Common Attributes for SAML Federation

IN PROGRESS

Introduction

This specification defines standardised names and semantics for attributes that may be communicated within a SAML federation. The attribute set is intended as a reference data set of attributes that may be released to Relying Parties.

The attributes described are intended to support generic identity and access management use cases, including user identification, naming, and contact information.

The specification is designed to be domain-neutral and applicable across different sectors and services. Its purpose is to promote consistency and interoperability between Identity Providers and Relying Parties by establishing a baseline for attribute naming, semantics, and usage.

Members participating in the federation that require the exchange of these attributes are expected to use the definitions provided in this specification.

This specification does not mandate a minimum set of attributes to be released. Relying Parties determine attribute requirements based on their specific needs. Identity Providers may also release additional attributes beyond those defined in this specification.

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

SAML Attribute Representation

SAML Attribute Format

When attributes defined in this specification are used, the following requirements apply:

- The `<saml:Attribute>` element represents an attribute in SAML 2.0.
- The `NameFormat` attribute **MUST** have the value `urn:oasis:names:tc:SAML:2.0:attrnameformat:uri`.
- The `Name` attribute **MUST** contain a URI as defined in this specification. Attribute names are expressed as URIs in the form of URLs.
- The `FriendlyName` attribute is **OPTIONAL**.
- The data type of the `<AttributeValue>` element is `xs:string` using UTF-8 encoding, unless otherwise specified in the attribute definition table. The type **MAY** be explicitly declared using `xsi:type="xs:string"`.
- Attributes marked as non-multi-valued **MUST NOT** contain more than one `<AttributeValue>` element.
- Attributes marked as multi-valued **MAY** contain multiple `<AttributeValue>` elements.
- String matching **SHOULD** be performed using the `caseIgnoreMatch` rule as defined in X.520.

Scoped Attributes

A scoped attribute expresses its value as a string of the form `value@scope`, where the scope represents the Identity Provider's security domain.

The scope typically corresponds to the organization’s domain name, but is not limited to it, and **MUST** be declared in the Identity Provider's metadata (the `<shibmd:Scope>` element).

An Identity Provider that releases scoped attributes **MUST** be authorized to use the corresponding scope values. Such scopes **MUST** be registered with the federation and, upon approval by the federation operator, included in the Identity Provider's metadata.

A Relying Party consuming a scoped attribute **SHOULD** verify that the issuing IdP is authorized to assert the given scope. This verification is performed by checking the Identity Provider's metadata entry, as described in Section 2.1.4 *Scope* of the SAML 2.0 WebSSO Technology Profile.

Example

The following example illustrates how attributes defined in this specification may be represented in a SAML 2.0 assertion issued by an Identity Provider.

```
<saml2:Attribute
    Name="https://example.org/attributes/subject-id"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    FriendlyName="subject-id">

    <saml2:AttributeValue
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xsi:type="xs:string">
        7803e459-881d-416f-a57c-4ce5eda0b79b@example.org
    </saml2:AttributeValue>

</saml2:Attribute>
```

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

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:2.5.4.42
Example	Anna Maj Björklund

mail

The email address of the subject.

Multiple email addresses **MAY** be provided. 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

*) The `mail` attribute **MUST** be treated as a scoped attribute if and only if the applicable attribute release policy explicitly designates it as scoped. Otherwise, it **MUST** be treated as non-scoped.

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