Entity Categories for the Swedish eID Framework

Version 1.5 - 2017-03-28

ELN-0606-v1.5

Table of Contents

1. Introduction

This specification contains the Entity Category definitions that are defined for the Swedish eID Framework and that should be supported by Service Providers and Identity Providers that are part of the federation.

The use of Entity Categories for the Swedish eID Framework is restricted to SAML metadata where Entity Categories are placed as SAML attributes under the `<mdattr:EntityAttributes>` element ([SAML2MetaAttr]) for an `<md:Extensions>` element ([SAML2Meta]).

```
<md:EntityDescriptor entityID="https://eid2.example.com/entityid">
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
    ...
      <saml:Attribute Name="http://macedir.org/entity-category"
                              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">
          http://id.elegnamnden.se/ec/1.0/loa3-pnr
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
```

The Entity Category identifier `http://id.elegnamnden.se/ec/1.0/loa3-pnr` *specified as an entity attribute for a Service Provider or Identity Provider.*

Three types of Entity Categories are used within the federation:

- Service entity category – Identifiers for entity categories representing alternative sets of requirements.
- Service property categories – Identifiers for defined service properties.
- Service type categories – Identifiers for defined service types.

1.1. Requirements Notation

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 [RFC2119].

The use of SHOULD, SHOULD NOT, and RECOMMENDED reflects broad consensus on deployment practices intended to foster both interoperability and guarantees of security and confidentiality needed to satisfy the requirements of many organizations that engage in the use of federated identity. Deviating may limit a deployment's ability to technically interoperate without additional negotiation, and should be undertaken with caution.

1.2. References to SAML 2.0 Standards and Profiles

When referring to elements from the SAML 2.0 core specification [SAML2Core], the following syntax is used:

- `<saml2p:Element>` – for elements from the SAML 2.0 Protocol namespace.
- `<saml2:Element>` – for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specifications, the following syntax is used:

- `<md:Element>` – for elements defined in [SAML2Meta].
- `<mdattr:Element>` – for elements defined in [SAML2MetaAttr].

1.3. Consuming and Providing Services

Entity categories are mainly used for service matching. This allows matching of a consuming service with an appropriate providing service. A consuming service in this context is an assertion or attribute consuming service of a service provider (Service described through an `<md:SPSSODescriptor>` element in the federation metadata). A providing service in this context is a service, represented in the federation metadata, providing assertions to a service provider.

The entity categories defined in this document have different meaning depending on whether they are declared by a consuming or a providing service. Further, different types of entity category identifiers defined in this document have different matching rules to determine whether particular providing service matches the requirements of a consuming service.

These differences are outlined in the following table:

EC type	Consuming service	Providing service	Service matching rule
Service Entity Category	Each declared category represents an alternative set of requirements for the service.	Represents the ability to deliver assertions in accordance with each declared category.	At least one of the entity categories declared by the consuming service MUST be declared by the providing service.
Service Property	Represents a property of this service.	Represents the ability to deliver assertions to a consuming service that has the declared property.	All properties declared by the consuming service MUST be declared by the providing service.
Service Type	Declares the type of service provided by this consuming service.	Not applicable.	No matching rule.

1.4. Use in Discovery

Entity Categories in metadata are declarations of requirements and capabilities of Service Providers and Identity Providers. A discovery process may make use of these declared Entity Categories when performing filtering, i.e., when deciding which Identity Providers to present for the end-user. The filtering algorithm is very simple:

For a Service Provider requesting discovery its metadata entry is scanned for Entity Category identifiers of the type Service Entity Category and Service Property. The algorithm then iterates over all Identity Providers found in the metadata repository for the federation. The discovery process SHOULD display Identity Providers as a plausible choice, if and only if, they have declared;

- at least one of the Service Entity Category identifiers declared by the Service Provider, and
- all of the Service Property identifiers declared by the Service Provider.

1.5. Representation of Entity Categories in Metadata

Entity categories defined in this document are placed in an entity's metadata record as an attribute value within an entity category attribute (SAML attribute with name `http://macedir.org/entity-category`). If more than one entity category identifier is included in the metadata of a service, it MUST be placed as multiple attribute values within a single entity category attribute.

```
<md:EntityDescriptor entityID="https://eid2.example.com/entityid">
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
    ...
      <saml:Attribute Name="http://macedir.org/entity-category"
                              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xsi:type="xs:string">
          http://id.elegnamnden.se/ec/1.0/loa3-pnr
        </saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">
          http://id.elegnamnden.se/sprop/1.0/mobile-auth
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  ...
```

Example of how entity categories are represented in metadata.

2. Definitions for Service Entity Categories

This section contains a listing of all Service Entity Categories that are defined within the framework for Swedish eID.

All service entity category identifiers are prefixed with `http://id.elegnamnden.se/ec`.

A service entity category identifies an arbitrary set of requirements and conditions that is required by the consuming service and provided by the providing service. Each service entity category specifies its own set of requirements and conditions. Typically such requirements and conditions include requirements on level of assurance (LoA) and requirements on mandatory attributes.

Note: This specification does not impose any limitations on what requirements or conditions that can be identified by a service entity category and there are no defined technical mechanisms to ensure that any service correctly implement any of these requirements. The purpose of the service entity category is limited to service matching in accordance with section 1.3 and any requirements and conditions that serves this purpose are considered valid.

Note: The service entity category may serve as a means to restrict a providing service to only those Service Providers that has made a deliberate choice to accept the providing service. This is achieved if an Identity Provider only lists a privately defined service entity category in its metadata which is understood and accepted by just a subset of all service providers. Each Service Provider can then make this Identity Provider selectable (matching its own service) by including this private service entity category in its metadata.

Example: Suppose that the Identity Provider X delivers assertions according to service entity category "loa3-pnr" (as described below), but only to relying parties to which it has a business agreement with. In order to facilitate the matching rules for discovery (see section 1.4 above) the service entity category, "loa3-pnr-X", is introduced. It has the same meaning as "loa3-pnr" with the additional requirement that there must exist a bilateral agreement between a Service Provider and Identity Provider X. This URI for this new service entity category should now be included in the metadata for the Identity Provider, and in metadata for the Service Providers that have an agreement with the Identity Provider.

2.1. loa3-pnr

URL: `http://id.elegnamnden.se/ec/1.0/loa3-pnr`

Description: User authentication according to assurance level 3 [EidTillit] and attribute release according to the attribute set “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01).

LoA-identifier: `http://id.elegnamnden.se/loa/1.0/loa3`

Attribute requirements: ELN-AP-Pnr-01 (`http://id.elegnamnden.se/ap/1.0/pnr-01`)

> Natural Personal Identity with Civic Registration Number (personnummer).

2.2. loa2-pnr

URL: `http://id.elegnamnden.se/ec/1.0/loa2-pnr`

Description: User authentication according to assurance level 2 [EidTillit] and attribute release according to the attribute set “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01).

LoA-identifier: `http://id.elegnamnden.se/loa/1.0/loa2`

Attribute requirements: ELN-AP-Pnr-01 (`http://id.elegnamnden.se/ap/1.0/pnr-01`)

> Natural Personal Identity with Civic Registration Number (personnummer).

2.3. loa4-pnr

URL: `http://id.elegnamnden.se/ec/1.0/loa4-pnr`

Description: User authentication according to assurance level 4 [EidTillit] and attribute release according to the attribute set “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01).

LoA-identifier: `http://id.elegnamnden.se/loa/1.0/loa4`

Attribute requirements: ELN-AP-Pnr-01 (`http://id.elegnamnden.se/ap/1.0/pnr-01`)

> Natural Personal Identity with Civic Registration Number (personnummer)

2.4. eidas-naturalperson

URL: `http://id.elegnamnden.se/ec/1.0/eidas-naturalperson`

Description: User authentication according to any of the eIDAS assurance levels and attribute release according to “eIDAS Natural Person Attribute Set” (ELN-AP-eIDAS-NatPer-01).

LoA-identifier: Not applicable

> It does not make sense to specify the level of assurance for a Service Entity Categories intended for eIDAS since this information is not known to the Swedish eIDAS-node.

Attribute requirements: ELN-AP-eIDAS-NatPer-01 (`http://id.elegnamnden.se/ap/1.0/eidas-natural-person-01`)

> eIDAS Natural Person Attribute Set

2.5. eidas-pnr-delivery

URL: `http://id.elegnamnden.se/ec/1.0/eidas-pnr-delivery`

Description: For asserting a Swedish identity to a foreign service provider via the Swedish eIDAS Proxy Service. This entity category MUST NOT be set by any entity other than Identity Provider providing identity assertions to the Swedish eIDAS Proxy Service and by the Swedish eIDAS Proxy Service itself.

Note that the Identity Providers release attributes according to the "Natural Personal Identity with Civic Registration Number" attribute set. It is the responsibility of the Swedish eIDAS Proxy Service to transform these attributes into eIDAS attributes.

LoA-identifier: Not applicable

> An Identity Provider delivering assertions to the eIDAS framework is obliged to announce which levels that it supports by including the corresponding eIDAS authentication context URIs defined in section 3.1.1 of [EidRegistry] as assurance certification attributes in its metadata as described in section 2.1.3 of [EidDeploy].

Attribute requirements: ELN-AP-Pnr-01 (`http://id.elegnamnden.se/ap/1.0/pnr-01`)

> Natural Personal Identity with Civic Registration Number (personnummer)

3. Definitions for Service Property Categories

A Service Property Entity Category identifier is specified as an attribute value in the entity category attribute in the federation metadata and has the purpose of representing a particular service property.

All Service Type identifiers are prefixed with `http://id.elegnamnden.se/sprop`.

3.1. mobile-auth

URL: `http://id.elegnamnden.se/sprop/1.0/mobile-auth`

Description: A service property declaring that the service is adapted to mobile clients and MUST allow users to authenticate using a mobile device that is used to access such service.

For a providing service, i.e. an Identity Provider, inclusion of the mobile-auth category states that the Identity Provider supports authentication using mobile devices, **and** that the end-user interface of the Identity Provider is adapted for mobile clients.

Note that an Identity Provider may of course support authentication for both desktop and mobile users. In these cases the service must be able to display end user interfaces for both types of clients.

A discovery process will use this Service Property when performing filtering of possible Identity Providers, as described in 1.4, “Use in Discovery”. This means that a consuming service may include the mobile-auth category in its metadata in order to have the discovery process especially displaying Identity Providers that offer authentication using mobile devices.

See [EidDiscovery] for a more extensive explanation of the use of the mobile-auth category.

4. Definitions for Service Type Entity Categories

A Service Type Entity Category identifier is specified as an entity attribute in the federation metadata and has the purpose of representing a particular service type.

All Service Type identifiers are prefixed with `http://id.elegnamnden.se/st`.

4.1. sigservice

URL: `http://id.elegnamnden.se/st/1.0/sigservice`

Description: A service type for a Service Provider that provides electronic signature services within the Swedish eID framework.

4.2. public-sector-sp

URL: `http://id.elegnamnden.se/st/1.0/public-sector-sp`

Description: A service type that indicates that an Service Provider is a "public sector" SP. This category MUST be used by public sector Service Providers wishing to use eIDAS authentication so that the Swedish eIDAS connector may include this information in the eIDAS authentication request.

4.3. private-sector-sp

URL: `http://id.elegnamnden.se/st/1.0/private-sector-sp`

Description: A service type that indicates that an Service Provider is a "private sector" SP. This category MUST be used by private sector Service Providers wishing to use eIDAS authentication so that the Swedish eIDAS connector may include this information in the eIDAS authentication request.

5. References

[RFC2119]

> Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997.

[SAML2Core]

> OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[SAML2Meta]

> OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[SAML2MetaAttr]

> OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009.

[EntCat]

> The Entity Category SAML Entity Metadata Attribute Type, March 2012.

[EidTillit]

> Tillitsramverk för Svensk e-legitimation.

[EidDeploy]

> Deployment Profile for the Swedish eID Framework.

[EidRegistry]

> Registry for identifiers assigned by the Swedish e-identification board.

[EidAttributes]

> Attribute Specification for the Swedish eID Framework.

6. Changes between versions

Changes between version 1.4 and version 1.5:

- Introduced the Service Entity Category “eidas-naturalperson” (section 2.4) for support of authentication against the eIDAS Framework.
- Introduced the Service Entity Category "eidas-pnr-delivery" (section 2.5) for use by Swedish Identity Providers delivering assertions to Service Providers within the eIDAS federation.
- Added the Service Type Entity Categories "public-sector-sp" and "private-sector-sp" to section 4.
- Minor changes regarding discovery.
- Updates to explanatory text in chapter 2 about usage of service entity categories.

Changes between version 1.3 and version 1.4:

- Version 1.3 of [Eid2Attributes] changed the terms “attribute profiles” to “attribute sets”. This specification has therefore been updated to reflect these changes.
- Chapter 1.5, “Representation of Entity Categories in Metadata”, was added to illustrate how entity categories are represented in metadata.
- Clarifications regarding the definition of Service Entity Categories were made to chapter 2.

Changes between version 1.2 and version 1.3:

- In chapter 1.4, “Use in Discovery Services”, the text that referred to the Discovery Service usage of Service Property Entity Categories when rendering user interfaces was removed.
- In chapter 3.1, “mobile-auth”, changes were made to reflect that the use of mobile-auth no longer governs which type of end user interface the Discovery Service should render.
- In chapter 2, “Definitions for Service Entity Categories”, URIs for attribute profiles were added in definitions of the service entity categories.

Changes between version 1.1 and version 1.2:

- In chapter 2, “Definitions for Service Entity Categories”, two new service entity categories have been defined, loa2-pnr and loa4-pnr.

Changes between version 1.0 and version 1.1:

- The service property category mobile-auth was added.
- Changes was made to chapter 1.4, “Use in Discovery Services”, where mobile-auth was referred.