



# Level of Assurance Authentication Context Profile for SAML 2.0

## Working Draft 02

24 March 2009

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sssc-saml-loa-authncontext-profile-draft-02.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sssc-saml-loa-authncontext-profile-draft-02.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/sssc-saml-loa-authncontext-profile-draft-02.pdf>

#### Previous Version:

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

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

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

### Technical Committee:

OASIS Security Services TC

### Chair(s):

Hal Lockhart, BEA Systems, Inc.

### Editor(s):

Eric Tiffany, Liberty Alliance

Paul Madsen, NTT

Scott Cantor, Internet2

### Related Work:

This specification profiles the SAML 2.0 Authentication Context [SAMLAC] mechanisms to allow SAML authentication requests and assertions to carry assurance policy information. Specifically, we profile SAML's Authentication Context for NIST 800-63.

### Declared XML Namespace(s):

- urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2

### Abstract:

This document profiles the use of SAML's Authentication Context mechanisms to express assurance policy on authentication requests and assertions. Level-of-Assurance (LOA) schemes are expressed as a set of authentication context classes. A general schema pattern for arbitrary

33 assurance frameworks is presented, along with specific authentication classes corresponding to  
34 the NIST 800-63 levels of assurance [NIST 800-63].

35 **Status:**

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

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

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

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

---

# 47 Notices

48 Copyright © OASIS® 2008. All Rights Reserved.

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

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

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

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

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

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

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

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

92

93 **Table of Contents**

94 1 Introduction.....5  
95 1.1 Motivation [Non-Normative].....5  
96 1.2 Limitations [Non-Normative].....5  
97 1.3 Terminology.....6  
98 1.4 Normative References.....6  
99 1.5 Non-normative References.....7  
100 2 General Level-of-Assurance Profile.....8  
101 3 NIST 800-63 LOA Using SAML LOA Profile.....9  
102 3.1 NIST 800-63 Level 1 Schema.....9  
103 3.2 NIST 800-63 Level 2 Schema.....9  
104 3.3 NIST 800-63 Level 3 Schema.....10  
105 3.4 NIST 800-63 Level 4 Schema.....11  
106 4 SAML LOA Profile Conformance.....12  
107 4.1 NIST 800-63 LOA Profile Conformance.....12

---

# 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 of any given assurance framework.
- A specific set of `AuthnContext` class schema derived from the general case which corresponds to the 4 NIST 800 63 [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 large number of possible combinations of registration processes, security procedures, and authentication methods that underly a given authentication statement. LOA serve to compress this large number into a smaller more manageable number of levels. Different combinations of processes and technology are rated according to the level of assurance they can engender. Typically, 3-5 sets are defined, with corresponding assurance level ranging from low to high. Relying parties then decide which level of assurance is required to access specific protected resources, based on an assessment of the risk associated with those resources – high risk requires high assurance etc.

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 assertion within any authentication response

## 1.2 Limitations [Non-Normative]

A limitation to using this approach is that:

- 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.

## 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]:

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

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

153 Listings of XML schemas appear like this.

154 Example code listings appear like this.

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

Prefix	XML Namespace	Comments
ds:	<a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a>	This is the XML Signature namespace .
xs:	<a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a>	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.

159 This specification uses the following typographical conventions in text: <SAML*E*lement>,  
160 <ns:ForeignElement>, Attribute, **Datatype**, OtherCode.

## 161 1.4 Normative References

- 162 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
163 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 164 **[NIST 800-63]** NIST Special Publication 800-63 Version 1.0.2, *Electronic Authentication*  
165 *Guideline*, NIST, April 2006. See  
166 [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)
- 167 **[SAMLAC]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup*  
168 *Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-  
169 context-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 170 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*  
171 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See  
172 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 173 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web  
174 Consortium Recommendation, May 2001. See <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>. Note that this specification normatively references  
175 [Schema2], listed below.
- 177 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide  
178 Web Consortium Recommendation, May 2001. See  
179 <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>.

## 180 1.5 Non-normative References

- 181 **[Reference]** [reference citation]
- 182 **[Reference]** [reference citation]

## 2 General Level-of-Assurance Profile

183

184 The following schema redefines the basic abstract `AuthnContextDeclarationBaseType` to limit the  
185 allowed elements to the `GoverningAgreements` element. It will be through this element that the  
186 appropriate external LOA scheme documentation will be referenced.

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

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

## 3 NIST 800-63 LOA Using SAML LOA Profile

242

243 The [NIST 800-63] LOA class schemas will extend the base LOA class schema. Each of the 4 NIST LOA  
244 class schemas will reference a particular section of the NIST 800063 document that stipulates the LOA  
245 requirements.

246 We define the following URIs to represent the four levels of assurance:

- 247 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:1
- 248 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:2
- 249 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:3
- 250 • urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:4

251 The above URIs correspond to the class schema in the respective following sections. Each class schema  
252 extends the base LOA profile schema listed in section 2.

### 3.1 NIST 800-63 Level 1 Schema

253

```
254 <?xml version="1.0" encoding="UTF-8"?>
255 <xs:schema
256   targetNamespace="urn:oasis:names:tc:SAML:
257 2.0:post:ac:classes:nist-800-63:v1-0-2:1"
258   xmlns:xs="http://www.w3.org/2001/XMLSchema"
259   xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:1"
260   finalDefault="extension"
261   blockDefault="substitution"
262   version="2.0">
263
264   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
265
266     <xs:annotation>
267       <xs:documentation>
268         Class identifier:
269         urn:oasis:names:tc:SAML:
270 2.0:post:ac:classes:nist-800-63:v1-0-2:1
271         Document identifier:
272         saml-schema-authn-context-nist-level1.xsd
273
274         Defines Level 1 of NIST LOA scheme.
275         See Section 8.2.1 of SP800-63V1_0_2.pdf (URL below)
276       </xs:documentation>
277     </xs:annotation>
278
279     <xs:complexType name="GoverningAgreementRefType">
280       <xs:complexContent>
281         <xs:restriction base="GoverningAgreementRefType">
282           <xs:attribute name="governingAgreementRef"
283 type="xs:anyURI"
284           fixed="http://csrc.nist.gov/publications/nistpubs/80
285 0-63/SP800-63V1_0_2.pdf"
286           use="required"/>
287         </xs:restriction>
288       </xs:complexContent>
289     </xs:complexType>
290   </xs:redefine>
291 </xs:schema>
```

## 292 3.2 NIST 800-63 Level 2 Schema

```
293 <?xml version="1.0" encoding="UTF-8"?>
294 <xs:schema
295   targetNamespace="urn:oasis:names:tc:SAML:
296   2.0:post:ac:classes:nist-800-63:v1-0-2:2"
297   xmlns:xs="http://www.w3.org/2001/XMLSchema"
298   xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:2"
299   finalDefault="extension"
300   blockDefault="substitution"
301   version="2.0">
302
303   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
304
305     <xs:annotation>
306       <xs:documentation>
307         Class identifier:
308         urn:oasis:names:tc:SAML:
309         2.0:post:ac:classes:nist-800-63:v1-0-2:2
310         Document identifier:
311         saml-schema-authn-context-nist-level2.xsd
312
313         Defines Level 2 of NIST LOA scheme.
314         See Section 8.2.2 of SP800-63V1_0_2.pdf (URL below)
315       </xs:documentation>
316     </xs:annotation>
317
318     <xs:complexType name="GoverningAgreementRefType">
319       <xs:complexContent>
320         <xs:restriction base="GoverningAgreementRefType">
321           <xs:attribute name="governingAgreementRef"
322             type="xs:anyURI"
323             fixed="http://csrc.nist.gov/publications/nistpubs/80
324             0-63/SP800-63V1_0_2.pdf"
325             use="required"/>
326         </xs:restriction>
327       </xs:complexContent>
328     </xs:complexType>
329   </xs:redefine>
330 </xs:schema>
```

## 331 3.3 NIST 800-63 Level 3 Schema

```
332 <?xml version="1.0" encoding="UTF-8"?>
333 <xs:schema
334   targetNamespace="urn:oasis:names:tc:SAML:
335   2.0:post:ac:classes:nist-800-63:v1-0-2:3"
336   xmlns:xs="http://www.w3.org/2001/XMLSchema"
337   xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:3"
338   finalDefault="extension"
339   blockDefault="substitution"
340   version="2.0">
341
342   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
343
344     <xs:annotation>
345       <xs:documentation>
346         Class identifier:
347         urn:oasis:names:tc:SAML:
348         2.0:post:ac:classes:nist-800-63:v1-0-2:3
349         Document identifier:
350         saml-schema-authn-context-nist-level3.xsd
351
352         Defines Level 3 of NIST LOA scheme.
```

```

353         See Section 8.2.3 of SP800-63V1_0_2.pdf (URL below)
354     </xs:documentation>
355 </xs:annotation>
356
357     <xs:complexType name="GoverningAgreementRefType">
358         <xs:complexContent>
359             <xs:restriction base="GoverningAgreementRefType">
360                 <xs:attribute name="governingAgreementRef"
type="xs:anyURI"
361                 fixed="http://csrc.nist.gov/publications/nistpubs/80
362 0-63/SP800-63V1_0_2.pdf"
363                 use="required"/>
364             </xs:restriction>
365         </xs:complexContent>
366     </xs:complexType>
367 </xs:redefine>
368 </xs:schema>
369

```

### 370 3.4 NIST 800-63 Level 4 Schema

```

371 <?xml version="1.0" encoding="UTF-8"?>
372 <xs:schema
373     targetNamespace="urn:oasis:names:tc:SAML:
374 2.0:post:ac:classes:nist-800-63:v1-0-2:4"
375     xmlns:xs="http://www.w3.org/2001/XMLSchema"
376     xmlns="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:4"
377     finalDefault="extension"
378     blockDefault="substitution"
379     version="2.0">
380
381     <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
382
383         <xs:annotation>
384             <xs:documentation>
385                 Class identifier:
386                 urn:oasis:names:tc:SAML:
387 2.0:post:ac:classes:nist-800-63:v1-0-2:4
388                 Document identifier:
389                 saml-schema-authn-context-nist-level4.xsd
390
391                 Defines Level 4 of NIST LOA scheme.
392                 See Section 8.2.4 of SP800-63V1_0_2.pdf (URL below)
393             </xs:documentation>
394         </xs:annotation>
395
396         <xs:complexType name="GoverningAgreementRefType">
397             <xs:complexContent>
398                 <xs:restriction base="GoverningAgreementRefType">
399                     <xs:attribute name="governingAgreementRef"
type="xs:anyURI"
400                     fixed="http://csrc.nist.gov/publications/nistpubs/80
401 0-63/SP800-63V1_0_2.pdf"
402                     use="required"/>
403                 </xs:restriction>
404             </xs:complexContent>
405         </xs:complexType>
406     </xs:redefine>
407 </xs:schema>
408

```

---

409 **4 SAML LOA Profile Conformance**

410 To conform to this profile, implementations **MUST** implement the provisions of sections 3.3.2.2.1 of  
411 [SAMLCore] concerning the processing of `<RequestedAuthnContext>`.

412 **4.1 NIST 800-63 LOA Profile Conformance**

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

---

416 **Appendix A. Acknowledgments**

417 The following individuals have participated in the creation of this specification and are gratefully  
418 acknowledged

419 **Participants:**

- 420 • [Participant name, affiliation | Individual member]
- 421 • [Participant name, affiliation | Individual member]
- 422 • [Participant name, affiliation | Individual member]

423

---

424

## Appendix B. Revision History

425

- Draft 01 – first draft

426

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

427

428

---

## Appendix C. Non-Normative Text

429