



Level of Assurance Authentication Context Profiles for SAML 2.0

Draft 01

01 April 2008

Specification URIs:

This Version:

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].html](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].html)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].odt](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].odt)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].pdf](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].pdf)

Previous Version:

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].html](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].html)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].odt](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].odt)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].pdf](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].pdf)

Latest Version:

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].html](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].html)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].odt](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].odt)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].pdf](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].pdf)

Latest Approved Version:

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].html](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].html)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].odt](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].odt)

[http://docs.oasis-open.org/security/saml/Post2.0/\[additional path/filename\].pdf](http://docs.oasis-open.org/security/saml/Post2.0/[additional path/filename].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

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]

35 **Abstract:**

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

40 **Status:**

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

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

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

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

52 Notices

53 Copyright © OASIS® 2007. All Rights Reserved.

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

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

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

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

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

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

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

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

97

98 **Table of Contents**

99 1 Introduction.....5
100 1.1 Motivation [Non-Normative].....5
101 1.2 Limitations [Non-Normative].....5
102 1.3 Terminology.....5
103 1.4 Normative References.....5
104 1.5 Non-normative References.....6
105 2 General Level-of-Assurance Profile.....7
106 3 NIST 800-63 LOA Using SAML LOA Profile.....8
107 4 SAML LOA Profile Conformance.....9

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 several related notions:

- 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 a 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].

1.4 Normative References

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

150 **[NIST 800-63]** NIST Special Publication 800-63 Version 1.0.2, *Electronic Authentication*
151 Guideline, NIST, April 2006. See
152 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
153 **[SAMLAC]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup*
154 *Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-
155 context-2.0-os. See <http://www.oasis-open.org/committees/security/>.
156 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*
157 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See
158 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

159 **1.5 Non-normative References**

160 **[Reference]** [reference citation]
161 **[Reference]** [reference citation]

162

2 General Level-of-Assurance Profile

163 The following schema redefines the basic abstract AuthnContextDeclarationBaseType to limit the allowed
 164 elements to the GoverningAgreements. The functional definition of the GoverningAgreementRefType is
 165 not changed from the original schema in [SAMLAC], but documentationj is added to serve as a reminder
 166 that definitions derived from this schema should redefine GoverningAgreementRefType to suit a
 167 particular LOA purpose.

```

168 <?xml version="1.0" encoding="UTF-8"?>
169 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" finalDefault="extension"
170   blockDefault="substitution" version="2.0">
171
172   <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
173
174     <xs:annotation>
175       <xs:documentation>
176         Base class for building level-of-assurance style AuthnContext
177         class definitions.
178       </xs:documentation>
179     </xs:annotation>
180
181     <xs:complexType name="AuthnContextDeclarationBaseType">
182       <xs:complexContent>
183         <xs:restriction base="AuthnContextDeclarationBaseType">
184           <xs:sequence>
185             <xs:element ref="Identification" minOccurs="0"/>
186             <xs:element ref="TechnicalProtection" minOccurs="0"/>
187             <xs:element ref="OperationalProtection" minOccurs="0"/>
188             <xs:element ref="AuthnMethod" minOccurs="0"/>
189             <xs:element ref="GoverningAgreements" minOccurs="1"
190               maxOccurs="1"/>
191             <xs:element ref="Extension" minOccurs="0"
192               maxOccurs="unbounded"/>
193           </xs:sequence>
194           <xs:attribute name="ID" type="xs:ID" use="optional"/>
195         </xs:restriction>
196       </xs:complexContent>
197     </xs:complexType>
198
199     <xs:complexType name="GoverningAgreementRefType">
200       <xs:annotation>
201         <xs:documentation>
202           A specific restriction of this type specifying or
203           enumerating the governing document(s) and/or section
204           within such document(s) that define this particular
205           level of assurance.
206         </xs:documentation>
207       </xs:annotation>
208       <xs:complexContent>
209         <xs:restriction base="GoverningAgreementRefType">
210           <xs:attribute name="governingAgreementRef"
211             type="xs:anyURI" use="required"/>
212         </xs:restriction>
213       </xs:complexContent>
214     </xs:complexType>
215
216   </xs:redefine>
217
218 </xs:schema>

```

219

2.1 Example Derived Class

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

```

222 <?xml version="1.0" encoding="UTF-8"?>
223 <xs:schema
224   targetNamespace="urn:oasis:loa:example"

```

```

225     xmlns:xs="http://www.w3.org/2001/XMLSchema"
226     xmlns="urn:oasis:loa:example"
227     finalDefault="extension"
228     blockDefault="substitution"
229     version="2.0">
230
231     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
232
233         <xs:annotation>
234             <xs:documentation>
235                 Class identifier: urn:oasis:loa:example
236                 Reference Documents: loa-1.pdf, loa-2.pdf
237             </xs:documentation>
238         </xs:annotation>
239
240         <xs:complexType name="GoverningAgreementRefType">
241             <xs:complexContent>
242                 <xs:restriction base="GoverningAgreementRefType">
243                     <xs:attribute name="governingAgreementRef" use="required">
244                         <xs:simpleType>
245                             <xs:restriction base="xs:anyURI">
246                                 <xs:enumeration
247 value="http://example.com/loa-1.pdf"/>
248                                 <xs:enumeration
249 value="http://example.com/loa-2.pdf"/>
250                             </xs:restriction>
251                         </xs:simpleType>
252                     </xs:attribute>
253                 </xs:restriction>
254             </xs:complexContent>
255         </xs:complexType>
256
257     </xs:redefine>
258
259 </xs:schema>

```


3 NIST 800-63 LOA Using SAML LOA Profile

260

261 The following schema define the following URIs to represent the four levels of assurance described in
262 [NIST 800-63].

- 263 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:1
- 264 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:2
- 265 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:3
- 266 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:4

267 *Editors Note: it occurs to me that these schema might also be represented as*
268 *AuthenticationContextDeclaration instances, based on a class defined with an enumeration such as the*
269 *example above. One might also employ an extension to explicitly indicate the numeric level as an*
270 *integer. I welcome comments as to whether this would be a more straightforward approach.*

```
271 <?xml version="1.0" encoding="UTF-8"?>
272 <xs:schema
273   targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:1"
274   xmlns:xs="http://www.w3.org/2001/XMLSchema"
275   xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:1"
276   finalDefault="extension"
277   blockDefault="substitution"
278   version="2.0">
279   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
280     <xs:annotation>
281       <xs:documentation>
282         Class identifier:
283         urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:1
284         Document identifier: saml-schema-authn-context-nist-level1.xsd
285       </xs:documentation>
286     </xs:annotation>
287     <xs:complexType name="GoverningAgreementRefType">
288       <xs:complexContent>
289         <xs:restriction base="GoverningAgreementRefType">
290           <xs:attribute name="governingAgreementRef" type="xs:anyURI"
291             fixed="http://csrc.nist.gov/publications/nistpubs/800-63
292 /SP800-63V1_0_2.pdf"
293             use="required"/>
294         </xs:restriction>
295       </xs:complexContent>
296     </xs:complexType>
297   </xs:redefine>
298 </xs:schema>
```

304

```
305 <?xml version="1.0" encoding="UTF-8"?>
306 <xs:schema
307   targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:2"
308   xmlns:xs="http://www.w3.org/2001/XMLSchema"
309   xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:2"
310   finalDefault="extension"
311   blockDefault="substitution"
312   version="2.0">
313   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
314     <xs:annotation>
315       <xs:documentation>
316         Class identifier:
317         urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:2
318         Document identifier: saml-schema-authn-context-nist-level2.xsd
319       </xs:documentation>
320     </xs:annotation>
321   </xs:redefine>
322 </xs:schema>
```

```

321         </xs:documentation>
322     </xs:annotation>
323
324     <xs:complexType name="GoverningAgreementRefType">
325         <xs:complexContent>
326             <xs:restriction base="GoverningAgreementRefType">
327                 <xs:attribute name="governingAgreementRef" type="xs:anyURI"
328                     fixed="http://csrc.nist.gov/publications/nistpubs/800-63
329 /SP800-63V1_0_2.pdf"
330                     use="required"/>
331             </xs:restriction>
332         </xs:complexContent>
333     </xs:complexType>
334
335 </xs:redefine>
336
337 </xs:schema>

```

338

```

339 <?xml version="1.0" encoding="UTF-8"?>
340 <xs:schema
341     targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:3"
342     xmlns:xs="http://www.w3.org/2001/XMLSchema"
343     xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:3"
344     finalDefault="extension"
345     blockDefault="substitution"
346     version="2.0">
347
348     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
349
350         <xs:annotation>
351             <xs:documentation>
352                 Class identifier:
353                 urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:3
354                 Document identifier: saml-schema-authn-context-nist-level3.xsd
355             </xs:documentation>
356         </xs:annotation>
357
358         <xs:complexType name="GoverningAgreementRefType">
359             <xs:complexContent>
360                 <xs:restriction base="GoverningAgreementRefType">
361                     <xs:attribute name="governingAgreementRef" type="xs:anyURI"
362                         fixed="http://csrc.nist.gov/publications/nistpubs/800-63
363 /SP800-63V1_0_2.pdf"
364                         use="required"/>
365                 </xs:restriction>
366             </xs:complexContent>
367         </xs:complexType>
368
369     </xs:redefine>
370
371 </xs:schema>

```

372

```

373 <?xml version="1.0" encoding="UTF-8"?>
374 <xs:schema
375     targetNamespace="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:4"
376     xmlns:xs="http://www.w3.org/2001/XMLSchema"
377     xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:4"
378     finalDefault="extension"
379     blockDefault="substitution"
380     version="2.0">
381
382     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
383
384         <xs:annotation>
385             <xs:documentation>
386                 Class identifier: urn:oasis:names:tc:SAML:
387 2.0:post:ac:classes:nist-800-63:4
388                 Document identifier: saml-schema-authn-context-nist-level4.xsd
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" type="xs:anyURI"
396                     fixed="http://csrc.nist.gov/publications/nistpubs/800-63
397 /SP800-63V1_0_2.pdf"
398                     use="required"/>
399             </xs:restriction>
400         </xs:complexContent>
401     </xs:complexType>
402
403 </xs:redefine>
404
405 </xs:schema>
```

406 **4 SAML LOA Profile Conformance**

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

409 **Appendix A. Acknowledgments**

410 The following individuals have participated in the creation of this specification and are gratefully
411 acknowledged

412 **Participants:**

413 **I** [Participant name, affiliation | Individual member]

414 **:** [Participant name, affiliation | Individual member]

415 **:** [Participant name, affiliation | Individual member]

416

417 **Appendix B. Revision History**

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

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

420