IDP Attribute Profile and Recommended Attributes

How to test if an Identity Provider is supporting the eduGAIN Attribute Profile

1. Which are the Recommended Attributes?
2. Configure the Shibboleth IdP to release the Recommended Attributes to an example Service Provider.
3. Test the release of the recommended attributes to the example Service Provider.

Recommended Attributes in eduGAIN

The following set of attributes is recommended to implement for all eduGAIN Identity Providers as it contains the most commonly used attributes:

Attribute	Description
eduPersonTargetedID /persistentID	Unique, persistent, opaque and targeted identifier of the user. *(Serialized) Example: https://aai-logon.switch.ch/idp/shibboleth!https://filesender.funet.fi!yrVdvdAmohZY+cE6dcGvqu/Dubc=*
eduPersonPrincipalName	Unique, persistent identifier of the user. *Example: jdoe@example.org*
displayName	Name and Surname of the user. *Example: John Doe*
commonName	Name and Surname of the user. Could be multi-valued but it is recommended to have only one value. *Example: Johne Doe*
mail	User's personal eMail address. *Example: john.doe@example.org*
eduPersonAffiliation	See the Controlled Vocabolaries. Multi-valued. *Example: student;member or staff;member*
eduPersonScopedAffiliation	See the Controlled Vocabolaries. Multi-valued. *Example: staff@example.org;member@example.org*
schacHomeOrganization	*Example: example.org*
schacHomeOrganizationType	See the Controlled Vocabolaries. *Example: urn:schac:homeOrganizationType:int:university* **This attribute is unfortunately underspecified. Therefore, this attribute is of little use as of 2015.**

How to configure the Recommended Attributes

The following paragraph describes how to support the recommended attributes listed above and how to create an attribute release rule to release the set of recommended attributes to a particular Service Provider. Please note that not all recommended attributes have to be release in general but only the ones that are required by the Service Provider.

Configure the Attribute Resolver of a Shibboleth IdP

How the attribute resolver can be configured to generate the above attributes without having to change or modify the user directory, is for example, described in **this guide** provided by SWITCH on section called "**2. Configure Attribute Resolver**". Probably, most values can be generated on existing values that are already in a typical user directory (e.g. displayName can be generated dynamically from an existing given name and surname).

Configure the Attribute Filter of a Shibboleth IdP

To release the recommended attributes to a particular Service Provider with a Shibboleth Identity Provider, edit the file "**/opt/shibboleth-idp/conf/attribute-filter.xml**". The add the following code before the "</AttributeFilterPolicyGroup>" tag and change the entityID (https://sp.example.org/shibboleth) to the entityID of an actual Service Provider:

```
<!-- Example SP -->
<AttributeFilterPolicy id="Example-SP">
    <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
    value="https://sp.example.org/shibboleth" />

    <afp:AttributeRule attributeID="displayName"><afp:PermitValueRule xsi:type="basic:ANY"/></afp:AttributeRule>
    <afp:AttributeRule attributeID="commonName"><afp:PermitValueRule xsi:type="basic:ANY"/></afp:AttributeRule>
    <afp:AttributeRule attributeID="email"><afp:PermitValueRule xsi:type="basic:ANY"/></afp:AttributeRule>
    <afp:AttributeRule attributeID="eduPersonPrincipalName"><afp:PermitValueRule xsi:type="basic:ANY"/></afp:
AttributeRule>
    <afp:AttributeRule attributeID="eduPersonAffiliation"><afp:PermitValueRule xsi:type="basic:ANY"/></afp:
AttributeRule>
    <afp:AttributeRule attributeID="eduPersonScopedAffiliation"><afp:PermitValueRule xsi:type="basic:ANY"/><
/afp:AttributeRule>
    <afp:AttributeRule attributeID="schacHomeOrganization"><afp:PermitValueRule xsi:type="basic:ANY"/></afp:
AttributeRule>
    <afp:AttributeRule attributeID="schacHomeOrganizationType"><afp:PermitValueRule xsi:type="basic:ANY"/></afp:
AttributeRule>
 </AttributeFilterPolicy>
```

Instead of manually configuring attribute release rules, you may also consider implementing the Data Protection Code of Conduct that helps to automatically release attributes to a particular Service Provider that signed the Code of Conduct.

How to test the release of the recommended attributes to the Example Service Provider

The Shibboleth Identity Provider comes with a script called AACLI that allows to test the release of attributes:
If you have installed the Shibboleth IdP into its default path, you can execute the command

```
/opt/shibboleth-idp/bin/aacli.sh \
  --principal=##USERID-on-LDAP## \
  --configDir=/opt/shibboleth-idp/conf \
  --requester=https://sp.example.com/shibboleth-sp
```

The script then should return a SAML assertion that would be released to the Example SP. This assertion then should look like below:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   <saml2:Attribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" 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">user@example.com</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="eduPersonAffiliation" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" 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">member</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="eduPersonScopedAffiliation" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
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">member@example.com</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="schacHomeOrganization" Name="urn:oid:1.3.6.1.4.1.25178.1.2.9" 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">example.com</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="cn" Name="urn:oid:2.5.4.3" 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">Test User</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="schacHomeOrganizationType" Name="urn:oid:1.3.6.1.4.1.25178.1.2.10"
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">urn:schac:homeOrganizationType:int:example</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="eduPersonTargetedID" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" NameFormat="urn:
oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml2:AttributeValue>
         <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="https://idp.
example.com/idp/shibboleth" SPNameQualifier="https://sp.example.com/shibboleth">60e669c7-bf1d-4be6-b1cd-
33e54099ed85</saml2:NameID>
      </saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" 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">test.user@example.com</saml2:AttributeValue>
   </saml2:Attribute>
   <saml2:Attribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" 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">Test User</saml2:AttributeValue>
   </saml2:Attribute>
</saml2:AttributeStatement>
```