

Service Provider

Shibboleth-asennuskoulutus 16-17.3.2010

Timo Mustonen

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

VM:n asentaminen

- Kirjaudu root /password

```
# setupVM
```

- participation number: 2
- keyboard: fi

- Poista reverse dns lookup käytöstä:

```
[root@idp2 ssh]# vi /etc/ssh/sshd_config
```

```
UseDNS no
```

```
[root@idp2 ssh]# service sshd restart
```

- VM Network Adapter → NAT
- Yhteys ssh-clientilla
 - 10.0.2.2 root/password

Shibboleth SP:n asentaminen

- Asennuspaketteja, lähdekoodia ym. saatavilla:

- <https://spaces.internet2.edu/display/SHIB2/Installation>

- Pakettien purkaminen SP VM:ssä

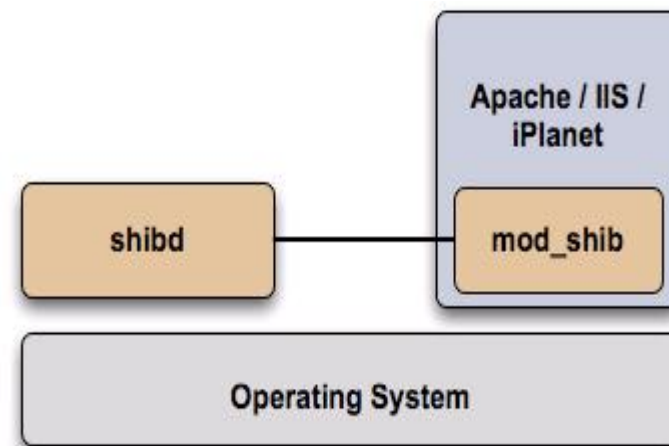
```
[root@idp2 ssh]# rpm -ivh /opt/installfest/distro/RPMS/*.rpm
```

- rpm-pakettien purkamisen jälkeen:

- Shibboleth konfiguraatio: `/etc/shibboleth/`
 - Shibd-prosessi: `/usr/sbin/`
 - Shibboleth logi-tiedostot: `/var/log/shibboleth/`
 - Apache konfiguraatio: `/etc/httpd/conf.d/shib.conf`
 - Apache logit: `/var/log/httpd/`

Osat

- Apache-moduli
 - `/usr/lib/shibboleth/`
 - Ladataan apachen konfiguraatiossa
 - `/etc/httpd/conf.d/shib.conf`
- Konfiguraatitiedostot
- Log-tiedostot
- Sovellukseen liittäminen
 - Pääsynvalvonta
 - Attribuuttien hyödyntäminen



Osat

- Shibd-prosessi
 - Oltava käynnissä SP:n toiminnan aikana, suorittaa www-palvelinmodulin sille luovuttamia tehtäviä
 - VM rpm-asennus luo automaattisesti käynnistys-skriptin
 - Windows asennus luo servicen
 - /usr/sbin/shibd
 - `/etc/init.d/shibd start`
 - `service shibd start|stop|status|restart`
 - Voidaan käyttää `-t` parametrilla konfiguroinnin tarkistamiseen:
 - `shibd -tc /etc/shibboleth/shibboleth2.xml`

Vinkkejä SP:n konfigurointiin

- Värikoodaava editori
- XML-tiedostojen tarkistaminen
 - `xmlwf /etc/shibboleth/shibboleth2.xml`
 - esim. virhe: `shibboleth2.xml:261:2:mismatched tag`
 - `/usr/sbin/shibd -tc /etc/shibboleth/shibboleth2.xml`
- Logien tarkistus
 - `tail -f /var/log/shibboleth/shibd.log`
 - `grep [CRIT|ERROR|WARN] /var/log/shibboleth/shibd.log`
 -

<https://spaces.internet2.edu/display/SHIB2/NativeSPTroubleshootingTactics>

```
[root@idp2 ssh]# vim /etc/shibboleth/shibd.logger
```

```
log4j.rootCategory=DEBUG, shibd_log
```

Shibboleth SP:n konfigurointi

- Pääkonfiguraatio shibboleth2.xml
- <https://spaces.internet2.edu/display/SHIB2/NativeSPShibbolethXML>

```
<OutOfProcess>  
<InProcess>  
<Listener>  
<StorageService>  
<SessionCache>  
<ReplayCache>  
<ArtifactMap>  
<RequestMapper>  
<ApplicationDefaults>  
<SecurityPolicies>  
<TransportOption>
```

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
clockSkew="180000"
```

Shibboleth SP:n konfigurointi

- Shibboleth SP: pääkonfiguraatiossa:
 - Palvelun ympäristö (RequestMapper)
 - Palvelun nimi (entityID)
 - Mistä saadaan metatieto (MetadataProvider)
 - Miten sessioita luodaan (SessionInitiator)
 - Käytettävät varmenteet (CredentialResolver)
 - Tuetut protokollat (AssertionConsumerService)
 - Missä sijaitsevat muut asetustiedostot (AttributeExtractor, AttributeFilter, logger)
 - Poikkeukset oletusasetuksiin (ApplicationOverride)

RequestMapper

- Session aloittaminen ja tiedon suojaaminen
 - Määrittää pyynnöt joihin shibboleth tarttuu
 - Käsi kädessä session luonnin kanssa (SessionInitiator)
- Pyyntöjen yhdistäminen oikeaan sovellukseen
- <https://spaces.internet2.edu/display/SHIB2/NativeSPRequestMapper>

```
<RequestMapper type="Native">  
  <RequestMap applicationId="default">  
    <Host name="palvelimen.nimi.fi"/>  
  </RequestMap>  
</RequestMapper>
```

Tiedon suojaaminen

- 1. Tiedon suojaaminen Apachen säännöillä
 - `/etc/httpd/conf.d/shib.conf`
 - `/var/www/html/secure/.htaccess`
 - <https://spaces.internet2.edu/display/SHIB2/NativeSPApacheConfig>
 - Sääntöesimerkkejä: <http://www.switch.ch/aai/support/serviceproviders/sp-access-rules.html>
- 2. Tiedon suojaaminen RequestMap:ia käyttäen
 - <https://spaces.internet2.edu/display/SHIB2/NativeSPRequestMap>
 - Session vaatimisen myötä vain tunnistetuilla käyttäjillä oikeudet suojattuun aineistoon
- 3. Tiedon suojaaminen sovelluksessa
 - Attribuuttien hyödyntäminen ympäristömuuttujista (PHP, Perl...)

Tiedon suojaaminen

	1.a httpd.conf	1.b .htaccess	2. XML AccessControl	3. Application Access Control
+	<ul style="list-style-type: none"> Easy to configure Can also protect locations or virtual files Regex Support 	<ul style="list-style-type: none"> Dynamic Easy to configure 	<ul style="list-style-type: none"> Platform independent Powerful boolean rules Regex Support Dynamic 	<ul style="list-style-type: none"> Very flexible and powerful with arbitrarily complex rules Regex Support
-	<ul style="list-style-type: none"> Only works for Apache Not dynamic Not very flexible rules 	<ul style="list-style-type: none"> Only works for Apache Only works with "real" files and directories 	<ul style="list-style-type: none"> XML editing Configuration error can prevent SP from restarting 	<ul style="list-style-type: none"> You have to build it yourself You have to maintain it yourself

SP:n entityID

- Tavallisesti palvelun nimen mukaan
- Uniikki, vapaasti valittavissa uniikkiusehdon täyttyessä
- SP:ssä voi olla määritettynä useampi entityID
- Käytetään/näkyvät mm. metadatatassa, attribuuttien filteröinnissä, logeissa, viestinvaihdossa
- <https://spaces.internet2.edu/display/SHIB2/NativeSPApplication>

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
entityID="https://sp2.example.org/shibboleth"  
homeURL="https://sp2.example.org/index.html"
```

Metadata

- XML dokumentti jossa kuvattuna kaikki luottamusverkoston entiteetit (SP:t ja IdP:t)
 - Uniikit tunnisteet (entityID)
 - Palveluosoitteet
 - Varmenteet viestien allekirjoittamiseen ja kryptaukseen
 - tietoja organisaatiosta ja henkilöiden yhteystiedoista
 - SP:n tarvitsemista attribuuteista
- Kertoo SP:lle minkä IdP-palvelinten kanssa voi keskustella ja miten
- Metadata jaetaan hyvin usein HTTP:n yli
 - Oikeellisuus voidaan tarkistaa allekirjoituksen avulla
- Päivittäminen tärkeää
- <https://spaces.internet2.edu/display/SHIB2/Metadata>

MetadataProvider

- Esim. metadata paikallisella levyllä

```
<MetadataProvider type="XML"  
file="/etc/shibboleth/haka_test_metadata_signed_local.xml"/>
```

<https://spaces.internet2.edu/display/SHIB2/NativeSPMetadataProvider>

- Esim. haetaan verkosta, mukana metadatan allekirjoituksen tarkistaminen

```
<MetadataProvider type="XML" uri="https://metadata.url"  
backingFilePath="kopio.xml" reloadInterval="7200">  
  <SignatureMetadataFilter certificate="/etc/shibboleth/org-  
signing-cert.crt"/>  
</MetadataProvider>
```

<https://spaces.internet2.edu/display/SHIB2/NativeSPReloadableXMLFile>

<https://spaces.internet2.edu/display/SHIB2/NativeSPMetadataFilter>

MetadataProvider

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<MetadataProvider type="XML"  
    uri="https://testidp.example.org/testidp-metadata.xml"  
    backingFilePath="/etc/shibboleth/testidp-metadata.xml"  
    reloadInterval="7200">  
</MetadataProvider>
```

SessionInitiator

- SP:n osa joka generoi SSO requestin
- Määrittää mihin ja miten käyttäjä ohjataan hakemaan sessiota IdP:ssä
 - Ohjataan tiettyyn IdP:hen tai WAYF/DS-palveluun
 - Voidaan kutsua myös suoraan selaimen linkillä
 - Mitä entityID:tä käytetään
- <https://spaces.internet2.edu/display/SHIB2/NativeSPSessionInitiator>

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<SessionInitiator type="Chaining" Location="/Login"
    isDefault="true" id="Intranet" relayState="cookie"
    entityID="https://testidp.example.org/idp/shibboleth">
```

Palveluosoitteet

- Kertoo missä SP:n palvelut sijaitsevat
 - Ottaa vastaan SessionInitiator:in aloittaman viestinvaihdon
- Ei yleensä tarvitse koskea
- Tarvitaan metadataan
- <https://spaces.internet2.edu/display/SHIB2/NativeSPAssertionConsumerService>

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

Lisäpalvelut

- SP:n metadatan generointi

- Kätevä testauksessa ja tarkistuksissa

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

Selaimella: <https://sp2.example.org/Shibboleth.sso/Metadata>

- Session tila

- Kätevä testauksessa, voi näyttää myös attribuuttien sisällöt

Selaimella: <https://sp2.example.org/Shibboleth.sso/Session>

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<Handler type="Session" Location="/Session" showAttributeValues="true" />
```

CredentialResolver

- Shibboleth tarvitsee varmenteet
 - IdP-SP -yhteyksien varmistamiseen
 - viestien allekirjoitukseen ja salaamiseen
- Hakassa Sonera tai Comodo CA:n toimittamat varmenteet
- Testauksessa mitä tahansa voi käyttää (luodaan VM asennuksessa)
- <https://spaces.internet2.edu/display/SHIB2/NativeSPCredentialResolver>

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

```
[root@idp2 ssh]# cp /opt/installfest/sps/sp2/sp.key /etc/shibboleth/sp-key.pem
```

```
[root@idp2 ssh]# cp /opt/installfest/sps/sp2/sp.crt /etc/shibboleth/sp-cert.pem
```

Kirjautuminen

```
[root@idp2 shibboleth]# shibd -tc /etc/shibboleth/shibboleth2.xml
```

```
[root@idp2 shibboleth]# service shibd start
```

```
[root@idp2 shibboleth]# service httpd start
```

Selaimella:

- <https://sp2.example.org/>
- <https://sp2.example.org/Shibboleth.sso/Session>
- <https://sp2.example.org/Shibboleth.sso/Metadata>
- <https://sp2.example.org/other-secure/> (ei suojattu)

```
[root@idp2 shibboleth]# tail /etc/httpd/conf.d/shib.conf
```

```
[root@idp2 shibboleth]# tail -f /var/log/shibboleth/shibd.log
```

- <https://sp2.example.org/secure/> (suojattu)
 - TestIdP-tunnus: demouser/password

TestIdP:n tilit

- demouser/password
 - GivenName: Pierre
 - Surname: Mustermann
 - Affiliation: staff
- demostudent/password
 - GivenName: John
 - Surname: Doe
 - Affiliation: student

Attribuutit, attribute-map.xml

- IdP:ltä saadaan attribuutit skeeman mukaisilla nimillä (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)
- Muunnetaan nimiksi(ympäristömuuttujiksi), joita SP:n sovelluksen on helppo käsitellä

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.2" id="nickname"/>
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" id="eppn">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>
```

- <https://spaces.internet2.edu/display/SHIB2/NativeSPAttributeExtractor>
- <https://spaces.internet2.edu/display/SHIB2/NativeSPAttributeDecoder>

Attribuutit, attribute-policy.xml

- säännöt joilla attribuuttien sisältöjä tarkistetaan ennen SP:n sovellukselle luovuttamista
- Oletuksena säännön puuttuessa attribuuttia ei luovuteta

```
<afp:AttributeRule attributeID="*">  
    <afp:PermitValueRule xsi:type="ANY" />  
</afp:AttributeRule>
```

- <https://spaces.internet2.edu/display/SHIB2/NativeSPAttributeFilter>

ApplicationOverride

- oletus konfirugoinnin ylikirjoitus valituille sovelluksille
- **Tavallisesti** asetukset joihin ei <ApplicationOverride> -elementin sisällä kosketa periytyvät <ApplicationDefaults> -elementin sisällön mukaan
- <https://spaces.internet2.edu/display/SHIB2/NativeSPApplicationOverride>

```
<RequestMap applicationId="default">
...
  <Host name="host.example.org" applicationId="app"/>
...
<ApplicationDefaults...>
...
  <ApplicationOverride id="app">
    <MetadataProvider type="XML"
      file="/etc/shibboleth/override_local_metadata.xml"/>
  </ApplicationOverride>
</ApplicationDefaults>
```

Tehtävä 1: Lisää attribuutteja

- Ota seuraavat attribuutit käyttöön SP:ssä:
 - sn (surname)
 - givenName
 - cn (commonName)

```
[root@idp2 ssh]# vim /etc/shibboleth/attribute-map.xml
    <Attribute name="urn:oid:2.5.4.4" id="surname"/>
    <Attribute name="urn:oid:2.5.4.42" id="givenName"/>
    <Attribute name="urn:oid:2.5.4.3" id="commonName"/>
```

Attribuutit Heti käytössä, kirjaudu:

<https://sp2.example.org/secure/> → Session Handler

Tehtävä 2: Lisää suojaa

- Suojaa kansio `/other/secure/` vaatimalla shibboleth sessio `.htaccess:ia` käyttäen

```
[root@idp2 ssh]# vim /var/www/html/other-secure/.htaccess
AuthType shibboleth
require shibboleth
ShibRequireSession On
```

- Kirjaudu:

<https://sp2.example.org/other-secure/>

Tehtävä 3: Lisää tietoturvaa

- Tarkista ladattavan metadatan allekirjoitus SP:ssä testidp:n varmenteella, joka löytyy osoitteesta <https://testidp.example.org/idp-cert.pem>

Noudetaan varmenne lokaalille levyille:

```
[root@idp2 ssh]# cd /etc/shibboleth/
```

```
[root@idp2 ssh]# curl -k -O https://testidp.example.org/idp-cert.pem
```

Otetaan varmenne käyttöön:

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
    <SignatureMetadataFilter certificate="idp-cert.pem"/>
```

Tehtävä 4: DS käyttöön

- Määritä SP käyttämään oletuksena Discovery Serviceä soitteessa <https://ds.example.org/DS/WAYF> (oletuksena tällä hetkellä testidp)

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<!--...specific IdP's SSO service...-->  
    isDefault="false"
```

```
<!-- ...the new-style of discovery service...-->  
    isDefault="true"
```

Tehtävä 5: Filtrointiä

- Lisää sääntö joka luovuttaa givenName -attribuutin vain jos SP:hen kirjaudutaan IdP-palvelimesta jonka entityID on <https://testidp.example.org/idp/shibboleth>

```
[root@idp2 ssh]# vim /etc/shibboleth/attribute-policy.xml

    <afp:AttributeRule attributeID="givenName">
        <afp:PermitValueRule xsi:type="AttributeIssuerString"
            value="https://testidp.example.org/idp/shibboleth"/>
    </afp:AttributeRule>
```

Kokeile putoaako attribuutti pois jos vaihdat sääntöön entityID:ksi vaikka: <https://dummy.somewhere.org/idp/shibboleth>

Tehtävä 6: Shibboleth Lazy Session

- muuta `/var/www/cgi-bin/` -hakemisto siten että hakemistossa oleva testiscripti on kaikkien käytettävissä mutta attribuutit näytetään vain tunnistetuille ja session omaaville käyttäjille (apuja tehtävästä 2)

```
[root@idp2 ssh]# vim /var/www/cgi-bin/.htaccess
AuthType shibboleth
require shibboleth
```

Tehtävä 7: RequestMap

- suojaa /var/www/cgi-bin/ -hakemistoa (ja sen sisällä olevaa scriptiä) RequestMap:n avulla siten että tunnistautuminen ja sessio vaaditaan kaikilta käyttäjiltä.

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<Host name="sp2.example.org">  
  <Path name="cgi-bin" authType="shibboleth"  
    requireSession="true" />  
</Host>
```

Selaimella: <http://sp2.example.org/cgi-bin/attribute-viewer>

HTTP-liikenne nyt mahdollista, uudelleen ohjaa HTTPS:ään (SSL, port 443) RequestMap:n avulla

```
<Host name="sp2.example.org">  
  <Path name="cgi-bin" authType="shibboleth"  
    requireSession="true" redirectToSSL="443" />  
</Host>
```

Tehtävä 8: ApplicationOverride

- Lisää SP:lle toinen entityID `altsp2.example.org` omalle `applicationId`:lle, joka käyttää omaa (non-default) `map`-tiedostoa ja määppää attribuutit `altsp2_`-
prefixillä:

<code>givenName</code>	→	<code>altsp2_givenName</code>
<code>surname</code>	→	<code>altsp2_surnam</code>

```
[root@idp2 ssh]# cp attribute-map.xml altsp2_attribute-map.xml
```

```
[root@idp2 ssh]# vim altsp2_attribute-map.xml
```

```
    <Attribute name="urn:oid:2.5.4.4" id="altsp2_surname"/>
    <Attribute name="urn:oid:2.5.4.42" id="altsp2_givenName"/>
```

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<Host name="altsp2.example.org" applicationId="altsp2"/>
```

```
...
```

```
<ApplicationOverride id="altsp2" entityID="https://altsp2.example.org/shibboleth">
  <AttributeExtractor type="XML" file="altsp2_attribute-map.xml"/>
</ApplicationOverride>
```

Valmistautuminen IdP:n asennukseen

- Ota käyttöön idp1.example.org:n metadata

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<MetadataProvider type="XML" file="/opt/installfest/idps/idp1/idp1-  
  metadata.xml" />
```

- Poista tai kommentoi ulos tehtävässä 5 tehty filteröinti
- Ohjaa tunnistautumaan IdP:lle jonka entityID = <https://idp1.example.org/idp/shibboleth>

```
[root@idp2 ssh]# vim /etc/shibboleth/shibboleth2.xml
```

```
<!--...specific IdP's SSO service...-->  
<SessionInitiator type="Chaining" Location="/Login"  
  isDefault="true" id="Intranet" relayState="cookie"  
  entityID="https://idp1.example.org/idp/shibboleth">  
  
...  
  
<!-- ...the new-style of discovery service...-->  
  isDefault="false"
```

Valmistautuminen IdP:n asennukseen

- Tarkista SP:n konfiguraatio ja käynnistä palvelut uudestaan

```
[root@idp2 ssh]# shibd -tc /etc/shibboleth/shibboleth2.xml
```

```
[root@idp2 ssh]# service httpd restart
```

```
[root@idp2 ssh]# service shibd restart
```