



2 Conformance Requirements for the 3 OASIS Security Assertion Markup 4 Language (SAML) V2.0

5 OASIS Standard, 15 March 2005

6 **Document identifier:**

7 saml-conformance-2.0-os

8 **Location:**

9 <http://docs.oasis-open.org/security/saml/v2.0/>

10 **Editors:**

11 Prateek Mishra, Principal Identity
12 Rob Philpott, RSA Security
13 Eve Maler, Sun Microsystems

14 **SAML V2.0 Contributors:**

15 Conor P. Cahill, AOL
16 John Hughes, Atos Origin
17 Hal Lockhart, BEA Systems
18 Michael Beach, Boeing
19 Rebekah Metz, Booz Allen Hamilton
20 Rick Randall, Booz Allen Hamilton
21 Thomas Wisniewski, Entrust
22 Irving Reid, Hewlett-Packard
23 Paula Austel, IBM
24 Maryann Hondo, IBM
25 Michael McIntosh, IBM
26 Tony Nadalin, IBM
27 Nick Ragouzis, Individual
28 Scott Cantor, Internet2
29 RL 'Bob' Morgan, Internet2
30 Peter C Davis, Neustar
31 Jeff Hodges, Neustar
32 Frederick Hirsch, Nokia
33 John Kemp, Nokia
34 Paul Madsen, NTT
35 Steve Anderson, OpenNetwork
36 Prateek Mishra, Principal Identity
37 John Linn, RSA Security
38 Rob Philpott, RSA Security
39 Jahan Moreh, Sigaba
40 Anne Anderson, Sun Microsystems
41 Eve Maler, Sun Microsystems
42 Ron Monzillo, Sun Microsystems
43 Greg Whitehead, Trustgenix

44 **Abstract:**

45 This normative specification provides the technical requirements for SAML V2.0 conformance and
46 specifies the entire set of documents comprising SAML V2.0.

47 **Status:**

48 This is an **OASIS Standard** document produced by the Security Services Technical Committee. It
49 was approved by the OASIS membership on 1 March 2005.

50 Committee members should submit comments and potential errata to the [security-](mailto:security-services@lists.oasis-open.org)
51 [services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org) list. Others should submit them by filling out the web form located
52 at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The
53 committee will publish on its web page (<http://www.oasis-open.org/committees/security>) a catalog
54 of any changes made to this document.

55 For information on whether any patents have been disclosed that may be essential to
56 implementing this specification, and any offers of patent licensing terms, please refer to the
57 Intellectual Property Rights web page for the Security Services TC ([http://www.oasis-](http://www.oasis-open.org/committees/security/ipr.php)
58 [open.org/committees/security/ipr.php](http://www.oasis-open.org/committees/security/ipr.php)).

59 **Table of Contents**

60 1 Introduction.....4

61 1.1 Overview and Specification of SAML V2.0.....4

62 1.2 Notation.....5

63 2 SAML V2.0 Profiles and Possible Implementations.....6

64 3 Conformance.....8

65 3.1 Operational Modes.....8

66 3.2 Feature Matrix.....8

67 3.3 Implementation of SAML-Defined Identifiers.....10

68 3.4 Implementation of Encrypted Elements.....11

69 3.5 Security Models for SOAP and URI Bindings.....11

70 4 XML Digital Signature and XML Encryption.....12

71 4.1 XML Signature Algorithms.....12

72 4.2 XML Encryption Algorithms.....12

73 5 Use of SSL 3.0 or TLS 1.0.....13

74 5.1 SAML SOAP and URI Binding13

75 5.2 Web SSO Profiles of SAML13

76 6 References.....14

77

78

1 Introduction

79

This normative specification describes features that are mandatory and optional for implementations claiming conformance to SAML V2.0 and also specifies the entire set of documents comprising SAML V2.0.

81

82

1.1 Overview and Specification of SAML V2.0

83

The SAML V2.0 standard consists of the following documents:

84

- This specification: Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0

85

86

- Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLCore]

87

88

- SAML assertions schema [SAMLAssn-xsd]

89

- SAML protocols schema [SAMLProt-xsd]

90

- Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLBind]

91

- Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLProf]

92

- SAML ECP profile schema [SAMLECP-xsd]

93

- SAML X.500/LDAP attribute profile schema [SAMLX500-xsd]

94

- SAML DCE PAC attribute profile schema [SAMLDCExsd]

95

- SAML XACML attribute profile schema [SAMLXAC-xsd]

96

- Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLMeta]

97

- SAML metadata schema [SAMLMeta-xsd]

98

- Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLAuthnCxt]

99

100

- SAML authentication context schema [SAMLAC-xsd]

101

- SAML authentication context schema types [SAMLACTyp-xsd]

102

- SAML context class schema for Internet Protocol [SAMLAC-IP]

103

- SAML context class schema for Internet Protocol Password [SAMLAC-IPP]

104

- SAML context class schema for Kerberos [SAMLAC-Kerb]

105

- SAML context class schema for Mobile One Factor Unregistered [SAMLAC-MOFU]

106

- SAML context class schema for Mobile Two Factor Unregistered [SAMLAC-MTFU]

107

- SAML context class schema for Mobile One Factor Contract [SAMLAC-MOFC]

108

- SAML context class schema for Mobile Two Factor Contract [SAMLAC-MTFC]

109

- SAML context class schema for Password [SAMLAC-Pass]

110

- SAML context class schema for Password Protected Transport [SAMLAC-PPT]

111

- SAML context class schema for Previous Session [SAMLAC-Prev]

112

- SAML context class schema for Public Key – X.509 [SAMLAC-X509]

113

- SAML context class schema for Public Key – PGP [SAMLAC-PGP]

114

- SAML context class schema for Public Key – SPKI [SAMLAC-SPKI]

115

- SAML context class schema for Public Key – XML Signature [SAMLAC-XSig]

116

- SAML context class schema for Smartcard [SAMLAC-Smart]

117

- SAML context class schema for Smartcard PKI [SAMLAC-SmPKI]

118

- SAML context class schema for Software PKI [SAMLAC-SwPKI]

- 119 • SAML context class schema for Telephony [SAMLAC-Tele]
- 120 • SAML context class schema for Telephony (“Nomadic”) [SAMLAC-TNom]
- 121 • SAML context class schema for Telephony (Personalized) [SAMLAC-TPers]
- 122 • SAML context class schema for Telephony (Authenticated) [SAMLAC-TAuthn]
- 123 • SAML context class schema for Secure Remote Password [SAMLAC-SRP]
- 124 • SAML context class schema for SSL/TLS Certificate-Based Client Authentication [SAMLAC-SSL]
- 125
- 126 • SAML context class schema for Time Sync Token [SAMLAC-TST]
- 127 • Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLSec]
- 128
- 129 • Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLGloss]

130 The term “SAML V2.0” or “SAML2” is often used informally to refer to the standard specified by the above
131 documents, or subsets thereof. However, the SAML V2.0 standard should be formally identified in other
132 documents by a normative reference to this document.

133 Additional non-normative documents, such as a Technical Overview [SAMLTechOvw], are available to
134 provide assistance to developers and others in understanding SAML. These documents are available at
135 the SAML website, <http://www.oasis-open.org/committees/security>.

136 SAML V2.0 defines a number of named profiles. Each profile (other than attribute profiles) describes
137 details of selected SAML message flows and can also be viewed as indivisible functionality that could be
138 implemented by a software component. Implementation of a profile involves use of a binding for each
139 message exchange included in the profile. A binding can be viewed as a specific implementation
140 technique for achieving a message exchange.

141 Section 2 of this document enumerates all of the different profiles defined by [SAMLProfiles]. For each
142 profile, the relevant SAML V2.0 message flows are listed, and for each message flow the set of possible
143 bindings is also described. The combination of profile, message exchange and a selected binding is
144 termed a SAML V2.0 *feature*.

145 Section 3 describes the conformance matrix for SAML V2.0. A number of different *operational modes* or
146 roles are identified. The conformance matrix describes the feature set that must be
147 implemented by each operational mode.

148 1.2 Notation

149 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
150 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted in this
151 specification and all of the SAML V2.0 specifications as described in IETF RFC 2119 [RFC 2119]:

152

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

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

2 SAML V2.0 Profiles and Possible Implementations

159 The following table enumerates all of the profiles defined by the SAML profiles specification [SAMLProf].
 160 For each profile, the message protocol flows (defined in the assertions and protocols specification
 161 [SAMLCore]) found within the profile are also described. For each message flow, a list of relevant bindings
 162 (defined in the bindings specification [SAMLBind]) is given in the final column.

Table 1: Possible Implementations

Profile	Message Flows	Binding
Web SSO	<AuthnRequest> from SP to IdP	HTTP redirect
		HTTP POST
		HTTP artifact
	IdP <Response> to SP	HTTP POST
HTTP artifact		
Enhanced Client/Proxy SSO	ECP to SP, SP to ECP to IdP	PAOS
	IdP to ECP to SP, SP to ECP	PAOS
Identity Provider Discovery	Cookie setter	HTTP
	Cookie getter	HTTP
Single Logout	<LogoutRequest>	HTTP redirect
		HTTP POST
		HTTP artifact
		SOAP
	<LogoutResponse>	HTTP redirect
		HTTP POST
		HTTP artifact
		SOAP
Name Identifier Management	<ManageNameIDRequest>	HTTP redirect
		HTTP POST
		HTTP artifact
		SOAP
	<ManageNameIDResponse>	HTTP redirect
		SOAP
Artifact Resolution	<ArtifactResolve>, <ArtifactResponse>	SOAP
Authentication Query	<AuthNQuery>, <Response>	SOAP
Attribute Query	<AttributeQuery>, <Response>	SOAP

Profile	Message Flows	Binding
Authorization Decision Query	<AuthZDecisionQuery>, <Response>	SOAP
Request for Assertion by Identifier	<AssertionIDRequest>, <Response>	SOAP
Name Identifier Mapping	<NameIDMappingRequest>, <NameIDMappingResponse>	SOAP
SAML URI binding	GET, HTTP Response	HTTP
UUID attribute profile		
DCE PAC attribute profile		
X.500 attribute profile		
XACML attribute profile		
Metadata	Consumption	
	Exchange	

163

164 **3 Conformance**

165 This section describes the technical conformance requirements for SAML V2.0.

166 **3.1 Operational Modes**

167 This document uses the phrase “operational mode” to describe a role that a software component can play
168 in conforming to SAML. The operational modes are as follows:

- 169 • IdP – Identity Provider
- 170 • IdP Lite – Identity Provider Lite
- 171 • SP – Service Provider
- 172 • SP Lite – Service Provider Lite
- 173 • ECP – Enhanced Client/Proxy
- 174 • SAML Attribute Authority
- 175 • SAML Authorization Decision Authority
- 176 • SAML Authentication Authority
- 177 • SAML Requester

178 **3.2 Feature Matrix**

179 The following matrices identify unique sets of conformance requirements by means of a triple taken from
180 Table 1 with the form: profile, message(s), binding The message component is not always included when
181 it is obvious from context.

Table 2: Feature Matrix

Feature	IdP	IdP Lite	SP	SP Lite	ECP
Web SSO, <AuthnRequest>, HTTP redirect	MUST	MUST	MUST	MUST	N/A
Web SSO, <Response>, HTTP POST	MUST	MUST	MUST	MUST	N/A
Web SSO, <Response>, HTTP artifact	MUST	MUST	MUST	MUST	N/A
Artifact Resolution, SOAP	MUST	MUST	MUST	MUST	N/A
Enhanced Client/Proxy SSO, PAOS	MUST	MUST	MUST	MUST	MUST
Name Identifier Management, HTTP redirect (IdP-initiated)	MUST	MUST NOT	MUST	MUST NOT	N/A
Name Identifier Management, SOAP (IdP-initiated)	MUST	MUST NOT	OPTIONAL	MUST NOT	N/A
Name Identifier Management, HTTP redirect	MUST	MUST NOT	MUST	MUST NOT	N/A
Name Identifier Management, SOAP (SP-initiated)	MUST	MUST NOT	OPTIONAL	MUST NOT	N/A
Single Logout (IdP-initiated) – HTTP redirect	MUST	MUST	MUST	MUST	N/A
Single Logout (IdP-initiated) – SOAP	MUST	OPTIONAL	MUST	OPTIONAL	N/A
Single Logout (SP-initiated) – HTTP redirect	MUST	MUST	MUST	MUST	N/A
Single Logout (SP-initiated) – SOAP	MUST	OPTIONAL	MUST	OPTIONAL	N/A
Identity Provider Discovery (cookie)	MUST	MUST	OPTIONAL	OPTIONAL	N/A

183

184 The following table summarizes operational modes that extend the IdP or SP modes defined above.
 185 These are to be understood as a combination of an IdP or SP mode from the table above with the
 186 corresponding extended feature set below.

Table 3: Extended IdP, SP

Feature	IdP Extended	SP Extended
Identity Provider proxy (Section 3.4.1.5 [SAMLCore])	MUST	MUST
Name identifier mapping, SOAP	MUST	MUST

188

189 The following table summarizes conformance requirements for SAML authorities and requesters .

Table 4: SAML Authority and Requester Matrix

Feature	SAML Authentication Authority	SAML Attribute Authority	SAML Authorization Decision Authority	SAML Requester
Authentication Query, SOAP	MUST	OPTIONAL	OPTIONAL	OPTIONAL
Attribute Query, SOAP	OPTIONAL	MUST	OPTIONAL	OPTIONAL
Authorization Decision Query, SOAP	OPTIONAL	OPTIONAL	MUST	OPTIONAL
Request for Assertion by Identifier, SOAP	MUST	MUST	MUST	OPTIONAL
SAML URI Binding	MUST	MUST	MUST	OPTIONAL

190

191 3.3 Implementation of SAML-Defined Identifiers

192 All relevant operational modes MUST implement the following SAML-defined identifiers:

- 193 • All Attribute Name Format identifiers defined in Section 8.2 of [SAMLCore]
- 194 • All Name Identifier Format identifiers defined in Section 8.3 of [SAMLCore]

195 Conforming SAML implementations MUST permit the use of all identifier constants described in Sections
 196 8.2 and 8.3 when producing and consuming SAML messages. SAML message producers MUST be able
 197 to create messages and SAML message consumers MUST be able to process messages with any of the
 198 constants defined in these sections.

199 Sections 8.3.7 (persistent name identifiers) and 8.3.8 (transient name identifiers) define normative
 200 processing rules for the producer of such identifiers. All normative processing rules in Sections 8.3.7 and
 201 8.3.8 MUST be supported by conforming implementations. The remaining identifiers in Sections 8.2 and
 202 8.3 specify no normative processing rules. Hence, generation and consumption of these identifiers is
 203 meaningful only when the generating and consuming parties have externally-defined agreement on the
 204 semantic interpretation of the identifiers.

205 **Note:** In this context, "process" means that the implementation must successfully parse
 206 and handle the identifier without failing or returning an error. How the implementation
 207 deals with the identifier once it is processed at this level is out of scope for this
 208 specification.

209 A SAML implementation may provide the facilities described above through direct

210 implementation support for the identifiers or through the use of supported programming
211 interfaces. Interfaces provided for this purpose must allow the SAML implementation to
212 be programmatically extended to handle all identifiers in Sections 8.2 and 8.3 that are not
213 natively handled by the implementation.

214 **3.4 Implementation of Encrypted Elements**

215 All relevant operational modes **MUST** be able to process or generate the following encrypted elements in
216 any context where they are required to process or generate the corresponding unencrypted elements,
217 namely <saml:NameID>, <saml:Assertion>, or <saml:Attribute>:

- 218 • <saml:EncryptedID>
- 219 • <saml:EncryptedAssertion>
- 220 • <saml:EncryptedAttribute>

221 **3.5 Security Models for SOAP and URI Bindings**

222 The following security models are mandatory to implement for all profiles implemented using the SOAP
223 binding as well as for the SAML URI binding. SAML authorities and requesters **MUST** implement the
224 following authentication methods:

- 225 • No client or server authentication.
- 226 • HTTP basic authentication [RFC 2617] with and without SSL 3.0 or TLS 1.0 (see Section 3 below).
227 The SAML requester **MUST** preemptively send the authorization header with the initial request.
- 228 • HTTP over SSL 3.0 or TLS 1.0 server authentication with server-side certificate.
- 229 • HTTP over SSL 3.0 or TLS 1.0 mutual authentication with both server-side and a client-side
230 certificate.

231 If a SAML authority uses SSL 3.0 or TLS 1.0, it **MUST** use a server-side certificate.

232 4 XML Digital Signature and XML Encryption

233 SAML V2.0 uses XML Signature [XMLSig] to implement XML signing and encryption functionality for
234 integrity, and source authentication. SAML V2.0 uses XML Encryption [XMLEnc] to implement
235 confidentiality, including encrypted identifiers, encrypted assertions, and encrypted attributes.

236 4.1 XML Signature Algorithms

237 XML Signature mandates use of the following algorithms in Section 6.1; therefore they MUST be
238 implemented by compliant SAML V2.0 implementations:

- 239 • Digest: SHA1
- 240 • MAC: HMAC-SHA1
- 241 • XML Canonicalization: CanonicalXML (Without comments),
- 242 • Transform: Enveloped Signature

243 In addition, to enable interoperability, the following MUST be implemented by compliant SAML V2.0
244 implementations:

- 245 • Signature: RSAwithSHA1 (recommended in XML Signature but needed for
246 interoperability)

247 Although XML Signature mandates the DSAwithSHA1 signature algorithm, it is not required by SAML
248 V2.0, but is RECOMMENDED.

249 4.2 XML Encryption Algorithms

250 XML Encryption mandates use of the following algorithms in Sections 5.2.1 and 5.2.2; therefore they
251 MUST be implemented by compliant SAML V2.0 implementations:

- 252 • Block Encryption: TRIPLE DES, AES-128, AES-256.
- 253 • Key Transport: RSA-v1.5, RSA-OAEP

254 **5 Use of SSL 3.0 or TLS 1.0**

255 In any SAML V2.0 use of SSL 3.0 [SSL3] or TLS 1.0 [RFC 2246], servers MUST authenticate to clients
256 using a X.509 v3 certificate. The client MUST establish server identity based on contents of the certificate
257 (typically through examination of the certificate's subject DN field).

258 **5.1 SAML SOAP and URI Binding**

259 TLS-capable implementations MUST implement the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher
260 suite and MAY implement the TLS_RSA_AES_128_CBC_SHA cipher suite [AES].

261 FIPS TLS-capable implementations MUST implement the corresponding
262 TLS_RSA_FIPS_WITH_3DES_EDE_CBC_SHA cipher suite and MAY implement the corresponding
263 TLS_RSA_FIPS_AES_128_CBC_SHA cipher suite [AES].

264 SSL-capable implementations MUST implement the SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher
265 suite.

266 FIPS SSL-capable implementations MUST implement the FIPS cipher suite corresponding to the SSL
267 SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

268 **5.2 Web SSO Profiles of SAML**

269 SSL-capable implementations of the Web SSO profile of SAML MUST implement the
270 SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. TLS-capable implementations MUST implement
271 the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315

6 References

- [AES]** FIPS-197, *Advanced Encryption Standard (AES)*. See <http://www.nist.gov/>.
- [RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- [RFC 2246]** T. Dierks et al. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. See <http://www.ietf.org/rfc/rfc2246.txt>.
- [RFC 2617]** J. Franks et al. *HTTP Authentication: Basic and Digest Access Authentication*. IETF RFC 2617, June 1999. See <http://www.ietf.org/rfc/rfc2617.txt>.
- [SAMLAssn-xsd]** S. Cantor et al. SAML assertions schema. OASIS SSTC, March 2005. Document ID saml-schema-assertion-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAuthnCxt]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-context-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-xsd]** J. Kemp et al. SAML authentication context schema. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLACTyp-xsd]** J. Kemp et al. SAML authentication context type declarations schema. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-types-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-IP]** J. Kemp et al. SAML context class schema for Internet Protocol. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-ip-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-IPP]** J. Kemp et al. SAML context class schema for Internet Protocol Password. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-ippword-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-Kerb]** J. Kemp et al. SAML context class schema for Kerberos. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-kerberos-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-MOFC]** J. Kemp et al. SAML context class schema for Mobile One Factor Contract. Document ID saml-schema-authn-context-mobileonefactor-reg-2.0. See OASIS SSTC, March 2005. <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-MOFU]** J. Kemp et al. SAML context class schema for Mobile One Factor Unregistered. Document ID saml-schema-authn-context-mobileonefactor-unreg-2.0. See OASIS SSTC, March 2005. <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-MTFC]** J. Kemp et al. SAML context class schema for Mobile Two Factor Contract. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-mobiletwofactor-reg-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-MTFU]** J. Kemp et al. SAML context class schema for Mobile Two Factor Unregistered. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-mobiletwofactor-unreg-2.0. See <http://www.oasis-open.org/committees/security/>.
- [SAMLAC-Pass]** J. Kemp et al. SAML context class schema for Password. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-pword-2.0. See <http://www.oasis-open.org/committees/security/>.

316	[SAMLAC-PGP]	J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-pgp-2.0. See http://www.oasis-open.org/committees/security/ .
317		
318		
319	[SAMLAC-PPT]	J. Kemp et al., SAML context class schema for Password Protected Transport. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-ppt-2.0. See http://www.oasis-open.org/committees/security/ .
320		
321		
322	[SAMLAC-Prev]	J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-session-2.0. See http://www.oasis-open.org/committees/security/ .
323		
324		
325	[SAMLAC-Smart]	J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-smartcard-2.0. See http://www.oasis-open.org/committees/security/ .
326		
327		
328	[SAMLAC-SmPKI]	J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-smartcardpki-2.0. See http://www.oasis-open.org/committees/security/ .
329		
330		
331	[SAMLAC-SPKI]	J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-spki-2.0. See http://www.oasis-open.org/committees/security/ .
332		
333		
334	[SAMLAC-SRP]	J. Kemp et al. SAML context class schema for Secure Remote Password. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-srp-2.0. See http://www.oasis-open.org/committees/security/ .
335		
336		
337	[SAMLAC-SSL]	J. Kemp et al. SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-sslcrt-2.0. See http://www.oasis-open.org/committees/security/ .
338		
339		
340	[SAMLAC-SwPKI]	J. Kemp et al. SAML context class schema for Software PKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-softwarepki-2.0. See http://www.oasis-open.org/committees/security/ .
341		
342		
343	[SAMLAC-Tele]	J. Kemp et al. SAML context class schema for Telephony. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
344		
345		
346	[SAMLAC-TNom]	J. Kemp et al. SAML context class schema for Telephony (“Nomadic”). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-nomad-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
347		
348		
349	[SAMLAC-TPers]	J. Kemp et al. SAML context class schema for Telephony (Personalized). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-personal-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
350		
351		
352	[SAMLAC-TAuthn]	J. Kemp et al. SAML context class schema for Telephony (Authenticated). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-auth-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
353		
354		
355	[SAMLAC-TST]	J. Kemp et al. SAML context class schema for Time Sync Token. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-timesync-2.0. See http://www.oasis-open.org/committees/security/ .
356		
357		
358	[SAMLAC-X509]	J. Kemp et al. SAML context class schema for Public Key – X.509. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-x509-2.0. See http://www.oasis-open.org/committees/security/ .
359		
360		
361	[SAMLAC-XSig]	J. Kemp et al. SAML context class schema for Public Key – XML Signature. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-xmlsig-2.0. See http://www.oasis-open.org/committees/security/ .
362		
363		
364	[SAMLBind]	S. Cantor et al. <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os. See http://www.oasis-open.org/committees/security/ .
365		
366		

368	[SAMLCore]	S. Cantor et al. <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-core-2.0-os. See http://www.oasis-open.org/committees/security/ .
369		
370		
371	[SAML DCE-xsd]	S. Cantor et al. SAML DCE PAC attribute profile schema. OASIS SSTC, March 2005. Document ID saml-schema-dce-2.0. See http://www.oasis-open.org/committees/security/ .
372		
373		
374	[SAML ECP-xsd]	S. Cantor et al. SAML ECP profile schema. OASIS SSTC, March 2005. Document ID saml-schema-ecp-2.0. See http://www.oasis-open.org/committees/security/ .
375		
376		
377	[SAML Gloss]	J. Hodges et al. <i>Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-glossary-2.0-os. See http://www.oasis-open.org/committees/security/ .
378		
379		
380	[SAML Meta]	S. Cantor et al. <i>Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os. See http://www.oasis-open.org/committees/security/ .
381		
382		
383	[SAML Meta-xsd]	S. Cantor et al. SAML metadata schema. OASIS SSTC, March 2005. Document ID saml-schema-metadata-2.0. See http://www.oasis-open.org/committees/security/ .
384		
385		
386	[SAML Prof]	S. Cantor et al. <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See http://www.oasis-open.org/committees/security/ .
387		
388		
389	[SAML Prot-xsd]	S. Cantor et al. SAML protocols schema. OASIS SSTC, March 2005. Document ID saml-schema-protocol-2.0. See http://www.oasis-open.org/committees/security/ .
390		
391		
392	[SAML Sec]	F. Hirsch et al. <i>Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-sec-consider-2.0-os. See http://www.oasis-open.org/committees/security/ .
393		
394		
395		
396	[SAML TechOvw]	J. Hughes et al. <i>Technical Overview for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, February 2005. Document ID sstc-saml-tech-overview-2.0-draft-03. See http://www.oasis-open.org/committees/security/ .
397		
398		
399	[SAML X500-xsd]	S. Cantor et al. SAML X.500/LDAP attribute profile schema. OASIS SSTC, March 2005. Document ID saml-schema-x500-2.0. See http://www.oasis-open.org/committees/security/ .
400		
401		
402	[SAML XAC-xsd]	S. Cantor et al. SAML XACML attribute profile schema. OASIS SSTC, March 2005. Document ID saml-schema-xacml-2.0. See http://www.oasis-open.org/committees/security/ .
403		
404		
405	[SSL3]	A. Frier et al. <i>The SSL 3.0 Protocol</i> , Netscape Communications Corp, November 1996.
406		
407	[XML Enc]	Donald Eastlake et al. <i>XML Encryption Syntax and Processing</i> . World Wide Web Consortium Recommendation, December 2002. See http://www.w3.org/TR/xmlenc-core/ .
408		
409		
410	[XML Sig]	Donald Eastlake et al. <i>XML-Signature Syntax and Processing</i> . World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/xmlsig-core/ .
411		
412		
413		

414 Appendix A. Acknowledgements

415 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
416 Committee, whose voting members at the time of publication were:

- 417 • Conor Cahill, AOL
- 418 • John Hughes, Atos Origin
- 419 • Hal Lockhart, BEA Systems
- 420 • Mike Beach, Boeing
- 421 • Rebekah Metz, Booz Allen Hamilton
- 422 • Rick Randall, Booz Allen Hamilton
- 423 • Ronald Jacobson, Computer Associates
- 424 • Gavenraj Sodhi, Computer Associates
- 425 • Thomas Wisniewski, Entrust
- 426 • Carolina Canales-Valenzuela, Ericsson
- 427 • Dana Kaufman, Forum Systems
- 428 • Irving Reid, Hewlett-Packard
- 429 • Guy Denton, IBM
- 430 • Heather Hinton, IBM
- 431 • Maryann Hondo, IBM
- 432 • Michael McIntosh, IBM
- 433 • Anthony Nadalin, IBM
- 434 • Nick Ragouzis, Individual
- 435 • Scott Cantor, Internet2
- 436 • Bob Morgan, Internet2
- 437 • Peter Davis, Neustar
- 438 • Jeff Hodges, Neustar
- 439 • Frederick Hirsch, Nokia
- 440 • Senthil Sengodan, Nokia
- 441 • Abbie Barbir, Nortel Networks
- 442 • Scott Kiester, Novell
- 443 • Cameron Morris, Novell
- 444 • Paul Madsen, NTT
- 445 • Steve Anderson, OpenNetwork
- 446 • Ari Kermaier, Oracle
- 447 • Vamsi Motukuru, Oracle
- 448 • Darren Platt, Ping Identity
- 449 • Prateek Mishra, Principal Identity
- 450 • Jim Lien, RSA Security
- 451 • John Linn, RSA Security
- 452 • Rob Philpott, RSA Security
- 453 • Dipak Chopra, SAP
- 454 • Jahan Moreh, Sigaba
- 455 • Bhavna Bhatnagar, Sun Microsystems
- 456 • Eve Maler, Sun Microsystems
- 457 • Ronald Monzillo, Sun Microsystems

- 458 • Emily Xu, Sun Microsystems
- 459 • Greg Whitehead, Trustgenix

460

461 The editors also would like to acknowledge the following former SSTC members for their contributions to
462 this or previous versions of the OASIS Security Assertions Markup Language Standard:

- 463 • Stephen Farrell, Baltimore Technologies
- 464 • David Orchard, BEA Systems
- 465 • Krishna Sankar, Cisco Systems
- 466 • Zahid Ahmed, CommerceOne
- 467 • Tim Alsop, CyberSafe Limited
- 468 • Carlisle Adams, Entrust
- 469 • Tim Moses, Entrust
- 470 • Nigel Edwards, Hewlett-Packard
- 471 • Joe Pato, Hewlett-Packard
- 472 • Bob Blakley, IBM
- 473 • Marlena Erdos, IBM
- 474 • Marc Chanliau, Netegrity
- 475 • Chris McLaren, Netegrity
- 476 • Lynne Rosenthal, NIST
- 477 • Mark Skall, NIST
- 478 • Charles Knouse, Oblix
- 479 • Simon Godik, Overxeer
- 480 • Charles Norwood, SAIC
- 481 • Evan Prodromou, Securant
- 482 • Robert Griffin, RSA Security (former editor)
- 483 • Sai Allarvarpu, Sun Microsystems
- 484 • Gary Ellison, Sun Microsystems
- 485 • Chris Ferris, Sun Microsystems
- 486 • Mike Myers, Traceroute Security
- 487 • Phillip Hallam-Baker, VeriSign (former editor)
- 488 • James Vanderbeek, Vodafone
- 489 • Mark O'Neill, Vordel
- 490 • Tony Palmer, Vordel

491

492 Finally, the editors wish to acknowledge the following people for their contributions of material used as
493 input to the OASIS Security Assertions Markup Language specifications:

- 494 • Thomas Gross, IBM
- 495 • Birgit Pfitzmann, IBM

Appendix B. Notices

497 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
498 might be claimed to pertain to the implementation or use of the technology described in this document or
499 the extent to which any license under such rights might or might not be available; neither does it represent
500 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to
501 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made
502 available for publication and any assurances of licenses to be made available, or the result of an attempt
503 made to obtain a general license or permission for the use of such proprietary rights by implementors or
504 users of this specification, can be obtained from the OASIS Executive Director.

505 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or
506 other proprietary rights which may cover technology that may be required to implement this specification.
507 Please address the information to the OASIS Executive Director.

508 **Copyright © OASIS Open 2005. All Rights Reserved.**

509 This document and translations of it may be copied and furnished to others, and derivative works that
510 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
511 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
512 this paragraph are included on all such copies and derivative works. However, this document itself does
513 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as
514 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights
515 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it
516 into languages other than English.

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

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