

SAML ja Shibboleth

Shibboleth 2 käyttöönotto
16.3.2010

Arto Tuomi

CSC – Tieteen tietotekniikan keskus Oy
CSC – IT Center for Science Ltd.

Security Assertion Markup Language



- OASIS-järjestön standardi
 - <http://www.oasis-open.org>
 - <http://saml.xml.org/>
- Protokollan määrittely nojaa SAML:iin, SOAP:iin ja XML:iin

SAML



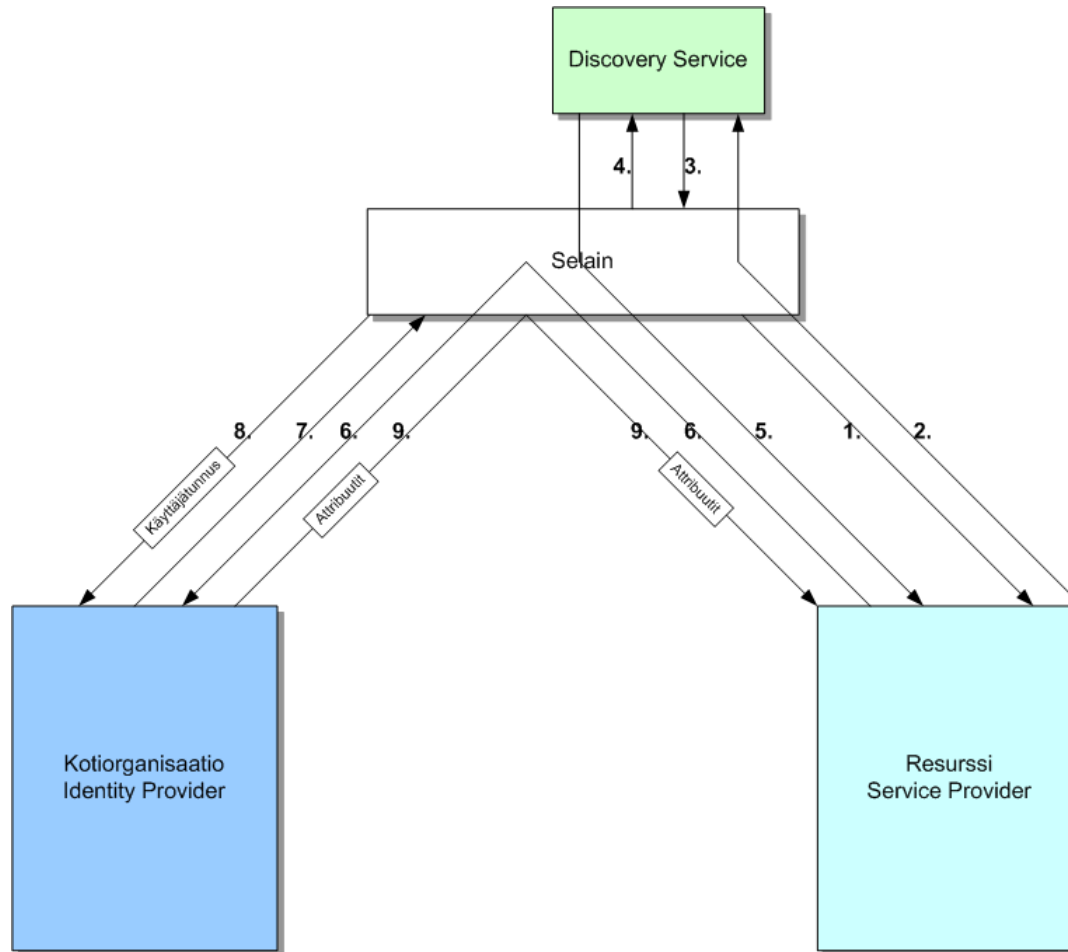
- Sisältää useita käyttötapauksia ja vaihtoehtoisia tapoja niiden suorittamiseen
 - Kurssilla sekä Hakassa että Virtussa käytetään WebSSO

SAML2-protokollan osat



- Assertion and Protocols (Core)
- Bindings
- Profiles
- Metadata
- Authentication Context
- Conformance, Sec. & Priv considerations
- Glossary

SAML-viestinvaihto (WebSSO)



Autentikointipyyntö



- AuthenticationRequest viestillä pyydetään käyttäjätunnistusta

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://industria.csc.fi/Shibboleth.sso/SAML2/POST"
  Destination="https://gravitas.csc.fi/idp/profile/SAML2/Redirect/SSO"
  ID="_7cc487fcea9de661fc7811dea4989a4" IssueInstant="2010-03-15T06:07:00Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    >https://industria.csc.fi/shibboleth</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1"/>
</samlp:AuthnRequest>
```

SAML Responsen osia



- Vastausviesti tunnistuspyyntöön

```
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  Destination="https://industria.csc.fi/Shibboleth.sso/SAML2/POST"
  ID="_fef867d8c13aa2c59e272a1781c8310f" InResponseTo="_dea5c26f437bf54f3765862f15e5f787"
  IssueInstant="2010-03-15T06:18:31.704Z" Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://gravitas.csc.fi/idp/shibboleth</saml2:Issuer>
```

- Tieto tunnistuksen onnistumisesta

```
<saml2p:Status>
  <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</saml2p:Status>
```

SAML Responsen osia



- Tunniste-/liitostietoja

```
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
    _448364114085fb85c4cdb43bd35ebab6
  </saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="193.166.2.228"
      InResponseTo="_dea5c26f437bf54f3765862f15e5f787"
      NotOnOrAfter="2010-03-15T06:23:31.704Z"
      Recipient="https://industria.csc.fi/Shibboleth.sso/SAML2/POST"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
```

- Tunnistustapa

```
<saml2:AuthnContext>
  <saml2:AuthnContextClassRef>http://www.valtiokonttori.fi/vip/virtu/AuthnContext/weak
</saml2:AuthnContextClassRef> </saml2:AuthnContext>
```

SAML Responsen osia



- Sisältää yleensä attribuutteja

```
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="street" Name="urn:oid:2.5.4.9"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue xmlns:xs=http://www.w3.org/2001/XMLSchema
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
      Karvakuonokuja 3
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Viestien turvallisuus

- Viestit varmistetaan XML-allekirjoituksella ja/tai salauksella
- Voidaan välittää https-yhteyden yli

SAML-profiili

- Poimittu SAML-standardeista halutut osa käytettäväksi
- Määrittää mm.
 - Viestien lähetystavat
 - Allekirjoitus-/salausasetukset
 - Attribuuttien esittäminen

SAML-profiili

- Hakassa ja Virtussa käytetään Interoperable SAML 2.0 Profile <http://saml2int.org/>
 - Redirect AuthenticationRequest
 - Browser/POST Response
- Lisäksi luottamusverkkojen omia käytäntöjä

Esimerkki



- Otetaan SAML-viestit lennossa talteen ja tarkistetaan niiden sisältö

Shibboleth



- Open source SAML-ohjelmisto
- Yhdysvaltojen yliopistojen Internet2-hanke
- v 1.0 6/2003, v 1.3 7/2005 (SAML1.1), v. 2.0 03/2008
- Tuotantokäytössä erityisesti yliopistoissa ympäri maailmaa
- Toteuttaa Identity Provider ja Service Provider toiminnot

Shibboleth



- Shibboleth ei tunne konseptia federaatio
 - Se tuntee joukon yksittäisiä palveluita
 - Federaatio muodostuu ihmisten tekemistä päätöksistä kohdella tiettyä joukkoa palveluita tietyllä tavalla
- Shibboleth ei varastoi käyttäjätietoja
 - Shibboleth välittää käyttäjätietoja, mutta Shibbolethilla ei ole kykyä varastoida käyttäjätietoja

Shibboleth



- Shibboleth ei tee käyttäjätunnistusta
 - Shibboleth tarvitsee käyttäjätunnistamista, mutta on muita paljon parempia ohjelmistoja käyttäjätunnistuksen suorittamiseen kuin Shibboleth
- Shibboleth ei varastoi käyttäjätietoja
 - Shibboleth välittää käyttäjätietoja, mutta Shibboleth ei ole ole käyttäjätietovarasto

Plussat ja miinukset

- + Avoin, taipuisa ja muokattava
- + Metadatan hallinnointi erityisesti moni-IdP käyttötapauksessa
- + Kevyt ja luotettava
- + Kehittäjät yhden mailin päässä
- Aloittelijan dokumentaatio
- Vaatii ylläpitäjältä kiinnostusta