Metadata for SAML 1.0 Web Browser Profiles

Working Draft 00, 12 November 2002

Document identifier:

draft-sstc-saml-meta-data-00

Location:

http://www.oasis-open.org/committees/security/docs

Editor:

Prateek Mishra, Netegrity <pmishra@netegrity.com>

Contributors:

Jeff Hodges, Sun Microsystems

Abstract:

The SAML 1.0 web browser profiles require agreement between a source and destination site about metadata in the form of URLs, authentication modes, certificate authorities etc. This document describes the required metadata together with appropriate XML schema.

Status:

Interim draft. Send comments to the editor.

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should subscribe to and send comments to the security-services-comment@lists.oasis-open.org list. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

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

Table of Contents

Introduction

The SAML 1.0 web browser profiles require agreement between a source and destination site about metadata in the form of URLs, authentication modes, certificate authorities etc. This document describes the required metadata together with appropriate XML schema.

1.1 Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 **[RFC2119]**.

```
Listings of productions or other normative code appear like this.
```

```
Example code listings appear like this.
```

Note: Non-normative notes and explanations appear like this.

Conventional XML namespace prefixes are used throughout this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:
The prefix `saml:` stands for the SAML assertion namespace **[SAMLCore]**.
The prefix `samlp:` stands for the SAML request-response protocol namespace **[SAMLCore]**.
The prefix `ds:` stands for the W3C XML Signature namespace, `http://www.w3.org/2000/09/xmldsig#` **[XMLSig]**.
The prefix `SOAP-ENV:` stands for the SOAP 1.1 namespace, `http://schemas.xmlsoap.org/soap/envelope` **Error! Reference source not found.**.
The prefix `wsse:` stands for the WS-Security 1.0 namespace `http://schemas.xmlsoap.org/ws/2002/04/secext` **Error! Reference source not found.**.

2 Metadata for SAML 1.0 Web Browser Profiles

For source and destination sites to communicate with each other, they must a priori have obtained metadata regarding each other. These provider metadata include items such as X.509 certificates and service endpoints. This specification defines metadata schemas for source and destination sites that may be used for metadata exchange. However, protocols for metadata exchange are outside the scope of this specification.

2.1 Source Site Descriptor

The complex type **SourceSiteDescriptorType** contains the following elements:

`ProfileID` [Required]

The identification URI of the profile which MUST be one of the URIs given in Section 4.1.1.1 or 4.1.2.1 of [SAMLbind].

Issuer [Required]

String used as the issuer attribute of SAML assertions originating from the source site.

`InterSiteTransferURL` [Required]

The inter-site transfer URL at the source site.

`ArtifactMetaData` [Optional]

An instance of **ArtifactMetaDataType** with metadata relevant to the source site in the Browser/Artifact profile.

`FORMPostMetaData` [optional]

An instance of **FORMPostMetaDataType** with metadata relevant to the source site in the Browser/POST profile.

2.1.1 Artifact Metadata

The complex type **ArtifactMetaDataType** contains the following elements:

SourceID [Required]

This MUST be the 20 byte Source ID value used by the source site. As it includes arbitrary binary data it is represented by XML schema type **hexbinary.** A 20 byte sequence is always encoded as a sequence of 40 hecadecimal digits.

SAMLProtocolBindingID [Required]

The identification URI of the SAML protocol binding supported by the source site. The SAML protocol binding is used by the destination site to map artifacts to assertions.

SOAPProtocolBindingMetaData [Optional]

An instance of **SOAPProtocolBindingMetaDataType** with metadata required when the selected protocol binding is the SAML 1.0 SOAP binding.

2.1.1.1 SOAP Protocol Binding Metadata

The complex type **SOAPProtocolBindingMetaDataType** contains the following elements:

`SOAPResponderURL` [Required]

URL for the SAML SOAP responder at the source site.

TrustModel [Required]

An instance of **TrustModelType** with metadata describing the trust relationship between the source and destination sites.

2.1.1.1.1 TrustModelType

The complex type **TrustModelType** contains the following elements:

TrustRelationship [Required]

An instance of **TrustRelationshipType** which describes the trust relationship between the source and destination sites:

1. NoAuth : Neither source nor destination site authenticate to each other.
2. BasicAuth: Destination site authenticates to source site using Basic authentication.
3. ServerSideSSL: Source site authenticates to the destination site using TLS/SSL with a server-side X509 certificate. Destination site does not authenticate to the source site.
4. BasicOverSSL: Source site authenticates to the destination site using TLS/SSL with a server-side X509 certificate. Destination site authenticates to source site using Basic authentication.
5. ClientSideCertificate: Source site authenticates to the destination site using TLS/SSL with a server-side X509 certificate. Destination site authenticates to source site using a client-side X509 certificate.

NameAndPassword [Optional]

Name and password to be used by destination site if it authenticates using Basic authentication.

Keyinfo [Optional]

X509 certificate used by source site for server-side SSL.

2.1.1.1.2 TrustModelType Schema

```
<xs:simpleType name="TrustRelationshipType">
```

```
        <xs:restriction base="xsi:string">
        <xs:enumeration value="NoAuth"/>
        <xs:enumeration value="BasicAuth"/>
        <xs:enumeration value="ServerSideSSL"/>
         <xs:enumeration value="BasicOverSSL"/>
         <xs:enumeration value="ClientSideCertificate"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="NameAndPasswordType">
            <xs:attribute name="Name" type="xsi:string"/>
            <xs:attribute name="Password" type="xsi:string"/>
    </xs:complexType>
    <xs:complexType name="TrustModelType">
        <xs:sequence>
        <xs:element name="TrustRelationship" type="TrustRelationshipType"/>
        <xs:element name="NameAndPassword" type="NameAndPasswordType" minOccurs="0"/>
        <xs:element ref= "ds:Keyinfo" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
```

2.1.2 FORMPost Metadata

The complex type **FORMPostMetadataType** contains the following element:

KeyInfo [Required]

X509 certificate or public key associated with the source site signature on the <saml:Response> element transmitted to the destination site.

2.2 Source Site Descriptor

The complex type **SourceSiteDescriptorType** contains the following elements:

ArtifactReceiverURL [Optional]

Required for Browser/Artifact Profile: URL corresponding to the artifact receiver host name and path (Section 4.1.1.5 of [SAMLbind]).

AssertionConsumerServiceURL [Optional]

Required for Browser/POST profile: URL corresponding the assertion consumer host name and path (Section 4.1.2.4 of [SAMLbind]).

KeyInfo [Optional]

May be required for Browser/Artifact Profile: X509 certificate used by destination site, when authenticating to source site with client-side certificates over SSL.

3 References

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[SAMLBind] P. Mishra (Editor), Bindings and Profiles for the OASIS *Security Assertion Markup Language (SAML)*, Committee Specification 01, available from http://www.oasis-open.org/committees/security, OASIS, May 2002.

[SAMLCore] P. Hallam-Baker, P., and E. Maler, (Editors), *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, Committee Specification 01, available from http://www.oasis-open.org/committees/security, OASIS, May 2002.

[SAMLReqs] D. Platt et al., SAML Requirements and Use Cases, OASIS, December 2001.

[SAMLSecure] Security and Privacy Cpnsiderations for the OASIS Security Assertion Markup Language (SAML), http://www.oasis-open.org/committees/security/docs/cs-sstc-sec-consider-01.doc.

[XMLSig] D. Eastlake et al., *XML-Signature Syntax and Processing*, http://www.w3.org/TR/xmldsig-core/, World Wide Web Consortium.

[LAProtSchema] John D. Beatty, John Kemp, Liberty Protocols and Schemas Specification, Draft Version 1.1-05, November 2002.

[SAMLInterOp] Prateek Mishra, Proposed InterOp Scenario for SAML at Catalyst 2002, April 26, 2002, available at http://lists.oasis-open.org/archives/saml-dev/200206/msg00209.html

Appendix A. Revision History

Rev	Date	By Whom	What
wd-00	2002-06-16	Prateek Mishra	First draft based on discussion with Jeff Hodges

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.