Attribute Specification for the Swedish eID Framework

ELN-0604-v1.1  
Version 1.1

2014-04-22

1 Introduction 3

1.1 Terminology 3

1.2 Requirement key words 3

1.3 Name space references 3

1.4 Structure 3

2 NameID 4

3 Attribute Profiles 4

3.1 Pseudonym Identity 4

3.2 Natural Personal Identity without Civic Registration Number 4

3.3 Natural Personal Identity with Civic Registration Number (Personnummer) 5

3.4 Organizational Identity for natural persons 5

4 Attribute Definitions 6

4.1 Attributes 6

4.2 SAML Attribute Format 7

5 References 7

6 Changes between versions 8

# Introduction

## 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]. |

## 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.

## 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]. |
| samlp | urn:oasis:names:tc:SAML:2.0:protocol | The SAML V2.0 protocol namespace, defined in the schema [SAMLP-XSD]. |
| md | urn:oasis:names:tc:SAML:2.0:metadata | The SAML V.2.0 metadata namespace, defined in [SAML-META-XSD] |
| xs | http://www.w3.org/2001/XMLSchema | The XML Schema namespace, representing definitions of data types in [XML-Schema] |

## Structure

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

# NameID

Each identity assertion issued according to this specification MUST have a <saml:Subject> element that specifies the principal that is the subject of all of the statements in the assertion.

The <saml:Subject> element MUST hold a pseudonym identifier of the subject, which SHALL be:

* Unique for the IDP – SP combination being the issuer and recipient for the assertion.
* Constructed in a manner that does not reveal the registered identity of the subject.

# Attribute Profiles

This section defines attribute profiles based on attribute definitions in section 4. Common to all these attribute profiles is that each attribute only can be provided once. An attribute that has more than one value is provided as one attribute with multiple <AttributeValue> sub-elements in accordance with section 4.1.

Requirement levels for attributes in the profiles in the following sections are:

|  |  |
| --- | --- |
| **Attribute requirement** | **Definition** |
| **REQUIRED** | Attributes that MUST be present. |
| **ALLOWED** | Attributes that MAY be present at the discretion of the Identity Provider or Attribute Authority. |
| **IF REQUESTED** | Attributes that MUST NOT be included except when this attribute is explicitly requested by a Service Provider that specifies this attribute in its metadata in a <md:RequestedAttribute> element. |
| **PROHIBITED** | Attributes that MUST NOT be present. |

An identifier, named “Profile Identifier”, identifies each attribute profile. This identifier is provided as means to allow other documents to reference a specific attribute profile. Profile identifiers are only defined to be unique within the context of this document.

## Pseudonym Identity

Profile identifier: **ELN-AP-Pseudonym-01**

The Pseudonym Identity profile is used to convey an identity which in itself does not reveal the true identity of the subject entity.

Assertions conformant with this attribute profile SHALL NOT contain any SAML attributes. (The subject is only identified using the present NameID).

## Natural Personal Identity without Civic Registration Number

Profile identifier: **ELN-AP-NaturalPerson-01**

The Personal Identity without civic registration number provides personal attributes of a subject without revealing the civic registration number of the subject.

|  |  |
| --- | --- |
| **Attribute requirement** | **Attributes** |
| **REQUIRED** | displayName (Display name) |
| **ALLOWED** | sn (Surname)  givenName (Given name) |
| **IF REQUESTED** | Any other attribute in section 4.1 that is not listed in this table. |
| **PROHIBITED** | personalIdentityNumber (National civic registration number)  organizationIdentifier (Organizational identifier code)  orgAffiliation (Personal identifier and organizational identifier code)  o (Organization name)  ou (Organizational unit name) |

## Natural Personal Identity with Civic Registration Number (Personnummer)

Profile identifier: **ELN-AP-Pnr-01**

The Personal Identity with civic registration number provides personal attributes of a subject which includes the civic registration number of the subject.

|  |  |
| --- | --- |
| **Attribute requirement** | **Attributes** |
| **REQUIRED** | sn (Surname)  givenName (Given name)  personalIdentityNumber (National civic registration number) |
| **ALLOWED** | displayName (Display name) |
| **IF REQUESTED** | Any other attribute in section 4.1 that is not listed in this table. Any address attributes SHALL represent the address on file in the Swedish central population database (Folkbokföringsregistret). |
| **PROHIBITED** | organizationIdentifier (Organizational identifier code)  orgAffiliation (Personal identifier and organizational identifier code)  o (Organization name)  ou (Organizational unit name) |

## Organizational Identity for natural persons

Profile identifier: **ELN-AP-OrgPerson-01**

The Organizational Identity provides an identity of a subject that has been provided by an organization. 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)  orgAffiliation (Personal identifier and organizational identifier code) |
| **ALLOWED** | displayName (Display name)  o (Organization name)  ou (Organizational unit name)  organizationIdentifier (Organizational identifier code) |
| **IF REQUESTED** | Any other attribute in section 4.1 that is not listed in this table. Any address attributes SHALL represent the address on file in the Swedish Companies Registration Office registry (Bolagsregistret). |
| **PROHIBITED** | personalIdentityNumber (National civic registration number). |

# Attribute Definitions

## Attributes

The following attributes are defined for use by attribute profiles in this specification:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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](http://www.skatteverket.se/download/18.1e6d5f87115319ffba380001857/70408.pdf) and [SKV 707](http://www.skatteverket.se/download/18.3dfca4f410f4fc63c86800016382/70702.pdf). 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](http://www.skatteverket.se/download/18.70ac421612e2a997f85800040302/70909svartvit.pdf). 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](http://www.skatteverket.se/download/18.70ac421612e2a997f85800040302/70909svartvit.pdf). 10 digits without hyphen. | YES | vlindman@5562265719 |

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 e-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.

## SAML Attribute Format

The <saml:attribute> element representing an attribute in 4.1 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 4.1.
* The FriendlyName attribute is OPTIONAL.
* All <AttributeValue> sub-elements SHALL, unless stated otherwise in the table in section 4.1, have an xsi:type attribute specifying the type "xs:string".

# 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)

[SKV704]

[Skatteverket, SKV 704 Utgåva 8, Personnummer](http://www.skatteverket.se/download/18.1e6d5f87115319ffba380001857/70408.pdf).

[SKV707]

[Skatteverket, SKV 707, Utgåva 2, Samordningsnummer.](http://www.skatteverket.se/download/18.3dfca4f410f4fc63c86800016382/70702.pdf)

[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/>.

[SAMLP-XSD]

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

[SAML-META-XSD]

S. Cantor et al. SAML metadata schema. OASIS SSTC, March 2005. Document ID saml-schema-metadata-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

# Changes between versions

**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.