European Student Identifier Entity Category

Overview

All Identity Providers are invited to use the European Student Identifier Entity Category to manage the release of the European Student Identifier [ESI] attribute value to Service Providers meeting the requirements described below.

This definition is written in compliance with the Entity Category SAML Entity Metadata Attribute Types specification [EntityCatTypes]; this specification may be extended to reference other protocol-specific formulations as circumstances warrant.

1. Definition

The purpose of the European Student Identifier entity category is to support Higher Education Institutions (HEI) in identifying students as part of formal learning and teaching activities and/or the administrative activities related to those. These activities require data exchanges to take place, primarily, within or between institutions. The ESI plays a significant role in reliably identifying the students throughout these data exchanges.

This entity category may be used together with other entity categories to transfer additional attributes.

2. Registration Criteria

This Entity Category is addressed to any Service Provider Organisation established in any of the Member States of the European Union and in any other countries belonging to the European Economic Area (Iceland, Liechtenstein and Norway).

Furthermore, Service Provider Organisations established in any third country or International organization offering an adequate level of data protection in the terms of Article 45 of the GDPR can also subscribe to this Entity Category.

The current list of Identity Federations that can issue this Entity Category to Service Providers is maintained by GEANT [ESI-EC-ID-Feds].

Services eligible for the ESI Entity Category:

- Student Mobility Services directly enabling mobility, for example, the Erasmus+ programme.
- Services that transfer student records or transcripts of records between educational institutions and which need to identify the students to which the records belong to.
- University Alliances scenarios where students' records are shared across (some of) the universities of the Alliance.
- Formal learning and teaching activities and/or the administrative activities related to those within an institution, for example, Learning Management Systems and remote e-assessment tools.

3. Syntax

The following URI is used as the attribute value for the Entity Category and Entity Category Support attribute:

```
https://myacademicid.org/entity-categories/esi
```

4. Semantics

By asserting a Service Provider to be a member of this Entity Category, a registrar claims that the Service Provider has applied for membership in the Category and complies with this entity category's registration criteria.

In possessing the Entity Category Attribute with the above value, a Service Provider claims that it will not use the ESI attribute for purposes that fall outside of the service definition as presented at the time of registration and referred to in metadata and will support this statement within their published Privacy Notice.

In possessing the Entity Category Support Attribute with the above value, an Identity Provider claims that it will release attributes to approved Service Providers as outlined in the "Identity Provider Requirements" section below.

5. Attribute

The European Student Identifier uses the attribute **schacPersonalUniqueCode** (urn:oid:1.3.6.1.4.1.25178.1.2.14) as defined in the [SCHAC] and further profiled in the European Student Identifier specification [ESI].

6. Deployment Guidance for Service Providers

Service Providers that conform to the registration criteria defined in Section 2 will be eligible for the ESI Entity Category. Service Providers that have been assigned the ESI Entity Category, need to exhibit the following entity attribute in SAML metadata:

An entity attribute for SPs that conform to the European Student Identifier Entity Category:

```
<mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category">
    <saml:AttributeValue>
        https://myacademicid.org/entity-categories/esi
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

7. Deployment Guidance for Identity Providers

By asserting the ESI attribute value, Identity Providers are indicating that they are able to support this entity category. Such an Identity Provider must, for those users that are in scope, release the ESI value as defined in Section 5 to all tagged Service Providers, either automatically or subject to user consent or notification, without administrative involvement by any party.

An entity attribute for IdPs that support the European Student Identifier Entity Category:

```
<mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category-support">
    <saml:AttributeValue>
        https://myacademicid.org/entity-categories/esi
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

Please note that the attribute schacPersonalUniqueCode is multivalued, therefore it is important to only release the ESI value.

8. References

[EntityCatTypes] Young, I., Ed., Johansson, L., and S. Cantor, "The Entity Category Security Assertion Markup Language (SAML) Attribute Types", RFC 8409, DOI 10.17487/RFC8409, August 2018, <https://www.rfc-editor.org/info/rfc8409>.

[ESI] "European Student Identifier", GÉANT, https://wiki.geant.org/display/SM/European+Student+Identifier

[SCHAC] "Schema for ACademia", REFEDS, https://wiki.refeds.org/display/STAN/SCHAC

[ESI-EC-ID-Feds] "ESI Entity Category Issuing Identity Federations", GÉANT, https://wiki.geant.org/display/SM/ESI+Entity+Category+Issuing+Federations