="/DiscoFeed"/>

  </Sessions>

  <Errors supportContact="tuki@esimerkki.fi" redirectErrors="https://esimerkki.fi"/>

  <MetadataProvider
   type="XML"
   uri="https://testi.apro.tunnistus.fi/static/metadata/idp-metadata.xml"
   backingFilePath="/var/cache/shibboleth/idp-metadata.xml" reloadInterval="7200">

  </MetadataProvider>

  <AttributeExtractor type="XML" validate="true" path="esimerkki/attribute-map.xml"/>

  <CredentialResolver type="File" key="esimerkki/sp-key.pem" certificate="esimerkki/sp-
cert.pem"/>

</ApplicationOverride>
```