



# Level of Assurance Authentication Context Profile for SAML 2.0

## Working Draft 03

11 May 2009

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-loa-authncontext-profile-draft-03.html>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-loa-authncontext-profile-draft-03.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-loa-authncontext-profile-draft-03.pdf>

#### Previous 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 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.

### Declared XML Namespace(s):

### 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 by which assurance levels for arbitrary assurance frameworks can be expressed is presented.

33 **Status:**

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

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

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

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

---

# 45 Notices

46 Copyright © OASIS® 2008. All Rights Reserved.

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

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

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

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

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

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

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

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

90

91 **Table of Contents**

92 1 Introduction.....5

93 1.1 Motivation [Non-Normative].....5

94 1.2 Limitations [Non-Normative].....5

95 1.3 Terminology.....5

96 1.4 Normative References.....6

97 1.5 Non-normative References.....6

98 2 General Level-of-Assurance Profile.....7

99 3 Example LOA Framework classes.....8

100 5 SAML LOA Profile Conformance.....10

---

# 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.

## 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]:

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

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

144 Listings of XML schemas appear like this.

145 Example code listings appear like this.

147 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for  
148 their respective namespaces as follows, whether or not a namespace declaration is present in the  
149 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.

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

## 151 1.4 Normative References

- 152 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
153 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 154 **[SAMLAC]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup  
155 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-  
156 context-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 157 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion  
158 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See  
159 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 160 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web  
161 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-  
162 xmldata-1-20010502/](http://www.w3.org/TR/2001/REC-xmldata-1-20010502/). Note that this specification normatively references  
163 [Schema2], listed below.
- 164 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide  
165 Web Consortium Recommendation, May 2001. See  
166 <http://www.w3.org/TR/2001/REC-xmldata-2-20010502/>.

## 167 1.5 Non-normative References

- 168 **[Reference]** [reference citation]
- 169 **[Reference]** [reference citation]

## 2 General Level-of-Assurance Profile

170

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

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

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

---

## 229 3 Example LOA Framework classes

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

233 We define the following URIs to represent the 3 LOA

- 234 ● <http://foo.example.com/assurance/loa1>
- 235 ● <http://foo.example.com/assurance/loa2>
- 236 ● <http://foo.example.com/assurance/loa3>

237

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

239

```
240 <?xml version="1.0" encoding="UTF-8"?>
241 <xs:schema
242   targetNamespace="http://foo.example.com/assurance/loa1"
243   xmlns:xs="http://www.w3.org/2001/XMLSchema"
244   xmlns="http://foo.example.com/assurance/loa1"
245   finalDefault="extension"
246   blockDefault="substitution"
247   version="2.0">
248
249   <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
250
251     <xs:annotation>
252       <xs:documentation>
253         Class identifier:
254         http://foo.example.com/assurance/loa1
255
256         Defines Level 1 of FAF
257       </xs:documentation>
258     </xs:annotation>
259
260     <xs:complexType name="GoverningAgreementRefType">
261       <xs:complexContent>
262         <xs:restriction base="GoverningAgreementRefType">
263           <xs:attribute name="governingAgreementRef"
264             type="xs:anyURI"
265             fixed="http://foo.example.com/foo_assurance.pdf#sect
266             ion1"
267             use="required"/>
268         </xs:restriction>
269       </xs:complexContent>
270     </xs:complexType>
271   </xs:redefine>
272 </xs:schema>
```

273

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



---

277

## 5 SAML LOA Profile Conformance

278

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

279

---

280 **Appendix A. Acknowledgments**

281 The following individuals have participated in the creation of this specification and are gratefully  
282 acknowledged

282 **Participants:**

- 283 • [Participant name, affiliation | Individual member]
- 284 • [Participant name, affiliation | Individual member]
- 285 • [Participant name, affiliation | Individual member]

286

---

287

## Appendix B. Revision History

288

- Draft 01 – first draft

289

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

290

291

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

---

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

293