How to choose the attributes to request and how to get them

Attributes

This page contains information about the SAML attributes that an eduGAIN-enabled service can use. The attributes below only cover those attributes that are recommended to implement for Identity Providers in eduGAIN Attribute Profile. However, additional attributes (e.g. givenName and surname) also can be used if both, Service Provider and Identity Provider, agree on what is being requested and released.

What user attributes can eduGAIN services use?

There are no strict requirements which attributes must be availble for a user accessing an eduGAIN service. The eduGAIN Attribute Profile however recommends that the following attributes are available for all users:

- Email (e.g. "john.doe@example.org")
- Display/Common name (e.g. "John Doe")
- Affiliation (e.g. "staff", "student")
- Scoped affiliation (e.g. "staff@example.org", "student@test.org")
- Principal name (e.g. "jdoe@example.org")
- Persistent/Targeted Identifier (e.g. "uN/7ycVJ9gGKP17HWgZnXPZKlXs=")
- SCHAC home organisation (e.g. "example.org")
- SCHAC home organisation type (e.g. "urn:schac:homeOrganizationType:ch:others")

More Information on the recommended attributes in the eduGAIN Attribute Profile specification.

A service using Shibboleth could use the above attributes by adding the following XML snippet to the attribute-map.xml file where all attributes are defined that the Service Provider can process:

```
<!-- OID-style name of the eduPersonTargetedID/persistentId attribute -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" id="persistent-id">
    <AttributeDecoder xsi:type="NameIDAttributeDecoder"
                          formatter="$NameQualifier!$SPNameQualifier!$Name"
                          defaultQualifiers="true"/>
</Attribute>

<!-- The SAML 2.0 NameID Format of the eduPersonTargetedID/persistentId attribute -->
<Attribute name="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" id="persistent-id">
    <AttributeDecoder xsi:type="NameIDAttributeDecoder"
                          formatter="$NameQualifier!$SPNameQualifier!$Name"
                          defaultQualifiers="true"/>
</Attribute>

<!-- Affiliation -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" id="unscoped-affiliation"/>

<!-- Scoped Affiliation -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" id="scoped-affiliation">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>

<!-- E-mail address -->
<Attribute name="urn:oid:0.9.2342.19200300.100.1.3" id="mail"/>

<!-- Display Name -->
<Attribute name="urn:oid:2.16.840.1.113730.3.1.241" id="displayName"/>

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

<!-- SCHAC Home Organisation -->
<Attribute name="urn:oid:1.3.6.1.4.1.25178.1.2.9" id="schacHomeOrganization"/>

<!-- SCHAC Home Organisation Type -->
<Attribute name="urn:oid:1.3.6.1.4.1.25178.1.2.10" id="schacHomeOrganizationType"/>

<!-- Principal name -->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" id="principalName">
     <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>
```

What about Data Privacy?

Most services won't require all those attributes listed above but only a subset of them. They will receive at maximum those attributes that they request. For services it is recommended to request only those attributes that are required for the service to operate. It is also recommended that all eduGAIN services support the GÉANT Data Protection Code of Conduct, a declaration stating that the operator of a service commits to the listed data protection principles. More Information in the GÉANT Data Protection Code of Conduct or on the Code of Conduct Cookbook page.

What attributes are effectively available for eduGAIN users?

An Identity Provider participating in eduGAIN should be able to provide for each of its users the attributes in the above-mentioned list. However, each eduGAIN-enabled organisation can decide for itself which attributes they release for their users who want to access eduGAIN services. It is however recommended to release those attributes in the list above that are requested by services that support the Code of Conduct. Also, like described below, there are some additional attributes that are available for "free" to web applications. These include standard attributes that are available by default to a service as well as attributes that are (upon configuration) made available to a service by extracting them from the SAML2 metadata about an Identity Provider.

What attributes to uniquely identify users? Generally, it is recommended to use the Persistent/Targeted Identifier attribute (eduPersonTargetedID attribute or persistentId NameIdentifier, urn:oid:1.3.6.1.4.1.5923.1.1.1.10) to identify users. Another attribute that could be used to uniquely identify users is the Principal name (eduPersonPrincipalName, urn:oid:1.3.6.1.4.1.5923.1.1.1.6). This attribute is widely implemented but has some disadvantages from a data protection point of view and some organisations are hesitant to release it. The same goes for the email address (urn:oid:0.9.2342.19200300.100.1.3), which also has the disadvantage that it is more likely to change and that it is not ensured that it is unique (one user can have multiple accounts at different Identity Providers with the same email address).

Are there more attributes a service can use?

Yes, every Service Provider requires metadata about the Identity Provider it accepts users from. The metadata contains information that can also be used in form of attributes by Service Provider. The best part of this is, that these "metadata" attributes are almost for free, which means that they don't have to be released by the Identity Provider. Instead, they just have to be read from the SAML metadata. Of course, the data in metadata is fairly generic and the same for all users for that Identity Provider, but still it contains valuable information that could be used by a service.

The Shibboleth Service Provider 2.5 or newer can extract some of these "metadata" attributes directly from the SAML2 metadata. The data that then is available about an Identity Provider typically includes organisation name, organisation URL, organisation logos and (support/technical) contact information. If available for an organisation, this information can be extracted and provided to the web application as attributes.

An example of the attributes that can be made available to a web application by a Shibboleth Service Provider is shown below. The gray attribute names are the default names Shibboleth uses. The red attributes names can be freely configured using the instructions below.

Shib-Metadata-HomeOrg-DisplayName	SWITCH
Shib-Metadata-HomeOrg-ErrorURL	http://www.switch.ch/aai/contact/
Shib-Metadata-HomeOrg-InformationURL	http://www.switch.ch/about/
Shib-Metadata-HomeOrg-Large-Logo	SWITCH
Shib-Metadata-HomeOrg-OrganizationURL	http://www.switch.ch/
Shib-Metadata-HomeOrg-Small-Logo	
Shib-Metadata-HomeOrg-Support-Contact	SWITCHaai Team
Shib-Application-ID	default
Shib-Assertion-01	https://localhost/Shibboleth.sso//GetAssertion?key=_4b0b093f1b70895d495cca702e3392ba&ID=_a60894b8335c55762aa754c8ba8550ef
Shib-Assertion-02	https://localhost/Shibboleth.sso//GetAssertion?key=_4b0b093f1b70895d495cca702e3392ba&ID=_7ebfb5e8677e2dd53cd7bae4edcaea8e
Shib-Assertion-Count	02
Shib-Authentication-Instant	2014-05-15T06:14:38.947Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
Shib-Identity-Provider	https://aai-logon.switch.ch/idp/shibboleth
Shib-Session-ID	_4b0b093f1b70895d495cca702e3392ba
Shib-Session-Index	_4255f97d6f947e0d637c40f136bf0ec4

To make a Shibboleth SP 2.5 (or newer) expose attributes read from metadata, please consult the Shibboleth Wiki on the Attribute Extractor features. To make the attributes available to a web application like in the above screenshot, the shibboleth2.xml file would have to include the following metadata extractor

```
<AttributeExtractor type="Chaining">
  <AttributeExtractor type="XML"
            validate="true"
            reloadChanges="false"
            path="attribute-map.xml"/>
  <AttributeExtractor
            type="Metadata"
            errorURL="ErrorURL"
            DisplayName="DisplayName"
            InformationURL="InformationURL"
            PrivacyStatementURL="PrivacyStatementURL"
            OrganizationURL="OrganizationURL">
    <ContactPerson id="Technical-Contact"
                contactType="technical"
                formatter="<a href='$EmailAddress'>$GivenName $SurName</a>" />
    <ContactPerson id="Support-Contact"
                contactType="support"
                formatter="<a href='$EmailAddress'>$GivenName $SurName</a>" />
    <ContactPerson id="Administrative-Contact"
                contactType="administrative"
                formatter="<a href='$EmailAddress'>$GivenName $SurName</a>" />
    <Logo id="Large-Logo"
                height="60" width="80"
                formatter="<img align='middle' src='$_string' height='$height' width='$width'/>"/>
    <Logo id="Small-Logo"
                height="16" width="16"
                formatter="<img align='middle' src='$_string' height='$height' width='$width'/>"/>
  </AttributeExtractor>
</AttributeExtractor>
```