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

Committee Draft 01, 15 March 2005

Document identifier:
sstc-saml1x-metadata-cd-01

Location:
http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editors:
Greg Whitehead (grw@trustgenix.com), Trustgenix, Inc.
Scott Cantor (cantor.2@osu.edu), Internet2

Contributors:
Prateek Mishra, Principal Identity
Tom Wisniewski, Entrust

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 is a **Committee Draft** approved by the Security Services Technical Committee on 15 March 2005.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them by filling out the web form located at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The committee will publish on its web page (http://www.oasis-open.org/committees/security) a catalog of any changes made to this document as a result of comments.

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 web page for the Security Services TC (http://www.oasis-open.org/committees/security/ipr.php).

Table of Contents

1 Introduction 4
1.1 Notation 4
2 SAML V1.x Metadata Profile 5
2.1 Element <md:EntitiesDescriptor> 5
2.2 Element <md:EntityDescriptor> 5
2.3 Element <md:IDPSSODescriptor> 6
2.4 Element <md:SPSSODescriptor> 7
2.5 Element <md:AttributeAuthorityDescriptor> 7
2.6 Element <md:AuthnAuthorityDescriptor> 8
2.7 Element <md:PDPDescriptor> 8
2.8 Element <md:KeyDescriptor> 8
3 References 9
3.1 Normative References 9
3.2 Non-Normative References 9

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 [SAML11Core].
`samlp:`	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V1.0 and V1.1 protocol namespace [SAML11Core].
`saml2:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAML2Core].
`md:`	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace [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`.

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.

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 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 1.1 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.

2.1 Element <md:EntitiesDescriptor>

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

2.2 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. Use of any other element of a type derived from **md:RoleDescriptorType** or the <md:AffiliationDescriptor> element is undefined.

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

2.3 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 urn:oasis:names:tc:SAML:1.0:protocol or urn:oasis:names:tc:SAML:1.1:protocol

It is RECOMMENDED that SAML V1.x identity providers supporting the Browser/Artifact profile and the mandatory "01" artifact format ([SAML11Bind]) use the SHA-1 hash of their entityID 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:v1metadata"
    xmlns:saml1md="urn:oasis:names:tc:SAML:profiles:v1metadata"
    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">
             <simpleType>
                   <restriction base="string">
                         <pattern value="[a-f0-9]{40}"/>
                   </restriction>
             </simpleType>
       </element>
</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 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 Browser/Artifact profile.

Related to this, the use of the `index` XML attribute on these elements, while required by the schema, cannot be referenced within the Browser/Artifact profile and its use is undefined. When supporting type "01" artifacts, all endpoints of this type within the role descriptor MUST 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.

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

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

2.4 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 `urn:oasis:names:tc:SAML:1.0:protocol` or `urn:oasis:names:tc:SAML:1.1:protocol`.

The `<md:AssertionConsumerService>` elements' `Binding` XML attributes MUST contain the value `urn:oasis:names:tc:SAML:1.0:profiles:browser-post` to indicate support for the SAML V1.1 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 (see [SAML11Bind]).

Related to this, the use of the `index` XML attribute on these elements, while required by the schema, cannot be referenced within the 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 bounds of this specification supported by the service provider.

The `<md:RequestedAttribute>` element (which can appear within the optional `<md:AttributeConsumingService>` child element) MAY be used to document requirements 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.

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

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 service providers MAY include a `<md:SingleLogoutService>` element with a `Binding` attribute that refers to a single logout profile defined elsewhere.

Use of the `<md:ManageNameIDService>` endpoint element is undefined.

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

2.5 Element <md:AttributeAuthorityDescriptor>

A SAML V1.x attribute authority MUST include this element in its metadata. The `protocolSupportEnumeration` XML attribute MUST include at least one of `urn:oasis:names:tc:SAML:1.0:protocol` or `urn:oasis:names:tc:SAML:1.1:protocol`.

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.

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

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

2.6 Element <md:AuthnAuthorityDescriptor>

A SAML V1.x authentication authority MUST include this element in its metadata. The `protocolSupportEnumeration` XML attribute MUST include at least one of `urn:oasis:names:tc:SAML:1.0:protocol` or `urn:oasis:names:tc:SAML:1.1:protocol`.

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

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

2.7 Element <md:PDPDescriptor>

A SAML V1.x policy decision point MUST include this element in its metadata. The `protocolSupportEnumeration` XML attribute MUST include at least one of `urn:oasis:names:tc:SAML:1.0:protocol` or `urn:oasis:names:tc:SAML:1.1:protocol`

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

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

2.8 Element <md:KeyDescriptor>

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

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

3 References

The following works are cited in the body of this specification.

3.1 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)*. OASIS, September 2003. Document ID oasis-sstc-saml-bindings-profiles-1.1. See http://www.oasis-open.org/committees/security/.

[SAML11Core] E. Maler et al. Assertions *and Protocols for the OASIS Security Assertion Markup Language (SAML)*. OASIS, September 2003. Document ID oasis-sstc-saml-core-1.1. See http://www.oasis-open.org/committees/security/.

[SAML1MD-xsd] S. Cantor et al. SAML V1.x metadata schema. OASIS SSTC, March 2005. Document ID sstc-saml1x-metadata. See http://www.oasisopen. org/committees/security/.

[SAML2Core] S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-core-2.0-os. See http://www.oasis-open.org/committees/security/.

[SAML2Meta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os. See http://www.oasis-open.org/committees/security/.

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/xmlschema-1/.

3.2 Non-Normative References

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

A. Acknowledgments

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

- Conor Cahill, AOL
- John Hughes, (formerly) Atos Origin
- Hal Lockhart, BEA Systems
- Mike Beach, Boeing
- Rebekah Metz, Booz Allen Hamilton
- Rick Randall, Booz Allen Hamilton
- Ronald Jacobson, Computer Associates
- Gavenraj Sodhi, Computer Associates
- Thomas Wisniewski, Entrust
- Carolina Canales-Valenzuela, Ericsson
- Dana Kaufman, Forum Systems
- Irving Reid, Hewlett-Packard
- Guy Denton, IBM
- Heather Hinton, IBM
- Maryann Hondo, IBM
- Michael McIntosh, IBM
- Anthony Nadalin, IBM
- Nick Ragouzis, individual
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Peter Davis, Neustar
- Jeff Hodges, Neustar
- Frederick Hirsch, Nokia
- Senthil Sengodan, Nokia
- Abbie Barbir, Nortel Networks
- Scott Kiester, Novell
- Cameron Morris, Novell
- Paul Madsen, NTT
- Steve Anderson, OpenNetwork
- Ari Kermaier, Oracle
- Vamsi Motukuru, Oracle
- Brian Campbell, Ping Identity
- Darren Platt, Ping Identity
- Prateek Mishra, Principal Identity
- Jim Lien, RSA Security
- John Linn, RSA Security
- Rob Philpott, RSA Security
- Deepak Chopra, SAP
- Jahan Moreh, Sigaba

- Eve Maler, Sun Microsystems
- Ronald Monzillo, Sun Microsystems
- Emily Xu, Sun Microsystems
- Greg Whitehead, Trustgenix

The editors also wish to acknowledge Tom Scavo for his contributions to this specification.

Appendix B. Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.