



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

Committee Draft 03, 14 December 2004

Document identifier:

sstc-saml-conformance-2.0-cd-03

Location:

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

Editors:

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

SAML V2.0 Contributors:

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

44 Ron Monzillo, Sun Microsystems
45 Greg Whitehead, Trustgenix

46 **Abstract:**

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

49 **Status:**

50 This is a **Committee Draft** approved by the Security Services Technical Committee on 14
51 December 2004.

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

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

61 **Table of Contents**

62	1 Introduction.....	4
63	1.1 Overview and Specification of SAML V2.0.....	4
64	1.2 Notation.....	5
65	2 SAML V2.0 Profiles and Possible Implementations.....	6
66	3 Conformance.....	8
67	3.1 Operational Modes.....	8
68	3.2 Feature Matrix.....	8
69	3.3 Implementation of SAML-Defined Identifiers.....	10
70	3.4 Implementation of Encrypted Elements.....	10
71	3.5 Security Models for SOAP and URI Bindings.....	11
72	4 XML Digital Signature and XML Encryption.....	12
73	4.1 XML Signature Algorithms.....	12
74	4.2 XML Encryption Algorithms.....	12
75	5 Use of SSL 3.0 or TLS 1.0.....	13
76	5.1 SAML SOAP and URI Binding	13
77	5.2 Web SSO Profiles of SAML	13
78	6 References.....	14
79		

1 Introduction

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.

1.1 Overview and Specification of SAML V2.0

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

- This specification: Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0
- Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLCore]
 - SAML assertions schema [SAMLAssn-xsd]
 - SAML protocols schema [SAMLProt-xsd]
- Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLBind]
- Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLProf]
 - SAML ECP profile schema [SAMLECP-xsd]
 - SAML LDAP attribute profile schema [SAMLLDAP-xsd]
 - SAML DCE PAC attribute profile schema [SAMLDCExsd]
 - SAML XACML attribute profile schema [SAMLXAC-xsd]
- Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLMeta]
- SAML metadata schema [SAMLMeta-xsd]
- Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLAuthnCxt]
 - SAML authentication context schema [SAMLAC-xsd]
 - SAML context class schema for Internet Protocol [SAMLAC-IP]
 - SAML context class schema for Internet Protocol Password [SAMLAC-IPP]
 - SAML context class schema for Kerberos [SAMLAC-Kerb]
 - SAML context class schema for Mobile One Factor Unregistered [SAMLAC-MOFU]
 - SAML context class schema for Mobile Two Factor Unregistered [SAMLAC-MTFU]
 - SAML context class schema for Mobile One Factor Contract [SAMLAC-MOFC]
 - SAML context class schema for Mobile Two Factor Contract [SAMLAC-MTFC]
 - SAML context class schema for Password [SAMLAC-Pass]
 - SAML context class schema for Password Protected Transport [SAMLAC-PPT]
 - SAML context class schema for Previous Session [SAMLAC-Prev]
 - SAML context class schema for Public Key – X.509 [SAMLAC-X509]
 - SAML context class schema for Public Key – PGP [SAMLAC-PGP]
 - SAML context class schema for Public Key – SPKI [SAMLAC-SPKI]
 - SAML context class schema for Public Key – XML Signature [SAMLAC-XSig]
 - SAML context class schema for Smartcard [SAMLAC-Smart]
 - SAML context class schema for Smartcard PKI [SAMLAC-SmPKI]
 - SAML context class schema for Software PKI [SAMLAC-SwPKI]

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

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

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

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

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

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

149 1.2 Notation

150 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
151 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted in this
152 specification and all of the SAML V2.0 specifications as described in IETF RFC 2119 [RFC2119]:
153

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

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

2 SAML V2.0 Profiles and Possible Implementations

160 The following table enumerates all of the profiles defined by the SAML profiles specification [SAMLProf].
 161 For each profile, the message protocol flows (defined in the assertions and protocols specification
 162 [SAMLCore]) found within the profile are also described. For each message flow, a list of relevant bindings
 163 (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

165 **3 Conformance**

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

167 **3.1 Operational Modes**

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

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

179 **3.2 Feature Matrix**

180 The following matrices identify unique sets of conformance requirements by means of a triple taken from
181 Table 1 with the form: profile, message(s), binding The message component is not always included when
182 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

184

185 The following table summarizes operational modes that extend the IdP or SP modes defined above.
 186 These are to be understood as a combination of an IdP or SP mode from the table above with the
 187 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

189

190

191 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

192

193 3.3 Implementation of SAML-Defined Identifiers

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

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

198 3.4 Implementation of Encrypted Elements

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

- 200 1. <saml:EncryptedID>,
- 201 2. <saml:EncryptedAssertion>,
- 202 3. <saml:EncryptedAttribute>

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

205

206 **3.5 Security Models for SOAP and URI Bindings**

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

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

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

217

218 4 XML Digital Signature and XML Encryption

219

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

223

224 4.1 XML Signature Algorithms

225

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

- 228 • Digest: SHA1
- 229 • MAC: HMAC-SHA1
- 230 • XML Canonicalization: CanonicalXML (Without comments),
- 231 • Transform: Enveloped Signature

232

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

235

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

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

240 4.2 XML Encryption Algorithms

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

243

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

246

247 **5 Use of SSL 3.0 or TLS 1.0**

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

252 **5.1 SAML SOAP and URI Binding**

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

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

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

261 FIPS SSL-capable implementations MUST implement the FIPS cipher suite corresponding to the SSL
262 SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

263 **5.2 Web SSO Profiles of SAML**

264 SSL-capable implementations of the Web SSO profile of SAML MUST implement the
265 SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. TLS-capable implementations MUST implement
266 the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.
267

6 References

268

- 269 [AES] FIPS-197, *Advanced Encryption Standard (AES)*, available from
270 <http://www.nist.gov/>.
- 271 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
272 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 273 [RFC2617] J. Franks et. al., *HTTP Authentication: Basic and Digest Access Authentication*,
274 IETF RFC 2617, June 1999.
- 275 [RFC2246] T. Dierks et. al., *The TLS Protocol Version 1.0*, IETF RFC 2246, January 1999.
- 276 [SAMLAssn-xsd] S. Cantor et al., *SAML assertions schema*. OASIS SSTC, December 2004.
277 Document ID sstc-saml-schema-assertion-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
278 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 279 [SAMLAuthnCxt] J. Kemp et al., *Authentication Context for the OASIS Security Assertion Markup*
280 *Language (SAML) V2.0*. OASIS SSTC, December 2004. Document ID sstc-saml-
281 authn-context-2.0-cd-03. See <http://www.oasis-open.org/committees/security/>.
- 282 [SAMLAC-xsd] J. Kemp et al., *SAML authentication context schema*. OASIS SSTC, December
283 2004. Document ID sstc-saml-schema-authn-context-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
284 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 285 [SAMLAC-IP] J. Kemp et al., *SAML context class schema for Internet Protocol*. OASIS SSTC,
286 December 2004. Document ID sstc-saml-schema-authn-context-ip-2.0. See
287 <http://www.oasis-open.org/committees/security/>.
- 288 [SAMLAC-IPP] J. Kemp et al., *SAML context class schema for Internet Protocol Password*.
289 OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-
290 ippword-2.0. See <http://www.oasis-open.org/committees/security/>.
- 291 [SAMLAC-Kerb] J. Kemp et al., *SAML context class schema for Kerberos*. OASIS SSTC,
292 December 2004. Document ID sstc-saml-schema-authn-context-kerberos-2.0.
293 See <http://www.oasis-open.org/committees/security/>.
- 294 [SAMLAC-MOFC] J. Kemp et al., *SAML context class schema for Mobile One Factor Contract*.
295 Document ID sstc-saml-schema-authn-context-mobileonefactor-reg-2.0. See
296 OASIS SSTC, December 2004. <http://www.oasis-open.org/committees/security/>.
- 297 [SAMLAC-MOFU] J. Kemp et al., *SAML context class schema for Mobile One Factor Unregistered*.
298 Document ID sstc-saml-schema-authn-context-mobileonefactor-unreg-2.0. See
299 OASIS SSTC, December 2004. <http://www.oasis-open.org/committees/security/>.
- 300 [SAMLAC-MTFC] J. Kemp et al., *SAML context class schema for Mobile Two Factor Contract*.
301 OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-
302 mobiletwofactor-reg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 303 [SAMLAC-MTFU] J. Kemp et al., *SAML context class schema for Mobile Two Factor Unregistered*.
304 OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-
305 mobiletwofactor-unreg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 306 [SAMLAC-Pass] J. Kemp et al., *SAML context class schema for Password*. OASIS SSTC,
307 December 2004. Document ID sstc-saml-schema-authn-context-pword-2.0. See
308 <http://www.oasis-open.org/committees/security/>.

309	[SAMLAC-PGP]	J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-pgp-2.0. See http://www.oasis-open.org/committees/security/ .
310		
311		
312	[SAMLAC-PPT]	J. Kemp et al., SAML context class schema for Password Protected Transport. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-ppt-2.0. See http://www.oasis-open.org/committees/security/ .
313		
314		
315	[SAMLAC-Prev]	J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-session-2.0. See http://www.oasis-open.org/committees/security/ .
316		
317		
318	[SAMLAC-Smart]	J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-smartcard-2.0. See http://www.oasis-open.org/committees/security/ .
319		
320		
321	[SAMLAC-SmPKI]	J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-smartcardpki-2.0. See http://www.oasis-open.org/committees/security/ .
322		
323		
324	[SAMLAC-SPKI]	J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-spki-2.0. See http://www.oasis-open.org/committees/security/ .
325		
326		
327	[SAMLAC-SRP]	J. Kemp et al., SAML context class schema for Secure Remote Password. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-srp-2.0. See http://www.oasis-open.org/committees/security/ .
328		
329		
330	[SAMLAC-SSL]	J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-sslcert-2.0. See http://www.oasis-open.org/committees/security/ .
331		
332		
333	[SAMLAC-SwPKI]	J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-softwarepki-2.0. See http://www.oasis-open.org/committees/security/ .
334		
335		
336	[SAMLAC-Tele]	J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
337		
338		
339	[SAMLAC-TNom]	J. Kemp et al., SAML context class schema for Telephony (“Nomadic”). OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-nomad-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
340		
341		
342	[SAMLAC-TPers]	J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-personal-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
343		
344		
345	[SAMLAC-TAuthn]	J. Kemp et al., SAML context class schema for Telephony (Authenticated). OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-auth-telephony-2.0. See http://www.oasis-open.org/committees/security/ .
346		
347		
348	[SAMLAC-TST]	J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-timesync-2.0. See http://www.oasis-open.org/committees/security/ .
349		
350		
351	[SAMLAC-X509]	J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-x509-2.0. See http://www.oasis-open.org/committees/security/ .
352		
353		
354	[SAMLAC-XSig]	J. Kemp et al., SAML context class schema for Public Key – XML Signature. OASIS SSTC, December 2004. Document ID sstc-saml-schema-authn-context-xmldsig-2.0. See http://www.oasis-open.org/committees/security/ .
355		
356		
357	[SAMLBind]	S. Cantor et al., <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, December 2004. Document ID sstc-saml-bindings-2.0-cd-03. See http://www.oasis-open.org/committees/security/ .
358		
359		

361	[SAMLCore]	S. Cantor et al., <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, December 2004. Document ID sstc-saml-core-2.0-cd-03. See http://www.oasis-open.org/committees/security/ .
362		
363		
364	[SAML DCE-xsd]	S. Cantor et al., SAML DCE PAC attribute profile schema. OASIS SSTC, December 2004. Document ID sstc-saml-schema-dce-2.0. See http://www.oasis-open.org/committees/security/ .
365		
366		
367	[SAML ECP-xsd]	S. Cantor et al., SAML ECP profile schema. OASIS SSTC, December 2004. Document ID sstc-saml-schema-ecp-2.0. See http://www.oasis-open.org/committees/security/ .
368		
369		
370	[SAML Gloss]	J. Hodges et al., <i>Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, December 2004. Document ID sstc-saml-glossary-2.0-cd-03. See http://www.oasis-open.org/committees/security/ .
371		
372		
373	[SAML LDAP-xsd]	S. Cantor et al., SAML LDAP attribute profile schema. OASIS SSTC, December 2004. Document ID sstc-saml-schema-ldap-2.0. See http://www.oasis-open.org/committees/security/ .
374		
375		
376	[SAML Meta]	S. Cantor et al., <i>Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, December 2004. Document ID sstc-saml-metadata-2.0-cd-03. See http://www.oasis-open.org/committees/security/ .
377		
378		
379	[SAML Meta-xsd]	S. Cantor et al., SAML metadata schema. OASIS SSTC, December 2004. Document ID sstc-saml-schema-metadata-2.0. See http://www.oasis-open.org/committees/security/ .
380		
381		
382	[SAML Prof]	S. Cantor et al., <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, December 2004. Document ID sstc-saml-profiles-2.0-cd-03. See http://www.oasis-open.org/committees/security/ .
383		
384		
385	[SAML Prot-xsd]	S. Cantor et al., SAML protocols schema. OASIS SSTC, December 2004. Document ID sstc-saml-schema-protocol-2.0. See http://www.oasis-open.org/committees/security/ .
386		
387		
388	[SAML Sec]	F. Hirsch et al., <i>Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, December 2004. Document ID sstc-saml-sec-consider-2.0-cd-03. See http://www.oasis-open.org/committees/security/ .
389		
390		
391		
392	[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/ .
393		
394		
395	[SAML XAC-xsd]	S. Cantor et al., SAML XACML attribute profile schema. OASIS SSTC, December 2004. Document ID sstc-saml-schema-xacml-2.0. See http://www.oasis-open.org/committees/security/ .
396		
397		
398	[SSL3]	A. Frier et al., <i>The SSL 3.0 Protocol</i> , Netscape Communications Corp, November 1996.
399		
400	[XML Enc]	Donald Eastlake et al., XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenc-core/ , World Wide Web Consortium, December 2002.
401		
402		
403	[XML Sig]	Donald Eastlake et al., XML-Signature Syntax and Processing, http://www.w3.org/TR/xmlsig-core/ , World Wide Web Consortium, February 2002.
404		
405		
406		

407 Appendix A. Acknowledgements

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

- 410 • Conor Cahill, AOL
- 411 • John Hughes, Atos Origin
- 412 • Hal Lockhart, BEA Systems
- 413 • Mike Beach, Boeing
- 414 • Rebekah Metz, Booz Allen Hamilton
- 415 • Rick Randall, Booz Allen Hamilton
- 416 • Ronald Jacobson, Computer Associates
- 417 • Paul Madsen, Entrust
- 418 • Dana Kaufman, Forum Systems
- 419 • Paula Austel, IBM
- 420 • Michael McIntosh, IBM
- 421 • Anthony Nadalin, IBM
- 422 • Nick Ragouzis, Individual
- 423 • Scott Cantor, Internet2
- 424 • Bob Morgan, Internet2
- 425 • Peter Davis, Neustar
- 426 • Jeff Hodges, Neustar
- 427 • Frederick Hirsch, Nokia
- 428 • John Kemp, Nokia
- 429 • Abbie Barbir, Nortel Networks
- 430 • Scott Kiestler, Novell
- 431 • Cameron Morris, Novell
- 432 • Charles Knouse, Oblix
- 433 • Steve Anderson, OpenNetwork
- 434 • Ari Kermaier, Oracle
- 435 • Vamsi Motukuru, Oracle
- 436 • Darren Platt, Ping Identity
- 437 • Prateek Mishra, Principal Identity
- 438 • Jim Lien, RSA Security
- 439 • Rob Philpott, RSA Security
- 440 • Dipak Chopra, SAP
- 441 • Jahan Moreh, Sigaba
- 442 • Bhavna Bhatnagar, Sun Microsystems
- 443 • Eve Maler, Sun Microsystems
- 444 • Ronald Monzillo, Sun Microsystems
- 445 • Emily Xu, Sun Microsystems
- 446 • Greg Whitehead, Trustgenix
- 447

448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476

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

- Stephen Farrell, Baltimore Technologies
- David Orchard, BEA Systems
- Krishna Sankar, Cisco Systems
- Zahid Ahmed, CommerceOne
- Carlisle Adams, Entrust
- Tim Moses, Entrust
- Nigel Edwards, Hewlett-Packard
- Joe Pato, Hewlett-Packard
- Bob Blakley, IBM
- Marlena Erdos, IBM
- Marc Chanliau, Netegrity
- Chris McLaren, Netegrity
- Lynne Rosenthal, NIST
- Mark Skall, NIST
- Simon Godik, Overxeer
- Charles Norwood, SAIC
- Evan Prodromou, Securant
- Robert Griffin, RSA Security (former editor)
- Sai Allarvarpu, Sun Microsystems
- Chris Ferris, Sun Microsystems
- Emily Xu, Sun Microsystems
- Mike Myers, Traceroute Security
- Phillip Hallam-Baker, VeriSign (former editor)
- James Vanderbeek, Vodafone
- Mark O'Neill, Vordel
- Tony Palmer, Vordel

477
478
479

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

- Thomas Gross, IBM
- Birgit Pfitzmann, IBM

482 **Appendix B. Notices**

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

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

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

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

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

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