Configuring the IdP for interfederation use

A short How-to

Daniel Lutz
aai@switch.ch

Interfederation Crash Course
Bern, 1. March 2013

High-level overview of the procedure (1)

Assumptions:

- Your IdP is running the currently supported release of the Shibboleth Identity Provider (as of February 2013, this is version 2.3.8)
- Your IdP is already registered in the SWITCHaai federation and is properly working for SWITCHaai users
- The SWITCHaai Interfederation Access Declaration has been signed by the organization

High-level overview of the procedure (2)

Required steps:

1. Enable user consent (module uApprove) on the Identity Provider
2. Adapt Identity Provider configuration
   - Load the interfederation metadata
   - Release all the attributes recommended for interfederation support
3. Adapt entry in Resource Registry
   - Enable Interfederation for the Home Organization
   - Enable the additional attributes
4. Pass Interfederation Test

Enable user consent: Install uApprove (1)

- Install uApprove following the installation instructions: http://www.switch.ch/aai/downloads/uApprove-manual/

- In case you haven't yet used uApprove:
  Optionally disable uApprove for some SWITCHaai Service Providers in the file `uApprove.properties` (e.g. Service Providers of your own organization)

Enable user consent: Install uApprove (2)

Disabling uApprove for some Service Providers by blacklisting them in the uApprove configuration (`uApprove.properties`):

- Disabling uApprove for your own organization's services only:

```
services = ^https://[^/]+\.example\.org/.*$ \
           ^https://[^/]+\.example\.edu/.*$
[...]
services.blacklist = true
```

- Disabling uApprove for all services in ".ch" domain:
  (Warning: might also match non-Swiss Service Providers that use a ".ch" domain)

```
services = ^https://[^/]+\.ch/.*$
[...]
services.blacklist = true
```

Add additional Attribute Definitions

- 6 additional attributes required for interfederation
- Values of these attributes are based on already existing information; no changes in user directory required
- Additional attributes:
  - Display Name
  - Common Name
  - Principal Name
  - SCHAC Home Organisation
  - SCHAC Home Organisation Type
  - Scoped Affiliation
- Add these attributes to `attribute-resolver.xml`
- Furthermore, you should make sure that the attribute "Affiliation" contains the value "member" for the affiliations "student", "staff" and "faculty".

Attributes: Example Values

Display Name: Peter Jones

Common Name: Peter Jones

Principal Name: 256973496@example.org

SCHAC Home Organisation: example.org

SCHAC Home Organisation Type:
urn:schac:homeOrganizationType:int:university
urn:schac:homeOrganizationType:ch:university

Scoped Affiliation:
student@example.org
member@example.org

Attributes: Example Configuration: Display Name

Case 1: Attribute is available in your LDAP directory
Use the value from the LDAP directory

```
<!-- Display Name (displayName) -->
<!-- Attribute displayName is contained in your LDAP directory:
     use the value from the LDAP directory-->
<resolver:AttributeDefinition id="displayName" xsi:type="ad:Simple"
    sourceAttributeID="displayName">

    <resolver:Dependency ref="myLDAP" />

    <resolver:DisplayName xml:lang="en">Display Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
          The name that should appear in white-pages-like applications for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:displayName" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.16.840.1.113730.3.1.241" friendlyName="displayName" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Display Name

Case 2: Attribute is not available in your LDAP directory
Compose the value with JavaScript

```
<!-- Attribute displayName is not contained in your LDAP directory:
     compose the value with JavaScript -->
<resolver:AttributeDefinition id="displayName" xsi:type="ad:Script">
    <resolver:Dependency ref="givenName" />
    <resolver:Dependency ref="surname" />

    <resolver:DisplayName xml:lang="en">Display Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        The name that should appear in white-pages-like applications for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:displayName" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.16.840.1.113730.3.1.241" friendlyName="displayName" />
```

(continued on next page)

Attributes: Example Configuration: Display Name

(continued from previous page)

```
    <ad:Script>
      <![CDATA[

         importPackage(Packages.edu.internet2.middleware.shibboleth.common
                .attribute.provider);

        // Initialize displayName
        displayName = new BasicAttribute("displayName");

        // compose value from givenName and surname
        displayName.getValues().add( givenName.getValues().get(0) + " " +
                surname.getValues().get(0) );
      ]]>
    </ad:Script>
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Common Name

Case 1: Attribute is available in your LDAP directory
Use the value from the LDAP directory

```
<!-- Common Name (commonName) -->
<!-- Attribute commonName is contained in your LDAP directory:
     use the value from the LDAP directory -->
<resolver:AttributeDefinition id="commonName" xsi:type="ad:Simple" sourceAttributeID="cn">
    <resolver:Dependency ref="myLDAP" />

    <resolver:DisplayName xml:lang="en">Common Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        One or more names that should appear in white-pages-like applications
        for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:cn" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.5.4.3" friendlyName="cn" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Common Name

Case 2: Attribute is not available in your LDAP directory
Use the same value as of displayName

```
<!-- Common Name (commonName) -->
<!-- Attribute commonName is not contained in your LDAP directory:
     Use the value of the attribute displayName -->
<resolver:AttributeDefinition id="commonName" xsi:type="ad:Simple"
     sourceAttributeID="displayName">

    <resolver:Dependency ref="displayName" />

    <resolver:DisplayName xml:lang="en">Common Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        One or more names that should appear in white-pages-like applications
        for this person.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:cn" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:2.5.4.3" friendlyName="cn" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Principal name

Use the same value as of swissEduPersonUniqueID

```
<!-- Principal name (eduPersonPrincipalName) -->
<!-- Use the same value as the attribute swissEduPersonUniqueID -->
<resolver:AttributeDefinition id="eduPersonPrincipalName" xsi:type="ad:Simple"
    sourceAttributeID="swissEduPersonUniqueID">

    <resolver:Dependency ref="swissEduPersonUniqueID" />

    <resolver:DisplayName xml:lang="en">Principal Name</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        A unique identifier for a person, mainly for inter-institutional
        user identification.
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:dir:attribute-def:eduPersonPrincipalName" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        friendlyName="eduPersonPrincipalName" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: SCHAC Home Organisation

Use static attributes

```
<!-- SCHAC Home Organisation (schacHomeOrganization) -->
<resolver:AttributeDefinition id="schacHomeOrganization" xsi:type="ad:Simple"
    sourceAttributeID="schacHomeOrganization">

    <resolver:Dependency ref="staticAttributes" />

    <resolver:DisplayName xml:lang="en">Home organization</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        Home Organization: Domain name of a Home Organization
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:terena.org:schac:schacHomeOrganization" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.25178.1.2.9"
        friendlyName="schacHomeOrganization" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: SCHAC Home Organisation Type

Use static attributes

```
<!-- SCHAC Home Organisation Type (schacHomeOrganizationType) -->
<resolver:AttributeDefinition id="schacHomeOrganizationType" xsi:type="ad:Simple"
    sourceAttributeID="schacHomeOrganizationType">

    <resolver:Dependency ref="staticAttributes" />

    <resolver:DisplayName xml:lang="en">Home organization type</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        Home Organization Type: Type of a Home Organization
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1String"
        name="urn:mace:terena.org:schac:schacHomeOrganizationType" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2String"
        name="urn:oid:1.3.6.1.4.1.25178.1.2.10"
        friendlyName="schacHomeOrganizationType" />
</resolver:AttributeDefinition>
```

Attributes: Example Configuration: Static Attributes

Static attributes

```
<!-- Static Connector -->
<resolver:DataConnector id="staticAttributes" xsi:type="dc:Static">
    <dc:Attribute id="swissEduPersonHomeOrganization">
        <dc:Value>example.org</dc:Value>
    </dc:Attribute>
    <dc:Attribute id="schacHomeOrganization">
        <dc:Value>example.org</dc:Value>
    </dc:Attribute>
    <dc:Attribute id="swissEduPersonHomeOrganizationType">
        <dc:Value>university</dc:Value>
    </dc:Attribute>
    <dc:Attribute id="schacHomeOrganizationType">
        <dc:Value>urn:schac:homeOrganizationType:int:university</dc:Value>
        <dc:Value>urn:schac:homeOrganizationType:ch:university</dc:Value>
    </dc:Attribute>
</resolver:DataConnector>
```

Attributes: Example Configuration: Scoped affiliation

Use value of eduPersonAffiliation with scope

```
<!-- Scoped affiliation (eduPersonScopedAffiliation) -->
<resolver:AttributeDefinition id="eduPersonScopedAffiliation" xsi:type="ad:Scoped"
    scope="example.org" sourceAttributeID="eduPersonAffiliation">

    <resolver:Dependency ref="eduPersonAffiliation" />

    <resolver:DisplayName xml:lang="en">Affiliation</resolver:DisplayName>
    <resolver:DisplayDescription xml:lang="en">
        Affiliation: Type of affiliation with Home Organization
    </resolver:DisplayDescription>

    <resolver:AttributeEncoder xsi:type="enc:SAML1ScopedString"
        name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation" />
    <resolver:AttributeEncoder xsi:type="enc:SAML2ScopedString"
        name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
        friendlyName="eduPersonScopedAffiliation" />
</resolver:AttributeDefinition>
```

Load the interfederation metadata (1)

- Change the metadata configuration in the file `relying-party.xml`:
  - Look for the existing **`MetadataProvider`** element which loads the SWITCHaai metadata and insert **just after** it the following snippet:

```
<metadata:MetadataProvider id="InterfederationURLMD"
    xsi:type="metadata:FileBackedHTTPMetadataProvider"
    metadataURL="http://metadata.aai.switch.ch/entities/interfederation+sp"
    backingFile="/opt/shibboleth-idp/metadata/metadata.interfederation-sps.xml"
    requireValidMetadata="true" maxRefreshDelay="PT1H">
    <metadata:MetadataFilter xsi:type="metadata:ChainingFilter">
        <metadata:MetadataFilter xsi:type="metadata:RequiredValidUntil"
            maxValidityInterval="P7D"/>
        <metadata:MetadataFilter xsi:type="metadata:SignatureValidation"
            trustEngineRef="shibboleth.InterfederationMetadataTrustEngine"
            requireSignedMetadata="true"/>
    </metadata:MetadataFilter>
</metadata:MetadataProvider>
```

Load the interfederation metadata (2)

- Make sure that the added `MetadataProvider` element inserted above is added within a **`MetadataProvider`** element of type="ChainingMetadataProvider". Otherwise the Identity Provider won't be able to start.
- Look for the **`TrustEngine`** element with **id="shibboleth.MetadataTrustEngine"**, which defines the metadata signature validation. Insert just after another trust engine with in form of the following configuration snippet:

```
<security:TrustEngine id="shibboleth.InterfederationMetadataTrustEngine"
    xsi:type="security:StaticPKIXSignature">
    <security:TrustedName>
        SWITCHaai Interfederation Metadata Signer
    </security:TrustedName>
    <security:ValidationInfo id="SWITCHaaiFederationCredentials"
        xsi:type="security:PKIXFilesystem" verifyDepth="2">
        <security:Certificate>
            /opt/shibboleth-idp/credentials/SWITCHaaiRootCA.crt.pem
        </security:Certificate>
    </security:ValidationInfo>
    <security:ValidationOptions xsi:type="security:CertPathValidationOptionsType"
        forceRevocationEnabled="true"/>
</security:TrustEngine>
```

Restart the Identity Provider

- Check that XML files are still well-formed:

```
# xmlwf attribute-resolver.xml
# xmlwf relying-party.xml
```

- Restart Identity Provider (e. g. Tomcat Java Container)

```
# /etc/init.d/tomcat6 restart
```

- Check for errors:

```
# tail -f /opt/shibboleth-idp/logs/idp-process.log
```

Test the configuration

You may want to test whether all still works by accessing the AAI Viewer:

https://av.aai.switch.ch/aai

Note: You can't yet see the newly configured attributes because they are not yet released.

Changes in Resource Registry

Changes to do:

1. Activate interfederation support for this Identity Provider (i.e. Home Organization)
2. Add the attributes configured above as supported attributes
3. Adapt the default attribute release policy for interfederation

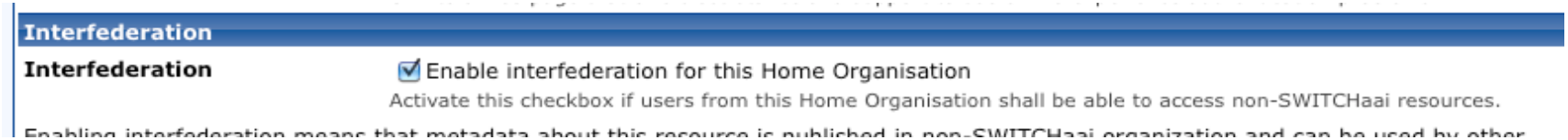
Access to Resource Registry: https://rr.aai.switch.ch

1. Click on the tab "Home Organizations"
2. Click on the link "Edit Home Organization Description" of your Home Organization

Activate Interfederation

- Click on "1. General Information"

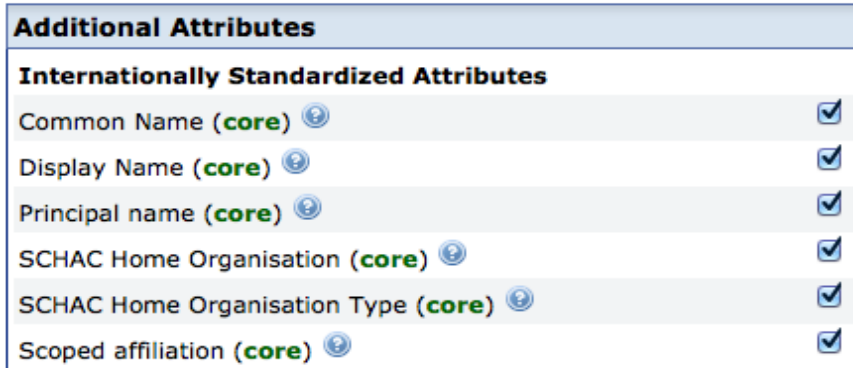
- Enable interfederation for this Home Organisation



Add additional supported attributes

- Click on "6. Supported Attributes"

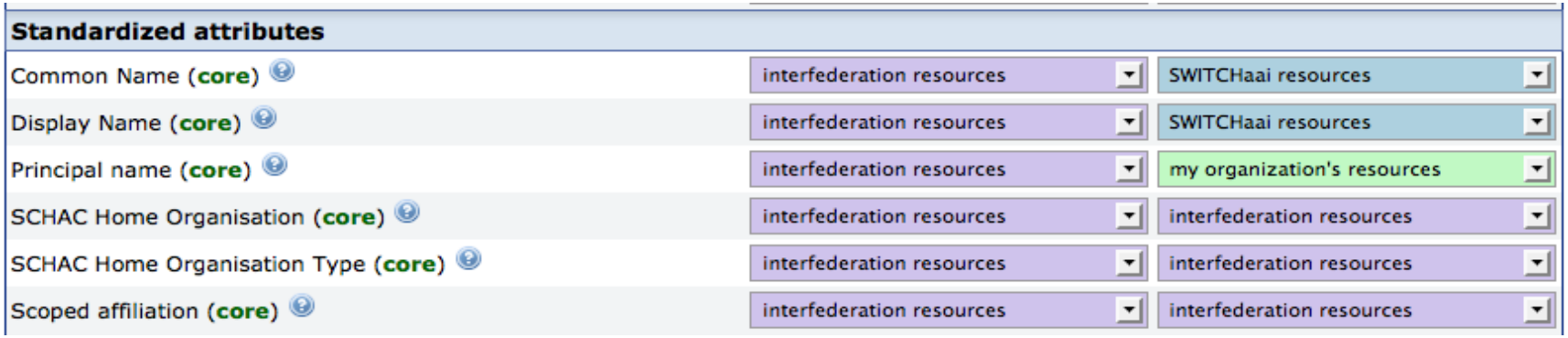
- Enable the new attributes previously added to the IdP's Attribute Resolver configuration



Adapt Attribute Release Policy (1)

- Click on "7. Default Attribute Policy Rules"

- Release the new attributes as required

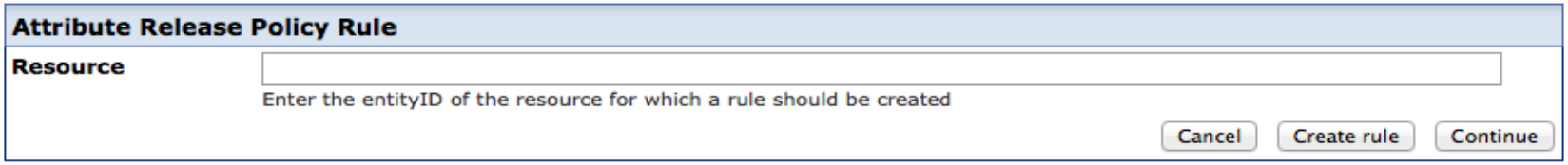


Note: All changes applied to the default Attribute Release Policy only will become active when the Identity Provider downloads the attribute-filter.xml the next time from the Resource Registry.

Adapt Attribute Release Policy (2)

- Set specific attribute release policy
  (allows to override the default attribute policy in order to release fewer or more attributes to very specific resources)

  Click on "8. Specific Attribute Policy Rules"



Note: All changes applied to the specific Attribute Release Policy only will become active when the Identity Provider downloads the attribute-filter.xml the next time from the Resource Registry.

Pass Interfederation Test

- Perform the Interfederation Attribute Test

  https://av.aai.switch.ch/interfederation-test/

- You should see all attributes required for interfederation:

Attributes	Values
principalName	532669@switch.ch
mail	daniel.lutz@switch.ch
cn	Daniel Lutz
displayName	Daniel Lutz
affiliation	member staff
scoped-affiliation	staff@switch.ch member@switch.ch
schacHomeOrganization	switch.ch
schacHomeOrganizationType	urn:schac:homeOrganizationType:ch:others urn:schac:homeOrganizationType:int:nren
persistent-id	https://aai-logon.switch.ch/idp/shibboleth! https://aai-viewer.switch.ch/interfederation-test/shibboleth! ghcXgnR3DLw+tYai5pGyaApMsV8=

Success: 

Failure: 

Links

- Further reading
  - Step-by-step guide to enable interfederation support for a Shibboleth Identity Provider in SWITCHaai:

    https://www.switch.ch/aai/docs/interfederation/idp-deployment.html

  - Add the remaining six international attributes:

    https://aai-viewer.switch.ch/aai/redirect-to-attribute-guide.php