



Metadata Profile for the OASIS Security Assertion Markup Language (SAML) V1.x

OASIS Standard
1 November 2007

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-os.html>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-os.odt>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-os.pdf>

Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-cs-01.html>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-cs-01.odt>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-cs-01.pdf>

Latest Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata.html>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata.odt>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata.pdf>

Technical Committee:

OASIS Security Services TC

Chairs:

Hal Lockhart, BEA Systems, Inc.
Brian Campbell, Ping Identity

Editors:

Greg Whitehead, Hewlett-Packard Company
Scott Cantor, Internet2

Related Work:

This specification supplements the SAML V2.0 metadata specification [SAML2Meta].

Declared XML Namespaces(s):

urn:oasis:names:tc:SAML:profiles:v1:metadata

Abstract:

This specification defines a profile of the OASIS SAML V2.0 metadata specification for use in describing SAML V1.0 and V1.1 entities. Readers should be familiar with the SAML V2.0 metadata specification [SAML2Meta] before reading this document.

Status:

This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://www.oasis-open.org/committees/security>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/security/ipr.php>).

Notices

Copyright © OASIS Open 2007. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

Table of Contents

91		
92	1 Introduction.....	5
93	1.1 Notation.....	5
94	1.2 Normative References.....	6
95	1.3 Non-Normative References.....	6
96	2 SAML V1.x Metadata Profile.....	7
97	2.1 Required Information.....	7
98	2.2 Profile Overview.....	7
99	2.3 Element <md:EntitiesDescriptor>.....	7
100	2.4 Element <md:EntityDescriptor>.....	7
101	2.5 Element <md:IDPSSODescriptor>.....	8
102	2.6 Element <md:SPSSODescriptor>.....	9
103	2.7 Element <md:AttributeAuthorityDescriptor>.....	10
104	2.8 Element <md:AuthnAuthorityDescriptor>.....	10
105	2.9 Element <md:PDPDescriptor>.....	10
106	2.10 Element <md:KeyDescriptor>.....	11
107	Appendix A. Acknowledgements.....	12

1 Introduction

This specification defines a profile of the SAML V2.0 metadata specification [SAML2Meta] for use in describing SAML V1.0 and V1.1 entities and profiles.

Unless specifically noted, nothing in this document should be taken to conflict with the SAML V2.0 metadata specification. Readers are advised to familiarize themselves with that specification first.

1.1 Notation

This specification uses normative text to describe the use of SAML V2.0 metadata with SAML V1.0 and V1.1 profiles.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC 2119]:

...they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)...

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application 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.

Listings of XML schemas appear like this.

Example code listings appear like this.

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:1.0:assertion	This is the SAML V1.0 and V1.1 assertion namespace [SAML1Core].
samlp:	urn:oasis:names:tc:SAML:1.0:protocol	This is the SAML V1.0 and V1.1 protocol namespace [SAML1Core].
saml2:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].
saml1md:	urn:oasis:names:tc:SAML:profiles:v1metadata	This is the namespace defined by this document and its accompanying schema [SAML1MD-xsd].
xs:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.

This specification uses the following typographical conventions in text: <SAMLElement>, <ns:ForeignElement>, Attribute, **Datatype**, OtherKeyword.

1.2 Normative References

- [RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- [SAML11Bind] E. Maler et al. *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1*. OASIS, September 2003. Document ID oasis-sstc-saml-bindings-1.1. See <http://www.oasis-open.org/committees/download.php/3405/oasis-sstc-saml-bindings-1.1.pdf>.
- [SAML11Core] E. Maler et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V1.1*. OASIS, September 2003. Document ID oasis-sstc-saml-core-1.1. See <http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf>.
- [SAML1MD-xsd] S. Cantor et al. *SAML V1.x metadata schema*. OASIS SSTC, July 2006. Document ID sstc-saml1x-metadata. See <http://www.oasis-open.org/committees/security/>.
- [SAML2Core] S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-core-2.0-os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- [SAML2Meta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- [Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web Consortium Recommendation, May 2001. See <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>.

1.3 Non-Normative References

- [SAML2Gloss] J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-glossary-2.0-os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf>.

2 SAML V1.x Metadata Profile

SAML profiles require agreements between system entities regarding identifiers, binding/profile support and endpoints, certificates and keys, and so forth. A metadata specification is useful for describing this information in a standardized way.

Although SAML V1.0 and V1.1 did not include such a specification, SAML V2.0 includes one in [SAML2Meta]. This specification profiles the SAML V2.0 metadata specification for use with the SAML V1.0 and V1.1-based profiles and exchanges expected between system entities.

2.1 Required Information

Identification: `urn:oasis:names:tc:SAML:profiles:vlmetadata`

Contact information: security-services-comment@lists.oasis-open.org

Description: Given below.

Updates: None

2.2 Profile Overview

SAML V2.0 metadata describes a system entity by means of the `<md:EntityDescriptor>` element and a set of "roles" supported by the entity. Role elements profiled for use with SAML V1.0 and V1.1 include `<md:IDPSSODescriptor>`, `<md:SPSSODescriptor>`, `<md:AttributeAuthorityDescriptor>`, `<md:AuthnAuthorityDescriptor>`, and `<md:PDPDescriptor>`. Specific use of these elements MUST adhere to the profile outlined in the following sections.

The SAML V2.0 roles of identity provider (IdP) and service provider (SP) correspond to the roles described in the SAML V1.0 and V1.1 specifications as "source site" and "destination site". This specification adopts the SAML V2.0 terminology [SAML2Gloss].

SAML V2.0 metadata uses a `protocolSupportEnumeration` attribute on each role element, the value of which is a list of protocol URIs, to indicate which protocols are supported by an entity in a role.

SAML V2.0 metadata specifies the use of the SAML V2.0 protocol namespace URI to indicate support for SAML V2.0. Since SAML V1.0 and V1.1 both use the same XML protocol namespace URI,

`urn:oasis:names:tc:SAML:1.0:protocol`, this convention is not adequate to distinguish between support for SAML V1.0 and V1.1.

For this reason, we define distinct values for use in identifying SAML V1.0 or V1.1 protocol support: the original value of `urn:oasis:names:tc:SAML:1.0:protocol` and a new value of `urn:oasis:names:tc:SAML:1.1:protocol` respectively.

2.3 Element `<md:EntitiesDescriptor>`

This element is used as described in [SAML2Meta]. Multiple entities can be collected into groups using this element.

2.4 Element `<md:EntityDescriptor>`

A SAML V1.x identity or service provider SHOULD be represented by exactly one `<md:EntityDescriptor>`. Its unique identifier MUST be placed in the `entityID` XML attribute. It is

RECOMMENDED that this identifier follow the rules for SAML V2.0 "entity" identifiers, as described in section 8.3.6 of [SAML2Core].

In the case of an identity provider, the `entityID` MUST match the `Issuer` attribute that the identity provider includes in the assertions that it generates. In the case of a service provider, the `entityID` MUST be the `<saml:Audience>` value that the service provider associates with itself (such as would be used in assertions that contain a `<saml:AudienceRestrictionCondition>`).

The schema definition for the `entityID` XML attribute requires that the value be a URI of no more than 1024 characters in length. Therefore, only SAML V1.x entities able to identify themselves in this fashion are able to use this profile.

For the purposes of SAML V1.x, only use of the `<md:IDPSSODescriptor>`, `<md:SPSSODescriptor>`, `<md:AttributeAuthorityDescriptor>`, `<md:AuthnAuthorityDescriptor>`, and `<md:PDPDescriptor>` elements is defined by this profile.

Use of the `<md:RoleDescriptor>` abstract element with an `xsi:type` derived from **`md:RoleDescriptorType`** is undefined by this profile, but MAY be defined elsewhere as appropriate; usage of the `protocolSupportEnumeration` attribute SHOULD be consistent with this profile when used with SAML V1.x entities.

The use of the `<md:AffiliationDescriptor>` element is also undefined by this profile, as the affiliation concept was introduced with SAML V2.0.

In other respects, this element is used as described in [SAML2Meta].

2.5 Element `<md:IDPSSODescriptor>`

A SAML V1.x identity provider MUST include this element in its metadata. The `protocolSupportEnumeration` XML attribute MUST include at least one of the following values:

```
urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:
1.1:protocol
```

For identity providers that support the SAML V1.x Browser/Artifact profile and the mandatory type 0x0001 artifact format [SAML11Bind], it is RECOMMENDED that the SHA-1 hash of their `entityID` be used as their `SourceID` when constructing artifacts.

SAML V1.x identity providers that do not use the SHA-1 hash of their `entityID` as their `SourceID` MUST include a `<saml1md:SourceID>` element containing the hex-encoded value of their 20-byte `SourceID` in the `<Extensions>` element of their `<md:IDPSSODescriptor>`.

The schema [SAML1MD-xsd] for the `<saml1md:SourceID>` element is as follows:

```
<schema
  targetNamespace="urn:oasis:names:tc:SAML:profiles:vlmetadata"
  xmlns:saml1md="urn:oasis:names:tc:SAML:profiles:vlmetadata"
  xmlns="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="unqualified"
  attributeFormDefault="unqualified"
  blockDefault="substitution"
  version="1.0">
  <annotation>
    <documentation>
      Document identifier: sstc-saml1x-metadata
      Location: http://www.oasis-open.org/committees/documents.php?
wg_abbrev=security
      Revision history:
      V1.0 (March 2005):
        Initial version.
    </documentation>
  </annotation>
  <element name="SourceID">
```



```

246     <simpleType>
247         <restriction base="string">
248             <pattern value="[a-f0-9]{40}"/>
249         </restriction>
250     </simpleType>
251 </element>
252 </schema>

```

Neither SAML V1.0 nor SAML V1.1 defines a protocol for initiating single sign-on at a service provider. Accordingly, this specification does not define any `Binding` URIs for use with the `<md:SingleSignOnService>` element. SAML V1.x identity providers MAY include a `<md:SingleSignOnService>` element with a `Binding` attribute that refers to a single sign-on request profile defined elsewhere. The `WantAuthnRequestsSigned` XML attribute MAY be used if it is applicable to the request profile in question.

Likewise, neither SAML V1.0 nor 1.1 defines a protocol for single logout. Accordingly, this specification does not define any `Binding` URIs for use with the `<md:SingleLogoutService>` element. SAML V1.x identity providers MAY include a `<md:SingleLogoutService>` element with a `Binding` attribute that refers to a single logout profile defined elsewhere.

The `<md:ArtifactResolutionService>` endpoint element is defined for use specifically in support of the SAML V1.x Browser/Artifact profile [SAML11Bind]. This is analogous but not identical to its purpose in [SAML2Meta]. In particular, SAML V2.0 artifacts are NOT the same as or interchangeable with SAML V1.x artifacts and CANNOT be used in the SAML V1.x Browser/Artifact profile.

Related to this, the `index` XML attribute on these elements, while required by the schema, cannot be used within the SAML V1.x Browser/Artifact profile and its use is undefined. That is, artifacts in SAML V1.x are not indexed by endpoint. All endpoints are assumed to be equivalent and MUST share state so as to have the ability to resolve any artifact issued by the identity provider.

The SAML V2.0 `<saml2:Attribute>` element (which can appear in this element) MAY be used to document support for particular SAML V1.x attributes and values. By convention, the `NameFormat` and `Name` XML attributes MUST be used to represent the SAML V1.x `AttributeNameSpace` and `AttributeName` XML attributes, respectively. Any other XML attributes, such as `FriendlyName`, MAY be present but are ignored for the purposes of identifying the corresponding SAML V1.x attribute.

Use of the `<md:ManageNameIDService>` and `<md:NameIDMappingService>` endpoint elements is undefined.

In other respects, this element is used as described in [SAML2Meta].

2.6 Element `<md:SPSSODescriptor>`

A SAML V1.x service provider MUST include this element in its metadata. The `protocolSupportEnumeration` XML attribute MUST include at least one of the following values:

```

282     urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:
283     1.1:protocol

```

The `<md:AssertionConsumerService>` element's `Binding` XML attribute MUST contain the value `urn:oasis:names:tc:SAML:1.0:profiles:browser-post` to indicate support for the SAML V1.x Browser/POST profile, or `urn:oasis:names:tc:SAML:1.0:profiles:artifact-01` to indicate support for the SAML V1.x Browser/Artifact profile [SAML11Bind].

Related to this, the use of the `index` XML attribute on these elements, while required by the schema, cannot be referenced within the SAML V1.x Browser/Artifact or Browser/POST profiles and its use is undefined.

The `AuthnRequestsSigned` XML attribute MAY be used if it is applicable to a request profile outside the scope of the SAML V1.x specifications but supported by the service provider.

The `<md:RequestedAttribute>` element (which can appear within the optional

294 <md:AttributeConsumingService> child element) MAY be used to document requirements for
295 particular SAML V1.x attributes and values. By convention, the NameFormat and Name XML attributes
296 MUST be used to represent the SAML V1.x AttributeNamespace and AttributeName XML
297 attributes, respectively. Any other XML attributes, such as FriendlyName, MAY be present but are
298 ignored for the purposes of identifying the corresponding SAML V1.x attribute.

299 As with the <md:AssertionConsumerService> element, the use of the index XML attribute on the
300 <md:AttributeConsumingService> element is required by the schema, but it cannot be referenced
301 within the SAML V1.x Browser profiles and its use is undefined. As a consequence, the use of multiple
302 <md:AttributeConsumingService> elements within a single parent element is also undefined.

303 Neither SAML V1.0 nor V1.1 defines a protocol for single logout. Accordingly, this specification does not
304 define any Binding URIs for use with the <md:SingleLogoutService> element. SAML V1.x service
305 providers MAY include a <md:SingleLogoutService> element with a Binding attribute that refers to
306 a single logout profile defined elsewhere.

307 Use of the <md:ManageNameIDService> and <md:ArtifactResolutionService> endpoint
308 elements are undefined.

309 In other respects, this element is used as described in [SAML2Meta].

310 2.7 Element <md:AttributeAuthorityDescriptor>

311 A SAML V1.x attribute authority MUST include this element in its metadata. The
312 protocolSupportEnumeration XML attribute MUST include at least one of the following values:

313 urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:
314 1.1:protocol

315 The SAML V2.0 <saml2:Attribute> element (which can appear in this element) MAY be used to
316 document support for particular SAML V1.x attributes and values. By convention, the NameFormat and
317 Name XML attributes MUST be used to represent the SAML V1.x AttributeNamespace and
318 AttributeName XML attributes, respectively.

319 In other respects, this element is used as described in [SAML2Meta].

320 Note that in most cases, the Binding attribute of the endpoints published within this element will have the
321 value urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding.

322 2.8 Element <md:AuthnAuthorityDescriptor>

323 A SAML V1.x authentication authority MUST include this element in its metadata. The
324 protocolSupportEnumeration XML attribute MUST include at least one of the following values:

325 urn:oasis:names:tc:SAML:1.0:protocol
326 urn:oasis:names:tc:SAML:1.1:protocol

327 In other respects, this element is used as described in [SAML2Meta].

328 Note that in most cases, the Binding attribute of the endpoints published within this element will have the
329 value urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding.

330 2.9 Element <md:PDPDescriptor>

331 A SAML V1.x policy decision point MUST include this element in its metadata. The
332 protocolSupportEnumeration XML attribute MUST include at least one of the following values:

333 urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:

334 1.1:protocol

335 In other respects, this element is used as described in [SAML2Meta].

336 Note that in most cases, the `Binding` attribute of the endpoints published within this element will have the
337 value `urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding`.

338 2.10 Element `<md:KeyDescriptor>`

339 The `<md:KeyDescriptor>` element is supported by this profile for the purpose of documenting the
340 public key(s) used by an entity to secure SAML V1.x profiles and bindings. Because the use of encryption
341 is not defined by SAML V1.x, use of the `<md:EncryptionMethod>` element and the `use XML` attribute
342 value of `encryption` are also undefined.

343 In other respects, this element is used as described in [SAML2Meta].

Appendix A. Acknowledgements

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

- Hal Lockhart, BEA Systems, Inc.
- Steve Anderson, BMC Software
- Rob Philpott, EMC Corporation
- Carolina Canales-Valenzuela, Ericsson
- Dana Kaufman, Forum Systems
- Ashish Patel, France Telecom
- Greg Whitehead, Hewlett-Packard Company
- Heather Hinton, IBM
- Anthony Nadalin, IBM
- Conor P. Cahill, Intel
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Tom Scavo, National Center for Supercomputing Applications
- Peter Davis, NeuStar
- Jeff Hodges, NeuStar
- Frederick Hirsch, Nokia
- Abbie Barbir, Nortel
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle
- Prateek Mishra, Oracle
- Brian Campbell, Ping Identity
- Bhavna Bhatnagar, Sun Microsystems
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- David Staggs, Veteran's Health Administration