REFEDS Data Protection Code of Conduct Entity Category
v.2.0 published 28th March 2022

Overview

This Code of Conduct defines a set of rules that Service Provider Organisations can commit to when they want to receive End Users' Attributes from Home Organisations or their Agent for enabling the End Users to access their Services. Home Organisations will feel more comfortable to release affiliated End Users' Attributes to the Service Provider Organisation if they can see that the Service Provider Organisation has taken measures to properly protect the Attributes.

This document defines a SAML 2.0 Entity Category attribute for Service Providers that claim conformance to the Data Protection Code of Conduct and a SAML 2.0 Entity Category support attribute for Identity Providers that are willing to interact with Service Providers conforming to the Data Protection Code of Conduct. This document also defines the SAML 2.0 metadata requirements for Identity and Service Providers claiming the Entity Category attribute.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [BCP14].

1. Definition

Candidates for the Code of Conduct Entity Category are Service Provider Organisations that are willing to support and implement the REFEDS Data Protection Code of Conduct Best Practice guidelines [CoCo].

This Code of Conduct 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, or
- appropriate safeguards in the terms of Article 46 of the GDPR

can also subscribe to this Code of Conduct.

2. Syntax

The following URI is used as the Attribute Value for the Entity Category attribute and Entity Category support attribute:

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

3. Semantics

By asserting a Service Provider to be a member of this Entity Category, a Registrar claims that:

1. The Service Provider has applied for membership in the Category and complies with this entity category's registration criteria.
2. The Service Provider's application for using the Code of Conduct Entity Category has been reviewed against the registration criteria and approved by the Registrar.

In possessing the Entity Category Attribute with the above value, a Service Provider claims:

- that it is bound by:
  - The data protection laws in the European Union or European Economic Area, or can demonstrate:
  - an adequate level of data protection in the terms of Article 45 of the GDPR;
  - appropriate safeguards in the terms of Article 46 of the GDPR;
- that it has committed to the REFEDS Data Protection Code of Conduct [CoCo].
- that it conforms to the Metadata Requirements for Service Providers (section 5).
- that it informs the Registrar about any material changes that may influence their ability to commit to the REFEDS Data Protection Code of Conduct [CoCo].

The Service Provider is responsible for the service it offers and its legal compliance with the Code of Conduct. The Service Provider is regarded as authoritative about its Privacy Notice and the attributes the service requests.

By asserting the Entity Category support attribute, an Identity Provider claims that it releases the requested attributes to a Code of Conduct committed Service Provider without administrative involvement.

4. Registration Criteria

When a Service Provider's Registrar (normally the Service Provider's home federation) registers the Service Provider in the Entity Category, the Registrar MUST at least establish:

1. the grounds under which the Service Provider supports transfer of data (see section 1) as either:
   a. 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;
   b. Using appropriate safeguards pursuant to GDPR Article 46 and committed to only receiving data from organisations where safeguards have been agreed.
2. that the Service Provider is committed to supporting the Code of Conduct Best Practice.
3. that the SAML 2.0 elements conform to the Metadata Requirements for Service Provider entities (see section 5).
4. that the Service Provider's mdui:Description and mdui:DisplayName elements are understandable and useful for common end users.
5. that the list of requested attributes is consistent with the Privacy Notice document.

6. that the Service Provider has an appropriate administrative contact that is aware of the Service Provider's commitment to the Code of Conduct.

The Registrar has the right to remove the Entity Category if the Service Provider can no longer demonstrate commitment to the REFEDS Data Protection Code of Conduct [CoCo].

5. Metadata Requirements for Service Providers

5.1 mdui Requirements

5.1.1. SPs MUST provide at least one mdui:PrivacyStatementURL value. The PrivacyStatementURL MUST resolve to a Privacy Notice which is available to browser users without requiring authentication of any kind.

5.1.2 SPs MUSTs provide at least one mdui:DisplayName value.

5.1.3 SPs MUST provide at least one mdui:Description value. It is RECOMMENDED that the length of the description is no longer than 140 characters.

5.1.4 For all mdui elements, at least an English version of the element MUST be available, indicated by an xml:lang="en" attribute.

5.2 Attribute Requirements

The Service Provider is responsible to define in metadata what user attributes are necessary for enabling access to the service. There are two different locations in metadata for requesting attributes; the subject-id:req entity attribute extension and RequestedAttribute elements.

5.2.1. If the SP is using SAML Subject Identifier Attribute Profile for identifier attribute release, it MUST provide subject-id:req entity attribute extension to indicate which one of the identifiers pairwise-id or subject-id is necessary.

5.2.2. If the SP is requesting other attributes than the identifiers above, it MUST provide RequestedAttribute elements describing the attributes relevant for the SP. The RequestedAttribute elements MUST include the optional isRequired="true" to indicate that the attribute is necessary

6. Deployment Guidance for Service Providers

A Service Provider that conforms to this entity category would exhibit the following entity attribute in SAML metadata:

An entity attribute for Service Providers that support the Entity Category:

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
  <Attribute xmlns="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">
    <AttributeValue>https://refeds.org/category/code-of-
```

```
conduct/v2</AttributeValue>
  </Attribute>
</EntityAttributes>
```

7. Deployment Guidance for Identity Providers

An Identity Provider indicates support for the Entity Category by exhibiting the Code of Conduct entity attribute in its metadata. By indicating this support, the Identity Providers asserts that they are willing to interact with and release attributes to Service Providers conforming to the Code of Conduct.
Further support guidance for Identity Providers is available [CoCoHomeOrg].

An entity attribute for Identity Providers that support the Entity Category:

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
  <Attribute xmlns="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">
    <AttributeValue>https://refeds.org/category/code-of-
conduct/v2</AttributeValue>
  </Attribute>
</EntityAttributes>
```

7. References

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997; and Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017: https://www.rfc-editor.org/info/bcp14.
[CoCo] REFEDS Data Protection Code of Conduct 2.0: https://refeds.org/category/code-of-conduct.
[CoCoHomeOrg] Data protection Code of Conduct 2.0, "Good Practice for Home Organisations": https://wiki.refeds.org/display/CODE/Good+practice+for+Home+organisations.