Service Categories

Service Categories (or Entity Categories) help managing the secure release of the right attributes to only appropriate Service Providers – within the edulD.at federation and beyond. The use of the Service Categories documented below constitutes global Best Current Practices for controlled and scalable attribute release policies/decisions. The ultimate responsibility for the release of any personal data to third parties under these terms rests with the institution releasing the data, though.

See also Attribute release in our Shibboleth IDP documentation.

Service Categories for Attribute Release

Inspired by prior work by RENATER the international Identity Federations community (lead by InCommon, REFEDS and GÉANT/eduGAIN) has started to create Service Categories (technically called “Entity Categories”, since they apply to SAML “entities”) in order to ease the management of release of personal data (“attributes”) to services within and across large-scale multi-party federations: It has long been apparent that manually writing and maintaining attribute release rules based on individual services does not scale sufficiently, esp. taking into account that e-research today requires international collaboration and does not stop at national or “federation” borders. Dealing with individual requests to access services on a case-by-case basis creates too much work for institutions and their staff, often resulting in students or scholars not being able to access needed (inter-)federated resources because the institutional SAML Identity Provider did not release the needed attributes to the accessed service.

Entity Categories solve this problem by grouping related services into clearly defined categories (taking into account purpose, risk/benefit and legal requirements) and scaling the management of those categories (i.e., which services are part of which category) across Identity Federations.

Below you'll find copy&paste-able attribute release filter rules for the widely used Shibboleth Identity Provider software for each of the most important Service Categories. Be sure to carefully read and understand each category's description/definition before use.

Make sure to get the use of these rules within your IT systems approved by management of your institution. Service Categories allow for such approval processes to occur only once per category, covering potentially unlimited numbers of services belonging to that category.

People managing technical infrastructure (such as servers and Shibboleth configuration files) should not be responsible for decisions resulting in the (non-) release of personal data to third parties. Contact ACOnet with any questions regarding Service Categories!

REFEDS Research & Scholarship

REFEDS has updated its guidance on the justification for attribute release with regard to the use of Service Categories (or Entity Categories) and the “REFEDS Research & Scholarship” category in particular. This now covers use under GDPR as well.

Membership in the category REFEDS R&S is reserved to services "that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part". This globally applicable category takes a risk-based approach to enabling access to high-benefit/low-risk services, releasing only low-risk personal data. Basically only the minimum personal data required for scientific collaboration and attribution of a person's work is released (name, email address and an identifier).

REFEDS R&S is purpose-limited: Only services fitting the purpose requirements may apply, and those services will only recieve a very limited set of low-risk attributes. It is being used gobally. Here's an up-to-date list of all REFEDS R&S services available to eduID.at members.

```
<AttributeFilterPolicy id="REFEDSResearchAndScholarship">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <!-- RandS requires: An identifier, email and a person's name. -->
  <AttributeRule attributeID="eduPersonPrincipalName" permitAny="true" />
  <AttributeRule attributeID="eduPersonTargetedID" permitAny="true" />
  <AttributeRule attributeID="mail" permitAny="true" />
  <AttributeRule attributeID="givenName" permitAny="true" />
  <AttributeRule attributeID="sn" permitAny="true" />
  <!-- Affiliation is optional but release is still "strongly recommended". -->
  <AttributeRule attributeID="eduPersonScopedAffiliation" permitAny="true" />
</AttributeFilterPolicy>
```
REFEDS R&S and reassigned ePPN attributes

Note if your deployment of the eduPersonPrincipalName (ePPN) attribute allows for reassigning ePPN values from one person to another that R&S v1 requires you to also release a SAML 2.0 persistent NameID then. Because SAML 2.0 persistent NameIDs prohibit reassignment also releasing those enables R&S Service Providers (that care and do the work) to detect ePPN reassignments by always looking at the combination of ePPN and persistent NameID (instead of just at the ePPN); if one day a known ePPN arrives together with a different/unknown persistent NameID that’s a sign that the ePPN likely has been reassigned to a different person and that access to data held at the SP from/about the former ePPN-NameID combination should be denied.

Of course that assumes that you can and do support proper SAML 2.0 persistent NameIDs and that you create those from source data that itself is not reassigned from one person to another. (If you don't have any such data and you also cannot mint it on the fly, as illustrated in our IDP attribute resolver documentation, you cannot produce spec-conformant persistent NameIDs and therefore also cannot support REFEDS R&S v1.)

Also note that if you don't have the (old, deprecated) eduPersonTargetedID (ePTID) attribute configured in your IDP then the Shibboleth IDP attribute filter rules given above may not be sufficient to conform to R&S v1: Technically (proper) SAML 2.0 persistent NameIDs are not "attributes" and consequently cannot be released using the Shibboleth IDP's attribute filter configuration (contrary to ePTID attributes, which wrap a persistent NameID in an attribute, but which are deprecated and their use should be phased out). Unless a REFEDS R&S Service Provider also signals that it wants to receive SAML 2.0 persistent NameIDs in its SAML Metadata using the NameIDFormat element (which other federations don’t even support and many SPs simply don't currently do) the above attribute filter snippet is insufficient to satisfy the R&S 1.x requirements – if your ePPN values may be reassigned and you don’t have ePTID available.

So (only) if all of the following 3 criteria apply to your deployment:

- ePPN attribute values may be reassigned from one person to another, over time,
- You have some other (internal) data available (or can mint it on the fly, as illustrated in our IDP attribute resolver documentation) that can serve as a basis for conformant (i.e., not-reassigned) attributes and persistent NameIDs,
- You don’t have the (old, deprecated) eduPersonTargetedID (ePTID) attribute configured in your IDP,

then you’d need to amend your IDP’s relying-party.xml configuration with a “relying party override” like the one shown below, forcing the NameIDFormat to “persistent” for all REFEDS R&S Service Providers (just in case those SPs don’t already request that NameID format in their metadata):

```xml
<util:list id="shibboleth.RelyingPartyOverrides">
<!-- [... -->
<bean parent="RelyingPartyByTag">
<!-- [... -->
  <constructor-arg name="candidates">
    <list>
      <bean parent="TagCandidate" c:name="http://macedir.org/entity-category"
        p:values="http://refeds.org/category/research-and-scholarship" />
    </list>
  </constructor-arg>
  <property name="profileConfigurations">
    <list>
      <bean parent="SAML2.SSO" p:nameIDFormatPrecedence="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" />
      <ref bean="SAML2.ECP" />
      <ref bean="SAML2.Logout" />
    </list>
  </property>
</bean>
</util:list>

N.B.: If your shibboleth.DefaultRelyingParty setting includes other properties on the bean with parent="SAML2.SSO" you should also include /repeat them here, e.g. p:postAuthenticationFlows="attribute-release".

Of course that’s overly complex (or plain crazy) which is exactly why ePPN, ePTID, persistent NameIDs and even R&S v1 are all more or less in the process of being replaced or phased out for newer, simpler replacements. For existing services relying on these standards, attributes and NameIDs, though, the above may be needed for proper support by the IDP.

GÉANT Data Protection Code of Conduct

GDPR update forthcoming

An updated version of the “GÉANT Data Protection Code of Conduct for Service Providers” is being worked on and will be submitted to the Data Protection Authorities for approval, now that GDPR has come into effect. Due to the expanded territorial scope of GDPR over the previous Data Protection Directive the new version can also be used globally (if adopted). Until that happens the existing version should provide sufficient justification and safeguards to continue its use under GDPR until its replacement is ready to be used.
As part of the GÉANT Data Protection Code of Conduct's Cookbook you'll find the Recipe for a Home Organisation providing complete instructions on the steps necessary for deployment. This Service Category only applies when the Service Provider (as well as the Identity Provider, which trivially will be case for all eduID.at Identity Providers) is based in the EU/EEA or countries with adequate data protection and uses the EU Data Protection Directive 95/46/EC as common frame for disparate implementations thereof throughout the EU. As such it is mostly meant as a reminder and a reassurance to both service owners and home organizations that the services covered are already subject to (national implementations of) EU data protection law.

**GÉANT Data Protection Code of Conduct is legislation-limited:** Only services from specific legislations may carry this category and only if they submit themselves to the GÉANT Data Protection Code of Conduct and all its requirements. Here's an up-to-date list of all GÉANT Code of Conduct services.

As this Category definition does not specify an attribute bundle (i.e., it doesn't reference one set of attributes which should be released to all category members) the set of attributes to be released may vary from service to service. The data to transmit under this category is limited to attributes "that are necessary for enabling access to the service provided by the Service Provider" (2.b, "purpose limitation"), though. In practice only a limited set of data will be exchanged within/across academic Identity Federations today: That could include a person's name, email address, identifier(s) and role information ("affiliation", such as "student" or "staff"), but could also be less than that if the service needs less data to perform appropriate access control.

The configuration below is an example based on the most commonly used attributes in Identity Federations today which most/all eduID.at Identity Providers should be able to generate. I.e., this constitutes the upper limit of what an IDP would release to Service Providers requesting data under the GÉANT Data Protection Code of Conduct category.

```
<AttributeFilterPolicy id="GeantEEDataProtectionCodeOfConduct">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://www.geant.net/uri/dataprotection-code-of-conduct/v1"/>
  <!-- Release data to EU/EEA/Adequate CoCo-SPs, based on RequestedAttributes in SAML metadata -->
  <AttributeRule attributeID="displayName">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="sn">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="mail">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonUniqueID">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
  </AttributeRule>
  <AttributeRule attributeID="eduPersonTargetedID">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
  </AttributeRule>
  <AttributeRule attributeID="schacPersonalUniqueCode">
    <PermitValueRule xsi:type="AND">
      <Rule xsi:type="AttributeInMetadata" onlyIfRequired="true"/>
      <Rule xsi:type="ValueRegex" regex="^urn:schac:personalUniqueCode:int:esi:.*$"/>
    </PermitValueRule>
  </AttributeRule>
  <AttributeRule attributeID="schacHomeOrganization">
    <PermitValueRule xsi:type="AttributeInMetadata" onlyIfRequired="false"/>
  </AttributeRule>
</AttributeFilterPolicy>
```

Again, be sure to check out the more general attribute release documentation in our Shibboleth IDP documentation, which contains more ready-to-use examples and approaches.