



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

Committee Draft 02, 24 September 2004

Document identifier:

sstc-saml-conformance-2.0-cd-02

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editors:

Prateek Mishra, Netegrity
Rob Philpott, RSA Security
Eve Maler, Sun Microsystems

SAML V2.0 Contributors:

Conor P. Cahill, AOL
Hal Lockhart, BEA Systems
Michael Beach, Boeing
Rick Randall, Booze, Allen, Hamilton
Tim Alsop, CyberSafe Limited
Nick Ragouzis, Enosis
John Hughes, Atos Origin
Paul Madsen, Entrust
Irving Reid, Hewlett-Packard
Paula Austel, IBM
Maryann Hondo, IBM
Michael McIntosh, IBM
Tony Nadalin, IBM
Scott Cantor, Internet2
RL 'Bob' Morgan, Internet2
Rebekah Metz, NASA
Prateek Mishra, Netegrity
Peter C Davis, Neustar
Frederick Hirsch, Nokia
John Kemp, Nokia
Charles Knouse, Oblix
Steve Anderson, OpenNetwork
John Linn, RSA Security
Rob Philpott, RSA Security
Jahan Moreh, Sigaba
Anne Anderson, Sun Microsystems
Jeff Hodges, Sun Microsystems
Eve Maler, Sun Microsystems
Ron Monzillo, Sun Microsystems

44 Greg Whitehead, Trustgenix

45 **Abstract:**

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

48 **Status:**

49 This is a **second Committee Draft** approved by the Security Services Technical Committee on
50 21 September 2004.

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

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

60 **Table of Contents**

61 1 Introduction.....4
62 1.1 Overview and Specification of SAML V2.0.....4
63 1.2 Notation.....5
64 2 SAML V2.0 Profiles and Possible Implementations.....6
65 3 Conformance.....8
66 3.1 Operational Modes.....8
67 3.2 Feature Matrix.....8
68 3.3 Implementation of SAML-Defined Identifiers.....10
69 3.4 Implementation of Encrypted Elements.....10
70 3.5 Security Models for SOAP and URI Bindings.....11
71 4 XML Digital Signature and XML Encryption.....12
72 4.1 XML Signature Algorithms.....12
73 4.2 XML Encryption Algorithms.....12
74 5 Use of SSL 3.0 or TLS 1.0.....13
75 5.1 SAML SOAP and URI Binding13
76 5.2 Web SSO Profiles of SAML13
77 6 References.....14
78

79

1 Introduction

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

83

1.1 Overview and Specification of SAML V2.0

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

- 85 • This specification: Conformance Requirements for the OASIS Security Assertion Markup Language
86 (SAML) V2.0
- 87 • Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
88 [SAMLCore]
 - 89 • SAML assertions schema [SAMLAssn-xsd]
 - 90 • SAML protocols schema [SAMLProt-xsd]
- 91 • Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLBind]
- 92 • Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLProf]
 - 93 • SAML ECP profile schema [SAMLECP-xsd]
 - 94 • SAML LDAP attribute profile schema [SAMLLDAP-xsd]
 - 95 • SAML DCE PAC attribute profile schema [SAMLDCExsd]
 - 96 • SAML XACML attribute profile schema [SAMLXAC-xsd]
- 97 • Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLMeta]
- 98 • SAML metadata schema [SAMLMeta-xsd]
- 99 • Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0
100 [SAMLAuthnCxt]
 - 101 • SAML authentication context schema [SAMLAC-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-SPKI]
- 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 [RFC2119]:

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

Profile	Message Flows	Binding
Attribute Query	<AttributeQuery>, <Response>	SOAP
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	

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 Responder
- 175 • SAML Authorization Decision Responder
- 176 • SAML Authentication Responder

177 **3.2 Feature Matrix**

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

182

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

186

Table 3: Extended IdP, SP

Feature	IdP Extended	SP Extended
Identity Provider proxy (Section of 3.4.1.6 [SAMLCore])	MUST	MUST
Name identifier mapping, SOAP	MUST	MUST

187

188

189 The following table summarizes conformance requirements for SAML responders.

Table 4: SAML Responder Matrix

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

190

191 **3.3 Implementation of SAML-Defined Identifiers**

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

- 193 1. All Attribute Name Format Identifiers as defined in Section 8.2 of [SAMLCore].
- 194 2. All Name Identifier Format Identifiers as defined in Section 8.3 of [SAMLCore].
- 195 3. All Consent Identifiers as defined in Section 8.4 of [SAMLCore].

196 **3.4 Implementation of Encrypted Elements**

197 All relevant operational modes MUST be able to process or generate the following encrypted elements:

- 198 1. <saml:EncryptedID>,
- 199 2. <saml:EncryptedAssertion>,
- 200 3. <saml:EncryptedAttribute>

201 In any context where they are required to process or generate the corresponding unencrypted elements,
202 namely, 1) <saml:NameID>, 2) <saml:Assertion>, 3) <saml:Attribute>.

203

204 **3.5 Security Models for SOAP and URI Bindings**

205 The following security models are mandatory to implement for all profiles implemented using the SOAP
206 binding as well as for the SAML URI binding. The SAML requester and responder **MUST** implement the
207 following authentication methods:

- 208 • No client or server authentication.
- 209 • HTTP basic authentication [RFC2617] with and without SSL 3.0 or TLS 1.0 (see Section 3 below).
210 The SAML requester **MUST** preemptively send the authorization header with the initial request.
- 211 • HTTP over SSL 3.0 or TLS 1.0 server authentication with server-side certificate.
- 212 • HTTP over SSL 3.0 or TLS 1.0 mutual authentication with both server-side and a client-side
213 certificate.

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

215

216
217
218
219
220
221

4 XML Digital Signature and XML Encryption

222
223

4.1 XML Signature Algorithms

224
225
226
227
228
229
230

XML Signature mandates use of the following algorithms in section 6.1, therefore they MUST be implemented by compliant SAML V2.0 implementations:

- Digest: SHA1
- MAC: HMAC-SHA1
- XML Canonicalization: CanonicalXML (Without comments),
- Transform: Enveloped Signature

231
232
233
234
235

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

- Signature: RSAwithSHA1 (recommended in Dsig but needed for interoperability)

236
237

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

238

4.2 XML Encryption Algorithms

239
240
241
242
243
244

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

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

245 **5 Use of SSL 3.0 or TLS 1.0**

246 In any SAML V2.0 use of SSL 3.0 [SSL3] or TLS 1.0 [RFC2246] , servers MUST authenticate to clients
247 using a
248 X.509 v3 certificate. The client MUST establish server identity based on contents of the certificate
249 (typically through examination of the certificate's subject DN field).

250 **5.1 SAML SOAP and URI Binding**

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

254 FIPS TLS-capable implementations MUST implement the corresponding
255 TLS_RSA_FIPS_WITH_3DES_EDE_CBC_SHA cipher suite and MAY implement the corresponding
256 TLS_RSA_FIPS_AES_128_CBC_SHA cipher suite [AES].

257 SSL-capable implementations MUST implement the SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher
258 suite.

259 FIPS SSL-capable implementations MUST implement the FIPS cipher suite corresponding to the SSL
260 SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

261 **5.2 Web SSO Profiles of SAML**

262 SSL-capable implementations of the Web SSO profile of SAML MUST implement the
263 SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. TLS-capable implementations MUST implement
264 the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.
265

6 References

266

- 267 **[AES]** FIPS-197, *Advanced Encryption Standard (AES)*, available from
268 <http://www.nist.gov/>.
- 269 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
270 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 271 **[RFC2617]** J. Franks et. al., *HTTP Authentication: Basic and Digest Access Authentication*,
272 IETF RFC 2617, June 1999.
- 273 **[RFC2246]** T. Dierks et. al., *The TLS Protocol Version 1.0*, IETF RFC 2246, January 1999.
- 274 **[SAMLAssn-xsd]** S. Cantor et al., *SAML assertions schema*. OASIS SSTC, September 2004.
275 Document ID sstc-saml-schema-assertion-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
276 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 277 **[SAMLAuthnCxt]** J. Kemp et al., *Authentication Context for the OASIS Security Assertion Markup*
278 *Language (SAML) V2.0*. OASIS SSTC, September 2004. Document ID sstc-
279 saml-authn-context-2.0-cd-02. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
280 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 281 **[SAMLAC-xsd]** J. Kemp et al., *SAML authentication context schema*. OASIS SSTC, September
282 2004. Document ID sstc-saml-schema-authn-context-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
283 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 284 **[SAMLAC-IP]** J. Kemp et al., *SAML context class schema for Internet Protocol*. OASIS SSTC,
285 September 2004. Document ID sstc-saml-schema-authn-context-ip-2.0. See
286 <http://www.oasis-open.org/committees/security/>.
- 287 **[SAMLAC-IPP]** J. Kemp et al., *SAML context class schema for Internet Protocol Password*.
288 OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-
289 ippword-2.0. See <http://www.oasis-open.org/committees/security/>.
- 290 **[SAMLAC-Kerb]** J. Kemp et al., *SAML context class schema for Kerberos*. OASIS SSTC,
291 September 2004. Document ID sstc-saml-schema-authn-context-kerberos-2.0.
292 See <http://www.oasis-open.org/committees/security/>.
- 293 **[SAMLAC-MOFC]** J. Kemp et al., *SAML context class schema for Mobile One Factor Contract*.
294 Document ID sstc-saml-schema-authn-context-mobileonefactor-reg-2.0. See
295 OASIS SSTC, September 2004. <http://www.oasis-open.org/committees/security/>.
- 296 **[SAMLAC-MOFU]** J. Kemp et al., *SAML context class schema for Mobile One Factor Unregistered*.
297 Document ID sstc-saml-schema-authn-context-mobileonefactor-unreg-2.0. See
298 OASIS SSTC, September 2004. <http://www.oasis-open.org/committees/security/>.
- 299 **[SAMLAC-MTFC]** J. Kemp et al., *SAML context class schema for Mobile Two Factor Contract*.
300 OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-
301 mobiletwofactor-reg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 302 **[SAMLAC-MTFU]** J. Kemp et al., *SAML context class schema for Mobile Two Factor Unregistered*.
303 OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-
304 mobiletwofactor-unreg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 305 **[SAMLAC-Pass]** J. Kemp et al., *SAML context class schema for Password*. OASIS SSTC,
306 September 2004. Document ID sstc-saml-schema-authn-context-pword-2.0. See
307 <http://www.oasis-open.org/committees/security/>.

308	[SAMLAC-PGP]	J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-pgp-2.0. See http://www.oasis-open.org/committees/security/ .
309		
310		
311	[SAMLAC-PPT]	J. Kemp et al., SAML context class schema for Password Protected Transport. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-ppt-2.0. See http://www.oasis-open.org/committees/security/ .
312		
313		
314	[SAMLAC-Prev]	J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-session-2.0. See http://www.oasis-open.org/committees/security/ .
315		
316		
317	[SAMLAC-Smart]	J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-smartcard-2.0. See http://www.oasis-open.org/committees/security/ .
318		
319		
320	[SAMLAC-SmPKI]	J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-smartcardpki-2.0. See http://www.oasis-open.org/committees/security/ .
321		
322		
323	[SAMLAC-SPKI]	J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-spki-2.0. See http://www.oasis-open.org/committees/security/ .
324		
325		
326	[SAMLAC-SRP]	J. Kemp et al., SAML context class schema for Secure Remote Password. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-srp-2.0. See http://www.oasis-open.org/committees/security/ .
327		
328		
329	[SAMLAC-SSL]	J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-sslcert-2.0. See http://www.oasis-open.org/committees/security/ .
330		
331		
332	[SAMLAC-SwPKI]	J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-softwarepki-2.0. See http://www.oasis-open.org/committees/security/ .
333		
334		
335	[SAMLAC-Tele]	J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
336		
337		
338	[SAMLAC-TNom]	J. Kemp et al., SAML context class schema for Telephony (“Nomadic”). OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-nomad-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
339		
340		
341	[SAMLAC-TPers]	J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-personal-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
342		
343		
344	[SAMLAC-TAuthn]	J. Kemp et al., SAML context class schema for Telephony (Authenticated). OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-auth-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
345		
346		
347	[SAMLAC-TST]	J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-timesync-2.0. See http://www.oasis-open.org/committees/security/ .
348		
349		
350	[SAMLAC-X509]	J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-x509-2.0. See http://www.oasis-open.org/committees/security/ .
351		
352		
353	[SAMLAC-XSig]	J. Kemp et al., SAML context class schema for Public Key – XML Signature. OASIS SSTC, September 2004. Document ID sstc-saml-schema-authn-context-xmldsig-2.0. See http://www.oasis-open.org/committees/security/ .
354		
355		
356	[SAMLBind]	S. Cantor et al., <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, September 2004. Document ID sstc-saml-bindings-2.0-cd-02. See http://www.oasis-open.org/committees/security/ .
357		
358		

360	[SAMLCore]	S. Cantor et al., <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, September 2004. Document ID sstc-saml-core-2.0-cd-02. See http://www.oasis-open.org/committees/security/ .
361		
362		
363	[SAML DCE-xsd]	S. Cantor et al., SAML DCE PAC attribute profile schema. OASIS SSTC, September 2004. Document ID sstc-saml-schema-dce-2.0. See http://www.oasis-open.org/committees/security/ .
364		
365		
366	[SAML ECP-xsd]	S. Cantor et al., SAML ECP profile schema. OASIS SSTC, September 2004. Document ID sstc-saml-schema-ecp-2.0. See http://www.oasis-open.org/committees/security/ .
367		
368		
369	[SAML Gloss]	J. Hodges et al., <i>Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, September 2004. Document ID sstc-saml-glossary-2.0-cd-02. See http://www.oasis-open.org/committees/security/ .
370		
371		
372	[SAML LDAP-xsd]	S. Cantor et al., SAML LDAP attribute profile schema. OASIS SSTC, September 2004. Document ID sstc-saml-schema-ldap-2.0. See http://www.oasis-open.org/committees/security/ .
373		
374		
375	[SAML Meta]	S. Cantor et al., <i>Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, September 2004. Document ID sstc-saml-metadata-2.0-cd-02. See http://www.oasis-open.org/committees/security/ .
376		
377		
378	[SAML Meta-xsd]	S. Cantor et al., SAML metadata schema. OASIS SSTC, September 2004. Document ID sstc-saml-schema-metadata-2.0. See http://www.oasis-open.org/committees/security/ .
379		
380		
381	[SAML Prof]	S. Cantor et al., <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, September 2004. Document ID sstc-saml-profiles-2.0-cd-02. See http://www.oasis-open.org/committees/security/ .
382		
383		
384	[SAML Prot-xsd]	S. Cantor et al., SAML protocols schema. OASIS SSTC, September 2004. Document ID sstc-saml-schema-protocol-2.0. See http://www.oasis-open.org/committees/security/ .
385		
386		
387	[SAML Sec]	F. Hirsch et al., <i>Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, September 2004. Document ID sstc-saml-sec-consider-2.0-cd-02. See http://www.oasis-open.org/committees/security/ .
388		
389		
390		
391	[SAML TechOvw]	J. Hughes et al., <i>Technical Overview for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, August 2004. Document ID sstc-saml-tech-overview-2.0-draft-01. See http://www.oasis-open.org/committees/security/ .
392		
393		
394	[SAML XAC-xsd]	S. Cantor et al., SAML XACML attribute profile schema. OASIS SSTC, September 2004. Document ID sstc-saml-schema-xacml-2.0. See http://www.oasis-open.org/committees/security/ .
395		
396		
397	[SSL3]	A. Frier et al., <i>The SSL 3.0 Protocol</i> , Netscape Communications Corp, November 1996.
398		
399	[XML Enc]	Donald Eastlake et al., XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenc-core/ , World Wide Web Consortium, December 2002.
400		
401		
402	[XML Sig]	Donald Eastlake et al., XML-Signature Syntax and Processing, http://www.w3.org/TR/xmlsig-core/ , World Wide Web Consortium, February 2002.
403		
404		
405		

406 Appendix A. Acknowledgements

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

- 409 • Conor Cahill, AOL
- 410 • John Hughes, ATOS Origin
- 411 • Hal Lockhart, BEA Systems
- 412 • Rick Randall, Booz Allen Hamilton
- 413 • Ronald Jacobson, Computer Associates
- 414 • Gavenraj Sodhi, Computer Associates
- 415 • Tim Alsop, CyberSafe Limited
- 416 • Paul Madsen, Entrust
- 417 • Carolina Canales-Valenzuela, Ericsson
- 418 • Dana Kaufman, Forum Systems
- 419 • Irving Reid, Hewlett-Packard
- 420 • Paula Austel, IBM
- 421 • Maryann Hondo, IBM
- 422 • Michael McIntosh, IBM
- 423 • Anthony Nadalin, IBM
- 424 • Nick Ragouzis, Individual
- 425 • Scott Cantor, Internet2
- 426 • Bob Morgan, Internet2
- 427 • Prateek Mishra, Netegrity
- 428 • Forest Yin, Netegrity
- 429 • Peter Davis, Neustar
- 430 • Frederick Hirsch, Nokia
- 431 • John Kemp, Nokia
- 432 • Senthil Sengodan, Nokia
- 433 • Scott Kiestler, Novell
- 434 • Cameron Morris, Novell
- 435 • Charles Knouse, Oblix
- 436 • Steve Anderson, OpenNetwork
- 437 • Ari Kermaier, Oracle
- 438 • Vamsi Motukuru, Oracle
- 439 • Darren Platt, Ping Identity
- 440 • Jim Lien, RSA Security
- 441 • John Linn, RSA Security
- 442 • Rob Philpott, RSA Security
- 443 • Dipak Chopra, SAP
- 444 • Jahan Moreh, Sigaba
- 445 • Bhavna Bhatnagar, Sun Microsystems
- 446 • Jeff Hodges, Sun Microsystems
- 447 • Eve Maler, Sun Microsystems

448

- 449 • Ronald Monzillo, Sun Microsystems
- 450 • Emily Xu, Sun Microsystems
- 451 • Mike Beach, BoeingGreg Whitehead, Trustgenix
- 452 •

453 The editors also would like to acknowledge the following people for their contributions to previous versions
454 of the OASIS Security Assertions Markup Language Standard:

- 455 • Stephen Farrell, Baltimore Technologies
- 456 • David Orchard, BEA Systems
- 457 • Krishna Sankar, Cisco Systems
- 458 • Zahid Ahmed, CommerceOne
- 459 • Carlisle Adams, Entrust
- 460 • Tim Moses, Entrust
- 461 • Nigel Edwards, Hewlett-Packard
- 462 • Joe Pato, Hewlett-Packard
- 463 • Bob Blakley, IBM
- 464 • Marlena Erdos, IBM
- 465 • Marc Chanliau, Netegrity
- 466 • Chris McLaren, Netegrity
- 467 • Lynne Rosenthal, NIST
- 468 • Mark Skall, NIST
- 469 • Simon Godik, Overxeer
- 470 • Charles Norwood, SAIC
- 471 • Evan Prodromou, Securant
- 472 • Robert Griffin, RSA Security (former editor)
- 473 • Sai Allarvarpu, Sun Microsystems
- 474 • Chris Ferris, Sun Microsystems
- 475 • Emily Xu, Sun Microsystems
- 476 • Mike Myers, Traceroute Security
- 477 • Phillip Hallam-Baker, VeriSign (former editor)
- 478 • James Vanderbeek, Vodafone
- 479 • Mark O'Neill, Vordel
- 480 • Tony Palmer, Vordel

481
482 Finally, the editors wish to acknowledge the following people for their contributions of material used as
483 input to the OASIS Security Assertions Markup Language specifications:

- 484 • Thomas Gross, IBM
- 485 • Birgit Pfitzmann, IBM

486 **Appendix B. Notices**

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

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

498 **Copyright © OASIS Open 2004. All Rights Reserved.**

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

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

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