Attribute Specification for the Swedish eID Framework

Version 1.7 - 2021-02-15 - *Draft version*

Registration number: **2019-310** (*previously: ELN-0604*)

Table of Contents

5. **Changes between versions**

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 Provider* 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.

Note: An Attribute Provider may also release other attributes, not specified by the defined attribute sets it supports. See further section 6.2.1, “Attribute Release Rules”, of “Deployment Profile for the Swedish eID Framework” ([EidDeployProf]).

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.

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

> [*]: 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.

2.1. 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	`sn` (Surname) `givenName` (Given name) `displayName` (Display name)

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

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

Attribute requirement	Attributes
REQUIRED	`sn` (Surname) `givenName` (Given name) `displayName` (Display name) `personalIdentityNumber` (National civic registration number)
RECOMMENDED	`dateOfBirth` (Date of birth)

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	`displayName` (Display name) `orgAffiliation` *(Personal identifier and organizational identifier code)*[*] `o` (Organization name)
RECOMMENDED	`organizationIdentifier` (Organizational identifier code)[*]

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

The "Organizational Identity for Natural Persons" attribute set defines a minimum set of attributes needed to provide organizational identity information about a person. Should an attribute consumer require additional attributes, such as surname and given name, the personal identity number or an

organizational unit name, this can be achieved by either requesting other attribute sets or by explicitly requesting individual attributes. See further section 6.2.1, “Attribute Release Rules”, of “Deployment Profile for the Swedish eID Framework” ([EidDeployProf]).

> [*]: The `displayName` attribute MAY contain personal information such as the given name or surname, but it MAY also be used as an anonymized display name, for example, "Administrator 123". This is decided by the issuing organization.
>
> [**]: See section 3.2.5.
>
> [***]: The organizational identifier can always be derived from the mandatory `orgAffiliation` attribute, but an attribute provider supporting the "Organizational Identity for Natural Persons" attribute set SHOULD also release the `organizationIdentifier` attribute individually.

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) `dateOfBirth` (Date of birth) `sn` (Surname) `givenName` (Given name) `c` (Country code for the eIDAS country that authenticated the subject) `transactionIdentifier` (ID of assertion issued by the member state node)[**]
REQUIRED (if available)[***]	`birthName` (Birth name) `placeOfBirth` (Place of birth) `eidasNaturalPersonAddress` (Address for natural person) `gender` (Gender)

Attribute requirement	Attributes
RECOMMENDED	`personalIdentityNumber` (National civic registration number) `personalIdentityNumberBinding` (National civic registration number Binding URI)

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 attribute provider 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 “added” and “converted” attributes.

Added attributes: Attributes that are not provided by the member state node, but added by the Swedish eIDAS node 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 the result of a conversion process where an eIDAS attribute is converted into a single-value string type attribute defined within the Swedish eID Framework (see section 3.3.3, “Conversion of eIDAS Attributes”). The reason for the conversion is to facilitate processing for attribute consumers. The eIDAS attributes are not simple string types, and this affects interoperability in a negative way since standard SAML software need to be modified to support these attributes. Therefore, the Swedish eID node will convert eIDAS attributes to their corresponding string value-typed attributes. The `eidasPersonIdentifier`, `sn`, `givenName` and `dateOfBirth` attributes are examples of “converted attributes”.

> [*]: Attributes “added” by the Swedish eID node and converted attributes for the mandatory attributes of the eIDAS minimum data set for natural persons.
>
> [**]: The transaction identifier attribute will contain the unique ID of the assertion that was issued by the member state node. This information together with the entityID of the member state node (found in the `<saml2:AuthenticatingAuthority>` element of an assertion) give a reference to the original assertion and authentication process.
>
> [***]: Converted attributes for the optional attributes of the eIDAS minimum data set for natural persons.

2.6. Natural Person Identity with HSA-ID

Attribute set identifier: **DIGG-AP-HSAid-01**

URI: `http://id.swedenconnect.se/ap/1.0/hsaid-01`

The “Natural Person Identity with HSA-ID” attribute set provides basic personal identity information including a HSA-ID of the subject (see [SambiAttr]).

Attribute requirement	Attributes
REQUIRED	`sn` (Surname) `givenName` (Given name) `displayName` (Display name) `employeeHsaId` (HSA-ID)
RECOMMENDED	`dateOfBirth` (Date of birth)

Typical use: In an attribute release policy that provides basic user name information together with the person’s HSA-ID.

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
			A one letter representation (“M”/”F”/”U” or “m”/“f”/”u”)		

Attribute abbreviation	SAML attribute name	Description	Use within this specification	Multi-valued	Example
gender	urn:oid:1.3.6.1.5.5.7.9.3	Gender	representing the subject's gender, where "M" represents male, "F" represents female and "U" is used for unspecified, or unknown, gender.	NO	M
personalIdentity-Number	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 format YYYY-MM-DD.	NO	1950-06-26
birthName	urn:oid:1.2.752.201.3.8	Name at the time of birth	Full name of a person at birth.	NO	Valfrid Danielsson
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

Attribute abbreviation	SAML attribute name	Description	Use within this specification	Multi-valued	Example
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	NO	5562265719

Attribute abbreviation	SAML attribute name	Description	Use within this specification	Multi-valued	Example
orgAffiliation	urn:oid:1.2.752.201.3.1	<uid>@<orgnr>	hyphen. *Personal ID* @ Swedish ”organisationsnummer” according to SKV 709. 10 digits without hyphen.	YES	vlindman@5562265719 See section 3.2.5 below.
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.
userCertificate	urn:oid:1.2.752.201.3.10	User certificate	Base64-encoding of a user certificate.	NO	See section 3.2.2 below.
userSignature	urn:oid:1.2.752.201.3.11	User signature	Base64-encoding of a signature object applied by the user.	NO	See section 3.2.2 below.
authServerSignature	urn:oid:1.2.752.201.3.13	Authentication server signature	Base64-encoding of a authentication server signature.	NO	See section 3.2.2 below.
sad	urn:oid:1.2.752.201.3.12	Signature activation data	Signature activation data required by signature services.	NO	See section 3.2.3 below.

Attribute abbreviation	SAML attribute name	Description	Use within this specification	Multi-valued	Example
signMessageDigest	urn:oid:1.2.752.201.3.14	Digest of sign message digest	Included in assertions as a proof that a user sign message was displayed.	NO	See section 3.2.4 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
personalIdentity-NumberBinding	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.example.se/presentedInP
eidasPersonIdentifier	urn:oid:1.2.752.201.3.7	eIDAS uniqueness identifier for	Maps the eIDAS PersonIdentifier attribute to a string attribute within the	NO	ES/AT/02635542Y (Spanish eID nu for an Austrian SP)

Attribute abbreviation	SAML attribute name	Description	Use within this specification	Multi-valued	Example
		natural persons	scope of the Swedish eID Framework attribute set.		for an Austrian SP)
eidasNatural-PersonAddress	urn:oid:1.2.752.201.3.9	eIDAS Natural Person Address	Attribute for converting the eIDAS CurrentAddress attribute into an attribute having a string type value.	NO	See section 3.3.3.1 below.
employeeHsaId	urn:oid:1.2.752.29.6.2.1	HSA-ID	Person identifier used by Swedish health care organizations.	NO	See [SambiAttr].

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 "ÅÄÖ", 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>
...
```

3.2.2. The userCertificate, userSignature and authServerSignature Attributes

Identity Providers that implement a PKI-based authentication method may make use of the `userCertificate` and `userSignature` attributes.

The `userCertificate` attribute holds, as its value, a base64-encoding of the X.509 certificate presented by the subject during authentication.

The `userSignature` attribute contains a base64-encoding of a signature object that was created by the subject during the authentication* process.

The `authServerSignature` may be included in assertions in cases where there are requirements to include a digitally signed proof from the authentication server at which the end user authenticated. This is mainly useful in cases where the SAML Identity Provider delegates end user authentication to a subordinate authentication server.

> [*]: Note that an authentication process, may be “authentication for signature” as specified in section 7 of [EidDeployProf].

3.2.3. The sad Attribute

The `sad` attribute holds Signature Activation Data that is required by a signature service in order to service a signature request in accordance with CEN EN 419 241-2. The `sad` attribute holds a single string attribute value. The format of the string value is defined in the "Signature Activation Protocol for Federated Signing" specification [SigSAP].

3.2.4. The signMessageDigest Attribute

The `signMessageDigest` attribute is included in an assertion as a proof that an Identity Provider displayed a sign message for the user and that the user actively confirmed acceptance of this sign message. This sign message is the `SignMessage` extension that may be included in an authentication request by Signature Service Service Providers. See section 7 of [EidDeployProf] for details.

The attribute value format for the `signMessageDigest` attribute is `digest-algorithm-identifier;sign-message-digest`, where `digest-algorithm-identifier` is the XML Security algorithm URI identifier of the selected digest algorithm and `sign-message-digest` is `base64(digest(msg))`. The `msg` is the UTF-8 encoded bytes of the sign message that was displayed. It equals the `csig:Message` element value of the `csig:SignMessage` ([DSSExt]). Thus, if the `csig:Message` element is encrypted into a `csig:EncryptedMessage`, the element value after decryption should be used.

Entities compliant with this specification MUST use `http://www.w3.org/2001/04/xmlenc#sha256` as the digest algorithm, unless the recipient of the `signMessageDigest` attribute has declared another digest algorithm as preferred in its metadata entry (see section 2.1.1.3 of [EidDeployProf]). In those cases this algorithm MAY be used.

Example:

Suppose that the unencrypted message is "I hereby confirm that I want to join example.com as a customer". This is represented as:

```
<csig:Message>
  SSBoZXJlYnkgY29uZmlybSB0aGF0IEkgd2FudCB0byBqb2luIGV4YW1wbGUuY29tIGFzIGEgY3VzdG9tZXI=
```

```
</csig:Message>
```

The input to the digesting operation is the value bytes of the `csig:Message` element which is UTF-8 encoded bytes of the actual sign message*.

The `signMessageDigest` attribute for the above example will then be:

```
<saml2:Attribute FriendlyName="signMessageDigest" Name="urn:oid:1.2.752.201.3.14"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xsi:type="xsd:string">
    http://www.w3.org/2001/04/xmlenc#sha256;0yKaSVsYeh+PX2Q6diqO2w89+a3Dm303tp3AVjgxwj0=
  </saml2:AttributeValue>
</saml2:Attribute>
```

3.2.5. The orgAffiliation Attribute

The `orgAffiliation` attribute is intended to be used as a primary identity attribute for personal organizational identities. It consists of a personal identifier **and** an organizational identifier code (`organizationIdentifier`).

This specification does not impose any specific requirements concerning the personal identifier part of the attribute other than that it MUST be unique for the given organization.

Note: In the general case, an attribute consumer MUST NOT assume a particular format or meaning of the personal identifier part since different organizations may use different formats. An attribute consumer should also be aware that a personal identifier separated from its organizational identifier code can not be regarded as unique.

3.3. Attributes for the eIDAS Framework

3.3.1. The prid and pridPersistence Attributes

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 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.

3.3.3. Conversion of eIDAS Attributes

The attributes specified within eIDAS ([eIDAS_Attr]) does not use simple string type values. 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 defines mappings for all eIDAS attributes to attributes having definitions that are more suitable for processing using standard SAML software.

Below follows a listing of how the attributes for the eIDAS minimum data set for Natural Persons are converted into attributes supported by the Swedish eID Framework.

eIDAS attribute	**Swedish eID attribute**
PersonIdentifier `http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier`	eidasPersonIdentifier urn:oid:1.2.752.201.3.7
FamilyName `http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName`	sn urn:oid:2.5.4.4
FirstName `http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName`	givenName urn:oid:2.5.4.42
DateOfBirth `http://eidas.europa.eu/attributes/naturalperson/DateOfBirth`	dateOfBirth urn:oid:1.3.6.1.5.5.7.9.1
BirthName `http://eidas.europa.eu/attributes/naturalperson/BirthName`	birthName urn:oid:1.2.752.201.3.8
PlaceOfBirth `http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth`	placeOfBirth urn:oid:1.3.6.1.5.5.7.9.2
CurrentAddress `http://eidas.europa.eu/attributes/naturalperson/CurrentAddress`	eidasNaturalPersonAddress urn:oid:1.2.752.201.3.9 See section 3.3.3.1 below.
Gender `http://eidas.europa.eu/attributes/naturalperson/Gender`	gender urn:oid:1.3.6.1.5.5.7.9.3

Note: When converting an eIDAS attribute that makes use of “transliteration” (as described in section 2.4 of [eIDAS_Attr]) attribute values having the `LatinScript` attribute set to `false` will not be part of the resulting attribute.

3.3.3.1. Conversion of eIDAS CurrentAddress

The eIDAS attribute `CurrentAddress` is defined in section 2.2.9 of [eIDAS_Attr]. Its value is a Base64-encoding of an XML-structure of the type CurrentAddressStructuredType.

```
<xsd:complexType name="CurrentAddressStructuredType">
  <xsd:annotation>
    <xsd:documentation>
      Current address of the natural person.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="PoBox" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="LocatorDesignator" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="LocatorName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="CvaddressArea" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="Thoroughfare" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="PostName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="AdminunitFirstline" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="AdminunitSecondline" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="PostCode" type="xsd:string" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
```

An example of an instance of a CurrentAddress attribute would look as follows:

```
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                         FriendlyName="CurrentAddress"
                         Name="http://eidas.europa.eu/attributes/naturalperson/CurrentAddress"
                         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xsi:type="eidas:CurrentAddressType">
    PGVpZGFzOkxvY2F0b3JEZXNpZ25hdG9yPjIyPC9laWRhczpMb2NhdG9yRGVzaWduYX
    Rvcj48ZWlkYXM6VGhvcm91Z2hmYXJlPkFyY2FjaWEgQXZlbnVlPC9laWRhczpUaG9y
    b3VnaGZhcmU+DQo8ZWlkYXM6UG9zdE5hbWU+TG9uZG9uPC9laWRhczpQb3N0TmFtZT
    4NCjxlaWRhczpQb3N0Q29kZT5TVzFBIDFBQTwvZWlkYXM6UG9zdENvZGU+
  </saml2:AttributeValue>
</saml2:Attribute>
```

The value is the Base64-encoding of the following XML-snippet:

```
<eidas:LocatorDesignator>22</eidas:LocatorDesignator>
<eidas:Thoroughfare>Arcacia Avenue</eidas:Thoroughfare>
<eidas:PostName>London</eidas:PostName>
<eidas:PostCode>SW1A 1AA</eidas:Postcode>
```

This is not easily processed by standard SAML-software, and requires several steps including XML-decoding of an incomplete XML-snippet. Therefore, the Swedish eID Framework defines the `eidasNaturalPersonAddress` attribute to be used when the Swedish eIDAS node converts the eIDAS `CurrentAddress` attribute.

The `eidasNaturalPersonAddress` attribute is defined to be a non-empty single-value attribute containing key-value pairs separated by semicolons. The keys are element names from the `CurrentAddressStructuredType` type and the value-parts are their corresponding values. The key and value of each pair is separated by a '=' character and both the key and value MUST be URL-encoded.

The eIDAS-attribute `CurrentAddress` above will thus be converted to the following attribute:

```
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          FriendlyName="eidasNaturalPersonAddress"
                          Name="urn:oid:1.2.752.201.3.9"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xsi:type="xs:string">
    LocatorDesignator=22;Thoroughfare=Arcacia%20Avenue;PostName=London;PostCode=SW1A%201AA
  </saml2:AttributeValue>
</saml2:Attribute>
```

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.

[SKV709]

> Skatteverket, SKV 709, Utgåva 8, Organisationsnummer.

[X.520]

> ITU-T X.520 - Open Systems Interconnection – The Directory: Selected attribute types.

[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.

[SambiAttr]

> Sambi Attributspecifikation, version 1.5.

[TillitRamv]

> Tillitsramverk för Svensk e-legitimation - 2018-158

[EidDeployProf]

> Deployment Profile for the Swedish eID Framework.

[ConstructedAttr]

> eIDAS Constructed Attributes Specification for the Swedish eID Framework.

[eIDAS_Attr]

> eIDAS SAML Attribute Profile, version 1.2, 21 May 2019.

[SigSAP]

> Signature Activation Protocol for Federated Signing.

[DSSExt]

> DSS Extension for Federated Central Signing Services.

5. Changes between versions

Changes between version 1.6 and version 1.7:

- Section 2.4, "Organizational Identity for Natural Persons", was updated to define a minimum set of attributes for providing personal orgazational identity information.
- Section 3.2.5, "The orgAffiliation Attribute", was introduced.

Changes between version 1.5 and version 1.6:

- References were updated to point at the latest versions of the "Tillitsramverk för Svensk e-legitimation" and "eIDAS SAML Attribute Profile" specifications.
- Section 2.5, "eIDAS Natural Person Attribute Set", was updated so that the `c` (country) attribute is a required attribute for this attribute set.
- The attribute `signMessageDigest` was introduced (see section 3.2.4).
- The HSA-ID attribute was specified.

Changes between version 1.4 and version 1.5:

- Section 3.2.3 was updated with a reference to the SAP specification as source for defining the content of the `sad` attribute.
- Fix of invalid links for SKV704 and SKV707.
- Section 2.3, "Natural Personal Identity with Civic Registration Number (Personnummer)", was updated so that the `dateOfBirth`-attribute is listed as a recommended attribute for the attribute set `http://id.elegnamnden.se/ap/1.0/pnr-01`.

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).
- The definition of the `gender`-attribute was extended to also include “U” (for unspecified or unknown).
- For interoperability and implementations reasons, the definition of the `dateOfBirth`-attribute has been changed so that it is represented as an `xs:string` type on the format YYYY-MM-DD, instead of the `xs:date` type.
- Attributes `userCertificate`, `userSignature`, `authServerSignature` and `sad` were added.

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.