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

Committee Draft 04, 15 January 2005

Document identifier:

sstc-saml-conformance-2.0-cd-04

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
Thomas Wisniewski, 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
Paul Madsen, NTT
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
Ron Monzillo, Sun Microsystems
Greg Whitehead, Trustgenix

Abstract:

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

Status:

This is a **Committee Draft** approved by the Security Services Technical Committee on 15 January 2005

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

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

Table of Contents

1 Introduction....4
1.1 Overview and Specification of SAML V2.0....4
1.2 Notation....5
2 SAML V2.0 Profiles and Possible Implementations....6
3 Conformance....8
3.1 Operational Modes....8
3.2 Feature Matrix....8
3.3 Implementation of SAML-Defined Identifiers....10
3.4 Implementation of Encrypted Elements....11
3.5 Security Models for SOAP and URI Bindings....11
4 XML Digital Signature and XML Encryption....12
4.1 XML Signature Algorithms....12
4.2 XML Encryption Algorithms....12
5 Use of SSL 3.0 or TLS 1.0....13
5.1 SAML SOAP and URI Binding....13
5.2 Web SSO Profiles of SAML....13
6 References....14

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 X.500/LDAP attribute profile schema [SAMLX500-xsd]
  - SAML DCE PAC attribute profile schema [SAMLDCE-xsd]
  - 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 authentication context schema types [SAMLACTyp-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]

- SAML context class schema for Telephony [SAMLAC-Tele]
- SAML context class schema for Telephony (“Nomadic”) [SAMLAC-TNom]
- SAML context class schema for Telephony (Personalized) [SAMLAC-TPers]
- SAML context class schema for Telephony (Authenticated) [SAMLAC-TAuthn]
- SAML context class schema for Secure Remote Password [SAMLAC-SRP]
- SAML context class schema for SSL/TLS Certificate-Based Client Authentication [SAMLAC-SSL]
- SAML context class schema for Time Sync Token [SAMLAC-TST]

- Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLSec]
- Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLGloss]

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

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

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

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

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

1.2 Notation

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

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

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

2 SAML V2.0 Profiles and Possible Implementations

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

166

3 Conformance

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

3.1 Operational Modes

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

- IdP – Identity Provider
- IdP Lite – Identity Provider Lite
- SP – Service Provider
- SP Lite – Service Provider Lite
- ECP – Enhanced Client/Proxy
- SAML Attribute Authority
- SAML Authorization Decision Authority
- SAML Authentication Authority
- SAML Requester

3.2 Feature Matrix

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

185

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

186

187 The following table summarizes operational modes that extend the IdP or SP modes defined above.
188 These are to be understood as a combination of an IdP or SP mode from the table above with the
189 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

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

3.3 Implementation of SAML-Defined Identifiers

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

1. All Attribute Name Format identifiers defined in Section 8.2 of [SAMLCore].
2. All Name Identifier Format identifiers defined in Section 8.3 of [SAMLCore].

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

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

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

specification.

A SAML implementation may provide the facilities described above through direct implementation support for the identifiers or through the use of supported programming interfaces. Interfaces provided for this purpose must allow the SAML implementation to be programmatically extended to handle all identifiers in section 8.2 and 8.3 that are not natively handled by the implementation.

3.4 Implementation of Encrypted Elements

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

1. <saml:EncryptedID>,
2. <saml:EncryptedAssertion>,
3. <saml:EncryptedAttribute>

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

3.5 Security Models for SOAP and URI Bindings

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

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

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

4 XML Digital Signature and XML Encryption

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

4.1 XML Signature Algorithms

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

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)

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

4.2 XML Encryption Algorithms

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

5 Use of SSL 3.0 or TLS 1.0

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

5.1 SAML SOAP and URI Binding

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

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

SSL-capable implementations MUST implement the SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite.

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

5.2 Web SSO Profiles of SAML

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

6 References

[AES] FIPS-197, *Advanced Encryption Standard (AES)*, available from http://www.nist.gov/.

[RFC 2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[RFC 2246] T. Dierks et. al., The TLS Protocol Version 1.0, IETF RFC 2246, January 1999.

[RFC 2617] J. Franks et. al., HTTP Authentication: Basic and Digest Access Authentication, IETF RFC 2617,June 1999.

[SAMLAssn-xsd] S. Cantor et al., SAML assertions schema. OASIS SSTC, January 2005. Document ID sstc-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, January 2005. Document ID sstc-saml-authn-context-2.0-cd-04. See http://www.oasis-open.org/committees/security/.

[SAMLAC-xsd] J. Kemp et al., SAML authentication context schema. OASIS SSTC, January 2005. Document ID sstc-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, January 2005. Document ID sstc-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, January 2005. Document ID sstc-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, January 2005. Document ID sstc-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, January 2005. Document ID sstc-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 sstc-saml-schema-authn-context-mobileonefactor-reg-2.0. See OASIS SSTC, January 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 sstc-saml-schema-authn-context-mobileonefactor-unreg-2.0. See OASIS SSTC, January 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, January 2005. Document ID sstc-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, January 2005. Document ID sstc-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, January 2005. Document ID sstc-saml-schema-authn-context-pword-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-PGP] J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-pgp-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-PPT] J. Kemp et al., SAML context class schema for Password Protected Transport. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-ppt-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Prev] J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-session-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Smart] J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-smartcard-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SmPKI] J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-smartcardpki-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SPKI] J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-spki-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SRP] J. Kemp et al., SAML context class schema for Secure Remote Password. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-srp-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SSL] J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-sslcert-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-SwPKI] J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-softwarepki-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-Tele] J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-telephony-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TNom] J. Kemp et al., SAML context class schema for Telephony ("Nomadic"). OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-nomad-telephony-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TPers] J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-personal-telephony-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TAuthn] J. Kemp et al., SAML context class schema for Telephony (Authenticated). OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-auth-telephony-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-TST] J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-timesync-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-X509] J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-x509-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLAC-XSig] J. Kemp et al., SAML context class schema for Public Key – XML Signature. OASIS SSTC, January 2005. Document ID sstc-saml-schema-authn-context-xmldsig-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLBind] S. Cantor et al., *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, January 2005. Document ID sstc-saml-bindings-2.0-cd-04. See http://www.oasis-open.org/committees/security/.

[SAMLCore] S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, January 2005. Document ID sstc-saml-core-2.0-cd-04. See http://www.oasis-open.org/committees/security/.

[SAMLDCE-xsd] S. Cantor et al., SAML DCE PAC attribute profile schema. OASIS SSTC, January 2005. Document ID sstc-saml-schema-dce-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLECP-xsd] S. Cantor et al., SAML ECP profile schema. OASIS SSTC, January 2005. Document ID sstc-saml-schema-ecp-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLGloss] J. Hodges et al., *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, January 2005. Document ID sstc-saml-glossary-2.0-cd-04. See http://www.oasis-open.org/committees/security/.

[SAMLMeta] S. Cantor et al., *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, January 2005. Document ID sstc-saml-metadata-2.0-cd-04. See http://www.oasis-open.org/committees/security/.

[SAMLMeta-xsd] S. Cantor et al., SAML metadata schema. OASIS SSTC, January 2005. Document ID sstc-saml-schema-metadata-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLProf] S. Cantor et al., *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, January 2005. Document ID sstc-saml-profiles-2.0-cd-04. See http://www.oasis-open.org/committees/security/.

[SAMLProt-xsd] S. Cantor et al., SAML protocols schema. OASIS SSTC, January 2005. Document ID sstc-saml-schema-protocol-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLSec] F. Hirsch et al., *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, January 2005. Document ID sstc-saml-sec-consider-2.0-cd-04. See http://www.oasis-open.org/committees/security/.

[SAMLTechOvw] J. Hughes et al., *Technical Overview for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, August 2004. Document ID sstc-saml-tech-overview-2.0-draft-01. See http://www.oasis-open.org/committees/security/.

[SAMLX500-xsd] S. Cantor et al., SAML X.500/LDAP attribute profile schema. OASIS SSTC, January 2005. Document ID sstc-saml-schema-x500-2.0. See http://www.oasis-open.org/committees/security/.

[SAMLXAC-xsd] S. Cantor et al., SAML XACML attribute profile schema. OASIS SSTC, January 2005. Document ID sstc-saml-schema-xacml-2.0. See http://www.oasis-open.org/committees/security/.

[SSL3] A. Frier et al., *The SSL 3.0 Protocol*, Netscape Communications Corp, November 1996.

[XMLEnc] Donald Eastlake et al., XML Encryption Syntax and Processing, http://www.w3.org/TR/xmlenc-core/, World Wide Web Consortium, December 2002.

[XMLSig] Donald Eastlake et al., XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/, World Wide Web Consortium, February 2002.

Appendix A. Acknowledgements

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

- Conor Cahill, AOL
- John Hughes, Atos Origin
- Hal Lockhart, BEA Systems
- Mike Beach, Boeing
- Rebekah Metz, Booz Allen Hamilton
- Rick Randall, Booz Allen Hamilton
- Ronald Jacobson, Computer Associates
- Carolina Canales-Valenzuela, Ericsson
- Dana Kaufman, Forum Systems
- Irving Reid, Hewlett-Packard
- Paula Austel, IBM
- Michael McIntosh, IBM
- Anthony Nadalin, IBM
- Nick Ragouzis, Individual
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Peter Davis, Neustar
- Jeff Hodges, Neustar
- Frederick Hirsch, Nokia
- Senthil Sengodan, Nokia
- Abbie Barbir, Nortel Networks
- Scott Kiester, Novell
- Cameron Morris, Novell
- Paul Madsen, NTT
- Steve Anderson, OpenNetwork
- Ari Kermaier, Oracle
- Vamsi Motukuru, Oracle
- Darren Platt, Ping Identity
- Prateek Mishra, Principal Identity
- Jim Lien, RSA Security
- John Linn, RSA Security
- Rob Philpott, RSA Security
- Dipak Chopra, SAP
- Jahan Moreh, Sigaba
- Bhavna Bhatnagar, Sun Microsystems
- Eve Maler, Sun Microsystems
- Ronald Monzillo, Sun Microsystems
- Emily Xu, Sun Microsystems
- Greg Whitehead, Trustgenix

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
- Mike Myers, Traceroute Security
- Phillip Hallam-Baker, VeriSign (former editor)
- James Vanderbeek, Vodafone
- Mark O'Neill, Vordel
- Tony Palmer, Vordel

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

Appendix B. Notices

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

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