



Level of Assurance Authentication Context Profiles for SAML 2.0

Working Draft 01

01 July 2008

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-loa-authncontext-profile-draft-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-loa-authncontext-profile-draft-01.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-loa-authncontext-profile-draft-01.pdf>

Technical Committee:

OASIS [official name of technical committee] TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.

Brian Campbell, Ping Identity Corporation

Editor(s):

Eric Tiffany, Liberty Alliance

Paul Madsen, NTT

Scott Cantor, Internet2

Related Work:

This specification is a profile of the SAML 2.0 Authentication Context specification [SAMLAC].

Declared XML Namespace(s):

[list namespaces here]

[list namespaces here]

Abstract:

This profile reduces the scope of the mechanisms described in the full Authentication Context specification so as to provide a simplified way of representing a Level-of-Assurance (LOA) authentication scheme. A general schema restriction is presented, along with specific examples implementing the NIST 800-63 levels of assurance [NIST 800-63].

Status:

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

34 TC members should send comments on this specification to the TC's email list.
35 Others should send comments to the TC by using the "Send A Comment" button on
36 the TC's web page at <http://www.oasis-open.org/committees/security>.
37 For information on whether any patents have been disclosed that may be essential to
38 implementing this specification, and any offers of patent licensing terms, please refer to the IPR
39 section of the TC web page (<http://www.oasis-open.org/committees/security/ipr.php>).
40 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/security)
41 [open.org/committees/security](http://www.oasis-open.org/committees/security).

Notices

42

43 Copyright © OASIS® 2008. All Rights Reserved.

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

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

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

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

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

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

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

82 The names "OASIS", [insert specific trademarked names, abbreviations, etc. here] are trademarks of
83 OASIS, the owner and developer of this specification, and should be used only to refer to the
84 organization and its official outputs. OASIS welcomes reference to, and implementation and use of,
85 specifications, while reserving the right to enforce its marks against misleading uses. Please see
86 <http://www.oasis-open.org/who/trademark.php> for above guidance.

87

88 **Table of Contents**

89	1 Introduction.....	5
90	1.1 Motivation [Non-Normative].....	5
91	1.2 Limitations [Non-Normative].....	5
92	1.3 Terminology.....	5
93	1.4 Normative References.....	6
94	1.5 Non-normative References.....	6
95	2 General Level-of-Assurance Profile.....	7
96	2.1 Example Derived Class.....	8
97	3 NIST 800-63 LOA Using SAML LOA Profile.....	9
98	3.1 Level 1 Schema.....	9
99	3.2 Level 2 Schema.....	10
100	3.3 Level 3 Schema.....	10
101	3.4 Level 4 Schema.....	11
102	4 SAML LOA Profile Conformance.....	13
103	4.1 NIST 800-63 LOA Profile Conformance.....	13

1 Introduction

The *Level of Assurance Authentication Context Profiles for SAML 2.0* describes two profiles of the SAML Authentication Context [SAMLAC] specification:

- A general, restricted version of the `AuthnContext` schema that may be used as the basis for representing levels of assurance (or other abstract authentication models) defined by external documentation.
- A specific set of `AuthnContextClass` schema derived from the general case which implements the [NIST 800-63] levels of assurance.

1.1 Motivation [Non-Normative]

Many existing (and potential) SAML federation deployments have adopted a “levels of assurance” (or LOA) model for categorizing the wide variety of authentication methods into a small number of levels, typically based on some notion of the strength of the authentication. Federation members (service providers or “relying parties”) then decide which level of assurance is required to access specific protected resources, based on some assessment of “value” or “risk”.

The SAML authentication context mechanisms provide a variety of possible options for representing the details of a LOA scheme. However, this profile is motivated by two related considerations:

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

The approach taken here simply represents each level in a LOA scheme as a separate authentication context class. Each level class is characterized by a URI, and the body of the schema simply contains a reference to the external documentation that defines the LOA scheme. These URI values are conveyed in the `<RequestedAuthnContext>` element of an authentication request and the `<AuthnContextClassRef>` element in the authentication response

1.2 Limitations [Non-Normative]

There are at least two limitations to using this approach:

- The URIs representing the levels must be configured into every system in the deployment, and the ordering of the URI levels must be decided and configured out-of-band.
- The authentication assertions carrying these LOA authentication context URIs do not convey any details about the authentication event, although such details are implied by the level indicated by the URI.

1.3 Terminology

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 IETF [RFC 2119]:

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

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

148 Listings of XML schemas appear like this.

149 Example code listings appear like this.

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

Prefix	XML Namespace	Comments
ds:	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace .
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.

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

156 1.4 Normative References

- 157 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
158 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 159 **[NIST 800-63]** NIST Special Publication 800-63 Version 1.0.2, *Electronic Authentication*
160 *Guideline*, NIST, April 2006. See
161 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- 162 **[SAMLAC]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup*
163 *Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-
164 context-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 165 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*
166 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See
167 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 168 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
169 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
170 xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/). Note that this specification normatively references
171 [Schema2], listed below.
- 172 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide
173 Web Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/
174 REC-xmlschema-2-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/).

175 1.5 Non-normative References

- 176 **[Reference]** [reference citation]
- 177 **[Reference]** [reference citation]

2 General Level-of-Assurance Profile

178

179 The following schema redefines the basic abstract `AuthnContextDeclarationBaseType` to limit the
180 allowed elements to the `GoverningAgreements`.

```
181 <?xml version="1.0" encoding="UTF-8"?>
182 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
183   finalDefault="extension"
184   blockDefault="substitution" version="2.0">
185   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
186     <xs:annotation>
187       <xs:documentation>
188         Base class for building level-of-assurance style AuthnContext
189         class definitions.
190       </xs:documentation>
191     </xs:annotation>
192
193     <xs:complexType name="AuthnContextDeclarationBaseType">
194       <xs:complexContent>
195         <xs:restriction base="AuthnContextDeclarationBaseType">
196           <xs:sequence>
197             <xs:element ref="Identification"
198               minOccurs="0" maxOccurs="0"/>
199             <xs:element ref="TechnicalProtection"
200               minOccurs="0" maxOccurs="0"/>
201             <xs:element ref="OperationalProtection"
202               minOccurs="0" maxOccurs="0"/>
203             <xs:element ref="AuthnMethod"
204               minOccurs="0" maxOccurs="0"/>
205             <xs:element ref="GoverningAgreements"
206               minOccurs="1" maxOccurs="1"/>
207             <xs:element ref="Extension" minOccurs="0"
208               maxOccurs="unbounded"/>
209           </xs:sequence>
210           <xs:attribute name="ID" type="xs:ID" use="optional"/>
211         </xs:restriction>
212       </xs:complexContent>
213     </xs:complexType>
214
215     <xs:complexType name="GoverningAgreementRefType">
216       <xs:annotation>
217         <xs:documentation>
218           A specific restriction of this type specifying or
219           enumerating the governing document(s) and/or section
220           within such document(s) that define this particular
221           level of assurance.
222         </xs:documentation>
223       </xs:annotation>
224       <xs:complexContent>
225         <xs:restriction base="GoverningAgreementRefType">
226           <xs:attribute name="governingAgreementRef"
227             type="xs:anyURI" use="required"/>
228         </xs:restriction>
229       </xs:complexContent>
230     </xs:complexType>
231   </xs:redefine>
232 </xs:schema>
```

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

236 2.1 Example Derived Class

237 The following schema is based on the general LOA schema above, and further constrains the governing
238 agreements to be limited to an enumerated set of references:

```
239 <?xml version="1.0" encoding="UTF-8"?>
240 <xs:schema
241   targetNamespace="urn:oasis:loa:example"
242   xmlns:xs="http://www.w3.org/2001/XMLSchema"
243   xmlns="urn:oasis:loa:example"
244   finalDefault="extension"
245   blockDefault="substitution"
246   version="2.0">
247
248   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
249
250     <xs:annotation>
251       <xs:documentation>
252         Class identifier: urn:oasis:loa:example
253         Reference Documents: loa-1.pdf, loa-2.pdf
254       </xs:documentation>
255     </xs:annotation>
256
257     <xs:complexType name="GoverningAgreementRefType">
258       <xs:complexContent>
259         <xs:restriction base="GoverningAgreementRefType">
260           <xs:attribute name="governingAgreementRef" use="required">
261             <xs:simpleType>
262               <xs:restriction base="xs:anyURI">
263                 <xs:enumeration
264 value="http://example.com/loa-1.pdf"/>
265                 <xs:enumeration
266 value="http://example.com/loa-2.pdf"/>
267               </xs:restriction>
268             </xs:simpleType>
269           </xs:attribute>
270         </xs:restriction>
271       </xs:complexContent>
272     </xs:complexType>
273
274   </xs:redefine>
275 </xs:schema>
```


3 NIST 800-63 LOA Using SAML LOA Profile

277

278 We define the following URIs to represent the four levels of assurance described in [NIST 800-63].

- 279 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:1
- 280 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:2
- 281 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:3
- 282 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:4

283 The following schema define these URIs using the SAML LOA Profile described in section 2.

284 *Editors Note: it occurs to me that these schema might also be represented as*
285 *AuthenticationContextDeclaration instances, based on a class defined with an enumeration such as the*
286 *example above. One might also employ an extension to explicitly indicate the numeric level as an integer.*
287 *I welcome comments as to whether this alternative approach should be presented.*

3.1 Level 1 Schema

288

```
289 <?xml version="1.0" encoding="UTF-8"?>
290 <xs:schema
291   targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v
292 1-0-2:1"
293   xmlns:xs="http://www.w3.org/2001/XMLSchema"
294   xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:1"
295   finalDefault="extension"
296   blockDefault="substitution"
297   version="2.0">
298
299   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
300
301     <xs:annotation>
302       <xs:documentation>
303         Class identifier:
304         urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1
305 -0-2:1
306         Document identifier:
307         saml-schema-authn-context-nist-level1.xsd
308
309         Defines Level 1 of NIST LOA scheme.
310         See Section 8.2.1 of SP800-63V1_0_2.pdf (URL below)
311       </xs:documentation>
312     </xs:annotation>
313
314     <xs:complexType name="GoverningAgreementRefType">
315       <xs:complexContent>
316         <xs:restriction base="GoverningAgreementRefType">
317           <xs:attribute name="governingAgreementRef"
318 type="xs:anyURI"
319           fixed="http://csrc.nist.gov/publications/nistpubs/800-
320 63/SP800-63V1_0_2.pdf"
321           use="required"/>
322         </xs:restriction>
323       </xs:complexContent>
324     </xs:complexType>
325   </xs:redefine>
326 </xs:schema>
```

327 3.2 Level 2 Schema

```
328 <?xml version="1.0" encoding="UTF-8"?>
329 <xs:schema
330     targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v
331 1-0-2:2"
332     xmlns:xs="http://www.w3.org/2001/XMLSchema"
333     xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:2"
334     finalDefault="extension"
335     blockDefault="substitution"
336     version="2.0">
337
338     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
339
340         <xs:annotation>
341             <xs:documentation>
342                 Class identifier:
343                 urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1
344 -0-2:2
345                 Document identifier:
346                 saml-schema-authn-context-nist-level2.xsd
347
348                 Defines Level 2 of NIST LOA scheme.
349                 See Section 8.2.2 of SP800-63V1_0_2.pdf (URL below)
350             </xs:documentation>
351         </xs:annotation>
352
353         <xs:complexType name="GoverningAgreementRefType">
354             <xs:complexContent>
355                 <xs:restriction base="GoverningAgreementRefType">
356                     <xs:attribute name="governingAgreementRef"
357 type="xs:anyURI"
358                 fixed="http://csrc.nist.gov/publications/nistpubs/800-
359 63/SP800-63V1_0_2.pdf"
360                 use="required"/>
361             </xs:restriction>
362         </xs:complexContent>
363     </xs:complexType>
364 </xs:redefine>
365 </xs:schema>
```

366 3.3 Level 3 Schema

```
367 <?xml version="1.0" encoding="UTF-8"?>
368 <xs:schema
369     targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v
370 1-0-2:3"
371     xmlns:xs="http://www.w3.org/2001/XMLSchema"
372     xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:3"
373     finalDefault="extension"
374     blockDefault="substitution"
375     version="2.0">
376
377     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
378
379         <xs:annotation>
380             <xs:documentation>
381                 Class identifier:
382                 urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1
383 -0-2:3
```

```

384         Document identifier:
385             saml-schema-authn-context-nist-level3.xsd
386
387         Defines Level 3 of NIST LOA scheme.
388         See Section 8.2.3 of SP800-63V1_0_2.pdf (URL below)
389     </xs:documentation>
390 </xs:annotation>
391
392     <xs:complexType name="GoverningAgreementRefType">
393         <xs:complexContent>
394             <xs:restriction base="GoverningAgreementRefType">
395                 <xs:attribute name="governingAgreementRef"
396 type="xs:anyURI"
397             fixed="http://csrc.nist.gov/publications/nistpubs/800-
398 63/SP800-63V1_0_2.pdf"
399             use="required"/>
400             </xs:restriction>
401         </xs:complexContent>
402     </xs:complexType>
403 </xs:redefine>
404 </xs:schema>

```

405 3.4 Level 4 Schema

```

406 <?xml version="1.0" encoding="UTF-8"?>
407 <xs:schema
408     targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v
409 1-0-2:4"
410     xmlns:xs="http://www.w3.org/2001/XMLSchema"
411     xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:4"
412     finalDefault="extension"
413     blockDefault="substitution"
414     version="2.0">
415
416     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
417
418         <xs:annotation>
419             <xs:documentation>
420                 Class identifier:
421                 urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1
422 -0-2:4
423
424                 Document identifier:
425                 saml-schema-authn-context-nist-level4.xsd
426
427                 Defines Level 4 of NIST LOA scheme.
428                 See Section 8.2.4 of SP800-63V1_0_2.pdf (URL below)
429             </xs:documentation>
430         </xs:annotation>
431
432         <xs:complexType name="GoverningAgreementRefType">
433             <xs:complexContent>
434                 <xs:restriction base="GoverningAgreementRefType">
435                 <xs:attribute name="governingAgreementRef"
436 type="xs:anyURI"
437             fixed="http://csrc.nist.gov/publications/nistpubs/800-
438 63/SP800-63V1_0_2.pdf"
439             use="required"/>
440             </xs:restriction>
441         </xs:complexContent>
442     </xs:complexType>
443 </xs:redefine>

```

```
</xs:schema>
```

444 **4 SAML LOA Profile Conformance**

445 To conform to this profile, implementations MUST implement the provisions of sections 3.3.2.2.1 of
446 [SAMLCore] concerning the processing of <RequestedAuthnContext>.

447 **4.1 NIST 800-63 LOA Profile Conformance**

448 To conform to the NIST 800-63 profile, implementations MUST understand the URIs described in section
449 3, and MUST process these according to their relative ordering, where level 1 is weakest and level 4 is
450 strongest.

451 *Editors Note: We may want to add additional conformance clauses describing the specific SAML Bindings*
452 *and other settings (e.g., encryption and signing) that must be used for each of the levels. This is*
453 *described in the NIST document, but a concise statement here might be beneficial.*

454 **Appendix A. Acknowledgments**

455 The following individuals have participated in the creation of this specification and are gratefully
456 acknowledged

457 **Participants:**

- 458 • [Participant name, affiliation | Individual member]
- 459 • [Participant name, affiliation | Individual member]
- 460 • [Participant name, affiliation | Individual member]

461

462 **Appendix B. Revision History**

463 [optional; should not be included in OASIS standards]

464 **Appendix C. Non-Normative Text**

465