

Document	Services and Attributes in SAML Metadata
Identifier	https://skolfederation.se/sasm
Version	V1.0.0
Last modified	2022-04-01
Pages	5
Status	Final
License	Creative Commons BY-SA 3.0

Services and Attributes in SAML Metadata

Stefan Halén

Abstract

This document describes how to declare services and attributes in SAML V2.0 metadata for the federations of The Swedish Internet Foundation.

Contents

1 Terminology and Typographical Conventions	2
1.1 Definition of terminology	2
2 Introduction	3
3 XML Namespaces	3
4 Language attributes (xml:lang)	3
5 Metadata - Identity Providers	3
5.1 <saml:Attribute> [One or More]	3
5.2 <saml:AttributeValue> [Zero or More]	4
5.3 Example IDPSSODescriptor	4
6 Metadata - Relying Parties (Service Providers)	4
6.1 <md:AttributeConsumingService> [One or More]	4
6.2 <md:RequestedAttribute>	5
6.3 Example SPSSODescriptor	5
7 Acknowledgements	5
8 References	5

1 Terminology and Typographical Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119 [1]

1.1 Definition of terminology

Member Organization: An organization that either is the owner of an Identity Provider or an Relaying Party registered in one of the federations of The Swedish Internet Foundation.

User Organization: A Member Organization with which a Subject is affiliated, operating the Identity Provider by itself or through a third party.

Service Owner: A Member Organization that is responsible and liable for operating a service registered in the federation. The Service Owner may delegate the technical operation of the Relying Party to another organization.

Subject: Any natural person affiliated with a User Organization

Identity Provider: The system component that issues attribute assertions on behalf of Subjects who use them to access the services of the Relying Party.

Relying Party: A Service that relies upon a Subject’s credentials, typically to process a transaction or grant access to information on a system. Also known as Service Provider (SP). The Relying Party is owned by a Service Owner.

Service Provider: See Relying Party

2 Introduction

This document specifies how services and attributes are advertised in metadata for the Swedish Internet Foundation SAML V2.0 federations. This document will be superseded by The Swedish Internet Foundation SAML WebSSO Technology Profile. The work to complete the technology profile is in progress and the date for publication has not yet been set.

3 XML Namespaces

Namespaces and prefixes used throughout this document.

Prefix	Namespace	Specification	Schema
saml:	urn:oasis:names:tc:SAML:2.0:assertion	[SAML2Core] [2]	[SAML-XSD]
md:	urn:oasis:names:tc:SAML:2.0:metadata	[SAML2Meta] [3]	[SAMLMeta-xsd]

4 Language attributes (xml:lang)

Definition of xml:lang for the elements <md:ServiceName> and <md:ServiceDescription>.

There MUST NOT be more than one instance of each **lang** value for the element in question.

A **lang** attribute value used MUST be present for both element.

The elements MUST have the **lang** attribute value set to a value from “ISO 639-1”

The elements MUST have a **lang** attribute with definition in English (**en**).

The elements MUST have a **lang** attribute with definition in Swedish (**sv**).

5 Metadata - Identity Providers

In federation metadata for an Identity Provider at least one <**saml:Attribute**> MUST be declared.

5.1 <saml:Attribute> [One or More]

One or more elements that identify the SAML attributes supported by the Identity Provider. Specific values MAY optionally be included, indicating that only certain values permitted by the attribute's definition are supported. In this context, “support” for an attribute means that the Identity Provider has the capability to include it when delivering assertions during single sign-on [3].

NameFormat [Required] A URI reference representing the classification of the attribute name for purposes of interpreting the name [2]. MUST be set to urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

Name [Required] The name of the attribute. The attribute MUST be included in the federation's attribute profile [2].

FriendlyName [Required] A string that provides a more human-readable form of the attribute's name, which may be useful in cases in which the actual Name is complex or opaque, such as an OID or a UUID. This attribute's value MUST NOT be used as a basis for formally identifying SAML attributes. The FriendlyName MUST belong to the Name in the federation's attribute profile [2].

<saml:AttributeValue> [Zero or More] Element that identify the value of the attribute supported by the Identity Provider (see [Section 5.2](#)).

5.2 <saml:AttributeValue> [Zero or More]

Contains a value of the attribute. If an attribute contains more than one discrete value, each value MUST appear in its own <saml:AttributeValue> element. If more than one <saml:AttributeValue> element is supplied for an attribute, and any of the elements have a datatype assigned through xsi:type, then all of the <saml:AttributeValue> elements must have the identical datatype assigned [2].

5.3 Example IDPSSODescriptor

The following is a non-normative example of metadata for an Identity Provider. Non relevant metadata is not displayed. In this example, the Identity Provider has the capability to include the attributes eduPersonPrincipalName and eduPersonEntitlement when delivering assertions. For eduPersonEntitlement, the Identity Provider only supports the value http://example.com/contracts/HEd123:

```
<md:EntityDescriptor entityID="https://example.com/">
  <md:IDPSSODescriptor
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml:Attribute
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
      FriendlyName="eduPersonPrincipalName">
    </saml:Attribute>
    <saml:Attribute
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oid: 1.3.6.1.4.1.5923.1.1.1.7"
      FriendlyName="eduPersonEntitlement">
      <saml:AttributeValue>
        http://example.com/contracts/HEd123
      </saml:AttributeValue>
    </saml:Attribute>
    </md:IDPSSODescriptor>
  </md:EntityDescriptor>
```

6 Metadata - Relying Parties (Service Providers)

In federation metadata for an Relying Party at least one <md:AttributeConsumingService> MUST be declared.

6.1 <md:AttributeConsumingService> [One or More]

The <AttributeConsumingService> element defines a particular service offered by the service provider in terms of the attributes the service requires or desires. Its AttributeConsumingService complex type contains the following elements and attributes [3]:

index [Required] A required attribute that assigns a unique integer value to the element so that it can be referenced in a protocol message [3].

isDefault [Optional] Identifies the default service supported by the service provider. Useful if the specific service is not otherwise indicated by application context. If omitted, the value is assumed to be false [3].

<md:ServiceName> [One or More] One or more language-qualified names for the service [3].

<md:ServiceDescription> [One or More] One or more language-qualified strings that describe the service [3].

<md:RequestedAttribute> [One or More] One or more elements specifying attributes required or desired by this service[3].

6.2 <md:RequestedAttribute>

The element specifies a service provider's interest in a specific SAML attribute, optionally including specific values. Its RequestedAttributeType complex type extends the saml:AttributeType (see Section 5.1) with the following attribute [3]:

isRequired [Optional] Optional boolean XML attribute indicates if the service requires the corresponding SAML attribute in order to function at all (as opposed to merely finding an attribute useful or desirable) [3].

If specific elements are included, then only matching values are relevant to the service (see Section 5.2).

6.3 Example SPSSODescriptor

The following is a non-normative example of metadata for an Relying Party. Non relevant metadata is not displayed. The element defines a service with the name of the service set in the languages Swedish and English. The service requests two attributes, eduPersonPrincipalName and eduPersonEntitlement. The service requires that the eduPersonPrincipalName attribute is provided. The eduPersonEntitlement attribute is optional, but if provided, the value must be set to <http://example.com/contracts/HED123>:

```
<md:EntityDescriptor entityID="https://example.com/">
  <md:SPSSODescriptor AuthnRequestsSigned="false">
    <md:AttributeConsumingService index="0">
      <md:ServiceName xml:lang="sv">Min exempel tjänst</md:ServiceName>
      <md:ServiceName xml:lang="en">My Example Service</md:ServiceName>
      <md:RequestedAttribute
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        isRequired="true"
        FriendlyName="eduPersonPrincipalName">
      </md:RequestedAttribute>
      <md:RequestedAttribute
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid: 1.3.6.1.4.1.5923.1.1.1.7"
        FriendlyName="eduPersonEntitlement">
        <saml:AttributeValue>
          http://example.com/contracts/HED123
        </saml:AttributeValue>
      </md:RequestedAttribute>
    </md:AttributeConsumingService>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

7 Acknowledgements

Portions of content in this document have been retrieved from [SWAMID SAML WebSSO Technology Profile](#) (c) by Sunet licensed under [CC BY-SA 3.0](#)

8 References

- [1] S. Bradner, Key words for use in RFCs to indicate requirement levels, RFC Editor; Internet Requests for Comments; RFC Editor, 1997. <http://www.rfc-editor.org/rfc/rfc2119.txt>.
- [2] S. Cantor, Assertions and protocols for the OASIS security assertion markup language (SAML) V2.0, OASIS, 2015. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- [3] S. Cantor, Metadata for the OASIS security assertion markup language (SAML) V2.0, OASIS, 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.