



# 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](mailto: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](mailto:security-services@lists.oasis-open.org) list. Others should subscribe to and send comments to the [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org) list. To subscribe, send an email message to [security-services-comment-request@lists.oasis-open.org](mailto: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/>).

---

28 **Table of Contents**

29 Introduction ..... 3  
30 1.1 Notation ..... 3  
31 2 Metadata for SAML 1.0 Web Browser Profiles ..... 4  
32 2.1 Source Site Descriptor ..... 4  
33 2.1.1 Artifact Metadata ..... 4  
34 2.1.1.1 SOAP Protocol Binding Metadata ..... 5  
35 2.1.2 FORMPost Metadata ..... 6  
36 2.2 Source Site Descriptor ..... 6  
37 3 References ..... 7  
38 Appendix A. Revision History ..... 8  
39 Appendix B. Notices ..... 9  
40

---

## 41 Introduction

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

### 45 1.1 Notation

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

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

50  
51 Example code listings appear like this.

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

53 Conventional XML namespace prefixes are used throughout this specification to stand for their  
54 respective namespaces as follows, whether or not a namespace declaration is present in the  
55 example:

56 The prefix `saml:` stands for the SAML assertion namespace [SAMLCore].

57 The prefix `samlp:` stands for the SAML request-response protocol namespace [SAMLCore].

58 The prefix `ds:` stands for the W3C XML Signature namespace,

59 `http://www.w3.org/2000/09/xmldsig#` [XMLSig].

60 The prefix `SOAP-ENV:` stands for the SOAP 1.1 namespace,

61 `http://schemas.xmlsoap.org/soap/envelope` **Error! Reference source not  
62 found..**

63 The prefix `wsse:` stands for the WS-Security 1.0 namespace

64 `http://schemas.xmlsoap.org/ws/2002/04/secext` **Error! Reference source not  
65 found..**

---

## 2 Metadata for SAML 1.0 Web Browser Profiles

66  
67  
68  
69  
70  
71  
72

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

73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100

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

101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113

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 hexadecimal 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.

114  
115 SOAPProtocolBindingMetaData [Optional]  
116  
117 An instance of **SOAPProtocolBindingMetaDataType** with metadata required when the selected  
118 protocol binding is the SAML 1.0 SOAP binding.  
119

### 120 **2.1.1.1 SOAP Protocol Binding Metadata**

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

122  
123 SOAPResponderURL [Required]  
124  
125 URL for the SAML SOAP responder at the source site.

126  
127 TrustModel [Required]

128  
129 An instance of **TrustModelType** with metadata describing the trust relationship between the  
130 source and destination sites.  
131

#### 132 **2.1.1.1.1 TrustModelType**

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

134  
135 TrustRelationship [Required]

136  
137 An instance of **TrustRelationshipType** which describes the trust relationship between the source  
138 and destination sites:

- 139
- 140 1. NoAuth : Neither source nor destination site authenticate to each other.
  - 141 2. BasicAuth: Destination site authenticates to source site using Basic authentication.
  - 142 3. ServerSideSSL: Source site authenticates to the destination site using TLS/SSL with a  
143 server-side X509 certificate. Destination site does not authenticate to the source site.
  - 144 4. BasicOverSSL: Source site authenticates to the destination site using TLS/SSL with a  
145 server-side X509 certificate. Destination site authenticates to source site using Basic  
146 authentication.
  - 147 5. ClientSideCertificate: Source site authenticates to the destination site using TLS/SSL  
148 with a server-side X509 certificate. Destination site authenticates to source site using a  
149 client-side X509 certificate.

150  
151 NameAndPassword [Optional]

152  
153 Name and password to be used by destination site if it authenticates using Basic authentication.

154  
155 Keyinfo [Optional]

156  
157 X509 certificate used by source site for server-side SSL.  
158  
159  
160

#### 161 **2.1.1.1.2 TrustModelType Schema**

162  
163 `<xs:simpleType name="TrustRelationshipType">`

```

164     <xs:restriction base="xsi:string">
165     <xs:enumeration value="NoAuth"/>
166     <xs:enumeration value="BasicAuth"/>
167     <xs:enumeration value="ServerSideSSL"/>
168     <xs:enumeration value="BasicOverSSL"/>
169     <xs:enumeration value="ClientSideCertificate"/>
170     </xs:restriction>
171 </xs:simpleType>
172 <xs:complexType name="NameAndPasswordType">
173     <xs:attribute name="Name" type="xsi:string"/>
174     <xs:attribute name="Password" type="xsi:string"/>
175 </xs:complexType>
176 <xs:complexType name="TrustModelType">
177     <xs:sequence>
178     <xs:element name="TrustRelationship" type="TrustRelationshipType"/>
179     <xs:element name="NameAndPassword" type="NameAndPasswordType" minOccurs="0"/>
180     <xs:element ref="ds:Keyinfo" minOccurs="0"/>
181     </xs:sequence>
182 </xs:complexType>
183
184
185

```

## 186 2.1.2 FORMPost Metadata

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

188  
189 KeyInfo [Required]  
190  
191 X509 certificate or public key associated with the source site signature on the <saml:Response>  
192 element transmitted to the destination site.  
193

## 194 2.2 Source Site Descriptor

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

196  
197 ArtifactReceiverURL [Optional]  
198  
199 Required for Browser/Artifact Profile: URL corresponding to the artifact receiver host name and  
200 path (Section 4.1.1.5 of [SAMLbind]).  
201  
202 AssertionConsumerServiceURL [Optional]  
203  
204 Required for Browser/POST profile: URL corresponding the assertion consumer host name and  
205 path (Section 4.1.2.4 of [SAMLbind]).  
206  
207 KeyInfo [Optional]  
208  
209 May be required for Browser/Artifact Profile: X509 certificate used by destination site, when  
210 authenticating to source site with client-side certificates over SSL.  
211  
212  
213  
214  
215

---

## 3 References

216

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

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

224 **[SAMLCore]** P. Hallam-Baker, P., and E. Maler, (Editors), *Assertions and*  
225 *Protocol for the OASIS Security Assertion Markup Language*  
226 *(SAML)*, Committee Specification 01, available from  
227 <http://www.oasis-open.org/committees/security>, OASIS, May  
228 2002.

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

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

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

238 **[LAProtSchema]** John D. Beatty, John Kemp, *Liberty Protocols and*  
239 *Schemas Specification*, Draft Version 1.1-05, November  
240 2002.

241

242 **[SAMLInterOp]** Prateek Mishra, *Proposed InterOp Scenario for SAML at*  
243 *Catalyst 2002*, April 26, 2002, available at [http://lists.oasis-](http://lists.oasis-open.org/archives/saml-dev/200206/msg00209.html)  
244 [open.org/archives/saml-dev/200206/msg00209.html](http://lists.oasis-open.org/archives/saml-dev/200206/msg00209.html)  
245

246

---

## Appendix A. Revision History

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

247



---

## Appendix B. Notices

249 OASIS takes no position regarding the validity or scope of any intellectual property or other rights  
250 that might be claimed to pertain to the implementation or use of the technology described in this  
251 document or the extent to which any license under such rights might or might not be available;  
252 neither does it represent that it has made any effort to identify any such rights. Information on  
253 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS  
254 website. Copies of claims of rights made available for publication and any assurances of licenses  
255 to be made available, or the result of an attempt made to obtain a general license or permission  
256 for the use of such proprietary rights by implementors or users of this specification, can be  
257 obtained from the OASIS Executive Director.

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

261 Copyright © OASIS Open 2002. *All Rights Reserved.*

262 This document and translations of it may be copied and furnished to others, and derivative works  
263 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,  
264 published and distributed, in whole or in part, without restriction of any kind, provided that the  
265 above copyright notice and this paragraph are included on all such copies and derivative works.  
266 However, this document itself does not be modified in any way, such as by removing the  
267 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS  
268 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual  
269 Property Rights document must be followed, or as required to translate it into languages other  
270 than English.

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

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