Common Attributes for SAML Federation

IN PROGRESS

Introduction

This specification defines a common attribute profile, consisting of attribute names and their associated semantics, for use in the Swedish Internet Foundation's SAML-based federations. The attribute set is intended to support consistent and interoperable attribute release from Identity Providers to Relying Parties.

The attributes defined in this specification support common identity and access management use cases, including subject identification, personal naming, and contact information.

The specification is domain-neutral and may be adopted across different sectors and federation environments. Its purpose is to promote consistency and interoperability by establishing common definitions for attribute naming, semantics, and usage.

Federations and other parties that choose to adopt this specification are expected to use the defined attributes consistently when exchanging attribute information.

This specification does not define a mandatory minimum set of attributes that must be released. Relying Parties determine attribute requirements based on their service-specific needs. Identity Providers may release additional attributes beyond those defined in this specification, subject to applicable policy and operational requirements.

Where applicable, references to external attribute definitions are included, such as corresponding Object Identifiers (OIDs).

Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals.

SAML Attribute Representation

SAML Attribute Format

When an attribute defined in this specification is conveyed in SAML 2.0, the following requirements apply:

- Each attribute **SHALL** be represented using a `<saml:Attribute>` element.
- The `NameFormat` attribute **MUST** have the value `urn:oasis:names:tc:SAML:2.0:attrnameformat:uri`.
- The `Name` attribute **MUST** contain the URI defined for the attribute in this specification. Attribute names defined by this specification use the https scheme.
- The `FriendlyName` attribute is **OPTIONAL**.
- Unless otherwise specified in the relevant attribute definition, each `<AttributeValue>` element **MUST** contain a value of type `xs:string`. The type **MAY** be explicitly declared using `xsi:type="xs:string"`.
- Attributes designated as single-valued **MUST NOT** contain more than one `<AttributeValue>` element.
- Attributes designated as multi-valued **MAY** contain more than one `<AttributeValue>` elements.
- Unless otherwise specified in the relevant attribute definition, this specification does not override the default SAML string comparison rules.

Scoped Attributes

A scoped attribute expresses its value as a string of the form `value@scope`.

The scope portion qualifies the value within a namespace controlled by the asserting Identity Provider. The meaning and interpretation of scope are attribute-specific unless otherwise defined for a particular attribute or profile.

An Identity Provider **MUST NOT** assert a scoped attribute value containing a scope that it is not authorized to use.

Where metadata-based scope validation is used, the permitted scope values for an Identity Provider **MUST** be declared in metadata using the `<shibmd:Scope>` element.

A Relying Party that consumes a scoped attribute **SHOULD** verify that the asserted scope is permitted for the issuing Identity Provider by comparing the scope portion of the attribute value against the `<shibmd:Scope>` values published in that Identity Provider's metadata. See also section 2.1.4 *Scope* in SAML 2.0 WebSSO Technology Profile.

Identifier Properties

This section describes identifier properties, including whether they are non-reassignable, opaque, persistent, and unique per relying party.

Identifier	Non-reassigned	Opaque	Persistent	Unique per Relying Party
subject-id	✅	✅	✅	❌
pairwise-id	✅	✅	✅	✅
personalIdentityNumber	✅	❌	❌	❌

Attribute Definitions

subject-id

The attribute is a technical identifier assigned by the subject's home organization to uniquely identify the subject across Relying Parties within the federation.

The value **MUST** be persistent, stable over time, and globally unique, and **MUST NOT** be reassigned to another subject.

The identifier **MUST** be designed such that its value does not directly or indirectly reveal the identity of an individual.

The identifier **MUST** be constructed as a locally unique value followed by "@" and a scope. The combination of the locally unique value and scope uniquely identifies the subject within the federation.

Name	https://openfed.se/attributes/subject-id
Friendly Name	subject-id
Data Type	xs:string
Multi-valued	NO
Scoped	YES
Reference	urn:oasis:names:tc:SAML:attribute:subject-id
Example	7803e459-881d-416f-a57c-4ce5eda0b79b@example.org

pairwise-id

The attribute is a technical identifier assigned by the subject's home organization to uniquely identify the subject on a per–Relying Party basis.

The value **MUST** be persistent and stable over time for a given subject–Relying Party pair, and **MUST NOT** be reassigned to another subject.

The identifier **MUST** be designed such that its value does not directly or indirectly reveal the identity of an individual.

The identifier **MUST** be generated in a manner that prevents the subject from being correlated across different Relying Parties.

The identifier **MUST** be constructed as a locally unique identifier followed by "@" and a scope.

Name	https://openfed.se/attributes/pairwise-id

Friendly Name	pairwise-id
Data Type	xs:string
Multi-valued	NO
Scoped	YES
Reference	urn:oasis:names:tc:SAML:attribute:pairwise-id
Example	9d666d80-c634-4f12-838b-c667de76762b@example.org

personalIdentityNumber

The subject's national civic registration number (i.e. the Swedish "personnummer" or "samordningsnummer" as defined in SKV 704 and SKV 707).

The value **MUST** consist of 12 digits without a hyphen.

Name	https://openfed.se/attributes/personalIdentityNumber
Friendly Name	personalIdentityNumber
Data Type	xs:string
Multi-valued	NO
Scoped	NO
Reference	urn:oid:1.2.752.29.4.13
Example	198611245807

givenName

The given name (first name) of the subject.

Name	https://openfed.se/attributes/givenName
Friendly Name	givenName
Data Type	xs:string
Multi-valued	NO
Scoped	NO
Reference	urn:oid:2.5.4.42
Example	Anna Maj

sn

The surname (family name) of the subject.

Name	https://openfed.se/attributes/sn
Friendly Name	sn
Data Type	xs:string
Multi-valued	NO
Scoped	NO

Reference	urn:oid:2.5.4.4
Example	Björklund

displayName

A name that is suitable for display to end-users, typically a combination of given name and surname.

Name	https://openfed.se/attributes/displayName
Friendly Name	displayName
Data Type	xs:string
Multi-valued	NO
Scoped	NO
Reference	urn:oid:2.16.840.1.113730.3.1.241
Example	Anna Maj Björklund

mail

The email address of the subject.

Values **MUST** be syntactically valid email addresses.

Field	Value
Name	https://openfed.se/attributes/mail
Friendly Name	mail
Data Type	xs:string
Multi-valued	YES
Scoped	NO
Reference	urn:oid:0.9.2342.19200300.100.1.3
Example	anna-maj.bjorklund@example.org

telephoneNumber

The telephone number of the subject.

Values **SHOULD** be formatted according to ITU-T Recommendation E.164 where possible.

Multiple values **MAY** be provided.

Name	https://openfed.se/attributes/telephoneNumber
Friendly Name	telephoneNumber
Data Type	xs:string
Multi-valued	YES
Scoped	NO
Reference	urn:oid:2.5.4.20
Example	+4684523567

mobile

A mobile (cellular) telephone number of the subject.

Values **SHOULD** be formatted according to ITU-T Recommendation E.164 where possible.

Multiple values **MAY** be provided.

Name	https://openfed.se/attributes/mobile
Friendly Name	mobile
Data Type	xs:string
Multi-valued	YES
Scoped	NO
Reference	urn:oid:0.9.2342.19200300.100.1.41
Example	+46704253567

o

The name of the organization to which the subject belongs.

Name	https://openfed.se/attributes/o
Friendly Name	o
Data Type	xs:string
Multi-valued	NO
Scoped	NO
Reference	urn:oid:2.5.4.10
Example	Example Institute AB

ou

The name of an organizational unit within the organization to which the subject belongs.

The value represents an organizational subdivision such as a department or unit. Multiple values **MAY** be provided if the subject is associated with more than one organizational unit.

The value is not guaranteed to be unique and **MUST NOT** be used as an identifier.

Name	https://openfed.se/attributes/ou
Friendly Name	ou
Data Type	xs:string
Multi-valued	YES
Scoped	NO
Reference	urn:oid:2.5.4.11
Example	Research and Development

organizationIdentifier

A unique identifier for the organization to which the subject is affiliated.

The value **MUST** be a Swedish company registration number (a.k.a. “organisationsnummer“) formatted as a 10-digit string without hyphens, in accordance with SKV 709.

Name	https://openfed.se/attributes/organizationIdentifier
Friendly Name	organizationIdentifier
Data Type	xs:string
Multi-valued	NO
Scoped	NO
Reference	urn:oid:2.5.4.97
Example	5562265719