



Metadata for SAML 1.0 Web Browser Profiles

Working Draft 01, 1 February 2003

Document identifier:

draft-sstc-saml-meta-data-01

Deleted: 0

Location:

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

Editor:

Prateek Mishra, Netegrity <pmishra@netegrity.com>

Contributors:

Jeff Hodges, Sun Microsystems

[Charles Knouse, Oblix](#)

[Jahan Moreh, Sigaba](#)

[Rob Philpott, RSA](#)

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/>).

Deleted: 2002

31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46

Table of Contents

[Introduction](#) [3](#)
[1.1 Notation](#) [3](#)
[1.2 Schema Organization and Namespaces](#) [3](#)
[2 Metadata for SAML 1.0 Web Browser Profiles](#) [4](#)
[2.1 Element <SourceSiteList>](#) [4](#)
[2.1.1 Element <SourceSiteDescriptor>](#) [4](#)
[2.1.2 Element <ArtifactMetadata>](#) [5](#)
[2.1.3 Element <FORMPost Metadata>](#) [7](#)
[2.2 Element <DestinationSiteList>](#) [7](#)
[2.2.1 Element <DestinationSiteDescriptor>](#) [8](#)
[2 Example](#) [9](#)
[References](#) [10](#)
[Appendix A. Revision History](#) [11](#)
[Appendix B. Notices](#) [12](#)

Deleted: 8

Deleted: 2002

47 **Introduction**

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

51 **1.1 Notation**

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

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

56 `Example code listings appear like this.`

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

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

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

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

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

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

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

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

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

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

71

72 **1.2 Schema Organization and Namespaces**

73 The SAML metadata structures are defined in a schema [SAMLMETA-XSD] associated with the
74 following namespace:

75 `urn:oasis:names:tc:SAML:1.1:metadata`
76
77

Formatted: Bullets and Numbering

Deleted: 2002

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 Element <SourceSiteList>

The <SourceSiteList> element is a container for one or more <SourceSiteDescriptor> elements.

```
<complexType name="SourceSiteListType">
  <sequence>
    <element ref="SourceSiteDescriptor" maxOccurs="unbounded" />
  </sequence>
</complexType>
<element name="SourceSiteList" type="samlmeta:SourceSiteListType" />
```

Formatted: Bullets and Numbering

2.1.1 Element <SourceSiteDescriptor>

```
<element name="SourceSiteDescriptor"
  type="samlmeta:SourceSiteDescriptorType"/>
<complexType name="SourceSiteDescriptorType">
  <sequence>
    <element name="SourceSiteName" type="string" />
    <element name="ProfileID" type="anyURI" />
    <element name="Issuer" type="string" />
    <element name="InterSiteTransferURL" type="anyURI" />
    <element name="NameIdentifierFormat" type="anyURI" maxOccurs="0" />
    <element ref="saml:AttributeDesignator" minOccurs="0"
      maxOccurs="unbounded" />
    <element ref="samlp:RespondWith" maxOccurs="unbounded" />
    <element ref="saml:SubjectLocality" maxOccurs="0" />
  <choice>
    <element ref="ArtifactMetaData" />
    <element ref="FORMPostMetaData" />
  </choice>
</sequence>
</complexType>
```

Formatted: Bullets and Numbering

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

[SourceSiteName](#) [Required]

[Descriptive name of the source site.](#)

Deleted: 2002

127 ProfileID [Required]
128
129 The identification URI of the profile which MUST be one of the URIs given in Section 4.1.1.1 or
130 4.1.2.1 of [SAMLbind].

131
132 Issuer [Required]
133
134 String used as the issuer attribute of SAML assertions originating from the source site.

135
136 InterSiteTransferURL [Required]
137
138 The inter-site transfer URL at the source site.

139 [NameIdentifierFormat](#) [Optional]
140
141 [The syntax used to describe the name of the subject. Its value MUST be one of the URI](#)
142 [references defined on lines 602-615 of \[SAMLCore\].](#)

143
144 [<saml:AttributeDesignator>](#) [Optional]
145
146 [One or more <saml:AttributeDesignator> elements describe attribute names and attribute](#)
147 [namespaces found in assertions transferred from source to destination sites.](#)

148
149 [<samlp:RespondWith>](#) [Required]
150
151 [One or more instances of the <samlp:RespondWith> element describe the types of statements](#)
152 [found in assertions transferred from source to destination sites.](#)

153
154 [<saml:SubjectLocality>](#) [Optional]
155
156 [The <saml:SubjectLocality> element indicates whether this element is included in the](#)
157 [authentication statement found in the SSO assertion. If attributes IPAddress or DNSAddress](#)
158 [together with their values are also included, then those attributes and values will also be found in](#)
159 [the SSO assertion.](#)

160
161 ArtifactMetaData [Optional]
162
163 An instance of **ArtifactMetaData** with metadata relevant to the source site in the
164 Browser/Artifact profile.

165
166 FORMPostMetaData [Optional]
167
168 An instance of **FORMPostMetaData** with metadata relevant to the source site in the
169 Browser/POST profile.

170 [2.1.2 Element <ArtifactMetadata>](#)

```
171  
172  
173  
174 <element name="ArtifactMetadata" type="samlmeta:ArtifactMetadataType"/>  
175 <complexType name="ArtifactMetadataType">  
176 <sequence>  
177 <element name="SourceID" type="hexBinary"/>  
178 <element name="SAMLProtocolBindingID" type="anyURI" />  
179 <element name="SOAPProtocolBindingMetadata"  
180 type="samlmeta:SOAPProtocolBindingMetadataType" minOccurs="0" />
```

Deleted: o

Deleted: ¶
¶

Formatted: Bullets and Numbering

Deleted:

Deleted: 2002

181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201

```
</sequence>  
</complexType>
```

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.

SOAPProtocolBindingMetadata [Optional]

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

202
203
204
205
206
207
208
209
210
211
212
213

2.1.2.1 Element <SOAPProtocolBindingMetadata>

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.

Deleted:
Formatted: Bullets and Numbering
Deleted:
Deleted:

214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233

2.1.2.1.1 Element <TrustModelType>

```
<simpleType name="TrustRelationshipType">  
  <restriction base="string">  
    <enumeration value="NoAuth"/>  
    <enumeration value="BasicAuth"/>  
    <enumeration value="ServerSideSSL"/>  
    <enumeration value="BasicOverSSL"/>  
    <enumeration value="ClientSideCertificate"/>  
  </restriction>  
</simpleType>  
  
<complexType name="NameAndPasswordType">  
  <attribute name="Name" type="string"/>  
  <attribute name="Password" type="hexBinary"/>  
</complexType>  
<complexType name="TrustModelType">  
  <sequence>  
    <element name="TrustRelationship"  
      type="samlmeta:TrustRelationshipType" />  
  </sequence>  
</complexType>
```

Formatted: Bullets and Numbering

Deleted: 2002

234
235
236
237
238

239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272

```
<element name="NameAndPassword" type="samlmeta:NameAndPasswordType"
minOccurs="0" />
<element ref="ds:X509Certificate" minOccurs="0"/>
</sequence>
</complexType>
```

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 [SHA-1 hash \[SHA\] of the password](#) to be used by destination site [should](#), it authenticate, using Basic authentication.

Deleted: if

Deleted: s

[<ds:X509Certificate>](#) [Optional]

Deleted: Keyinfo

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

Formatted: Bullets and Numbering

[2.1.3 Element <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 Element <DestinationSiteList>](#)

The [<DestinationSiteList>](#) element is a container for one or more [<DestinationSiteDescriptor>](#) elements.

Deleted: 2002

```
286 <element name="DestinationSiteList"  
287 type="samlmeta:DestinationSiteListType" />  
288 <complexType name="DestinationSiteListType">  
289 <sequence>  
290 <element ref="samlmeta:DestinationSiteDescriptor" maxOccurs="unbounded"  
291 />  
292 </sequence>  
293 </complexType>
```

Formatted: Bullets and Numbering

2.2.1 Element <DestinationSiteDescriptor>

```
296 <element name="DestinationSiteDescriptor"  
297 type="samlmeta:DestinationSiteDescriptorType" />  
298 <complexType name="DestinationSiteDescriptorType">  
299 <sequence>  
300 <element name="DestinationSiteName" type="string" />  
301 <element name="ArtifactReceiverURL" type="anyURI" minOccurs="0" />  
302 <element name="AssertionConsumerURL" type="anyURI" minOccurs="0" />  
303 <element ref="ds:X509Certificate" minOccurs="0" />  
304 </sequence>  
305 </complexType>
```

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

Deleted: Source

[DestinationSiteName](#) [Required]

[Descriptive name of the source site.](#)

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]).

[<ds:X509Certificate>](#) [Optional]

Deleted: KeyInfo

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

Deleted: SL.¶
¶

Deleted: 2002

331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364

```
Example<SourceSiteList>  
<SourceSiteDescriptor>  
  <SourceSiteName>example.com</SourceSiteName>  
  
  <ProfileID>urn:oasis:names:tc:SAML:1.0:profiles:artifact_01</ProfileID>  
  <Issuer>www.baltimore.com</Issuer>  
  
  <InterSiteTransferURL>https://samltest.baltimore.com:9985/saml_in/</InterSiteTransferURL>  
  <ArtifactMetaData>  
  
    <SourceID>1ea6b9afbc7e9fa72b95f73362624fe13da6be65</SourceID>  
  
    <SAMLProtocolBindingID>urn:oasis:names:tc:SAML:1.0:bindings:SOAPbinding</SAMLProtocolBindingID>  
    <SOAPProtocolBindingMetaData>  
  
      <SOAPResponderURL>https://samltest.baltimore.com:9984/saml_responder/</SOAPResponderURL>  
      <TrustModel>  
  
        <TrustRelationship>ClientSideCertificate</TrustRelationship>  
        <X509Certificate>  
          . . .  
        </X509Certificate>  
      </TrustModel>  
    </SOAPProtocolBindingMetaData>  
  </ArtifactMetaData>  
</SourceSiteDescriptor>  
</SourceSiteList>
```

Deleted: ¶

TBD

Deleted: 2002

365

References

366

[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.

367

368

369

[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.

370

371

372

[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.

373

374

375

376

377

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

378

379

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

380

381

382

383

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

384

385

386

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

387

388

389

390

[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>

391

392

393

394

[\[SALMETA-XSD\] draft-sstc-schema-meta-data-01.xsd](#)

395

396

Appendix A. Revision History

Rev	Date	By Whom	What
wd-00	2002-06-16	Prateek Mishra	First draft based on discussion with Jeff Hodges
01	2003-02-01	Prateek Mishra	Review from TC

397

398

Deleted: 2002

Appendix B. Notices

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

409 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
410 applications, or other proprietary rights which may cover technology that may be required to
411 implement this specification. Please address the information to the OASIS Executive Director.
412 Copyright © OASIS Open 2002. *All Rights Reserved.*

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

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

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