Entity Categories for the Swedish eID Framework

Version 1.7 - 2020-01-09 - *Draft version*

ELN-0606-v1.7

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.*

Five types of Entity Categories are used within the federation:

- Service entity category – Identifiers for entity categories representing sets of requirements.
- Service property categories – Identifiers for defined service properties.
- Service type categories – Identifiers for defined service types.
- Service contract categories - Identifiers for labelling entities based on contracts or business agreements.
- General categories - Identifiers defined within the Swedish eID Framework for miscellaneous purposes.

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 service 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.
Service Contract	Each declared category represents a contract, or business agreement, that the service is affiliated to.	Represents the contracts, or business agreements, under which the providing service may deliver services.	At least one of the service contract identifiers declared by a providing service must be declared by the consuming service. A providing service that does not declare any service contract identifiers match all consuming services regarding service contract matching.
General	An entity category type for miscellaneous purposes.	An entity category type for miscellaneous purposes.	No general matching rule. However, the meaning of a general entity category may be such that it affects matching.

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, Service Contract 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, the following conditions apply;

- the Identity Provider declares at least of the Service Entity Category identifiers declared by the Service Provider,
- if the Identity Provider declares at least one Service Contract identifier, the Service Provider must declare at least one of declared identifiers, and,
- all of the Service Property identifiers declared by the Service Provider must be declared by the Identity 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.swedenconnect.se/contract/sc/1.0/eidas
        </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` or `http://id.swedenconnect.se/ec` (defined after Aug. 2018).

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. For contract- or business agreement requirements Service Contract Categories should be used.

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: A providing service that does not comply with any of the defined service entity categories may define its own service entity category identifier in order to utilize the entity category matching rules. Any service entity category identifier defined outside of this specification should use the prefix `http://id.swedenconnect.se/ec/<org>`, where `org` is the defining organization's identifier.

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).
>
> **Note**: The `http://id.elegnamnden.se/ap/1.0/pnr-01` attribute set includes the `personalIdentityNumber` attribute, which is defined to hold either a Swedish identity personal number (”personnummer”) defined in [SKV 704], or a Swedish coordination number (”samordningsnummer”) as defined in [SKV 707].
>
> However, since a Swedish coordination number (”samordningsnummer”) is not consistent with assurance level 3, the `personalIdentityNumber` attribute is only allowed to hold a Swedish personal identity number ("personnummer") if the scope of the `loa3-pnr` service entity category.

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)
>
> **Note**: See the restriction described in section 2.1, loa3-pnr.

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.

Attribute release is based on the "Natural Personal Identity with Civic Registration Number" attribute set with the addition of a mandatory `dateOfBirth`-attribute (`urn:oid:1.3.6.1.5.5.7.9.1`). The reason for the mandatory `dateOfBirth`-attribute is that this information is required by the eIDAS minimum dataset and therefore must be obtained by the receiving eIDAS Proxy Service. Date of birth can not always reliably be derived from the `personalIdentityNumber` attribute.

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)

- `dateOfBirth`-attribute (`urn:oid:1.3.6.1.5.5.7.9.1`).

2.6. loa3-hsaid

URL: `http://id.swedenconnect.se/ec/1.0/loa3-hsaid`

Description: User authentication according to assurance level 3 [EidTillit] and attribute release according to the attribute set “Natural Person Identity with HSA-ID” (DIGG-AP-HSAid-01).

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

Attribute requirements: DIGG-AP-HSAid-01 (`http://id.swedenconnect.se/ap/1.0/hsaid-01`)

> Natural Person Identity with HSA-ID.

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.

3.2. scal2

URL: `http://id.elegnamnden.se/sprop/1.0/scal2`

Description: A service property declaring that the service is adapted to support Sole Control Assurance Level 2 (SCAL2) in accordance with [SigSAP].

For a providing service, i.e. an Identity Provider, inclusion of the scal2 service property states that the Identity Provider will return a "SAD" in response to a `SADRequest` in an authentication requests from a signing service.

For consuming services, Signature Services MAY include this service property if all authentication requests from the particular Signature Service include a `SADRequest` extension. A Service Provider that is not declared as a Signature Service MUST NOT include this service property in its metadata.

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 a 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 a 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. Service Contract Categories

Service Contract Entity Category identifiers are indented for performing service matching based on contracts, or business agreements, between providing and consuming services.

All Service Contract identifiers are prefixed with `http://id.swedenconnect.se/contract/<org>`, where `org` is identifier for the defining organization.

The meaning of different contracts and business agreements are out of scope for this specification. Instead the federation operator, or other parties, may define identifiers suitable for representing how consuming and providing services should be matched based on their respective agreements.

6. General Entity Categories

An entity category of the General Entity Category type is a category that does not fit into any of the other category types regarding definitions and matching rules.

General category identifiers are prefixed with `http://id.swedenconnect.se/general-ec`.

6.1. secure-authenticator-binding

URL: `http://id.swedenconnect.se/general-ec/1.0/secure-authenticator-binding`

Description: Some authentication schemes use an authentication device (*authenticator*) that is external, i.e., not bound to the user agent. These types of authentication schemes may be vulnerable to certain types of phishing attacks where a fraudster who controls the user agent can trick, or persuade, the user to initiate an operation on the authentication device.

A typical example of the threat described above is where an Identity Provider implements an authentication scheme that uses a mobile app as the authenticator. In those cases the user normally enters some input (often the user identity) in the web browser (user agent) that is then used by the Identity Provider to initiate an authentication session against the app running on the user's mobile device. The problem here is that there is no way we can now that the person initiating the operation in the web browser by entering a user identity is the same person who opens, and performs the authentication in the app.

In order to prevent attacks of this type many authentication schemes offer alternative ways of initiating authentication (or signature) sessions, where some sort of binding between the user agent and the authentication device is performed. An good example of this is when Identity Providers prompt the user to scan a QR-code displayed in the web browser using the authentication app instead of prompting for the user identity. This effectively binds the user agent to the same physical location as the authentication device, and in practice makes the attacks described above impossible.

This profile defines the `http://id.swedenconnect.se/general-ec/1.0/secure-authenticator-binding` entity category to be declared by Service Providers that require that a secure authenticator binding is performed by the Identity Providers supporting this.

An Identity Provider that supports different methods of initiating authentication, or signature, operations, and where at least one of these methods is a "secure authenticator binding" SHOULD declare the `http://id.swedenconnect.se/general-ec/1.0/secure-authenticator-binding` entity category in its metadata.

An Identity Provider that has declared the `http://id.swedenconnect.se/general-ec/1.0/secure-authenticator-binding` category in its metadata MUST perform a secure authenticator binding for requests sent from Service Providers that have declared this entity category in their metadata entries.

7. 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]

> RFC8409 - The Entity Category Security Assertion Markup Language (SAML) Attribute Types, August 2018.

[SKV704]

> Skatteverket, SKV 704 Utgåva 8, Personnummer.

[SKV707]

> Skatteverket, SKV 707, Utgåva 2, Samordningsnummer.

[EidTillit]

> Tillitsramverk för Svensk e-legitimation, version 1.4.

[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.

[SigSAP]

> Signature Activation Protocol for Federated Signing.

8. Changes between versions

Changes between version 1.6 and version 1.7:

- A new entity category type, Service Contract, was added to section 5.
- The reference [EntCat] now refers to RFC-8409 instead of https://tools.ietf.org/html/draft-young-entity-category.
- Chapter 6, "General Entity Categories", introduced a general entity category type for miscellaneous purposes.
- Section 6.1, "secure-authenticator-binding", was added defining the `http://id.swedenconnect.se/general-ec/1.0/secure-authenticator-binding` entity category.

Changes between version 1.5 and version 1.6:

- The Service Property Category "scal2" was added to section 3.2.
- Section 2.5, "eidas-pnr-delivery", was updated to also require attribute release of the `dateOfBirth`-attribute.
- Section 2.1, "loa3-pnr", was updated with a restriction stating that the `personalIdentityNumber` only may contain a Swedish personal identity number ("personnummer") and not a coordination number ("samordningsnummer"), if attribute release is made in `loa3-pnr` scope.
- The loa3-hsaid Service Entity Category was defined in section 2.6.

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.