4.1 Entity Categories for Service Providers

This is a set of entity categories in use by SWAMID. Entity categories for SAML is defined by REFEDS in the RFC8409 specification.

For an example on how to consume and process this information in an Identity Provider look at the page Example of a standard attribute filter for Shibboleth IdP v3.4.0 and above. ADFS Toolkit support the use of entity categories.

Attribute release comparison between REFEDS Entity Categories with fixed attribute bundles

REFEDS (the Research and Education FEDerations group) is the standard organisation within the academic identity federation community. To enable, simplify and minimalize attribute release from Identity Providers to Service Providers SWAMID uses entity categories. A service should never ask for more attributes that they need for delivering the service to the end user. Based on this assumption REFEDS has created three new hierarchal entity categories where:

- Anonymous Access is for services that don't need any personalized information,
- Pseudonymous Access is for services that support personalization between sessions but don't have any need of personal identifiable information, and
- Personalized Access is for services that need personal identifiable information.

You should never use more than one of these entity categories for the same service due to undefined behaviour. SWAMID recommends all Identity Providers to only release attribute for the most data minimalistic entity category, i.e. if a Service Provider asks for Pseudonymous Access and Personalized Access the service will get the attribute for Pseudonymous Access.

The entity category Research and Scholarship (R&S) is more or less the same as Personalized Access but have more restricted use cases and another set of identifiers.

The entity category European Student Identifier is a category to primary support student exchange programs like Erasmus+. This entity category only supports one value in one specific attribute and expected to be used together with other entity categories, for example Personalized Access.

For services that needs other attributes than supported by the fixed attribute bundles the entity category REFEDS Data Protection Code of Conduct, and the older GÉANT Data Protection Code of Conduct, is recommended.

	Anonymous Access	**Pseudonymous Access**	**Personalized Access**	**Research and Scholarship (R&S)**
Organisation	eduPersonScopedAffiliation schacHomeOrganization	eduPersonScopedAffiliation schacHomeOrganization	eduPersonScopedAffiliation schacHomeOrganization	eduPersonScopedAffiliation *(optional)*
User identifier		samlPairwiseID	samlSubjectID	eduPersonPrincipalName *(if non-reassigned)* eduPersonPrincipalName + eduPersonTargetedID *(not used within SWAMID)*
Assurance		eduPersonAssurance	eduPersonAssurance	eduPersonAssurance *(only within SWAMID)*
Person name			displayName givenName sn	displayName or givenName + sn
Email address			mail	mail

REFEDS Anonymous Access Entity Category

entity-category URI	https://refeds.org/category/anonymous

Definition

Candidates for the Anonymous Access Entity Category are Service Providers that offer a level of service based on proof of successful authentication. None of the attributes in this entity category are specifically intended to provide authorization information.

By asserting this entity category, Service Providers are signaling that they do not wish to receive personalized data.

Please note that the first of the REFEDS Anonymous Access Entity Category, then called REFEDS Anonymous Authorization Entity Category, was published early 2021 and therefore not so many Identity Providers has support for it yet. SWAMID recommends that you complement the REFEDS Anonymous Access Entity Category with the entity category GÉANT Data Protection Code of Conduct until end of 2024 to get the expected attribute release.

The Anonymous Access Entity Category is used both within SWAMID and in the eduGAIN interfederation to make services available to users of the higher education institutions in Sweden and around the world. The entity category makes it possible to automatically release a set of mostly harmless attributes to Service Providers registered in the academic federations.

The expected Identity Provider behaviour is to release to the Service Provider a predefined set of attributes. Service Providers signals their need of Anonymous Access Entity Category via an entity category tag in metadata. There is furthermore an identity provider entity support category that should be registered for all Identity Providers that supports the Anonymous Access Entity Category.

Expected attribute release from an Identity Provider

Attribute(s)	SAML2 Attribute Identifier	Comment
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	
schacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	

Process for applying for tagging a service with entity category REFEDS Anonymous Access Entity Category

For a service to be tagged with REFEDS Anonymous Access Entity Category it must contact the federation that it has registered with. If the service is registered within the SWAMID federation the service operator updates the service metadata in the SWAMID Metadata Tool.

The request must besides the metadata update contain the following administrative information:

- Purpose and scope of the service.

The entity category has the following metadata requirements:

- Well functional SAML2 metadata for the service with an entityid in URL-form as described in the SWAMID SAML WebSSO Technology Profile.
- Display name for the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- URL to an informational web page that describes the service in English and preferable also in Swedish.
- At least one of the administrative, technical and support contact for the service and it's recommended that security contact is also given.

The request is highly recommended to also have the following information for metadata publication:

- URL beginning with https to the service logotype for use in Identity Providers login pages and Discovery Services.

Besides the formal requirements and recommendations of REFEDS Anonymous Access Entity Category are Service Providers it is highly recommended that the service also adheres to the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi).

REFEDS Pseudonymous Access Entity Category

entity-category URI	https://refeds.org/category/pseudonymous

Definition

Candidates for the Pseudonymous Access Entity Category are Service Providers that offer a level of service based on proof of successful authentication and offer personalization based on a pseudonymous user identifier. The Service Provider must be able to effectively demonstrate this need to their federation registrar (normally the Service Provider's home federation) and demonstrate their compliance with regulatory requirements concerning personal data through a published Privacy Notice.

None of the attributes in this entity category are specifically intended to provide authorization information.

Please note that the first of the REFEDS Pseudonymous Access Entity Category, then called REFEDS Pseudonymous Authorization Entity Category, was published early 2021 and therefore not so many Identity Providers has support for it yet. SWAMID recommends that you complement the REFEDS Pseudonymous Access Entity Category with the entity category GÉANT Data Protection Code of Conduct until end of 2024 to get the expected attribute release.

The Pseudonymous Access Entity Category is used both within SWAMID and in the eduGAIN interfederation to make services available to users of the higher education institutions in Sweden and around the world. The entity category makes it possible to automatically release a set of mostly harmless attributes to Service Providers registered in the academic federations.

The expected Identity Provider behaviour is to release to the Service Provider a predefined set of attributes. Service Providers signals their need of Pseudonymous Access Entity Category via an entity category tag in metadata. There is furthermore an identity provider entity support category that should be registered for all Identity Providers that supports the Pseudonymous Access Entity Category.

For REFEDS Pseudonymous Access Entity Category there is a formal requirement that the service shall publish a public Privacy Policy. SWAMID have published a Service Provider Privacy Policy Template for GÉANT Data Protection Code of Conduct that can be used except for the requirement for mention the GÉANT Data Protection Code of Conduct.

Expected attribute release from an Identity Provider

Attribute(s)	SAML2 Attribute Identifier	Comment
samlPairwiseID	urn:oasis:names:tc:SAML:attribute:pairwise-id	
eduPersonAssurance	urn:oid:1.3.6.1.4.1.5923.1.1.1.11	
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	
schacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	

Process for applying for tagging a service with entity category REFEDS Pseudonymous Access Entity Category

For a service to be tagged with REFEDS Pseudonymous Access Entity Category it must contact the federation that it has registered with. If the service is registered within the SWAMID federation the service operator updates the service metadata in the SWAMID Metadata Tool.

The request must besides the metadata update contain the following administrative information:

- Purpose and scope of the service.
- Documentation which proves that the service has fulfilled all the requirements for REFEDS Pseudonymous Access Entity Category if it isn't defined by purpose and scope of the service.
    - The service has a proven and documented need for the pseudonymous information that forms the attribute bundle for this entity category.
    - The Service Provider has committed to data minimisation and will not use the attributes for purposes other than as described in their application.

The entity category has the following metadata requirements:

- Well functional SAML2 metadata for the service with an entityid in URL-form as described in the SWAMID SAML WebSSO Technology Profile.
- Display name for the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- URL to an informational web page that describes the service in English and preferable also in Swedish.
- URL to a web page with the service privacy policy in English and preferable also in Swedish, a privacy policy example template: SWAMID Service Provider Privacy Policy Template.
- At least one of the administrative, technical and support contact for the service and it's recommended that security contact is also given.

The request is highly recommended to also have the following information for metadata publication:

- URL beginning with https to the service logotype for use in Identity Providers login pages and Discovery Services.

Besides the formal requirements and recommendations of REFEDS Pseudonymous Access Entity Category are Service Providers it is highly recommended that the service also adheres to the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi).

REFEDS Personalized Access Entity Category

entity-category URI	https://refeds.org/category/personalized

Definition

Candidates for the Personalized Entity Category are Service Providers that have a proven need to receive a small set of personally identifiable information about their users in order to effectively provide their service to the user or to enable the user to signal their identity to other users within the service. The Service Provider must be able to effectively demonstrate this need to their federation registrar (normally the Service Provider's home federation) and demonstrate their compliance with regulatory requirements concerning personal data through a published Privacy Notice.

None of the attributes in this entity category are specifically intended to provide authorization information.

Please note that the first version of the REFEDS Personalized Access Entity Category was published late 2021 and therefore not so many Identity Providers has support for it yet. SWAMID recommends that you complement the REFEDS Personalized Access Entity Category with the entity category GÉANT Data Protection Code of Conduct until end of 2024 to get the expected attribute release.

The Personalized Access Entity Category is used both within SWAMID and in the eduGAIN interfederation to make services available to users of the higher education institutions in Sweden and around the world. The entity category makes it possible to automatically release a set of mostly harmless attributes to Service Providers registered in the academic federations.

The expected Identity Provider behaviour is to release to the Service Provider a predefined set of attributes. Service Providers signals their need of Personalized Access Entity Category via an entity category tag in metadata. There is furthermore an identity provider entity support category that should be registered for all Identity Providers that supports the Personalized Access Entity Category.

For REFEDS Personalized Access Entity Category there is a formal requirement that the service shall publish a public Privacy Policy. SWAMID have published a Service Provider Privacy Policy Template for GÉANT Data Protection Code of Conduct that can be used except for the requirement for mention the GÉANT Data Protection Code of Conduct.

Expected attribute release from an Identity Provider

Attribute(s)	SAML2 Attribute Identifier	Comment
samlSubjectID	urn:oasis:names:tc:SAML:attribute:subject-id	
mail	urn:oid:0.9.2342.19200300.100.1.3	Can be more than one address released but Identity Providers are recommended to release only one.
displayName	urn:oid:2.16.840.1.113730.3.1.241	
givenName	urn:oid:2.5.4.42	
sn	urn:oid:2.5.4.4	
eduPersonAssurance	urn:oid:1.3.6.1.4.1.5923.1.1.1.11	
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	
schacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	

Process for applying for tagging a service with entity category REFEDS Personalized Access Entity Category

For a service to be tagged with REFEDS Personalized Access Entity Category it must contact the federation that it has registered with. If the service is registered within the SWAMID federation the service operator updates the service metadata in the SWAMID Metadata Tool.

The request must besides the metadata update contain the following administrative information:

- Purpose and scope of the service.
- Documentation which proves that the service has fulfilled all the requirements for REFEDS Personalized Access Entity Category if it isn't defined by purpose and scope of the service.
    - The service has a proven and documented need for the personally identifiable information that forms the attribute bundle for this entity category.
    - The Service Provider has committed to data minimisation and will not use the attributes for purposes other than as described in their application.

The entity category has the following metadata requirements:

- Well functional SAML2 metadata for the service with an entityid in URL-form as described in the SWAMID SAML WebSSO Technology Profile.
- Display name for the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- URL to an informational web page that describes the service in English and preferable also in Swedish.

- URL to a web page with the service privacy policy in English and preferable also in Swedish, a privacy policy example template: SWAMID Service Provider Privacy Policy Template.
- At least one of the administrative, technical and support contact for the service and it's recommended that security contact is also given.

The request is highly recommended to also have the following information for metadata publication:

- URL beginning with https to the service logotype for use in Identity Providers login pages and Discovery Services.

Besides the formal requirements and recommendations of REFEDS Personalized Access Entity Category are Service Providers it is highly recommended that the service also adheres to the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi).

REFEDS Research and Scholarship (R&S)

entity-category URI	http://refeds.org/category/research-and-scholarship

Definition

Candidates for the Research and Scholarship (R&S) Category are Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part. For more information please see REFEDS Entity Category Research and Scholarship.

R&S is used both within SWAMID and in the eduGAIN interfederation to make services available to users of the higher education institutions in Sweden and around the world. The R&S makes it possible to automatically release mostly harmless attributes to Service Providers within the higher educational sector.

The expected IdP behaviour is to release to the Service Provider a predefined set of R&S Category Attributes. Service Providers signals their need of R&S via an entity category tag in metadata. There is furthermore an identity provider entity support category that should be registered for all Identity Providers that supports the R&S entity category and this can be used for filter purpose in a discovery service.

Example of services that uses the entity category includes (but are not limited to) collaborative tools and services such as wikis, blogs, project and grant management tools that require some personal information about users to work effectively. This Entity Category should not be used for access to licensed content such as e-journals.

For REFEDS Research and Scholarship there is no formal requirement that the service shall publish a public Privacy Policy. However all services that are registered in SWAMID must have a Privacy Policy to inform end users about how personal data are processed. SWAMID have published a Service Provider Privacy Policy Template for GÉANT Data Protection Code of Conduct that can be used except for mention the GÉANT Data Protection Code of Conduct.

Expected attribute release from an Identity Provider

Attribute(s)	SAML2 Attribute Identifier	Comment
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	Should only be released by the Identity Provider if eduPersonPrincipalName is re-assignable to another user. Within SWAMID reassignment of the eduPersonPrincipalName is not allowed and therefore this attribute will not be released from Identity Providers within SWAMID.
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	
mail	urn:oid:0.9.2342.19200300.100.1.3	Can be more than one address released but Identity Providers are recommended to release only one.
displayName and/or givenName and sn	urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.42	A user's name can be released in different ways and it's expected that the Service Provider can handle this.

	urn:oid: 2.5.4.4	
eduPersonAssurance	urn:oid: 1.3.6.1.4.1.5923.1.1.1.11	Local addon within SWAMID. Services shall only expect this attribute to be available from Identity Providers within SWAMID.
eduPersonScopedAffiliation	urn:oid: 1.3.6.1.4.1.5923.1.1.1.9	

Process for applying for tagging a service with entity category REFEDS Research and Scholarship

For a service to be tagged with REFEDS Research and Scholarship (R&S) it must contact the federation that it has registered with. If the service is registered within the SWAMID federation the service operator updates the service metadata in the SWAMID Metadata Tool.

The request must besides the metadata update contain the following administrative information:

- Purpose and scope of the service.
- Documentation which proves that the service has fulfilled all the requirements for R&S if it's not defined by purpose and scope of the service:
  - The service enhances the research and scholarship activities of some subset of the user community.
  - The Service Provider is a production SAML deployment that supports SAML V2.0 HTTP-POST binding.
  - The Service Provider claims to refresh federation metadata at least daily.

Unless the following is already published in current service metadata, the metadata update request must contain:

- Well functional SAML2 metadata for the service with an entityid in URL-form as described in the SWAMID SAML WebSSO Technology Profile.
- Display name for the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- Technical contact for the service and it's recommended that administrative, support and security contact is also given.
- URL to an informational web page that describes the service in English and preferable also in Swedish.
- URL to a web page with the service privacy policy in English and preferable also in Swedish, a privacy policy example template: SWAMID Service Provider Privacy Policy Template (specific for SWAMID).
- The Service Provider is a production SAML deployment that supports SAML V2.0 HTTP-POST binding.

The request is highly recommended to also have the following information for metadata publication:

- URL beginning with https to the service logotype for use in Identity Providers login pages and Discovery Services.

Besides the formal requirements and recommendations of REFEDS R&S it is highly recommended that the service also adheres to the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi).

REFEDS Data Protection Code of Conduct (CoCo v2)

entity-category URI	https://refeds.org/category/code-of-conduct/v2

Definition

The REFEDS Data protection Code of Conduct (CoCo v2) entity category defines an approach at a European level to meet the requirements of the European General Data Protection Regulation (GDPR) for releasing mostly harmless personal attributes to a Service Provider (SP) from an Identity Provider (IdP). For more information please see REFEDS Data Protection Code of Conduct.

REFEDS Data Protection Code of Conduct entity category is used both within SWAMID and in the eduGAIN interfederation to make services available to users of the higher education institutions in Sweden and around Europe. The entity category makes it possible to automatically release mostly harmless attributes to Service Providers in the spririt of the EU Data Protection legislation. The expected Identity Provider behaviour is to release the Service Provider required attributes if the IdP is able to. Required attributes means attributes the service must have to be able to work for the user. However it's possible to require more than one attribute of a specific type, i.e. name and identifier attributes, to increase the possibility to get the needed set of attributes. The required attributes for a specific service is defined in the the service metadata and must be described in the mandatory Service Provider Privacy Policy. There is furthermore an identity provider entity support category that should be registered for all Identity Provider that supports the REFEDS Data Protection Code of Conduct entity category that can be used for filter purpose in a discovery service.

Expected attribute availability from an Identity Provider for attributes required by indication in metadata

Attribute(s)	SAML2 Attribute	Comment

	Identifier	
samlPairwiseID	urn:oasis:names:tc:SAML:attribute:pairwise-id	
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	This attribute is deprecated!
samlSubjectID	urn:oasis:names:tc:SAML:attribute:subject-id	
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	
eduPersonOrcid	urn:oid:1.3.6.1.4.1.5923.1.1.1.16	
norEduPersonNIN	urn:oid:1.3.6.1.4.1.2428.90.1.5	This attribute is for students systems that needs to be synchronised with the the student documentations system directly or indirectly. Within SWAMID norEduPersonNIN can besides Swedish Personal Numbers and Swedish Co-ordination Numbers also contain Interim Personal Numbers from the student documentation system Ladok and the Swedish national study enrolment system. SWAMID Identity Providers only release this attribute to services registered in SWAMID.
personalIdentityNumber	urn:oid:1.2.752.29.4.13	Within SWAMID personalIdentityNumber only contain Swedish Personal Numbers or Swedish Co-ordination Numbers. SWAMID Identity Providers only release this attribute to services registered in SWAMID.
schacDateOfBirth	urn:oid:1.3.6.1.4.1.25178.1.2.3	
displayName	urn:oid:2.16.840.1.113730.3.1.241	
givenName	urn:oid:2.5.4.42	
sn *(aka surname)*	urn:oid:2.5.4.4	

norEduPersonLegalName	urn:oid:1.3.6.1.4.1.2428.90.1.10	The full legal name from the population registry or from official travel documents defined in ICAO 9306, i.e. passports and European national identity cards.
cn *(aka commonName)*	urn:oid:2.5.4.3	Due to that cn is use for different things in different identity management systems it's highly recommended to use the attribute displayName instead.
mail	urn:oid:0.9.2342.19200300.100.1.3	Can be more than one address released but Identity Providers are recommended to release only one.
mailLocalAddress	urn:oid:2.16.840.1.113730.3.1.13	For services that need to get all active mail aliases for the user. For example to process mail invite flows correctly when the given mail address is not the primary for the user. mailLocalAddress is used as a multi-valued attribute with all active mail alises for the user.
eduPersonAssurance	urn:oid:1.3.6.1.4.1.5923.1.1.1.11	Services shall only expect this attribute to be available from Identity Providers within SWAMID.
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	
eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1	Due to eduPersonAffiliations non domain scoped nature it's highly recommended to use the attribute eduPersonScopedAffiliation instead.
o *(aka organizationName)*	urn:oid:2.5.4.10	This attribute is also be available as an metadata attribute.
norEduOrgAcronym	urn:oid:1.3.6.1.4.1.2428.90.1.6	
c *(aka countryName)*	urn:oid:2.5.4.6	
co *(aka friendlyCountryName)*	urn:oid:0.9.2342.19200300.100.1.43	
schacHomeOrganization	urn:oid:1.3.6.1.4.1.25178.1.2.9	
schacHom	urn:oid:	

eOrganizati onType	1.3.6.1.4.1.2 5178.1.2.10

Multivalued attributes that have different values for different services shall not be requested via metadata, examples of such attributes are eduPersonEntitlement, norEduPersonLIN and schacPersonalUniqueCode. The reason for this is that an Identity Provider may unintensional release sensitive information to services that are not eligable for these values. SWAMID recommends member Identity Providers to not release this type of attributes based on reqeusted attributes in metadata.

Process for applying for tagging a service with entity category REFEDS Data Protection Code of Conduct

For a service to be tagged with REFEDS Data Protection Code of Conduct it must contact the federation that it has registered with. If the service is registered within the SWAMID federation the service operator updates the service metadata in the SWAMID Metadata Tool.

The request must besides the metadata update contain the following administrative information:

- Purpose and scope of the service.
- Documentation which proves that the service has fulfilled all the requirements for CoCo and lawfullness of processing as described in GDPR if it's not defined by purpose and scope of the service:
  - the grounds under which the Service Provider supports transfer of data as either:
    - Operating in a country within the European Union or European Economic Area or a country, territory, sector or international Organisation with an adequacy decision pursuant to GDPR Article 45, and
    - Using appropriate safeguards pursuant to GDPR Article 46 and committed to only receiving data from organisations where safeguards have been agreed.
  - that the service has committed to theREFEDS/GÉANT Data Protection Code of Conduct,
  - that it informs the Registrar about any material changes that may influence their ability to commit to the REFEDS/GÉANTData Protection Code of Conduct
- A list of the required attributes that the service needs to function (the list is also required in the privacy policy of the service). It is possible to require more than one attribute of a specific type, i.e. name and identifier attributes, to increase the possibility to get the needed set of attributes.

Unless the following is already published in current service metadata, the metadata update request must contain:

- Well functional SAML2 metadata for the service with an entityid in URL-form as described in the SWAMID SAML WebSSO Technology Profile.
- Display name for the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- Short description of the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- A list of required attributes of the Service.
- Administrative contact for the service and it's recommended that technical, support and security contact is also given.
- URL to a publicly accessible web page (not a pdf document) with the service privacy policy in English and preferable also in Swedish, a privacy policy example template: SWAMID Service Provider Privacy Policy Template. The privacy policy must at least contain:
  - the name, address and jurisdiction of the Service Provider;
  - the purpose or purposes of the processing of the Attributes;
  - a description of the Attributes being processed;
  - the third party recipients or categories of third party recipient to whom he Attributes might be disclosed, and proposed transfers of Attributes to countries outside of the European Economic Area;
  - the existence of the rights to access, rectify and delete the Attributes held about the End User; and
  - the retention period of the Attributes.

It's also a highly recommended that the service adheres to the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi).

GÉANT Data Protection Code of Conduct (CoCo v1)

entity-category URI	http://www.geant.net/uri/dataprotection-code-of-conduct/v1

Definition

The GÉANT Data protection Code of Conduct (CoCo v1) defines an approach at a European level to meet the requirements of the European Union Data Protection Directive. The Data Protection Directive has been superseded by General Data Protection Regulation (GDPR) and therefore GDPR must be taken into account for the entity category. GÉANT Data Protection Code of Conduct is in the same spirit as GDPR, i.e. the Charter of Fundamental Rights of the European Union. For more information please see GEANT Data Protection Code of Conduct.

GÉANT Data Protection Code of Conduct is superseded by REFEDS Data Protection Code of Conduct but will will exist in parallell with the new entity category for an extended time and therefore we recommend all services that uses CoCo v2 to also declare CoCo v1 and the other way around.

GÉANT Data Protection Code of Conduct entity category is used both within SWAMID and in the eduGAIN interfederation to make services available to users of the higher education institutions in Sweden and around Europe. The entity category makes it possible to automatically release mostly harmless attributes to Service Providers in the spririt of the EU Data Protection legislation. The expected Identity Provider behaviour is to release the Service Provider required attributes if the IdP is able to. Required attributes means attributes the service must have to be able to work for the user. However it's possible to require more than one attribute of a specific type, i.e. name and identifier attributes, to increase the possibility to get the needed set of

attributes. The required attributes for a specific service is defined in the the service metadata and must be described in the mandatory Service Provider Privacy Policy. There is furthermore an identity provider entity support category that should be registered for all Identity Provider that supports the GÉANT Data Protection Code of Conduct entity category that can be used for filter purpose in a discovery service.

Expected attribute availability from an Identity Provider for attributes required by indication in metadata

Attribute (s)	SAML2 Attribute Identifier	Comment
samlPairwiseID	urn:oasis:names:tc:SAML:attribute:pairwise-id	
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	This attribute is deprecated!
samlSubjectID	urn:oasis:names:tc:SAML:attribute:subject-id	
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	
eduPersonOrcid	urn:oid:1.3.6.1.4.1.5923.1.1.1.16	
norEduPersonNIN	urn:oid:1.3.6.1.4.1.2428.90.1.5	This attribute is for students systems that needs to be synchronised with the the student documentations system directly or indirectly. Within SWAMID norEduPersonNIN can besides Swedish Personal Numbers and Swedish Co-ordination Numbers also contain Interim Personal Numbers from the student documentation system Ladok and the Swedish national study enrolment system. SWAMID Identity Providers only release this attribute to services registered in SWAMID.
personalIdentityNumber	urn:oid:1.2.752.29.4.13	Within SWAMID personalIdentityNumber only contain Swedish Personal Numbers or Swedish Co-ordination Numbers. SWAMID Identity Providers only release this attribute to services registered in SWAMID.
schacDateOfBirth	urn:oid:1.3.6.1.4.1.25178.1.2.3	
displayName	urn:oid:2.16.840.1.113730.3.1.241	
givenName	urn:oid:2.5.4.42	
sn *(aka surname)*	urn:oid:2.5.4.4	
norEduPersonLegalName	urn:oid:1.3.6.1.4.1.2428.90.1.10	The full legal name from the population registry or from official travel documents defined in ICAO 9306, i.e. passports and European national identity cards.
cn *(aka commonName)*	urn:oid:2.5.4.3	Due to that cn is use for different things in different identity management systems it's highly recommended to use the attribute displayName instead.
mail	urn:oid:0.9.2342.19200300.100.1.3	Can be more than one address released but Identity Providers are recommended to release only one.
mailLocalAddress	urn:oid:2.16.840.1.113730.3.1.13	For services that need to get all active mail aliases for the user. For example to process mail invite flows correctly when the given mail address is not the primary for the user. mailLocalAddress is used as a multi-valued attribute with all active mail alises for the user.

eduPerson Assurance	urn:oid: 1.3.6.1.4.1.5923.1.1.1.11	Services shall only expect this attribute to be available from Identity Providers within SWAMID.
eduPerson ScopedAffiliation	urn:oid: 1.3.6.1.4.1.5923.1.1.1.9	
eduPerson Affiliation	urn:oid: 1.3.6.1.4.1.5923.1.1.1.1	Due to eduPersonAffiliations non domain scoped nature it's highly recommended to use the attribute eduPersonScopedAffiliation instead.
o *(aka organizationName)*	urn:oid: 2.5.4.10	This attribute is also be available as an metadata attribute.
norEduOrgAcronym	urn:oid: 1.3.6.1.4.1.2428.90.1.6	
c *(aka countryName)*	urn:oid: 2.5.4.6	
co *(aka friendlyCountryName)*	urn:oid: 0.9.2342.19200300.100.1.43	
schacHomeOrganization	urn:oid: 1.3.6.1.4.1.25178.1.2.9	
schacHomeOrganizationType	urn:oid: 1.3.6.1.4.1.25178.1.2.10	

Multivalued attributes that have different values for different services shall not be requested via metadata, examples of such attributes are eduPersonEntitlement, norEduPersonLIN and schacPersonalUniqueCode. The reason for this is that an Identity Provider may unintensional release sensitive information to services that are not eligable for these values. SWAMID recommends member Identity Providers to not release this type of attributes based on reqeusted attributes in metadata.

Process for applying for tagging a service with entity category GÉANT Data Protection Code of Conduct

For a service to be tagged with GÉANT Data Protection Code of Conduct it must contact the federation that it has registered with. If the service is registered within the SWAMID federation the service operator updates the service metadata in the SWAMID Metadata Tool.

The request must besides the metadata update contain the following administrative information:

- Purpose and scope of the service.
- Documentation which proves that the service has fulfilled all the requirements for CoCo and lawfullness of processing as described in GDPR if it's not defined by purpose and scope of the service:
    - the grounds under which the Service Provider supports transfer of data as either:
        - Operating in a country within the European Union or European Economic Area or a country, territory, sector or international Organisation with an adequacy decision pursuant to GDPR Article 45, and
        - Using appropriate safeguards pursuant to GDPR Article 46 and committed to only receiving data from organisations where safeguards have been agreed.
    - that the service has committed to theREFEDS/GÉANT Data Protection Code of Conduct,
    - that it informs the Registrar about any material changes that may influence their ability to commit to the REFEDS/GÉANTData Protection Code of Conduct
- A list of the required attributes that the service needs to function (the list is also required in the privacy policy of the service). It is possible to require more than one attribute of a specific type, i.e. name and identifier attributes, to increase the possibility to get the needed set of attributes.

Unless the following is already published in current service metadata, the metadata update request must contain:

- Well functional SAML2 metadata for the service with an entityid in URL-form as described in the SWAMID SAML WebSSO Technology Profile.
- Display name for the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- Short description of the Service in English and preferable also in Swedish for use in Identity Providers' login pages and Discovery Services.
- A list of required attributes of the Service.
- Administrative contact for the service and it's recommended that technical, support and security contact is also given.
- URL to a publicly accessible web page (not a pdf document) with the service privacy policy in English and preferable also in Swedish, a privacy policy example template: SWAMID Service Provider Privacy Policy Template. The privacy policy must at least contain:
    - the name, address and jurisdiction of the Service Provider;
    - the purpose or purposes of the processing of the Attributes;
    - a description of the Attributes being processed;

- the third party recipients or categories of third party recipient to whom he Attributes might be disclosed, and proposed transfers of Attributes to countries outside of the European Economic Area;
- the existence of the rights to access, rectify and delete the Attributes held about the End User;
- the retention period of the Attributes; and
- a reference to this Code of Conduct including the formal reference URL http://www.geant.net/uri/dataprotection-code-of-conduct/v1.

It's also a highly recommended that the service adheres to the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi).

European Student Identifier Entity Category

entity-category URI	https://myacademicid.org/entity-categories/esi

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 European Student Identifier (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.

The European Student Identifier Entity Category is used both within SWAMID and in the eduGAIN interfederation to make services available to users of the higher education institutions in Sweden and around Europe. The entity category makes it possible to automatically release the European Student Identifier as defined at https://wiki.geant.org/display/SM/European+Student+Identifier.

The expected Identity Provider behaviour for universites and university colleges is to release to the Service Provider the European Student Identifier. Service Providers signals their need of European Student Identifier via an entity category tag in metadata. There is furthermore an identity provider entity support category that should be registered for all Identity Providers that supports the European Student Identifier Entity Category.

Expected attribute release from an Identity Provider

Attribute(s)	SAML2 Attribute Identifier	Comment
schacPersonalUniqueCode	urn:oid:1.3.6.1.4.1.25178.1.2.14	This attribute is a multi-valued attribute but the expected behaviour is that the Identity Provider only releases the ESI value to the service if no other values are released by bilateral agreement.

Process for applying for tagging a service with entity category European Student Identifier Entity Category

For a service to be tagged with European Student Identifier Entity Category it must contact the federation that it has registered with. If the service is registered within the SWAMID federation the service operator updates the service metadata in the SWAMID Metadata Tool.

The request must besides the metadata update contain the following administrative information:

- Purpose and scope of the service.
- Description on fulfillment of the eligible criteria 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.

The entity category has the following metadata requirements:

- Well functional SAML2 metadata for the service with an entityid in URL-form as described in the SWAMID SAML WebSSO Technology Profile.

The request is highly recommended to also have the following information for metadata publication:

- URL beginning with https to the service logotype for use in Identity Providers login pages and Discovery Services.

Besides the formal requirements and recommendations of European Student Identifier Entity Category are Service Providers it is highly recommended that the service also adheres to the REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi).

Release without any recognised Entity Categories

Most Identity Providers within SWAMID release no attributes to a service when it is not marked with the entity categories above.