



Expressing Identity Assurance in SAML V2.0

Working Draft 01

24 August 2009

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-draft-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-draft-01.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-draft-01.pdf>

Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-draft-00.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-00.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-00.pdf>

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.

Thomas Hardjono, MIT Kerberos Consortium

Editor(s):

Eric Tiffany, Liberty Alliance

Paul Madsen, NTT

Scott Cantor, Internet2

RL "Bob" Morgan, Internet2

Related Work:

This specification profiles the SAML 2.0 Authentication Context [SAMLAC] mechanisms to allow SAML authentication requests and assertions to carry assurance information. It relies the features specified in [SAMLMA] to represent information about a SAML entity as a SAML attribute associated with a metadata entry.

Declared XML Namespace(s):

Abstract:

This document specifies methods of representing assurance information as used in two aspects of SAML. It profiles the use of SAML's Authentication Context mechanisms to express

35 per-authentication assurance information via authentication requests and assertions. Level-of-
36 Assurance (LOA) definitions in Identity Assurance Frameworks are expressed as a set of
37 authentication context classes. The document also specifies a means for representing
38 assurance certification status of entities in SAML metadata.

39 **Status:**

40 This document was last revised or approved by the SSTC on the above date. The level of
41 approval is also listed above. Check the current location noted above for possible later
42 revisions of this document. This document is updated periodically on no particular schedule.

43 TC members should send comments on this specification to the TC's email list.

44 Others should send comments to the TC by using the "Send A Comment" button on
45 the TC's web page at <http://www.oasis-open.org/committees/security>.

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

49 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/security)
50 [open.org/committees/security](http://www.oasis-open.org/committees/security).

51 Notices

52 Copyright © OASIS® 2009. All Rights Reserved.

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

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

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

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

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

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

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

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

95 **Table of Contents**

96 1 Introduction.....5

97 1.1 Motivation [Non-Normative].....5

98 1.2 Limitations [Non-Normative].....5

99 1.3 Terminology.....6

100 1.4 Normative References.....6

101 1.5 Non-normative References.....7

102 1.6 Conformance.....7

103 1.6.1 AuthnContext Level-of-Assurance Profile Conformance.....7

104 1.6.2 Attribute Profile Conformance.....7

105 2 AuthnContext Level-of-Assurance Profile.....8

106 2.1 Required Information.....8

107 2.2 AuthnContext Schema.....8

108 2.3 Example LOA Framework classes.....9

109 3 Identity Assurance Certification Attribute Profile.....11

110 3.1 Required Information.....11

111 3.2 Profile Overview.....11

112 3.3 SAML Attribute Naming.....11

113 3.4 Profile-Specific XML Attributes.....11

114 3.5 SAML Attribute Values.....11

1 Introduction

115

116 *Expressing Identity Assurance in SAML 2.0* provides standard means for parties using SAML to
117 exchange information regarding identity assurance. It defines, as a profile of the SAML Authentication
118 Context [SAMLAC] specification, a restricted version of the AuthnContext schema for representing
119 assurance indicators (sometimes called levels of assurance) defined by external documentation of any
120 given assurance framework. In addition, it defines a SAML attribute profile that may be used to
121 represent the certification status of an issuer of authentication statements (i.e., an Identity Provider)
122 regarding its conformance with the requirements of an identity assurance framework.

1.1 Motivation [Non-Normative]

123

124 Many organizations using federated service access have found it useful to define or adopt “identity
125 assurance frameworks,” such as [LibertyIAF]. Such frameworks offer a model for categorizing the
126 large number of possible combinations of registration processes, security mechanisms, and
127 authentication methods that underlie authentication processes into a smaller, more manageable set.
128 The term “levels of assurance” (LOA) is often used to refer to this concept, or a particular such set
129 (“assurance profiles” is also used). Different combinations of processes and technology are rated
130 according to the quality of assurance they can provide. Typically, a framework defines 3-5 levels or
131 profiles, ranging from low to high assurance. Relying parties then decide which LOA is required to
132 access specific protected resources, based on an assessment of the risk associated with those
133 resources – high risk requires high assurance, for example – and work with identity providers to ensure
134 that the requirements of that level are met.

135 Given this interest, it is useful for parties using SAML for federation to express in SAML authentication
136 messages the LOA requested by a relying party, and the LOA that is applicable to an authentication
137 response. The SAML authentication context specification [SAMLAC] defines a variety of options for
138 representing the details of identity management processes and mechanisms. The LOA profile in this
139 document is motivated by two related considerations:

- 140 • The SAML authentication context scheme is comprehensive, but quite complex. Deployers find
141 that this complexity is a barrier to designing authentication contexts that match their LOA
142 requirements.
- 143 • Representing the details of a LOA definition using the full expressiveness of the authentication
144 context schema results in XML documents that must be passed in-band with authentication
145 events and parsed by SAML implementations. In most cases, the processing requirements are
146 not sustainable and interoperability issues have not been explored.

147 The approach taken here simply represents each LOA in an assurance framework as a separate
148 authentication context class. Each LOA class is characterized by a URI, and the body of the schema
149 simply contains a reference to the external documentation that defines the LOA. These URI values are
150 conveyed in the `<RequestedAuthnContext>` element of an authentication request and the
151 `<AuthnContextClassRef>` element in the assertion within any authentication response.

152 Another common element in assurance programs is certification. See section 5.2 for background and
153 motivation for expressing assurance certification status in a standard fashion in SAML.

1.2 Limitations [Non-Normative]

154

155 A limitation to the LOA profile defined in this document is that the URIs representing the levels must be
156 configured into every system in the deployment, and the ordering of the URI levels must be decided
157 and configured out-of-band.

158 **1.3 Terminology**

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

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

164 These keywords are thus capitalized when used to unambiguously specify requirements over protocol
165 and application features and behavior that affect the interoperability and security of implementations.
166 When these words are not capitalized, they are meant in their natural-language sense.

167 Listings of XML schemas appear like this.

168 Example code listings appear like this.

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

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAMLCore].
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace defined in the SAML V2.0 core specification [SAMLCore].
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.

173 This specification uses the following typographical conventions in text: <SAML*Element*>,
174 <ns:ForeignElement>, Attribute, **Datatype**, OtherCode.

175 **1.4 Normative References**

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

178

179 **[SAMLAC]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup
180 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-
181 context-2.0-os. See <http://www.oasis-open.org/committees/security/>.

182 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
183 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See
184 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

185 **[SAMLMA]** S. Cantor *SAML V2.0 Metadata Extension for Entity Attributes*. OASIS SSTC,
186 August 2009. Document ID sstc-metadata-attrib-cs-01. See [http://www.oasis-
187 open.org/committees/security/](http://www.oasis-open.org/committees/security/).

188 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
189 (SAML) V2.0*. OASIS Standard, March 2005. See [http://docs.oasis-
190 open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

- 191 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
192 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/)
193 [xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/). Note that this specification normatively references
194 [Schema2], listed below.
- 195 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide
196 Web Consortium Recommendation, May 2001. See
197 <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>.

198 **1.5 Non-normative References**

- 199 **[LibertyIAF]** Russ Cutler, ed. Liberty Identity Assurance Framework 1.0, Liberty Alliance
200 Project, 2008.

201 **1.6 Conformance**

202 **1.6.1 AuthnContext Level-of-Assurance Profile Conformance**

- 203 To conform to this profile, implementations MUST support the use of the
204 <samlp:RequestedAuthnContext> and <saml:AuthnContext> elements defined by [SAMLCore].

205 **1.6.2 Identity Assurance Certification Attribute Profile Conformance**

- 206 An asserting party (typically, a metadata publisher) conforms to this profile if it can generate valid
207 SAML instances containing the SAML attribute defined in this profile.
- 208 A relying party (typically, a metadata consumer) conforms to this profile if it can process the SAML
209 attribute defined in this profile and make the results available for further processing.
- 210 All parties must also meet the conformance requirements in [SAMLMA].

211 2 AuthnContext Level-of-Assurance Profile

212 2.1 Required Information

213 **Identification:** urn:oasis:names:tc:SAML:2.0:ac:profiles:assurance

214 **Contact Information:** security-services-comment@lists.oasis-open.org

215 **Description:** Given below.

216 **Updates:** None.

217 2.2 AuthnContext Schema

218 The following schema redefines the basic abstract `AuthnContextDeclarationBaseType` to limit the
219 allowed elements to the `GoverningAgreements` element. It will be through this element that the
220 appropriate external assurance framework documentation will be referenced.

```
221 <?xml version="1.0" encoding="UTF-8"?>
222 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
223   finalDefault="extension"
224   blockDefault="substitution" version="2.0">
225   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
226     <xs:annotation>
227       <xs:documentation>
228         Base class for building level-of-assurance style AuthnContext
229         class definitions.
230       </xs:documentation>
231     </xs:annotation>
232
233     <xs:complexType name="AuthnContextDeclarationBaseType">
234       <xs:complexContent>
235         <xs:restriction base="AuthnContextDeclarationBaseType">
236           <xs:sequence>
237             <xs:element ref="Identification"
238               minOccurs="0" maxOccurs="0"/>
239             <xs:element ref="TechnicalProtection"
240               minOccurs="0" maxOccurs="0"/>
241             <xs:element ref="OperationalProtection"
242               minOccurs="0" maxOccurs="0"/>
243             <xs:element ref="AuthnMethod"
244               minOccurs="0" maxOccurs="0"/>
245             <xs:element ref="GoverningAgreements"
246               minOccurs="1" maxOccurs="1"/>
247             <xs:element ref="Extension" minOccurs="0"
248               maxOccurs="unbounded"/>
249           </xs:sequence>
250           <xs:attribute name="ID" type="xs:ID" use="optional"/>
251         </xs:restriction>
252       </xs:complexContent>
253     </xs:complexType>
254
255     <xs:complexType name="GoverningAgreementRefType">
256       <xs:annotation>
257         <xs:documentation>
258           A specific restriction of this type specifying or
259           enumerating the governing document(s) and/or section
260           within such document(s) that define this particular
261           level of assurance.
```

```

262         </xs:documentation>
263     </xs:annotation>
264     <xs:complexContent>
265         <xs:restriction base="GoverningAgreementRefType">
266             <xs:attribute name="governingAgreementRef"
267                 type="xs:anyURI" use="required"/>
268         </xs:restriction>
269     </xs:complexContent>
270 </xs:complexType>
271 </xs:redefine>
272 </xs:schema>

```

273 The functional definition of the `GoverningAgreementRefType` is not changed from the original
274 schema in [SAMLAC], but documentation is added to serve as a reminder that definitions derived from
275 this schema should redefine `GoverningAgreementRefType` to suit a particular LOA purpose.

276 2.3 Example LOA Framework classes

277 We show here a set of LoA classes for a fictional FAF (Foo Assurance Framework) with three different
278 levels of assurance. The 3 LOA schemas will extend the base LOA schema defined above. Each LOA
279 schema will reference the corresponding section of the FAF documentation.

280 We define the following URIs to represent the 3 LOA

- 281 ● <http://foo.example.com/assurance/loa1>
- 282 ● <http://foo.example.com/assurance/loa2>
- 283 ● <http://foo.example.com/assurance/loa3>

284 As an example, the schema for the level 1 might look like:

```

285 <?xml version="1.0" encoding="UTF-8"?>
286 <xs:schema
287     targetNamespace="http://foo.example.com/assurance/loa1"
288     xmlns:xs="http://www.w3.org/2001/XMLSchema"
289     xmlns="http://foo.example.com/assurance/loa1"
290     finalDefault="extension"
291     blockDefault="substitution"
292     version="2.0">
293
294     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
295
296         <xs:annotation>
297             <xs:documentation>
298                 Class identifier:
299                 http://foo.example.com/assurance/loa1
300
301                 Defines Level 1 of FAF
302             </xs:documentation>
303         </xs:annotation>
304
305         <xs:complexType name="GoverningAgreementRefType">
306             <xs:complexContent>
307                 <xs:restriction base="GoverningAgreementRefType">
308                     <xs:attribute name="governingAgreementRef"
309                         type="xs:anyURI"
310                         fixed="http://foo.example.com/foo_assurance.pdf#sect
311 ion1"
312                         use="required"/>

```

```
313         </xs:restriction>
314     </xs:complexContent>
315 </xs:complexType>
316 </xs:redefine>
317 </xs:schema>
```

318

319 The class schemas for the other 2 FAF LOA would refer to the corresponding section of the FAF
320 documentation.

321 **3 Identity Assurance Certification Attribute Profile**

322 A SAML attribute is defined to represent the certification status of an Identity Provider regarding its
323 conformance to the elements of an identity assurance framework.

324 **3.1 Required Information**

325 **Identification:** urn:oasis:names:tc:SAML:2.0:attribute:profiles:assurance-certification

326 **Contact Information:** security-services-comment@lists.oasis-open.org

327 **Description:** Given below.

328 **Updates:** None.

329 **3.2 Profile Overview**

330 In some relatively simple scenarios where identity assurance is used, a relying party may have a direct
331 business relationship with an organization operating an Identity Provider that satisfies the relying party
332 that the practices of the Identity Provider conform to the requirements of an assurance framework. In a
333 larger-scale scenario, a relying party may wish to rely on a third party (a “certification service”) to certify
334 the practices of the Identity Provider organization. In this scenario, it is useful for the IdP's certification
335 status as determined by that certification service to be represented in a standard fashion, in a way that
336 can be communicated securely among the various parties involved. The SAML metadata specification
337 [SAMLMeta] defines means for information about SAML entities to be represented and communicated
338 securely.

339 This profile defines a SAML attribute that can be applied to entries in a SAML metadata document to
340 express certification status. To indicate that an Identity Provider (or group of Identity Providers) is
341 certified as conformant with an LOA, the attribute defined in this profile is added to that identity
342 Provider's entity metadata as described in [SAMLMA]. This may be done using a <saml:Attribute>
343 or a <saml:Assertion> element. A <saml:Assertion> element can be used to include an
344 assurance certification attribute that is signed independently from the enclosing metadata.

345 **3.3 SAML Attribute Naming**

346 The NameFormat XML attribute in <Attribute> elements MUST be
347 urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

348 This profile defines a single SAML attribute name:

349 urn:oasis:names:tc:SAML:attribute:assurance-certification

350 **3.4 Profile-Specific XML Attributes**

351 No additional XML attributes are defined for use with this attribute.

352 **3.5 SAML Attribute Values**

353 Values of this attribute are URIs representing LOAs as defined in section 2 of this document. Multiple
354 values may be present. This document does not define any relationship between LOAs or define
355 relying party behavior if multiple values are present. It is the responsibility of assurance framework
356 documentation to specify whether, for example, certification at a “higher” LOA implies approval to
357 assert a “lower” LOA.

358 3.6 Example

359 In this example a metadata publisher would place the SAML attribute statement in the IdP's entity
360 descriptor to indicate that the practices of the indicated IdP had been certified as conformant with the
361 requirements of the stated LOA. A party relying on this metadata could use this value as part of
362 determining whether and how to accept SAML authentication assertions from this IdP.

363

```
364 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"  
365   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  
366   xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"  
367   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
368   entityID="https://IdentityProvider.example.com/SAML">  
369   <Extensions>  
370     <attr:EntityAttributes>  
371       <saml:Attribute  
372         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
373         Name="urn:oasis:names:tc:SAML:attribute:assurance-  
374 certification">  
375         <saml:AttributeValue>  
376           http://foo.example.com/assurance/loa1  
377         </saml:AttributeValue>  
378       </saml:Attribute>  
379     </attr:EntityAttributes>  
380   </Extensions>  
381   <IDPSSODescriptor WantAuthnRequestsSigned="true"  
382     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  
383     <KeyDescriptor use="signing"> ... </KeyDescriptor>  
384     <NameIDFormat>...</NameIDFormat>  
385     <SingleSignOnService  
386       Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
387       Location="https://IdentityProvider.example.com/SAML/SSO/Browser"/>  
388     ...  
389   </IDPSSODescriptor>  
390   ...  
391 </EntityDescriptor>
```

392

393 **Appendix A. Acknowledgments**

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

- 396 • TBD

397

398

Appendix B. Revision History

399

- Draft 01 – first draft of sstc-saml-loa-authncontext-profile

400

401

- Draft 02 - minor tweaks to text. Removed editorial comments. Removed example class derived from base class.

402

- Draft 03 – removed the NIST 800 63 specific references and schema.

403

404

- Draft 00 sstc-saml-assurance-profile : renamed to reflect added material. Added certification motivation and specification.

405

406

407

- Draft 01 sstc-saml-assurance-profile : added attribute profile conformance, added attribute profile example, more description of certification usage, reorganized section numbering, put conformance material in section 1.