Samleikin Attribute Specification

Version (Final): 1.0 - 20.05.2020. Effective Date: 28.05.2020

1. Introduction

This document specifies an attribute profile for Samleikin. The attribute profile defines attributes for use within Samleikin, 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

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 Faroese "p-tal" according to [Nr41Nr36] and [Nr73Nr24].
Pseudo-civic registration number	A unique identifier assigned to each natural person in a national population register where the natural person is not a citizen of the Faroe Islands but is registered in the population registry. Within the context of this specification this is a so called "pseudo p-tal", but not specified as such in the legislation but is implemented as such in the national identity registry, according to [Nr41Nr36] and [Nr73Nr24].

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:

`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`.

1.5. 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 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12483&lang=en. 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 Faroese eID Framework is: 1.2.208.189.1

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

- 1 = ISO
- 2 = ISO member body
- 208 = Denmark
- 189 = Gjaldstovan
- 1 = Faroese eID

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

1.2.208.189.1.{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.

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 a 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.

Persistent NameID's are not released in attribute statements of assertions, but is instead a part of the subject statement. Persistent means they will be persistent per Service Provider, so two Service Providers will never get the same pseudonym for the same identity.

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

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.

2.1. Pseudonym Identity

Attribute set identifier: **TS-AP-Pseudonym-01**

URI: http://id.samleiki.fo/ap/1.0/pseudonym-01

This attribute set specifies the condition where there are no mandatory or recommended attributes. This will be released as a SAML2 standard Persistent `<NameID>` element, which is part of the SAML-core schema.

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

2.2. Natural Person Identity without Civic Registration Number (p-tal)

Attribute set identifier: **TS-AP-NaturalPerson-01**

URI: http://id.samleiki.fo/ap/1.0/natural-person-01

The “Natural Person Identity without Civic Registration Number” attribute set provides basic natural person information without revealing the civic registration number of the subject, even if it should be present. Note that this attribute set also includes a persistent pseudonym.

REQUIRED	`subjectID`
	`sn (Surname)`
	`givenName (Given name)`
	`displayName (Display name)`

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

2.3. Natural Person Identity without Civic Registration Number (p-tal), Age Only

Attribute set identifier: **TS-AP-NaturalPerson-01**

URI: http://id.samleiki.fo/ap/1.0/age-01

The "Natural Person Identity without Civic Registration Number (p-tal), Age Only" attribute set provides information about the age of a subject only.

REQUIRED	`subjectID`
	`DateOfBirth (Date of birth)`

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

2.4. Natural Personal Identity with Civic Registration Number (p-tal)

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

URI: http://id.gjaldstovan.fo/ap/1.0/pnr-01

The “Personal Identity with Civic Registration Number” attribute set provides basic personal identity information including a Faroese civic registration number of the subject. Note that this attribute set also includes a persistent pseudonym.

REQUIRED	`subjectID`
	`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 Faroese civic registration number.

3. Attribute Definitions

3.1. Attributes

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

sn	urn:oid:2.5.4.4	Surname	Registered surname.	NO	Hansen
givenName	urn:oid:2.5.4.42	Given Name	Registered given name.	NO	Hans
displayName	urn:oid:2.16.840.1.113730.3.1.241	Display Name	A name in any preferred presentation format.	NO	Hans Hansen
personalIdentityNumber	urn:oid:1.2.208.189.1.2.1	National civic registration number/code	Faroese "p-tal" according to Løgtingslóg nr. 41. 9 digits without hyphen.	NO	010117023

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	1957-01-01
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	FO DK
subjectID		Subject identifier, unique for by Service Provider	Serves the same purpose as the SAML2 NameID but as a normal attribute rather than a universally defined SAML2 identifier.	NO	

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 may 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 URN 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">
Hansen</saml2:AttributeValue>
</saml2:Attribute>
```

The following is an example of the SubjectID attribute. Its value is represented using a string type and it as specified in [SubjID].

```
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

                           NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

  <saml2:AttributeValue
>HA2TKNZZGE2TOZDCGMZWKOLDHBQWIMBSGM4TGZBYGUYGINRQHAYTINBZGYZDOZBZMZRGKNZTME3TMNBXGYYTIOBYGMYWKNLFMYYDAYY=@talgild
fo

  </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.*

[DeployProf]

> *Samleikin Deployment Profile*

[Nr41Nr36]

> *Løgtingslóg nr. 41 frá 8. mai 2007 um fólkayvirlit, sum broytt við løgtingslóg nr. 36 frá 6. mai 2011*

[Nr73Nr24]

> *Løgtingslóg nr. 73 frá 8. mai 2001 um viðgerð av persónsupplýsingum, sum broytt við løgtingslóg nr. 24 frá 17. mai 2004*

[SubjID]

> *SAML V2.0 Subject Identifier Attributes Profile Version 1.0*

5. Changes Between Versions