

haka

Uutta Shibboleth versiota kohti ja vähän muuta

Haka kokoontuminen 15.1.2008

Arto Tuomi, CSC



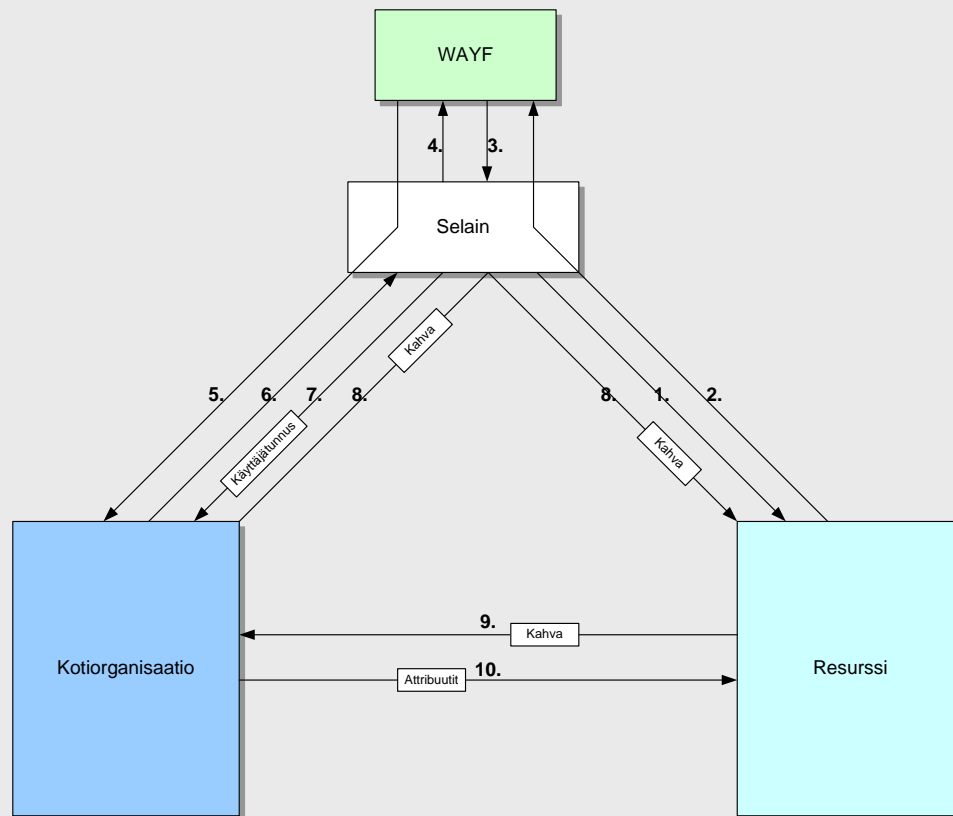
Shibboleth 2.0

- **Service Provider:sta saatavilla ”viimeinen” beta**
 - Valmiin oloinen
- **Identity Provider:sta piti tulla pari viikkoa sitten release candidate**
 - Toistaiseksi ollut vähemmän valmiin oloinen
 - Dokumentoimatta keskeneräisyyden vuoksi

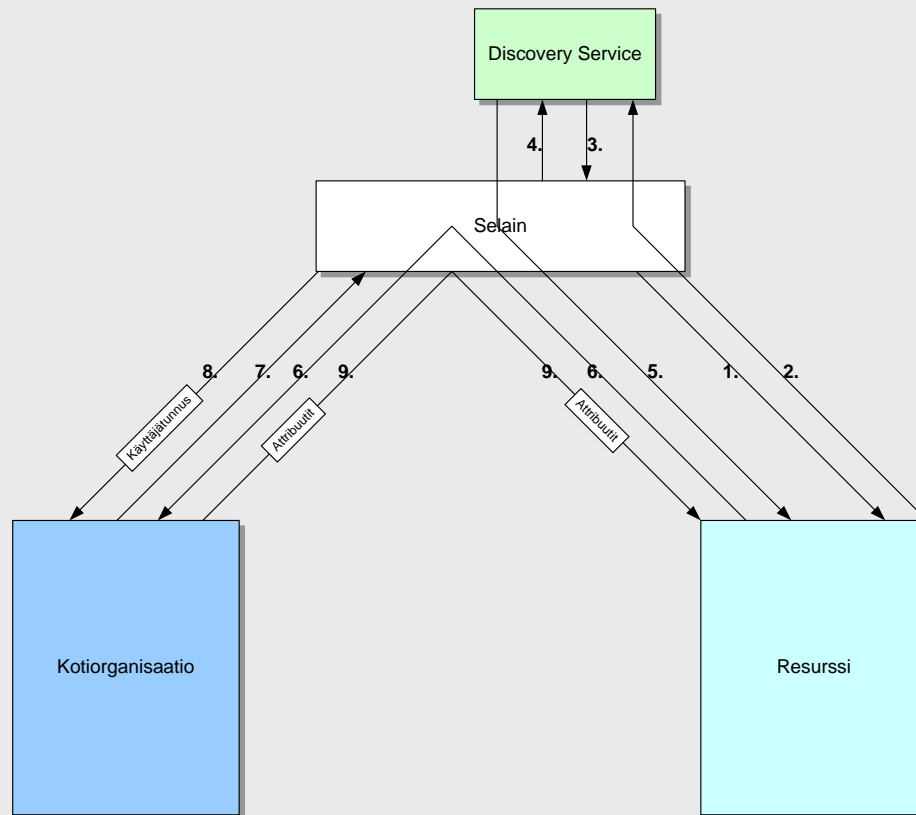
Shibboleth 2.0

- **Yhteensopiva Shibboleth 1.3:n kanssa**
- **Monen protokollan tuki**
 - Shibboleth 1.3
 - SAML 1.1
 - SAML 2
- **Oletusprofiili muuttuu**
 - Attribuutit salataan ja kuljetetaan käyttäjän mukana
 - Vaatii varmenteita metatietoihin
 - IdP ja SP eivät keskustele keskenään
- **Palveluiden osoitteet muuttuvat**
- **Discovery Service**
 - WAYF:n vastine tukien SAML discovery protokollaa

Nykyinen toiminta



Shibboleth 2



Shibboleth 2.0 IdP

- **Oma autentikointijärjestelmä**
 - LDAP, Kerberos, SecureID, IP-osoite
 - Voi käyttää edelleen myös muuta autentikointia
- **Attribuuttisäännöt muuttuvat**
 - Arp-tiedostot poistuvat
 - Attribuuttifiltterit korvaavat
 - Vaikutus Hakan toiminnassa vielä arvioitavana
- **Asetustiedostot muuttuvat**
- **Metadatojen päivittäminen helpottuu**
 - Luetaan verkosta
 - Cachetaan paikallisesti

Shibboleth 2.0 SP

- **Shibboleth 2 muutokset**
- **Attribuuttisäännöt muuttuvat**
- **Asetustiedostot muuttuvat**
- **Metadatojen päivittäminen helpottuu**
 - Luetaan verkosta
 - Cachetaan paikallisesti

Vaikutukset Hakaan

- **Ei rikota olemassaolevia toimintoja**
 - Uudet ominaisuudet vaiheittain käyttöön
 - Shibboleth 1.2 kuitenkin liipasimella
- **Mahdollisuus hyödyntää SAML2 yhteensopivia ohjelmistoja Hakassa**
 - Käytännön yhteensopivuus Shibbolethin kanssa testaamatta
 - Shibboleth 1.3 ei yhteensopiva
- **Uudet ominaisuudet edellyttävät varmenteiden sisällyttämistä metatietoihin**
 - Esitys asiasta myöhemmin

Vaikutukset Hakaan

- **Julkiset Shibboleth 2 testipalvelimet CSC:lle**
 - SP
 - IdP
- **Shibboleth 1.2 tuki lopetetaan**
 - Ei tue varmenteita metadatoissa
 - Aikataulu avoinna
- **Selvitetään WAYF:n toiminta suhteessa uuteen Discovery Service –toimintoon**
 - Hakan käyttämässä WAYF:ssa tuki olemassa
- **Nykyiset Haka-sovellukset päivitettävä 2.0 aikaan**
 - Tietosuojaseloste ym.

Vapaaehtoisia

➤ **SAML2 testaukseen**

- Selvitetään yhteensopivuutta Shibboleth 2.0:n ja kaupallisten sovellusten (Sun Federation Manager, Novell Access Manager ...) kanssa
- Mielellään myös simpleSAMLphp mukaan
<http://rnd.feide.no/simplesamlphp>

➤ **Etuina**

- Mahdollisuus käyttää valitsemaansa ohjelmistoa myös Hakan suuntaan
- Saavuttaa yhteensopivuus muiden SAML2-verkostojen kanssa
- Ei tarvetta ylläpitää Shibbolethia

eduPersonTargetedId

- **Yksilöllinen tunniste käyttäjästä**
 - SP käyttää käyttäjätilien erottelijana
 - Käytännössä siis kuin eduPersonPrincipalName
- **Luodaan IdP:ssä**
 - Tulee säilyä samana käyttäjällä eri kirjautumiskerroilla
- **Ei paljasta käyttäjän henkilöllisyyttä**
 - Ei tarvetta tietosuojaselosteelle
- **Muotoa**
 - `rw3V404ODnd59VeP4X1X1Pcc7kw=@domain.com`
- **Tarvitaan joidenkin tulevien ulkomaisten palveluiden kanssa**

eduPersonTargetedId

➤ Muodostetaan IdP:n resolver-tiedostossa

```
<PersistentIDAttributeDefinition
  id="urn:mace:dir:attribute-def:eduPersonTargetedID"
  scope="domain.com"
  sourceName="schacPersonalUniqueID">
  <DataConnectorDependency requires="directory"/>
  <Salt>joku_aika_pitka_string_88237</Salt>
</PersistentIDAttributeDefinition>
```