



Attribute Specification for the Swedish eID Framework

ELN-0604-v1.4
Version 1.4
2016-08-30



1	INTRODUCTION	3
1.1	TERMINOLOGY	3
1.2	REQUIREMENT KEY WORDS	3
1.3	NAME SPACE REFERENCES	3
1.4	STRUCTURE	3
2	ATTRIBUTE SETS	4
2.1	PSEUDONYM IDENTITY	4
2.2	NATURAL PERSONAL IDENTITY WITHOUT CIVIC REGISTRATION NUMBER	4
2.3	NATURAL PERSONAL IDENTITY WITH CIVIC REGISTRATION NUMBER (PERSONNUMMER)	5
2.4	ORGANIZATIONAL IDENTITY FOR NATURAL PERSONS	5
2.5	EIDAS NATURAL PERSON ATTRIBUTE SET	5
2.6	EIDAS LEGAL PERSON ATTRIBUTE SET	6
3	ATTRIBUTE DEFINITIONS	7
3.1	ATTRIBUTES	7
3.2	SAML ATTRIBUTE FORMAT	8
3.2.1	THE AUTHCONTEXTPARAMS ATTRIBUTE	9
3.3	ATTRIBUTES FOR THE EIDAS FRAMEWORK	9
3.3.1	THE PRID AND PRIDPERSISTENCE ATTRIBUTE	9
3.3.2	THE PERSONALIDENTITYNUMBERBINDING ATTRIBUTE	10
4	REFERENCES	11
5	CHANGES BETWEEN VERSIONS	12

Draft



1 Introduction

This document specifies an attribute profile for the Swedish eID Framework. The attribute profile defines attributes for use within the Swedish eID Framework, and a number of defined attribute sets that may be referenced by other documents as means to specify specific attribute release requirements.

1.1 Terminology

Term	Defined meaning
Attribute	A property, quality or characteristic of a person, thing or object. This term is used in general in this specification to denote an attribute of a person/entity that is represented by a set of attributes in a SAML attribute statement (see SAML Attribute). This term is also used in this specification when describing XML syntax to denote an attribute (property) of an XML element.
SAML attribute	An attribute of an entity represented by a set of attributes in a SAML attribute statement (<saml:AttributeStatement> element).
IDP	Identity Provider
SP	Service Provider
Natural person	Natural person is legal term for a real human being, as opposed to a legal person, which may be a private (i.e., business entity) or public (i.e., government) organization.
Civic registration number	A unique identifier assigned to each natural person in a national population register. Within the context of this specification this is a Swedish "personnummer" or "samordningsnummer" according to [SKV704] and [SKV707].

1.2 Requirement key words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119].

These keywords are capitalized when used to unambiguously specify requirements over protocol features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.3 Name space references

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

Prefix	XML Namespace	Comments
saml	urn:oasis:names:tc:SAML:2.0:assertion	The SAML V2.0 assertion namespace, defined in the schema [SAML-XSD].
xs	http://www.w3.org/2001/XMLSchema	The XML Schema namespace, representing definitions of data types in [XML-Schema]

1.4 Structure

This specification uses the following typographical conventions in text: <ns:Element>, Attribute, **Datatype**, OtherCode.



2 Attribute Sets

This section defines attribute sets based on attribute definitions in section 3. Common to all attribute sets is that each attribute **MUST NOT** be present more than once. An attribute that has more than one value **MUST** be provided as one attribute with multiple `<AttributeValue>` sub-elements in accordance with section 3.1.

An identifier, named “Attribute Set Identifier”, and an URI, are defined for each attribute set as means for other documents to reference specific attribute sets.

Each attribute set defines a number of mandatory attributes that **MUST** be released by an Attribute Provider¹ that provides attributes according to the given attribute set, and optionally recommended attributes that **SHOULD** be released as part of the attribute set if they are available to the provider.

In order to comply with a defined attribute set, the following attribute requirements apply:

Attribute requirement	Definition
REQUIRED	Attributes that MUST be present.
RECOMMENDED	Attributes that SHOULD be present, if available.
POSSIBLE	Attributes that MAY be present, if available.

A defined attribute set does not define any rules for attributes other than those listed as required or recommended.

2.1 Pseudonym Identity

Attribute set identifier: **ELN-AP-Pseudonym-01**
URI: <http://id.elegnamnden.se/ap/1.0/pseudonym-01>

This attribute set specifies the condition where there are no mandatory or recommended attributes.

Typical use: In a pseudonym attribute release policy that just provides a persistent `NameID` identifier in the assertion but no attributes.

2.2 Natural Personal Identity without Civic Registration Number

Attribute set identifier: **ELN-AP-NaturalPerson-01**
URI: <http://id.elegnamnden.se/ap/1.0/natural-person-01>

The “Personal Identity without Civic Registration Number” attribute set provides basic natural person information without revealing the civic registration number of the subject.

Attribute requirement	Attributes
REQUIRED	<code>sn</code> (Surname) <code>givenName</code> (Given name) <code>displayName</code> (Display name)

Typical use: In an attribute release policy that provides basic user name information together with a persistent `NameID` identifier in the assertion.

¹ An Attribute Provider is an entity that releases attributes to a requesting entity. In all practical cases within the Swedish eID Framework this entity is an Identity Provider or an Attribute Authority. Within the eIDAS Framework, the Swedish eIDAS node acts as the Attribute Provider for the Service Providers.

2.3 Natural Personal Identity with Civic Registration Number (Personnummer)

Attribute set identifier: **ELN-AP-Pnr-01**

URI: <http://id.elegnamnden.se/ap/1.0/pnr-01>

The “Personal Identity with Civic Registration Number” attribute set provides basic personal identity information including a Swedish civic registration number of the subject.

Attribute requirement	Attributes
REQUIRED	sn (Surname) givenName (Given name) displayName (Display name) personalIdentityNumber (National civic registration number)

Typical use: In an attribute release policy that provides basic user name information together with the person’s Swedish civic registration number.

2.4 Organizational Identity for Natural Persons

Attribute set identifier: **ELN-AP-OrgPerson-01**

URI: <http://id.elegnamnden.se/ap/1.0/org-person-01>

The “Organizational Identity for Natural Persons” attribute set provides basic organizational identity information about a person. The organizational identity does not necessarily imply that the subject has any particular relationship with or standing within the organization, but rather that this identity has been issued/provided by that organization for any particular reason (employee, customer, consultant, etc.)

Attribute requirement	Attributes
REQUIRED	sn (Surname) givenName (Given name) displayName (Display name) orgAffiliation (Personal identifier and organizational identifier code) o (Organization name)
RECOMMENDED	organizationIdentifier (Organizational identifier code) ou (Organizational unit name)

Typical use: In an attribute release policy that provides basic organizational identity information about a natural person.

2.5 eIDAS Natural Person Attribute Set

Attribute set identifier: **ELN-AP-eIDAS-NatPer-01**

URI: <http://id.elegnamnden.se/ap/1.0/eidas-natural-person-01>

The “eIDAS Natural Person Attribute Set” provides personal identity information for a subject that has been authenticated via the eIDAS Framework.

Attribute requirement	Attributes
REQUIRED	prId (Provisional ID) prIdPersistence (Provisional ID persistence indicator) eidasPersonIdentifier (Mapping of the eIDAS PersonIdentifier attribute)



	<p>dateOfBirth (Date of birth) sn (Surname) givenName (Given name)</p> <p>And: eIDAS mandatory attributes for Natural Persons according to section 2.2.1 of the [eIDAS_Attr] specification.</p>
POSSIBLE	<p>personalIdentityNumber (National civic registration number) personalIdentityNumberBinding (National civic registration number Binding URI)</p> <p>And: eIDAS optional attributes for Natural Persons according to section 2.2.1 of the [eIDAS_Attr] specification and any other attributes delivered from the member state node to the Swedish eIDAS connector.</p>

Typical use: In an attribute release policy implemented by an eIDAS connector that provides a complete set of attributes to a requesting Service Provider.

Note: The `personalIdentityNumber` and `personalIdentityNumberBinding` attributes will be part of the attribute release if the issuer has access to enough information to provide a reliable binding between eIDAS attributes and an Swedish identity number (see section 3.3.2).

The eIDAS attribute set comprises of attributes of different categories:

- **Added attributes.** Attributes that are not provided by the member state node, but added by the Swedish eIDAS connector in order to provide additional information about the authenticated subject obtained from relevant domestic attribute sources. The `prid`, `pridPersistence` and `personalIdentityNumber` attributes are “added attributes”.
- **Converted attributes.** Attributes that are converted to attribute definitions according to the Swedish eID Framework (see section 3 below) in order to facilitate the processing for attribute consumers². The `eidasPersonIdentifier`, `sn`, `givenName` and `dateOfBirth` attributes are “converted attributes” (meaning that they have a different representation when released from the Identity Provider that performed the actual authentication).
- **Original attributes.** The attributes that are released according to the eIDAS Framework by the member state eIDAS node. These are delivered “as is”.
- **Additional attributes.** Any other attributes³ delivered by the member state node.

For an attribute consumer compliant with the Swedish eID Framework it should be sufficient to only process “added” and “converted” attributes.

2.6 eIDAS Legal Person Attribute Set

To be defined.

² The attributes specified within eIDAS ([eIDAS_Attr]) are not simple string types. Instead each attribute is represented using its own dedicated XML data type. This affects interoperability in a negative way since most standard SAML software need to be modified to support these attributes. Therefore, the Swedish eID Framework will offer mappings for all (mandatory) eIDAS attributes where they are represented as XML strings.

³ That is, attributes that are not defined by the eIDAS attribute specification.



3 Attribute Definitions

3.1 Attributes

The following attributes are defined for use within the attribute profile for the Swedish eID Framework:

Attribute abbreviation	SAML attribute name	Description	Use within this specification	Multi-valued	Example
sn	urn:oid:2.5.4.4	Surname	Registered surname.	NO	Lindeman
givenName	urn:oid:2.5.4.42	Given Name	Registered given name.	NO	Valfrid
displayName	urn:oid:2.16.840.1.113730.3.1.241	Display Name	A name in any preferred presentation format.	NO	Valfrid Lindeman
gender	urn:oid:1.3.6.1.5.5.7.9.3	Gender	A one letter representation ("M"/"F" or "m"/"f") representing the subject's gender in accordance with [RFC3739]	NO	M
personalIdentityNumber	urn:oid:1.2.752.29.4.13	National civic registration number/code	Swedish "personnummer" or "samordningsnummer" according to SKV 704 and SKV 707. 12 digits without hyphen.	NO	195006262546
dateOfBirth	urn:oid:1.3.6.1.5.5.7.9.1	Date of birth	Date of birth expressed using the datatype xs:date	NO	1950-06-26
street	urn:oid:2.5.4.9	Street address	Street address.	NO	Mosebacke torg 3
postOfficeBox	urn:oid:2.5.4.18	Post box	Post box.	NO	Box 1122
postalCode	urn:oid:2.5.4.17	Postal code	Postal code.	NO	11826
l	urn:oid:2.5.4.7	Locality	Locality.	NO	Stockholm
c	urn:oid:2.5.4.6	Country	ISO 3166-1 alpha-2 [ISO3166] two letter country code.	NO	SE
placeOfBirth	urn:oid:1.3.6.1.5.5.7.9.2	Place of birth	A string representing the place of birth	NO	Stockholm
countryOfCitizenship	urn:oid:1.3.6.1.5.5.7.9.4	Country of citizenship	ISO 3166-1 alpha-2 [ISO3166] two letter country code representing a country of citizenship.	YES	SE
countryOfResidence	urn:oid:1.3.6.1.5.5.7.9.5	Country of Residence	ISO 3166-1 alpha-2 [ISO3166] two letter country code representing the country of residence.	NO	SE
telephoneNumber	urn:oid:2.5.4.20	Telephone number	Telephone number.	YES	+46890510
mobile	urn:oid:0.9.2342.19200300.100.1.41	Mobile number	Mobile number.	YES	+46703419886
mail	urn:oid:0.9.2342.19200300.100.1.3	E-mail address	E-mail address.	YES	vfl@mosebackemonarki.se
o	urn:oid:2.5.4.10	Organization name	Registered organization name.	NO	Skatteverket
ou	urn:oid:2.5.4.11	Organizational unit name	Organizational unit name.	YES	IT-Avdelningen
organizationIdentifier	urn:oid:2.5.4.97	Organizational identifier code	Swedish "organisationsnummer" according to SKV 709. 10 digits without hyphen.	NO	5562265719
orgAffiliation	urn:oid:1.2.752.201.3.1	<uid>@<orgnr>	Personal ID @ Swedish "organisationsnummer" according to SKV 709. 10 digits without hyphen.	YES	vblindman@5562265719
transactionIdentifier	urn:oid:1.2.752.201.3.2	Transaction identifier	Transaction identifier for an event, e.g. an authentication process.	NO	9878HJ6687 (arbitrary string)
authContextParams	urn:oid:1.2.752.201.3.3	Authentication Context Parameters.	Key-value pairs from an authentication process. Defined by issuing entity.	NO	See section 3.2.1 below.



prid	urn:oid:1.2.752.201.3.4	Provisional identifier	Unique identifier for an authentication performed against the eIDAS Framework. See section 3.3.1 below.	NO	NO:5068907693
pridPersistence	urn:oid:1.2.752.201.3.5	Provisional identifier persistence indicator	Indicator for the expected persistence of the prid attribute. See section 3.3.1 below.	NO	A
personalIdentityNumber Binding	urn:oid: 1.2.752.201.3.6	National civic registration number/code binding URI	The type of binding performed of personalIdentityNumber attribute added by eIDAS connector. See section 3.3.2 below.	NO	http://eid.org.se/presentedInPerson
eidasPersonIdentifier	urn:oid: 1.2.752.201.3.7	eIDAS uniqueness identifier for natural persons	Maps the eIDAS PersonIdentifier attribute to a string attribute within the scope of the Swedish eID Framework attribute set.	NO	ES/AT/02635542Y (Spanish eIDNumber for an Austrian SP)

All attributes, unless stated otherwise in this table, holds string values using the UTF-8 character set using the `xs:string` data type. Certain attributes such as `mail`, `personalIdentityNumber`, `organizationIdentifier`, `telephoneNumber` and `mobile` use a restricted character set according to its defined usage within this specification.

All attributes use the “caseIgnoreMatch” matching rule as defined by X.520 [X.520]. That is, case-insensitive comparison where insignificant spaces are ignored.

Attributes with a “NO” value in the multivalued column MUST NOT have more than one `<AttributeValue>` sub-element. Attributes with a “YES” value in the multivalued column MAY have one or more `<AttributeValue>` sub-elements.

3.2 SAML Attribute Format

The `<saml:Attribute>` element representing an attribute in 3.1 SHALL comply with the following requirements:

- The `NameFormat` attribute SHALL have the value "urn:oasis:names:tc:SAML:2.0:attrname-format:uri".
- The `Name` attribute SHALL hold a URI according to the table in section 3.1.
- The `FriendlyName` attribute is OPTIONAL.
- All `<AttributeValue>` sub-elements SHALL, unless stated otherwise in the table in section 3.1, have an `xsi:type` attribute specifying the type "xs:string".

The following is an example of the surname attribute. Its name is “urn:oid:2.5.4.4”, its friendly name is “sn” and the value is represented using a string type.

```
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  FriendlyName="sn"
  Name="urn:oid:2.5.4.4"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xsi:type="xs:string">Eriksson</saml2:AttributeValue>
</saml2:Attribute>
```




3.2.1 The `authContextParams` Attribute

The attribute `authContextParams` holds key-value pairs. Its purpose is to store key-value pairs representing data from an authentication process. The data stored in this attribute is generally not defined by the Swedish eID Framework, but instead by the issuing party (i.e., the Identity Provider).

The `authContextParams` attribute is a non-empty single-value attribute where the attribute value contains the key-value pairs separated by semicolons. The key and value of each pair is separated by a '=' character and both the key and value MUST be URL-encoded.

Below follows an example of how the `authContextParams` attribute is populated with two key-value pairs, `foo` that stores the value "ÄÖ", and `bar` that stores the value "123".

```
...  
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
    FriendlyName="authContextParams"  
    Name="urn:oid:1.2.752.201.3.3"  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
  <saml2:AttributeValue xsi:type="xs:string">foo=%C3%85%C3%84%C3%96;bar=123</saml2:AttributeValue>  
</saml2:Attribute>  
...
```

3.3 Attributes for the eIDAS Framework

3.3.1 The `prid` and `pridPersistence` Attribute

Assertions (with attribute statements) issued from a member state eIDAS node contain a set of attributes identifying the authenticated subject. Attributes obtained from other conformant eIDAS nodes will provide an eIDAS unique identifier but it can not be ruled out that the Swedish eIDAS node may be adopted to accept authentication from non eIDAS compliant nodes, such as when accepting authentication from countries outside of EU such as the USA.

Therefore, the Swedish eIDAS connector enriches attribute statements with the provisional ID (`prid`) and provisional ID persistence (`pridPersistence`) attributes.

The `prid` attribute is designed to provide one common unique attribute of the user in a common format regardless of the composition of the original attributes received from the authenticating source. The `prid` attribute value is not stored in any registry, but derived from the received attributes at each authentication instant according to defined algorithms specified in [ConstructedAttr]. The algorithm ensures that each `prid` is unique for each authenticated entity, but does not ensure persistence. If the attributes received for an entity changes over time, the `prid` attribute may also change dependent on the defined `prid` generation algorithm for that attribute source.

The `pridPersistence` attribute provides an indication of the expected persistence over time for a present `prid` attribute value. The value of this attribute is determined from the selected `prid` generation algorithm in combination with the attribute source. For example, a `prid` derived from a Norwegian eIDAS unique identifier has a longer persistence expectancy than a `prid` derived from the same attribute from the UK or Germany. This attribute helps Service Providers to apply different UI and service functions for users with different persistence expectancy. This may assist users with low persistence expectancy to regain control of their user account, should their `prid` change in the future.

The specification "eIDAS Constructed Attributes Specification for the Swedish eID Framework", [ConstructedAttr], declares the details for how the `prid` and `pridPersistence` attributes are generated and how they should be processed.

3.3.2 The `personalIdentityNumberBinding` Attribute

When an authentication for a natural person is performed against the eIDAS Framework the `personalIdentityNumber` attribute (Swedish “personnummer” or “samordningsnummer”) MAY be included in the assertion being delivered to the requesting Service Provider. The member state eIDAS node does not provide this attribute, but instead the assertion may be extended by the Swedish eIDAS connector, that in some cases knows how to map from the eIDAS attributes to a `personalIdentityNumber` attribute.

This binding can be performed using a number of different processes, where some are considered to be strong and where others only may be a “good guess”. Therefore, an eIDAS connector that extends an assertion with a `personalIdentityNumber` attribute MUST also include the `personalIdentityNumberBinding` attribute. This attribute contains a value that is an URI that identifies the process that was used to link a set of eIDAS attributes to a `personalIdentityNumber` attribute.

This specification does not specify any defined URI identifiers that may be included in this attribute. Such URI identifiers will be specified in documents specifying appropriate binding mechanisms.

Draft



4 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.](#)

[SKV704]

[Skatteverket, SKV 704 Utgåva 8, Personnummer.](#)

[SKV707]

[Skatteverket, SKV 707, Utgåva 2, Samordningsnummer.](#)

[SAML-XSD]

S. Cantor et al., SAML assertions schema. OASIS SSTC, March 2005. Document ID saml-schema-assertion-2.0. See <http://www.oasisopen.org/committees/security/>.

[XML-Schema]

XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2004. See <http://www.w3.org/TR/xmlschema-2/>.

[ISO3166]

Codes for the representation of names of countries and their subdivisions Part 1: Country codes, ISO standard, ISO 3166-1.

[TillitRamv]

Tillitsramverk för Svensk E-legitimation.

[ConstructedAttr]

eIDAS Constructed Attributes Specification for the Swedish eID Framework.

[eIDAS_Attr]

[eIDAS SAML Attribute Profile](#), 22 June 2015.

5 Changes between versions

Changes between version 1.3 and version 1.4:

- Attributes for mapping eIDAS-attributes have been defined (section 3.1 and 3.3).
- The eIDAS Natural Person Attribute Set has been defined (section 2.5).

Changes between version 1.2 and version 1.3:

- This specification no longer uses the term “attribute profile” for named collections of attributes for different scenarios. Instead the term “attribute set” is used.
- Definitions of attribute sets (profiles) have been changed to be more flexible and to focus only on which attributes that should be included in an attribute release. Attribute set requirements now include “required” and “recommended” attributes instead of “required”, “allowed”, “if requested” and “prohibited”. See section 2.
- The contents of the previous chapter 2, “NameID”, were moved to the “Deployment Profile for the Swedish eID Framework” document.
- The attribute `displayName` is now specified as “required” for the “Natural Personal Identity with Civic Registration Number (Personnummer)” (ELN-AP-NaturalPerson-01) attribute set (profile). See section 2.3.
- The attributes `o` (Organization) and `displayName` are now specified as “required” for the “Organizational Identity for Natural Persons” (ELN-AP-OrgPerson-01) attribute set (profile). See section 2.4.
- The attributes `givenName` and `sn` (surname) are now specified as “required” for the “Natural Personal Identity without Civic Registration Number” (ELN-AP-NaturalPerson-01) attribute set (profile). See section 2.2.
- The attributes `transactionIdentifier` and `authContextParams` were introduced (see sections 3.1 and 3.2.1).

Changes between version 1.1 and version 1.2:

- Attribute Profiles are now also represented with valid URIs as well as their textual identifiers.

Changes between version 1.0 and version 1.1:

- In chapter 3.4, “Organizational Identity for Natural Persons”, some attributes were listed as both prohibited and allowed. This has been fixed.