Entity Categories for the Swedish eID Framework

ELN-0606

Version 1.2

2014-04-22

1 Introduction 3

1.1 Requirements Notation 3

1.2 References to SAML 2.0 Standards and Profiles 3

1.3 Consuming and providing services 4

1.4 Use in Discovery Services 4

2 Definitions for Service Entity Categories 5

2.1 loa3-pnr 5

2.2 loa2-pnr 5

2.3 loa4-pnr 6

3 Definitions for Service Property Categories 7

3.1 mobile-auth 7

4 Definitions for Service Type Entity Categories 7

4.1 sigservice 7

5 References 8

6 Changes between versions 8

# 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](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html)]) for an <md:Extensions> element ([[SAML2Meta](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)]).

<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>

...

Example 1: The Entity Category **http://id.elegnamnden.se/ec/1.0/loa3-pnr** specified in the entity attributes for an 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.

## 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](http://www.ietf.org/rfc/rfc2119.txt)].

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.

## References to SAML 2.0 Standards and Profiles

When referring to elements from the SAML 2.0 core specification [[SAML2Core](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)], 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](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)].
* <mdattr:Element> – for elements defined in [[SAML2MetaAttr](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html)].

## 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 |

## Use in Discovery Services

Aside from the fact that declarations of Entity Categories in metadata serve as a contract between Service Providers and Identity Providers, there is another case where these categories are used. The Discovery Service for the federation makes use of the declared Entity Categories when performing filtering, i.e., when deciding which Identity Providers to present for the end-user when the Service Provider directs he or she to the Discovery Service. 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 Service should display Identity Providers as a possible 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.

The Discovery Service may also make use of Service Property Entity Categories when deciding how the user interface presented to the end user should be rendered. See 3.1, “mobile-auth”.

# Definitions for Service Entity Categories

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

Service entity category requirements may be a combination of the following types of requirements:

* Level of assurance (LoA) attributes as specified in [Eid2Registry].
* For a Service Provider the meaning is that only services conforming to the specified level are allowed to provide the Service Provider with assertions.
* For a service that is providing assertions, such as an Identity Provider, the meaning is that the service conforms to the given level of assurance.
* Attribute profiles as specified in [Eid2Attributes].
* For a Service Provider the meaning is that only services that implement the given attribute profile are allowed to issue assertions to the Service Provider.
* For an assertion providing service, such as an Identity Provider, the meaning is that the service implements the attribute profile, i.e., are capable of issuing assertions according to this profile.
* SAML attributes. Offers a way to extend the attribute profile with additionally required attributes (i.e., attributes that are not specified in an attribute profile).
* For a Service Provider the meaning is that these attributes are requested to be delivered in assertions received from the Identity Provider in the same way as if the Service Provider would have specified the same attributes as <md:RequestedAttribute> in its metadata entry.
* For an assertion providing service, such as an Identity Provider, the meaning is that it commits to include the specified attributes in the assertions being produced.

All Assertion Requirements identifiers are prefixed with “**http://id.elegnamnden.se/ec**”.

## loa3-pnr

|  |  |
| --- | --- |
| **URL** | http://id.elegnamnden.se/ec/1.0/loa3-pnr |
| **LoA-identifier** | http://id.elegnamnden.se/loa/1.0/loa3 |
| **Attribute profile identifier** | ELN-AP-Pnr-01 Natural Personal Identity with Civic Registration Number (personnummer) |
| **Attributes** | No additional attribute requirements. |
| **Description** | Users should be authenticated according to assurance level 3 according to [TillitRamv] and the issued SAML Assertion messages are defined by the attribute profile “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01). |

## loa2-pnr

|  |  |
| --- | --- |
| **URL** | http://id.elegnamnden.se/ec/1.0/loa2-pnr |
| **LoA-identifier** | <http://id.elegnamnden.se/loa/1.0/loa2> |
| **Attribute profile identifier** | ELN-AP-Pnr-01 Natural Personal Identity with Civic Registration Number (personnummer) |
| **Attributes** | No additional attribute requirements. |
| **Description** | Users should be authenticated according to assurance level 2 according to [TillitRamv] and the issued SAML Assertion messages are defined by the attribute profile “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01). |

## loa4-pnr

|  |  |
| --- | --- |
| **URL** | http://id.elegnamnden.se/ec/1.0/loa4-pnr |
| **LoA-identifier** | <http://id.elegnamnden.se/loa/1.0/loa4> |
| **Attribute profile identifier** | ELN-AP-Pnr-01 Natural Personal Identity with Civic Registration Number (personnummer) |
| **Attributes** | No additional attribute requirements. |
| **Description** | Users should be authenticated according to assurance level 4 according to [TillitRamv] and the issued SAML Assertion messages are defined by the attribute profile “Natural Personal Identity with Civic Registration Number (personnummer)” (ELN-AP-Pnr-01). |

# Definitions for Service Property Categories

A Service Property Entity Category identifier is specified as an entity 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**”.

## 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. |

The Discovery Service for the Swedish eID Framework also uses the mobile-auth Service Property when it decides how the user interface should be rendered. If this property is assigned to a Service Provider’s metadata entry the Discovery Service will assume that the Service Provider end user interface is adapted for mobile clients and will render the Discovery Service user interface accordingly.

Note that the Discovery Service also will use this Service Property when performing filtering of Identity Providers to display, as described in 1.4, “Use in Discovery Services”.

# 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**”.

## 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. |

# References

[RFC2119]

[Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997.](http://www.ietf.org/rfc/rfc2119.txt)

[SAML2Core]

[OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

[SAML2Meta]

[OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

[SAML2MetaAttr]

[OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009.](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html)

[EntCat]

[The Entity Category SAML Entity Metadata Attribute Type, March 2012.](http://macedir.org/entity-category/)

[EidTillit]

[Tillitsramverk för Svensk E-legitimation.](ELN-0700+-+Tillitsramverk+f%C3%B6r+Svensk+e-legitimation.pdf)

[Eid2Registry]

[Registry for identifiers assigned by the Swedish e-identification board.](ELN-0603+-+Bilaga+Tekniskt+ramverk+-+Registry_for_identifiers.pdf)

[Eid2Attributes]

[Attribute Specification for the Swedish eID Framework.](ELN-0604+-+Bilaga+Tekniskt+ramverk+-+Attribute+Specification+for+the+Swedish+eID+Framework.pdf)

# Changes between versions

**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.