



**E-LEGITIMATIONS
NÄMNDEN**

Registry for identifiers assigned by the Swedish e-identification board

Version 1.4 - 2017-03-28

ELN-0603-v1.4

Table of Contents

1. **Background**
2. **Structure**
 - 2.1. URI Identifiers
 - 2.2. OID Identifiers
3. **Assigned Identifiers**
 - 3.1. URL Identifiers
 - 3.1.1. Authentication Context URIs
 - 3.1.2. Attribute Sets
 - 3.1.3. Entity Category Identifiers
 - 3.1.3.1. Service Entity Categories
 - 3.1.3.2. Entity Categories for Service Properties
 - 3.1.3.3. Entity Categories for Service Type
 - 3.1.4. SAML Protocol Status Codes
 - 3.1.5. Central Signing
 - 3.1.6. Authentication Context
 - 3.1.7. Sign Response Status Codes
 - 3.2. OID Identifiers
 - 3.2.1. ASN.1 Declarations
4. **References**
5. **Changes between versions**

1. Background

The implementation of a Swedish infrastructure for electronic identification and electronic signature requires various types of identifiers to represent objects in protocols and data structures.

This document defines the structure for identifiers assigned by the Swedish e-identification board and provides a registry for assigned identifiers.

The following types of identifiers are assigned in this document:

- URI (Uniform Resource Identifier)
- OID (Object Identifier)

This registry is limited to registering assigned identifiers. Identifiers in this registry are typically defined within the context of a separate specification, which defines the semantic meaning of the identifier within the context of a particular protocol and/or data structure. Where applicable, this registry provides references to the documents where the exact meaning of each identifier is defined.

2. Structure

The basic structure of identifiers assigned by the Swedish e-identification board is based on the following components:

Parameter	Description
Prefix	The leading portion of the identifier that associates the identifier with this registry and identifies the Swedish e-identification board as the assigner of the identifier.
Category	A code for the category of an identifier. Each category is a defined context for a collection of identifiers within the scope of a protocol, service or object type.
Version (optional)	An indicator of the version of the object represented by this identifier. The exact semantic of the version indicator, if present, is defined within each category.
Identifier	A sequence of characters or numbers (according to the syntax of the identifier type), which distinguish this identifier among all other identifiers within a particular prefix, category and version.

2.1. URI Identifiers

All URI identifiers in this registry are of URL type (Uniform Resource Locator), assigned under the prefix `http://id.elegnamnden.se`.

These URL identifiers are defined using the following structure:

```
http://id.elegnamnden.se/{category}[/{version}]/{identifier}
```

2.2. OID Identifiers

An object identifier consists of a node in a hierarchically-assigned namespace, formally defined using the ITU-T's ASN.1 standard, X.690. Successive numbers of the nodes, starting at the root of the tree, identify each node in the tree. Designers set up new nodes by registering them under the node's registration authority. The root of the tree contains the following three arcs:

- 0: ITU-T
- 1: ISO
- 2: joint-iso-itu-t

Object identifiers are in this document represented as a string containing a sequence of integers separated by a dot (“.”), e.g. 2.3.4.25, where each integer represents a node in the hierarchy.

The node assigned to the Swedish e-identification board is: **1.2.752.201**.

This represents a hierarchical structure of nodes in the following sequence:

- 1 = ISO
- 2 = ISO member body
- 752 = The Swedish Standardization Institute (SIS-ITS)
- 201 = Swedish e-identification board

This node is used as the Prefix (root node) for all OID identifiers in this registry, using the following structure:

1.2.752.201.{category}.{identifier}

OID identifiers according to this structure assign a node for each category and an identifier node under this category node. No node in this structure is assigned as version node. Version is handled, when necessary, within the identifier portion of the OID, typically by assigning a new identifier.

3. Assigned Identifiers

3.1. URL Identifiers

The following category codes are defined:

Code	Category
loa	Level of Assurance. Identifiers representing level of assurance for federated identity (Tillitsnivå).
ac	Attribute profile.
ec	Entity Category. Generic service type declarations for service matching.
sprop	Service Property. Specific entity category identifiers for specific service property.
st	Service Type. Specific entity category identifiers for defined types of services in the federation.
csig	Central Signing Service – Identifiers used by the central signing service infrastructure.
auth-cont	Authentication context information schema.
status	SAML Protocol status codes.
sig-status	Sign response status codes.
ns	XML Schema namespaces.

3.1.1. Authentication Context URIs

Authentication Context URIs representing assurance levels (Tillitsnivåer) according to the assurance framework for the Swedish eID Framework (Tillitsramverket för Svensk e-legitimation).

URL	Object	Reference
http://id.elegnamnden.se/loa/1.0/loa1	Assurance level 1	[TillitRamv]
http://id.elegnamnden.se/loa/1.0/loa2	Assurance level 2	[TillitRamv]
http://id.elegnamnden.se/loa/1.0/loa3	Assurance level 3	[TillitRamv]
http://id.elegnamnden.se/loa/1.0/loa4	Assurance level 4	[TillitRamv]
http://id.elegnamnden.se/loa/1.0/eidas-low	Authentication accordance to eIDAS assurance level low	[eIDAS]
http://id.elegnamnden.se/loa/1.0/eidas-sub	Authentication accordance to eIDAS assurance level substantial	[eIDAS]
http://id.elegnamnden.se/loa/1.0/eidas-high	Authentication accordance to eIDAS assurance level high	[eIDAS]
http://id.elegnamnden.se/loa/1.0/eidas-nf-sub	Authentication accordance to eIDAS assurance level substantial using an eID scheme that MUST be notified	[eIDAS]
http://id.elegnamnden.se/loa/1.0/eidas-nf-high	Authentication accordance to eIDAS assurance level high using an eID scheme that MUST be notified	[eIDAS]

NOTE: eIDAS assurance levels low, substantial and high have the following AuthnContextClassRef URI:s defined by the EU commission:

- <http://eidas.europa.eu/LoA/low>
- <http://eidas.europa.eu/LoA/substantial>
- <http://eidas.europa.eu/LoA/high>

The eIDAS technical specifications are currently unclear regarding how to specify requirements for notified eID and how to communicate to a Service Provider whether a notified eID was used. The URI:s defined above for eIDAS assurance level low, substantial and high are equivalent to the commission defined URI:s but adds specifically defined rules for notified eID.

For example, the URI <http://id.elegnamnden.se/loa/1.0/eidas-sub> is valid for eIDAS assurance level substantial for both notified and non notified eIDs, while <http://id.elegnamnden.se/loa/1.0/eidas-nf-sub> is only valid for eIDAS assurance level substantial if the eID used to authenticate the user is notified according to the eIDAS regulation.

Authentication Context URIs extending the above URIs with specific meaning for use with authentication requests that includes a sign message that must be displayed to the user (see section 7 of [DeployProf]).

URL	Object	Reference
http://id.elegnamnden.se/loa/1.0/loa2-sigmessage	Authentication according to assurance level 2 with extended requirements for displaying signature messages.	[DeployProf]
http://id.elegnamnden.se/loa/1.0/loa3-sigmessage	Authentication according to assurance level 3 with extended requirements for displaying signature messages.	[DeployProf]
http://id.elegnamnden.se/loa/1.0/loa4-sigmessage	Authentication according to assurance level 4 with extended requirements for displaying signature messages.	[DeployProf]
http://id.elegnamnden.se/loa/1.0/eidas-low-sigm	Authentication accordance to eIDAS assurance level low with extended requirements for displaying signature messages.	[DeployProf]
http://id.elegnamnden.se/loa/1.0/eidas-sub-sigm	Authentication accordance to eIDAS assurance level substantial with extended requirements for displaying signature messages.	[DeployProf]
http://id.elegnamnden.se/loa/1.0/eidas-high-sigm	Authentication accordance to eIDAS assurance level high with extended requirements for displaying signature messages.	[DeployProf]
http://id.elegnamnden.se/loa/1.0/eidas-nf-sub-sigm	Authentication accordance to eIDAS assurance level substantial using an eID scheme that MUST be notified, with extended requirements for displaying signature messages.	[DeployProf]
http://id.elegnamnden.se/loa/1.0/eidas-nf-high-sigm	Authentication accordance to eIDAS assurance level high with an eID scheme that MUST be notified, with extended requirements for displaying signature messages.	[DeployProf]

3.1.2. Attribute Sets

Identifiers for attribute sets defined in the Attribute Profile Specification for the Swedish eID Framework.

Identifier	URL	Object	Reference
ELN-AP-Pseudonym-01	http://id.elegnamnden.se/ap/1.0/pseudonym-01	Pseudonym identity attribute set.	[AttrProf]
ELN-AP-NaturalPerson-01	http://id.elegnamnden.se/ap/1.0/natural-person-01	Personal identity without civic registration number attribute set.	[AttrProf]
ELN-AP-Pnr-01	http://id.elegnamnden.se/ap/1.0/pnr-01	Personal identity with civic registration number attribute set.	[AttrProf]
ELN-AP-OrgPerson-01	http://id.elegnamnden.se/ap/1.0/org-person-01	Organizational identity attribute set.	[AttrProf]
ELN-AP-eIDAS-NatPer-01	http://id.elegnamnden.se/ap/1.0/eidas-natural-person-01	Natural person identity for the eIDAS Framework.	[AttrProf]

3.1.3. Entity Category Identifiers

Identifiers for categories of service entities, specified as an “Entity Attribute” in the federation metadata.

3.1.3.1. Service Entity Categories

Identifiers for entity categories representing alternative sets of requirements.

URL	Object	Reference
http://id.elegnamnden.se/ec/1.0/loa2-pnr	Service consuming/providing assertions based on assurance level 2, implementing the attribute set "ELN-AP-Pnr-01".	[EntityCat]
http://id.elegnamnden.se/ec/1.0/loa3-pnr	Service consuming/providing assertions based on assurance level 3, implementing the attribute set "ELN-AP-Pnr-01".	[EntityCat]

URL	Object	Reference
http://id.elegnamnden.se/ec/1.0/loa4-pnr	Service consuming/providing assertions based on assurance level 4, implementing the attribute set "ELN-AP-Pnr-01".	[EntityCat]
http://id.elegnamnden.se/ec/1.0/eidas-naturalperson	Service consuming/providing assertions based on any eIDAS assurance level, implementing the attribute set "ELN-AP-eIDAS-NatPer-01".	[EntityCat]
http://id.elegnamnden.se/ec/1.0/eidas-pnr-delivery	Service providing assertions to eIDAS services via Swedish eIDAS-node	[EntityCat]

3.1.3.2. Entity Categories for Service Properties

Identifiers for defined service properties.

URL	Object	Reference
http://id.elegnamnden.se/sprop/1.0/mobile-auth	Service adapted to require/provide user authentication based on mobile devices.	[EntityCat]

3.1.3.3. Entity Categories for Service Type

Identifiers for defined service types.

URL	Object	Reference
http://id.elegnamnden.se/st/1.0/sigservice	Electronic signature service	[EntityCat]
http://id.elegnamnden.se/st/1.0/public-sector-sp	Public sector Service Provider	[EntityCat]
http://id.elegnamnden.se/st/1.0/private-sector-sp	Private sector Service Provider	[EntityCat]

3.1.4. SAML Protocol Status Codes

Status code identifiers for use in SAML Response messages. The list below extends the list of second-level status codes defined in section 3.2.2.2 of [SAML2Core].

URL	Object	Reference
http://id.elegnamnden.se/status/1.0/cancel	Status code representing a cancelled operation.	[DeployProf]
http://id.elegnamnden.se/status/1.0/fraud	Status code indicating a fraudulent request.	[DeployProf]
http://id.elegnamnden.se/status/1.0/possibleFraud	Status code indicating a possible fraudulent request.	[DeployProf]

3.1.5. Central Signing

Identifiers used in the protocol for requesting services form a central signing service.

URL	Object	Reference
http://id.elegnamnden.se/csig/1.0/dss-ext/ns	Deprecated. XML schema name space for the protocol extensions to the OASIS DSS protocol (version 1.0).	
http://id.elegnamnden.se/csig/1.0/eid2-dss/profile	Deprecated. Implementation profile identifier for the protocol extensions to the OASIS DSS protocol (version 1.0).	
http://id.elegnamnden.se/csig/1.1/dss-ext/ns	XML schema name space for the protocol extensions to the OASIS DSS protocol (version 1.1).	[CSignProt]
http://id.elegnamnden.se/csig/1.1/dss-ext/profile	Implementation profile identifier for the protocol extensions to the OASIS DSS protocol (version 1.1).	[CSignProf]

3.1.6. Authentication Context

Identifiers associated with the Authentication Context X.509 extension

URL	Object	Reference
http://id.elegnamnden.se/auth-cont/1.0/saci	XML schema name space for SAML Authentication Context Information in the Authentication Context X.509 certificate extension	[AuthContExt]

3.1.7. Sign Response Status Codes

Status code identifiers for the DSS Extension for SAML based Central Signing service. The following identifiers provide defined status codes for inclusion in a <ResultMinor> element of the <Result> element of a sign response message according to the OASIS standard “Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0”.

URL	Object	Reference
http://id.elegnamnden.se/sig-status/1.0/req-expired	The time window for the signature request has expired.	[CSignProf]
http://id.elegnamnden.se/sig-status/1.0/user-mismatch	The authenticated user does not match the signer identity attributes in the request.	[CSignProf]
http://id.elegnamnden.se/sig-status/1.0/unsupported-loa	The requested level of assurance for user authentication is not supported.	[CSignProf]
http://id.elegnamnden.se/sig-status/1.0/sigmessage-error	A requirement to display sign message was included in the sign request, but the sign service could not establish that the sign message was displayed to the user.	[CSignProf]
http://id.elegnamnden.se/sig-status/1.0/user-cancel	The end user cancelled the signature operation.	[CSignProf]

3.2. OID Identifiers

Defined categories:

Code	Category
------	----------

Code	Category
0	ASN.1 modules
1	Test identifiers
2	Policy identifiers
3	Attribute identifiers
4	"Qualified Certificate" Statement identifiers (RFC 3739)
5	X.509 certificate extension identifiers

The following OIDs are defined in the ASN.1 declarations in [3.2.1](#):

OID	Object	Reference
1.2.752.201.5.1	Authentication Context extension	[AuthContExt]
1.2.752.201.3.1	Organization Affiliation Attribute	[AttrProf]
1.2.752.201.3.2	Transaction Identifier	[AttrProf]
1.2.752.201.3.3	Authentication Context Parameters	[AttrProf]
1.2.752.201.3.4	Provisional ID	[AttrProf]
1.2.752.201.3.5	Provisional ID Persistence Indicator	[AttrProf]
1.2.752.201.3.6	Personal Identity Number Binding URI	[AttrProf]
1.2.752.201.3.7	eIDAS Person Identifier	[AttrProf]
1.2.752.201.3.8	Birth name	[AttrProf]

OID	Object	Reference
1.2.752.201.3.9	eIDAS Natural Person Address	[AttrProf]
1.2.752.201.3.10	User Certificate	[AttrProf]
1.2.752.201.3.11	User Signature	[AttrProf]
1.2.752.201.3.12	Signature Activation Data	[AttrProf]
1.2.752.201.3.13	Authentication Server Signature	[AttrProf]

3.2.1. ASN.1 Declarations

```

-- Object Identifier Registry for the Swedish E-identification board

id-eleg OBJECT IDENTIFIER ::= {iso(1) member-body(2) se(752) e-legitimationsnamnden(201)}

-- E-legnamnden arcs
id-mod  OBJECT IDENTIFIER ::= { id-eleg 0 }  -- ASN.1 modules
id-test OBJECT IDENTIFIER ::= { id-eleg 1 }  -- OIDs for test
id-pol  OBJECT IDENTIFIER ::= { id-eleg 2 }  -- Policy
id-attr OBJECT IDENTIFIER ::= { id-eleg 3 }  -- Attributes
id-qcs  OBJECT IDENTIFIER ::= { id-eleg 4 }  -- QC Statement
id-ce   OBJECT IDENTIFIER ::= { id-eleg 5 }  -- Cert Extensions

-- E-legnamnden modules

id-mod-qcAuthContext OBJECT IDENTIFIER ::= { id-mod 1 }

-- E-legnamnden OIDs for test

-- E-legnamnden Policy

-- E-legnamnden Attributes
id-attr-org-affiliation OBJECT IDENTIFIER ::= { id-attr 1 }  -- Organizational affiliation
id-attr-transaction-id  OBJECT IDENTIFIER ::= { id-attr 2 }  -- Transaction identifier

```

```
id-attr-auth-context-params OBJECT IDENTIFIER ::= { id-attr 3 } -- Authentication context parameters
id-attr-prid                OBJECT IDENTIFIER ::= { id-attr 4 } -- Provisional ID
id-attr-prid-persistence   OBJECT IDENTIFIER ::= { id-attr 5 } -- Provisional ID persistence indicator
id-attr-pnr-binding        OBJECT IDENTIFIER ::= { id-attr 6 } -- Personal Identity Number binding URI
id-attr-eidas-pid          OBJECT IDENTIFIER ::= { id-attr 7 } -- eIDAS Person Identifier
id-attr-birth-name         OBJECT IDENTIFIER ::= { id-attr 8 } -- Birth name
id-attr-eidas-np-address   OBJECT IDENTIFIER ::= { id-attr 9 } -- eIDAS Natural Person Address
id-attr-user-certificate   OBJECT IDENTIFIER ::= { id-attr 10 } -- User certificate
id-attr-user-signature     OBJECT IDENTIFIER ::= { id-attr 11 } -- User signature
id-attr-sad                OBJECT IDENTIFIER ::= { id-attr 12 } -- Signature activation data
id-attr-auth-srv-signature OBJECT IDENTIFIER ::= { id-attr 13 } -- Authentication server signature

-- E-legnamnden QC Statement extension
id-qcs-sid                 OBJECT IDENTIFIER ::= { id-qcs 1 } -- Semantics Identifiers
id-qcs-statement          OBJECT IDENTIFIER ::= { id-qcs 2 } -- QC statements

-- E-legnamnden Certificate Extensions
id-ce-authContext         OBJECT IDENTIFIER ::= { id-ce 1 }
```

4. References

[SAML2Core]

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

[OASIS-DSS]

[Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0.](#)

[TillitRamv]

[Tillitsramverk för Svensk e-legitimation.](#)

[AuthContExt]

[RFC 7773: Authentication Context Certificate Extension.](#)

[DeployProf]

[Deployment Profile for the Swedish eID Framework.](#)

[EntityCat]

[Entity Categories for the Swedish eID Framework.](#)

[CSignProt]

[DSS Extension for Federated Central Signing Services.](#)

[CSignProf]

[Implementation Profile for Using OASIS DSS in Central Signing Services.](#)

[AttrProf]

[Attribute Specification for the Swedish eID Framework.](#)

[eIDAS]

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Including implementation acts of the regulation and associated technical specifications.

5. Changes between versions

Changes between version 1.3 and version 1.4:

- Attributes and URI:s for the eIDAS Framework was added.
- The SAML status code identifier <http://id.elegnamnden.se/status/1.0/cancel> was added to be used in SAML Response messages to indicate a cancelled operation.
- Added the SAML status code identifiers <http://id.elegnamnden.se/status/1.0/fraud> and <http://id.elegnamnden.se/status/1.0/possibleFraud> were added to be used in SAML Response messages to alert fraudulent requests.
- Added attribute definitions for “Birth name”, “User certificate”, “User signature”, “Authentication Server Signature” and “Signature activation data”. See chapter 3.2.
- Added the Service Type Entity Categories <http://id.elegnamnden.se/st/1.0/public-sector-sp> and <http://id.elegnamnden.se/st/1.0/private-sector-sp> to section 3.1.3.3.

Changes between version 1.2 and version 1.3:

- Object identifiers for the attributes “Transaction identifier”, “Authentication Context Parameters”, “Provisional ID” and “Provisional ID quality indicator” were defined and added to section 3.2.
- Chapter 3.1.7, “XML Schema namespaces”, was removed since the “Level of Assurance context class declarations” are deprecated and thus, the namespace <http://id.elegnamnden.se/ns/1.0/loa-context-params> is no longer part of the Swedish eID Framework.
- Authentication Context URIs for use by signature services during authentication was added to section 3.1.1.
- Service entity categories for future use within the eIDAS Framework were added to section 3.1.3.1.
- The status code identifier <http://id.elegnamnden.se/sig-status/1.0/sigmessage-error> was added to section 3.1.6 and the signature response status code <http://id.elegnamnden.se/sig-status/1.0/user-cancel> was added to section 3.1.7.

Changes between version 1.1 and version 1.2:

- URI identifiers for Attribute Profiles as specified in [AttrProf] were introduced.

Changes between version 1.0 and version 1.1:

- In chapter 3.1.3.1, “Service Entity Categories”, service entity categories for Level of Assurance 2 and 4 were introduced.
- Chapter 3.1.7, “XML Schema namespaces”, was added.
- Typos were fixed.