Configuring the SP for interfederation use

A short How-to

SWITCH

Kaspar Brand
aai@switch.ch

Interfederation Crash Course
Berne, 1 March 2013

High-level overview of the procedure

- Assumptions
  - your AAI-enabled resource is running the currently supported release of the Shibboleth Service Provider (as of 2013, this is version 2.5.x)
  - your resource is already registered in the SWITCHaai federation and is properly working for users of that federation
- Required steps
  1. Making the SP aware of additional attributes:
     `attribute-map.xml`
  2. Enabling the retrieval of interfederation metadata:
     `shibboleth2.xml`
  3. Adapting access control rules:
     `httpd.conf`, **`.htaccess`**, **`<RequestMap>/<Host>`** et al.
  4. Adapting the IdP discovery process: → next presentation
  5. Reconfiguring the description in the AAI Resource Registry

Making the SP aware of additional attributes

Either download the current recommended **`attribute-map.xml`** from the SP configuration guide and store it in the configuration directory:
https://www.switch.ch/aai/docs/shibboleth/SWITCH/latest/sp/deployment/download/attribute-map.xml

or manually add the following attributes to the **`attribute-map.xml`** file in the configuration directory, if not yet present:

```
<!-- Display Name -->
<Attribute name="urn:mace:dir:attribute-def:displayName" id="displayName"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.241" id="displayName"/>

<!-- Common Name -->
<Attribute name="urn:mace:dir:attribute-def:cn" id="cn"/>
<Attribute name="urn:oid:2.5.4.3" id="cn"/>

<!-- SCHAC Home Organisation -->
<Attribute name="urn:mace:terena.org:schac:homeOrganization” id="schacHomeOrganization"/>
<Attribute name="urn:oid:1.3.6.1.4.1.25178.1.2.9” id="schacHomeOrganization"/>

<!-- SCHAC Home Organisation Type -->
<Attribute name="urn:mace:terena.org:schac:homeOrganizationType” id="schacHomeOrganizationType"/>
<Attribute name="urn:oid:1.3.6.1.4.1.25178.1.2.10” id="schacHomeOrganizationType"/>
```

Enabling the retrieval of interfederation metadata

Either download a customized shibboleth2.xml file from the SP configuration guide (with the “Configure Service Provider for Interfederation” checkbox ticked):
https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.5/sp/deployment/configuration.html

or manually add the following MetadataProvider element to the shibboleth2.xml file in the configuration directory:

```
<!-- Interfederation Metadata -->
<MetadataProvider type="XML" validate="true"
                  uri="http://metadata.aai.switch.ch/entities/interfederation+idp"
                  backingFilePath="metadata.interfederation-idps.xml"
                  reloadInterval="3600">
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="604800"/>
  <MetadataFilter type="Signature">
    <TrustEngine type="StaticPKIX"
                 certificate="SWITCHaaiRootCA.crt.pem" verifyDepth="2"
                 checkRevocation="fullChain"
                 policyMappingInhibit="true" anyPolicyInhibit="true">
      <TrustedName>SWITCHaai Interfederation Metadata Signer</TrustedName>
      <PolicyOID>2.16.756.1.2.6.8</PolicyOID>
    </TrustEngine>
  </MetadataFilter>
</MetadataProvider>
```

Adapting access control rules

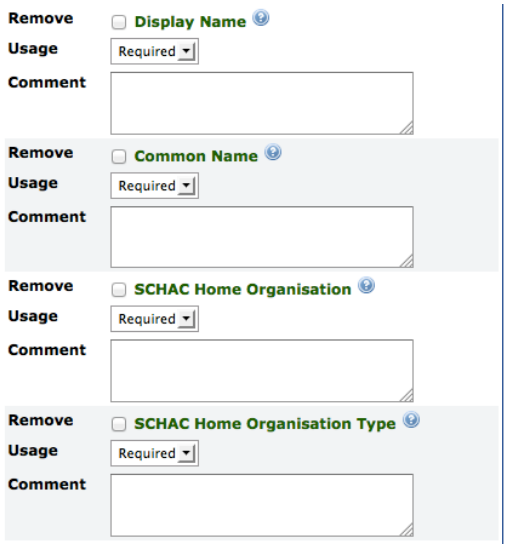
- Access control (authorization) can be configured in multiple ways:
  - for Apache httpd only: either in the global or a **`VirtualHost`** specific configuration file, or in per-directory **`.htaccess`** or XML access rule files
  - in the **`shibboleth2.xml`** file
  - in a separate XML file referenced by **`shibboleth2.xml`**
- If you are interfederation-enabling your SP, verify that you're not inadvertently opening up access to an audience larger than the intended one, i.e.
  - configure attribute requirements for *affiliation* or *homeOrganizationType* etc. accordingly
  - make sure that your existing rules are still specific enough, e.g. when using regular expressions for attribute values

Adapting the IdP discovery process

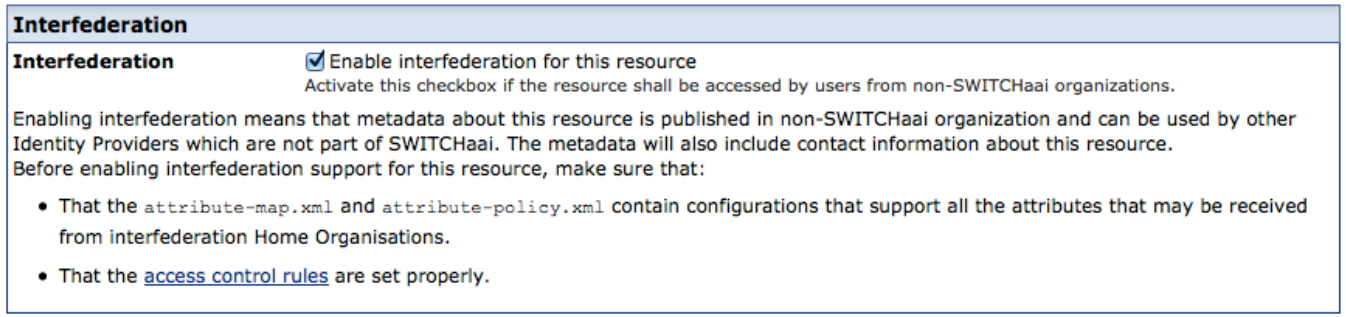
→ next presentation “Discovery Service Options”

Reconfiguring the SP description in the Resource Registry

- under “Required Attributes”, mark the relevant attributes as “Required”:



- under “Intended Audience”, enable the publication of the resource description in interfederation metadata:



Summary

- Required steps
  - making the SP aware of additional attributes
  - enabling the retrieval of interfederation metadata
  - adapting access control rules
  - adapting the IdP discovery process: → next presentation
  - reconfiguring the description in the AAI Resource Registry

- Further reading: step-by-step guide at https://www.switch.ch/aai/docs/interfederation/sp-deployment.html