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

Working Draft 06~~5~~, 17~~5~~ August 2004

Document identifier:

sstc-saml-conformance-2.0-draft-06~~5~~

Location:

http://www.oasis-open.org/apps/org/workgroup/security/download.php

Editors:

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

Contributors:

John Kemp, Nokia
<other contributors>

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 specification is a SAML V2.0 working draft.

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 vetted errata on the Security Services TC web page (http://www.oasis-open.org/committees/security/).

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

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 [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 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 key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF RFC 2119 .

```
Listings of productions or other normative code appear like this.
```

```
Example code listings appear like this.
```

Note: Non-normative notes and explanations appear like this.

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
X.500 attribute profile		
XACML attribute profile		
Metadata	Consumption	
	Exchange	

129

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 Responder
- SAML Authorization Decision Responder
- SAML Authentication Responder

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.

149

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	~~OPTIONAL~~ MUST	OPTIONAL	~~OPTIONAL~~ MUST	OPTIONAL	N/A
Single Logout (SP-initiated) – HTTP redirect	MUST	MUST	MUST	MUST	N/A
Single Logout (SP-initiated) – SOAP	~~OPTIONAL~~ MUST	OPTIONAL	~~OPTIONAL~~ MUST	OPTIONAL	N/A
Identity Provider Discovery (cookie)	MUST	MUST	OPTIONAL	OPTIONAL	N/A

150

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

154

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

155

156 An implementation conforming to any of the IdP or SP operational modes MUST implement all of the
157 Name Identifier Format Identifiers described in Section 8.3 of [SAMLCore].

158 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		
Attribute Query, SOAP		MUST	
Authorization Decision Query, SOAP			MUST
Request for Assertion by Identifier, SOAP	MUST	MUST	MUST
SAML URI Binding	MUST	MUST	MUST

159

160 3.3 Security Models for SOAP and URI Bindings

161
162

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

166 1. No client or server authentication.

167 2. HTTP basic authentication [RFC2617] with and without SSL 3.0 or TLS 1.0 (see Section 3 below). The
168 SAML requester MUST preemptively send the authorization header with the initial request.

169 3. HTTP over SSL 3.0 or TLS 1.0 server authentication with server-side certificate.

170 4. HTTP over SSL 3.0 or TLS 1.0 mutual authentication with both server-side and a client-side certificate.

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

4 Use of SSL 3.0 or TLS 1.0

In any SAML use of SSL 3.0 [SSL3] or TLS 1.0 **[RFC2246]** , 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).

4.1 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]**.

4.2 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.

5 References

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

RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[RFC2617] J. Franks et. al.**,** *HTTP Authentication: Basic and Digest Access Authentication*, IETF RFC 2617,June 1999.

[RFC2246] T. Dierks et. al., *The TLS Protocol Version 1.0,* IETF RFC 2246, January 1999.

[SAMLAssn-xsd] S. Cantor et al., SAML assertions schema. OASIS SSTC, 2004. 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, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-xsd] J. Kemp et al., SAML authentication context schema. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-IP] J. Kemp et al., SAML context class schema for Internet Protocol. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-IPP] J. Kemp et al., SAML context class schema for Internet Protocol Password. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-Kerb] J. Kemp et al., SAML context class schema for Kerberos. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-MOFC] J. Kemp et al., SAML context class schema for Mobile One Factor Contract. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-MOFU] J. Kemp et al., SAML context class schema for Mobile One Factor Unregistered. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-MTFC] J. Kemp et al., SAML context class schema for Mobile Two Factor Contract. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-MTFU] J. Kemp et al., SAML context class schema for Mobile Two Factor Unregistered. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-Pass] J. Kemp et al., SAML context class schema for Password. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-PGP] J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-PPT] J. Kemp et al., SAML context class schema for Password Protected Transport. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-Prev] J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-Smart] J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-SmPKI] J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-SPKI] J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-SRP] J. Kemp et al., SAML context class schema for Secure Remote Password. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-SSL] J. Kemp et al., SAML context class schema for SSL/TLS Certificate-Based Client

open.org/committees/security/.

[SAMLAC-SwPKI] J. Kemp et al., SAML context class schema for Software PKI. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-Tele] J. Kemp et al., SAML context class schema for Telephony. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-TNom] J. Kemp et al., SAML context class schema for Telephony ("Nomadic"). OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-TPers] J. Kemp et al., SAML context class schema for Telephony (Personalized). OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-TAuthn] J. Kemp et al., SAML context class schema for Telephony (Authenticated). OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-TST] J. Kemp et al., SAML context class schema for Time Sync Token. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-X509] J. Kemp et al., SAML context class schema for Public Key – X.509. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLAC-XSig] J. Kemp et al., SAML context class schema for Public Key – XML Signature. OASIS SSTC, 2004. 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, 2004. 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, 2004. http://www.oasis-open.org/committees/security/.

[SAMLDCE-xsd] S. Cantor et al., SAML DCE PAC attribute profile schema. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

[SAMLECP-xsd] S. Cantor et al., SAML ECP profile schema. OASIS SSTC, 2004. 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, 2004. http://www.oasis-open.org/committees/security/.

[SAMLLDAP-xsd] S. Cantor et al., SAML LDAP attribute profile schema. OASIS SSTC, 2004. 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, 2004. http://www.oasis-open.org/committees/security/.

[SAMLMeta-xsd] S. Cantor et al., SAML metadata schema. OASIS SSTC, 2004. 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, 2004. http://www.oasis-open.org/committees/security/.

[SAMLProt-xsd] S. Cantor et al., SAML protocols schema. OASIS SSTC, 2004. 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, 2004. 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, 2004. http://www.oasis-open.org/committees/security/.

[SAMLXAC-xsd] S. Cantor et al., SAML XACML attribute profile schema. OASIS SSTC, 2004. http://www.oasis-open.org/committees/security/.

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

A. Revision History

Rev	Date	By Whom	What
0	15 Jun 2004	Prateek Mishra	Initial draft based on list proposal
1	7 Jul 2004	Prateek Mishra	Includes Rob Philpott's conformance matrix
2	15 Jul 2004	Prateek Mishra	Introduced operational mode terminology, ECP
3	29 Jul 2004	Prateek Mishra	Re-started conformance matrix with ID-FF 1.2 SCR foundation, added SAML Responder operational modes
4	6 Aug 2004	Prateek Mishra, Eve Maler	Updated to act as entry point for entire specification set; updated with motions from previous conference call
5	15 Aug 2004	Eve Maler, Prateek Mishra, Rob Philpott	Updated with full entry-point references, added reference to Section 8.3 of Core, MTI security modes for SOAP and URI binding.Final editorial changes before CD vote.
6	17 Aug 2004	Eve Maler	Changed op modes IdP and SP to have MUST for SLO (SOAP binding), whether IdP-initiated or SP-initiated.

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.