

---

# Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite

Working Draft, ~~12 February~~December 20097

## Document identifier:

sstc-saml-conformance-errata-2.0-wd-043

## Location:

[http://www.oasis-open.org/committees/documents.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)

## Editors:

Prateek Mishra, Principal Identity  
Rob Philpott, RSA Security  
Eve Maler, Sun Microsystems (errata editor)  
[Scott Cantor, Internet2 \(errata editor\)](#)

## Contributors to the Errata:

Rob Philpott, EMC Corporation  
Nick Ragouzis, Enosis Group  
Thomas Wisniewski, Entrust  
Greg Whitehead, HP  
Heather Hinton, IBM  
Connor P. Cahill, Intel  
Scott Cantor, Internet2  
Nate Klingenstein, Internet2  
RL 'Bob' Morgan, Internet2  
John Bradley, Individual  
Jeff Hodges, Individual  
Joni Brennan, Liberty Alliance  
Eric Tiffany, Liberty Alliance  
Thomas Hardjono, M.I.T.  
Tom Scavo, NCSA  
Peter Davis, NeuStar, Inc.  
Frederick Hirsch, Nokia Corporation  
Paul Madsen, NTT Corporation  
Ari Kermaier, Oracle Corporation  
Hal Lockhart, Oracle Corporation  
Prateek Mishra, Oracle Corporation  
Brian Campbell, Ping Identity  
Anil Saldhana, Red Hat Inc.  
Jim Lien, RSA Security  
Jahan Moreh, Sigaba  
Kent Spaulding, Skyworth TTG Holdings Limited  
Emily Xu, Sun Microsystems  
David Staggs, Veteran's Health Administration

## SAML V2.0 Contributors:

46 Conor P. Cahill, AOL  
47 John Hughes, Atos Origin  
48 Hal Lockhart, BEA Systems  
49 Michael Beach, Boeing  
50 Rebekah Metz, Booz Allen Hamilton  
51 Rick Randall, Booz Allen Hamilton  
52 Thomas Wisniewski, Entrust  
53 Irving Reid, Hewlett-Packard  
54 Paula Austel, IBM  
55 Maryann Hondo, IBM  
56 Michael McIntosh, IBM  
57 Tony Nadalin, IBM  
58 Nick Ragouzis, Individual  
59 Scott Cantor, Internet2  
60 RL 'Bob' Morgan, Internet2  
61 Peter C Davis, Neustar  
62 Jeff Hodges, Neustar  
63 Frederick Hirsch, Nokia  
64 John Kemp, Nokia  
65 Paul Madsen, NTT  
66 Steve Anderson, OpenNetwork  
67 Prateek Mishra, Principal Identity  
68 John Linn, RSA Security  
69 Rob Philpott, RSA Security  
70 Jahan Moreh, Sigaba  
71 Anne Anderson, Sun Microsystems  
72 Eve Maler, Sun Microsystems  
73 Ron Monzillo, Sun Microsystems  
74 Greg Whitehead, Trustgenix

#### 75 **Abstract:**

76 The SAML V2.0 Conformance specification provides the technical requirements for SAML V2.0  
77 conformance and specifies the entire set of documents comprising SAML V2.0. This document,  
78 known as an "errata composite", combines corrections to reported errata with the original  
79 specification text. By design, the corrections are limited to clarifications of ambiguous or  
80 conflicting specification text. This document shows deletions from the original specification as  
81 struck-through text, and additions as colored underlined text. The "[*Errn*]" designations embedded  
82 in the text refer to particular errata and their dispositions.

#### 83 **Status:**

84 This errata composite document is a **working draft** based on the [original](#) OASIS Standard  
85 document that had been produced by the Security Services Technical Committee and approved  
86 by the OASIS membership on 1 March 2005. While the errata corrections appearing here are  
87 non-normative, they reflect changes specified by the Approved Errata document (currently at  
88 Working Draft revision 02), which is on an OASIS standardization track. In case of any  
89 discrepancy between this document and the Approved Errata, the latter has precedence. ~~See also~~  
90 ~~the Errata Working Document (currently at revision 39), which provides background on the~~  
91 ~~changes specified here.~~

92 This document includes corrections for errata E11, E25, E28, E29, E42, ~~and~~ E50, ~~and~~ E74.

93 Committee members should submit comments and potential errata to the [security-](mailto:security-services@lists.oasis-open.org)  
94 [services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org) list. Others should submit them by following the instructions at  
95 [http://www.oasis-open.org/committees/comments/form.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security).

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

---

# Table of Contents

100		
101	1 Introduction.....	4
102	1.1 Overview and Specification of SAML V2.0.....	4
103	1.2 Notation.....	5
104	2 SAML V2.0 Profiles and Possible Implementations.....	6
105	3 Conformance.....	8
106	3.1 Operational Modes.....	8
107	3.2 Feature Matrix.....	8
108	3.3 Implementation of SAML-Defined Identifiers.....	10
109	3.4 Implementation of Encrypted Elements.....	11
110	3.5 Security Models for SOAP and URI Bindings.....	11
111	3.6 [E25]Metadata Structures.....	11
112	3.7 Metadata Interoperation.....	11
113	4 XML Digital Signature and XML Encryption.....	13
114	4.1 XML Signature Algorithms.....	13
115	4.2 XML Encryption Algorithms.....	13
116	5 Use of SSL 3.0 or TLS 1.0.....	14
117	5.1 SAML SOAP and URI Binding .....	14
118	5.2 Web SSO Profiles of SAML .....	14
119	6 References.....	15
120		

---

# 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 [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 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]

- 162 • SAML context class schema for Telephony [SAMLAC-Tele]
- 163 • SAML context class schema for Telephony (“Nomadic”) [SAMLAC-TNom]
- 164 • SAML context class schema for Telephony (Personalized) [SAMLAC-TPers]
- 165 • SAML context class schema for Telephony (Authenticated) [SAMLAC-TAuthn]
- 166 • SAML context class schema for Secure Remote Password [SAMLAC-SRP]
- 167 • SAML context class schema for SSL/TLS Certificate-Based Client Authentication [SAMLAC-
- 168 SSL]
- 169 • SAML context class schema for Time Sync Token [SAMLAC-TST]
- 170 • Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML)
- 171 V2.0 [SAMLSec]
- 172 • Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAMLGloss]

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

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

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

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

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

## 191 1.2 Notation

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

195  
196 *...they MUST only be used where it is actually required for interoperation or to limit behavior*  
197 *which has potential for causing harm (e.g., limiting retransmissions)...*

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

201

## 2 SAML V2.0 Profiles and Possible Implementations

202 The following table enumerates all of the profiles defined by the SAML profiles specification [SAMLProf].  
 203 For each profile, the message protocol flows (defined in the assertions and protocols specification  
 204 [SAMLCore]) found within the profile are also described. For each message flow, a list of relevant bindings  
 205 (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
<a href="#">[E28]Artifact Resolution</a>	<ArtifactResolve>, <ArtifactResponse>	SOAP
Authentication Query	<AuthNQuery>, <Response>	SOAP

Profile	Message Flows	Binding
<a href="#">Attribute Query</a>	<a href="#">&lt;AttributeQuery&gt;</a> , <a href="#">&lt;Response&gt;</a>	SOAP
<a href="#">Authorization Decision Query</a>	<a href="#">&lt;AuthzDecisionQuery&gt;</a> , <a href="#">&lt;Response&gt;</a>	SOAP
<a href="#">Assertion Query/Request</a>	<a href="#">Artifact resolution:</a> <a href="#">&lt;ArtifactResolve&gt;</a> , <a href="#">&lt;ArtifactResponse&gt;</a>  <a href="#">Authentication query:</a> <a href="#">&lt;AuthnQuery&gt;</a> , <a href="#">&lt;Response&gt;</a>  <a href="#">Attribute query:</a> <a href="#">&lt;AttributeQuery&gt;</a> , <a href="#">&lt;Response&gt;</a>  <a href="#">Authorization decision query:</a> <a href="#">&lt;AuthzDecisionQuery&gt;</a> , <a href="#">&lt;Response&gt;</a>	SOAP
Request for Assertion by Identifier	<a href="#">&lt;AssertionIDRequest&gt;</a> , <a href="#">&lt;Response&gt;</a>	SOAP
Name Identifier Mapping	<a href="#">&lt;NameIDMappingRequest&gt;</a> , <a href="#">&lt;NameIDMappingResponse&gt;</a>	SOAP
<a href="#">[E28]SAML URI binding</a>	<a href="#">GET, HTTP Response</a>	HTTP
UUID attribute profile		
DCE PAC attribute profile		
X.500 attribute profile		
XACML attribute profile		
<a href="#">[E28]Metadata</a>	<a href="#">Consumption</a>	
	<a href="#">Exchange</a>	

---

## 207 **3 Conformance**

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

### 209 **3.1 Operational Modes**

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

- 212 • IdP – Identity Provider
- 213 • IdP Lite – Identity Provider Lite
- 214 • SP – Service Provider
- 215 • SP Lite – Service Provider Lite
- 216 • ECP – Enhanced Client/Proxy
- 217 • SAML Attribute Authority
- 218 • SAML Authorization Decision Authority
- 219 • SAML Authentication Authority
- 220 • SAML Requester

### 221 **3.2 Feature Matrix**

222 The following matrices identify unique sets of conformance requirements by means of a triple taken from  
223 Table 1 with the form: profile, message(s), binding The message component is not always included when  
224 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 <a href="#">[E11](IdP-initiated)</a> , HTTP redirect ( <del>IdP-initiated</del> )	MUST	MUST NOT	MUST	MUST NOT	N/A
Name Identifier Management ( <del>IdP-initiated</del> ), SOAP ( <del>IdP-initiated</del> )	MUST	MUST NOT	OPTIONAL	MUST NOT	N/A
Name Identifier Management <a href="#">(SP-initiated)</a> , HTTP redirect-	MUST	MUST NOT	MUST	MUST NOT	N/A
Name Identifier Management <a href="#">(SP-initiated)</a> , SOAP ( <del>SP-initiated</del> )	MUST	MUST NOT	OPTIONAL	MUST NOT	N/A
Single Logout (IdP-initiated) <sub>2</sub> — HTTP redirect	MUST	MUST	MUST	MUST	N/A
Single Logout (IdP-initiated) <sub>2</sub> — SOAP	MUST	OPTIONAL	MUST	OPTIONAL	N/A
Single Logout (SP-initiated) <sub>2</sub> — HTTP redirect	MUST	MUST	MUST	MUST	N/A
Single Logout (SP-initiated) <sub>2</sub> — SOAP	MUST	OPTIONAL	MUST	OPTIONAL	N/A
Identity Provider Discovery (cookie)	MUST	MUST	OPTIONAL	OPTIONAL	N/A
<a href="#">[E29]Request for Assertion by Identifier</a>	<a href="#">OPTIONAL</a>	<a href="#">N/A</a>	<a href="#">N/A</a>	<a href="#">N/A</a>	<a href="#">N/A</a>
<a href="#">SAML URI Binding</a>	<a href="#">OPTIONAL</a>	<a href="#">N/A</a>	<a href="#">N/A</a>	<a href="#">N/A</a>	<a href="#">N/A</a>
<a href="#">[E25]Metadata Structures</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">N/A</a>
<a href="#">Metadata Interoperation</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">N/A</a>

226

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

230

**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

231

232 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	<a href="#">[E42]OPTIONAL/N/A</a>	<a href="#">OPTIONAL/N/A</a>	OPTIONAL
Attribute Query, SOAP	<a href="#">OPTIONAL/N/A</a>	MUST	<a href="#">OPTIONAL/N/A</a>	OPTIONAL
Authorization Decision Query, SOAP	<a href="#">OPTIONAL/N/A</a>	<a href="#">OPTIONAL/N/A</a>	MUST	OPTIONAL
Request for Assertion by Identifier, SOAP	MUST	MUST	MUST	OPTIONAL
SAML URI Binding	MUST	MUST	MUST	OPTIONAL
<a href="#">[E25]Metadata Structures</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>
<a href="#">Metadata Interoperation</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>	<a href="#">OPTIONAL</a>

233

### 234 3.3 Implementation of SAML-Defined Identifiers

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

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

238 Conforming SAML implementations MUST permit the use of all identifier constants described in Sections  
239 8.2 and 8.3 when producing and consuming SAML messages. SAML message producers MUST be able  
240 to create messages and SAML message consumers MUST be able to process messages with any of the  
241 constants defined in these sections.

242 Sections 8.3.7 (persistent name identifiers) and 8.3.8 (transient name identifiers) define normative  
243 processing rules for the producer of such identifiers. All normative processing rules in Sections 8.3.7 and  
244 8.3.8 MUST be supported by conforming implementations. The remaining identifiers in Sections 8.2 and  
245 8.3 specify no normative processing rules. Hence, generation and consumption of these identifiers is  
246 meaningful only when the generating and consuming parties have externally-defined agreement on the  
247 semantic interpretation of the identifiers.

248 **Note:** In this context, "process" means that the implementation must successfully parse  
249 and handle the identifier without failing or returning an error. How the implementation

250 deals with the identifier once it is processed at this level is out of scope for this  
251 specification.

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

### 257 **3.4 Implementation of Encrypted Elements**

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

- 261 • <saml:EncryptedID>
- 262 • <saml:EncryptedAssertion>
- 263 • <saml:EncryptedAttribute>

### 264 **3.5 Security Models for SOAP and URI Bindings**

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

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

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

### 275 **3.6 [E25]Metadata Structures**

276 [Implementations claiming conformance to SAML V2.0 may declare each operational mode's conformance](#)  
277 [to SAML V2.0 Metadata \[SAMLMeta\] through election of the Metadata Structures option.](#)

278 [With respect to each operational mode, such conformance entails the following:](#)

- 279 • [Implementing SAML metadata according to the extensible SAML V2.0 Metadata format in all cases](#)  
280 [where an interoperating peer has the option, as stated in SAML V2.0 specifications, of depending on](#)  
281 [the existence of SAML V2.0 Metadata. Electing the Metadata Structures option has the effect of](#)  
282 [requiring that such metadata be available to the interoperating peer. The Metadata Interoperation](#)  
283 [feature, described below, provides a means of satisfying this requirement.](#)
- 284 • [Referencing, consuming, and adhering to the SAML metadata, according to \[SAMLMeta\], of an](#)  
285 [interoperating peer when the known metadata relevant to that peer and the particular operation, and](#)  
286 [the current exchange, has expired or is no longer valid in cache, provided the metadata is available](#)  
287 [and is not prohibited by policy or the particular operation and that specific exchange.](#)

### 288 **3.7 Metadata Interoperation**

289 [Election of the Metadata Interoperation option requires the implementation to offer, in addition to any other](#)  
290 [mechanism, the well-known location publication and resolution mechanism described in the SAML](#)  
291 [metadata specification \[SAMLMeta\].](#)

---

## 292 4 XML Digital Signature and XML Encryption

293 SAML V2.0 uses XML Signature [XMLSig] to implement XML signing and encryption functionality for  
294 integrity, and source authentication. SAML V2.0 uses XML Encryption [XMLEnc] to implement  
295 confidentiality, including encrypted identifiers, encrypted assertions, and encrypted attributes. [\[E50\]The](#)  
296 [algorithms listed below as being required for SAML V2.0 conformance are based on the mandated](#)  
297 [algorithms in the W3C recommendations for XML Signature and for XML Encryption, but modified by the](#)  
298 [SSTC to ensure interoperability of conformant SAML implementations. While the SAML-defined set of](#)  
299 [algorithms is a minimal set for conformance, additional algorithms supported by XML Signature and XML](#)  
300 [Encryption MAY be used. Note, however, that the use of non-mandated algorithms may introduce](#)  
301 [interoperability issues if those algorithms are not widely implemented. As additional algorithms become](#)  
302 [mandated for use in XML Signature and XML Encryption, the set required for SAML conformance may be](#)  
303 [extended.](#)

### 304 4.1 XML Signature Algorithms

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

- 307 • Digest: SHA1
- 308 • MAC: HMAC-SHA1
- 309 • XML Canonicalization: CanonicalXML (Without comments),
- 310 • Transform: Enveloped Signature

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

- 313 • Signature: RSAwithSHA1 (recommended in XML Signature but needed for  
314 interoperability)

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

### 317 4.2 XML Encryption Algorithms

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

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

---

## 322 5 Use of SSL 3.0 or TLS 1.0

323 In any SAML V2.0 use of SSL 3.0 [SSL3] or TLS 1.0 [RFC 2246], servers MUST authenticate to clients  
324 using a X.509 v3 certificate. The client MUST establish server identity based on contents of the certificate  
325 (typically through examination of the certificate's subject DN field). [\[E50\]The set of algorithms required for](#)  
326 [SAML V2.0 conformance is equivalent to that defined in SAML V1.0 and SAML V1.1. These mandated](#)  
327 [algorithms were chosen by the SSTC because of their wide implementation support in the industry. While](#)  
328 [the algorithms defined below are the minimal set for SAML conformance, additional algorithms supported](#)  
329 [by SSL 3.0 and TLS 1.0 MAY be used.](#)

### 330 5.1 SAML SOAP and URI Binding

331 TLS-capable implementations MUST implement the TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher  
332 suite and MAY implement the TLS\_RSA\_AES\_128\_CBC\_SHA cipher suite [AES].

333 FIPS TLS-capable implementations MUST implement the corresponding  
334 TLS\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite and MAY implement the corresponding  
335 TLS\_RSA\_FIPS\_AES\_128\_CBC\_SHA cipher suite [AES].

336 SSL-capable implementations MUST implement the SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher  
337 suite.

338 FIPS SSL-capable implementations MUST implement the FIPS cipher suite corresponding to the SSL  
339 SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite.

### 340 5.2 Web SSO Profiles of SAML

341 SSL-capable implementations of the Web SSO profile of SAML MUST implement the  
342 SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite. TLS-capable implementations MUST implement  
343 the TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite.

---

## 6 References

344

- 345 **[AES]** FIPS-197, *Advanced Encryption Standard (AES)*. See <http://www.nist.gov/>.
- 346 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
347 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- 348 **[RFC 2246]** T. Dierks et al. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999.  
349 See <http://www.ietf.org/rfc/rfc2246.txt>.
- 350 **[RFC 2617]** J. Franks et al. *HTTP Authentication: Basic and Digest Access Authentication*.  
351 IETF RFC 2617, June 1999. See <http://www.ietf.org/rfc/rfc2617.txt>.
- 352 **[SAMLAssn-xsd]** S. Cantor et al. SAML assertions schema. OASIS SSTC, March 2005. Document  
353 ID saml-schema-assertion-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)  
354 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 355 **[SAMLAuthnCxt]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup  
356 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-  
357 context-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 358 **[SAMLAC-xsd]** J. Kemp et al. SAML authentication context schema. OASIS SSTC, March 2005.  
359 Document ID saml-schema-authn-context-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)  
360 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 361 **[SAMLACTyp-xsd]** J. Kemp et al. SAML authentication context type declarations schema. OASIS  
362 SSTC, March 2005. Document ID saml-schema-authn-context-types-2.0. See  
363 <http://www.oasis-open.org/committees/security/>.
- 364 **[SAMLAC-IP]** J. Kemp et al. SAML context class schema for Internet Protocol. OASIS SSTC,  
365 March 2005. Document ID saml-schema-authn-context-ip-2.0. See  
366 <http://www.oasis-open.org/committees/security/>.
- 367 **[SAMLAC-IPP]** J. Kemp et al. SAML context class schema for Internet Protocol Password.  
368 OASIS SSTC, March 2005. Document ID saml-schema-authn-context-ippword-  
369 2.0. See <http://www.oasis-open.org/committees/security/>.
- 370 **[SAMLAC-Kerb]** J. Kemp et al. SAML context class schema for Kerberos. OASIS SSTC, March  
371 2005. Document ID saml-schema-authn-context-kerberos-2.0. See  
372 <http://www.oasis-open.org/committees/security/>.
- 373 **[SAMLAC-MOFC]** J. Kemp et al. SAML context class schema for Mobile One Factor Contract.  
374 Document ID saml-schema-authn-context-mobileonefactor-reg-2.0. See OASIS  
375 SSTC, March 2005. <http://www.oasis-open.org/committees/security/>.
- 376 **[SAMLAC-MOFU]** J. Kemp et al. SAML context class schema for Mobile One Factor Unregistered.  
377 Document ID saml-schema-authn-context-mobileonefactor-unreg-2.0. See  
378 OASIS SSTC, March 2005. <http://www.oasis-open.org/committees/security/>.
- 379 **[SAMLAC-MTFC]** J. Kemp et al. SAML context class schema for Mobile Two Factor Contract.  
380 OASIS SSTC, March 2005. Document ID saml-schema-authn-context-  
381 mobiletwofactor-reg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 382 **[SAMLAC-MTFU]** J. Kemp et al. SAML context class schema for Mobile Two Factor Unregistered.  
383 OASIS SSTC, March 2005. Document ID saml-schema-authn-context-  
384 mobiletwofactor-unreg-2.0. See <http://www.oasis-open.org/committees/security/>.
- 385 **[SAMLAC-Pass]** J. Kemp et al. SAML context class schema for Password. OASIS SSTC, March  
386 2005. Document ID saml-schema-authn-context-pword-2.0. See  
387 <http://www.oasis-open.org/committees/security/>.

388	<b>[SAMLAC-PGP]</b>	J. Kemp et al., SAML context class schema for Public Key – PGP. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-pgp-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
389		
390		
391	<b>[SAMLAC-PPT]</b>	J. Kemp et al., SAML context class schema for Password Protected Transport. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-ppt-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
392		
393		
394	<b>[SAMLAC-Prev]</b>	J. Kemp et al., SAML context class schema for Previous Session. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-session-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
395		
396		
397	<b>[SAMLAC-Smart]</b>	J. Kemp et al., SAML context class schema for Smartcard. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-smartcard-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
398		
399		
400	<b>[SAMLAC-SmPKI]</b>	J. Kemp et al., SAML context class schema for Smartcard PKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-smartcardpki-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
401		
402		
403	<b>[SAMLAC-SPKI]</b>	J. Kemp et al., SAML context class schema for Public Key – SPKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-spki-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
404		
405		
406	<b>[SAMLAC-SRP]</b>	J. Kemp et al. SAML context class schema for Secure Remote Password. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-srp-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
407		
408		
409	<b>[SAMLAC-SSL]</b>	J. Kemp et al. SAML context class schema for SSL/TLS Certificate-Based Client Authentication. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-sslcert-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
410		
411		
412	<b>[SAMLAC-SwPKI]</b>	J. Kemp et al. SAML context class schema for Software PKI. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-softwarepki-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
413		
414		
415	<b>[SAMLAC-Tele]</b>	J. Kemp et al. SAML context class schema for Telephony. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
416		
417		
418	<b>[SAMLAC-TNom]</b>	J. Kemp et al. SAML context class schema for Telephony (“Nomadic”). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-nomad-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
419		
420		
421	<b>[SAMLAC-TPers]</b>	J. Kemp et al. SAML context class schema for Telephony (Personalized). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-personal-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
422		
423		
424	<b>[SAMLAC-TAuthn]</b>	J. Kemp et al. SAML context class schema for Telephony (Authenticated). OASIS SSTC, March 2005. Document ID saml-schema-authn-context-auth-telephony-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
425		
426		
427	<b>[SAMLAC-TST]</b>	J. Kemp et al. SAML context class schema for Time Sync Token. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-timesync-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
428		
429		
430	<b>[SAMLAC-X509]</b>	J. Kemp et al. SAML context class schema for Public Key – X.509. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-x509-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
431		
432		
433	<b>[SAMLAC-XSig]</b>	J. Kemp et al. SAML context class schema for Public Key – XML Signature. OASIS SSTC, March 2005. Document ID saml-schema-authn-context-xmlsig-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
434		
435		
436	<b>[SAMLBind]</b>	S. Cantor et al. <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
437		
438		

440	<b>[SAMLCore]</b>	S. Cantor et al. <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-core-2.0-os. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
441		
442		
443	<b>[SAML DCE-xsd]</b>	S. Cantor et al. SAML DCE PAC attribute profile schema. OASIS SSTC, March 2005. Document ID saml-schema-dce-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
444		
445		
446	<b>[SAML ECP-xsd]</b>	S. Cantor et al. SAML ECP profile schema. OASIS SSTC, March 2005. Document ID saml-schema-ecp-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
447		
448		
449	<b>[SAML Gloss]</b>	J. Hodges et al. <i>Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-glossary-2.0-os. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
450		
451		
452	<b>[SAML Meta]</b>	S. Cantor et al. <i>Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
453		
454		
455	<b>[SAML Meta-xsd]</b>	S. Cantor et al. SAML metadata schema. OASIS SSTC, March 2005. Document ID saml-schema-metadata-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
456		
457		
458	<b>[SAML Prof]</b>	S. Cantor et al. <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
459		
460		
461	<b>[SAML Prot-xsd]</b>	S. Cantor et al. SAML protocols schema. OASIS SSTC, March 2005. Document ID saml-schema-protocol-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
462		
463		
464	<b>[SAML Sec]</b>	F. Hirsch et al. <i>Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, March 2005. Document ID saml-sec-consider-2.0-os. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
465		
466		
467		
468	<b>[SAML TechOvw]</b>	J. Hughes et al. <i>Technical Overview for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS SSTC, February 2005. Document ID sstc-saml-tech-overview-2.0-draft-03. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
469		
470		
471	<b>[SAML X500-xsd]</b>	S. Cantor et al. SAML X.500/LDAP attribute profile schema. OASIS SSTC, March 2005. Document ID saml-schema-x500-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
472		
473		
474	<b>[SAML XAC-xsd]</b>	S. Cantor et al. SAML XACML attribute profile schema. OASIS SSTC, March 2005. Document ID saml-schema-xacml-2.0. See <a href="http://www.oasis-open.org/committees/security/">http://www.oasis-open.org/committees/security/</a> .
475		
476		
477	<b>[SSL3]</b>	A. Frier et al. <i>The SSL 3.0 Protocol</i> , Netscape Communications Corp, November 1996.
478		
479	<b>[XML Enc]</b>	Donald Eastlake et al. <i>XML Encryption Syntax and Processing</i> . World Wide Web Consortium Recommendation, December 2002. See <a href="http://www.w3.org/TR/xmlenc-core/">http://www.w3.org/TR/xmlenc-core/</a> .
480		
481		
482	<b>[XML Sig]</b>	Donald Eastlake et al. <i>XML-Signature Syntax and Processing</i> , <a href="#">[E74]Second Edition</a> . World Wide Web Consortium Recommendation, <a href="#">February 2002 June 2008</a> . See <a href="http://www.w3.org/TR/xmlsig-core/">http://www.w3.org/TR/xmlsig-core/</a> .
483		
484		
485		



---

## Appendix A. Acknowledgements

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

- 489 • Conor Cahill, AOL
- 490 • John Hughes, Atos Origin
- 491 • Hal Lockhart, BEA Systems
- 492 • Mike Beach, Boeing
- 493 • Rebekah Metz, Booz Allen Hamilton
- 494 • Rick Randall, Booz Allen Hamilton
- 495 • Ronald Jacobson, Computer Associates
- 496 • Gavenraj Sodhi, Computer Associates
- 497 • Thomas Wisniewski, Entrust
- 498 • Carolina Canales-Valenzuela, Ericsson
- 499 • Dana Kaufman, Forum Systems
- 500 • Irving Reid, Hewlett-Packard
- 501 • Guy Denton, IBM
- 502 • Heather Hinton, IBM
- 503 • Maryann Hondo, IBM
- 504 • Michael McIntosh, IBM
- 505 • Anthony Nadalin, IBM
- 506 • Nick Ragouzis, Individual
- 507 • Scott Cantor, Internet2
- 508 • Bob Morgan, Internet2
- 509 • Peter Davis, Neustar
- 510 • Jeff Hodges, Neustar
- 511 • Frederick Hirsch, Nokia
- 512 • Senthil Sengodan, Nokia
- 513 • Abbie Barbir, Nortel Networks
- 514 • Scott Kiestler, Novell
- 515 • Cameron Morris, Novell
- 516 • Paul Madsen, NTT
- 517 • Steve Anderson, OpenNetwork
- 518 • Ari Kermaier, Oracle
- 519 • Vamsi Motukuru, Oracle
- 520 • Darren Platt, Ping Identity
- 521 • Prateek Mishra, Principal Identity
- 522 • Jim Lien, RSA Security
- 523 • John Linn, RSA Security
- 524 • Rob Philpott, RSA Security
- 525 • Dipak Chopra, SAP
- 526 • Jahan Moreh, Sigaba
- 527 • Bhavna Bhatnagar, Sun Microsystems
- 528 • Eve Maler, Sun Microsystems
- 529 • Ronald Monzillo, Sun Microsystems

- 530 • Emily Xu, Sun Microsystems
- 531 • Greg Whitehead, Trustgenix

532

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

- 535 • Stephen Farrell, Baltimore Technologies
- 536 • David Orchard, BEA Systems
- 537 • Krishna Sankar, Cisco Systems
- 538 • Zahid Ahmed, CommerceOne
- 539 • Tim Alsop, CyberSafe Limited
- 540 • Carlisle Adams, Entrust
- 541 • Tim Moses, Entrust
- 542 • Nigel Edwards, Hewlett-Packard
- 543 • Joe Pato, Hewlett-Packard
- 544 • Bob Blakley, IBM
- 545 • Marlena Erdos, IBM
- 546 • Marc Chanliau, Netegrity
- 547 • Chris McLaren, Netegrity
- 548 • Lynne Rosenthal, NIST
- 549 • Mark Skall, NIST
- 550 • Charles Knouse, Oblix
- 551 • Simon Godik, Overxeer
- 552 • Charles Norwood, SAIC
- 553 • Evan Prodromou, Securant
- 554 • Robert Griffin, RSA Security (former editor)
- 555 • Sai Allarvarpu, Sun Microsystems
- 556 • Gary Ellison, Sun Microsystems
- 557 • Chris Ferris, Sun Microsystems
- 558 • Mike Myers, Traceroute Security
- 559 • Phillip Hallam-Baker, VeriSign (former editor)
- 560 • James Vanderbeek, Vodafone
- 561 • Mark O'Neill, Vordel
- 562 • Tony Palmer, Vordel

563

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

- 566 • Thomas Gross, IBM
- 567 • Birgit Pfitzmann, IBM

568 The editors also would like to gratefully acknowledge Jahan Moreh of Sigaba, who during his tenure on  
569 the SSTC was the primary editor of the errata working document and who made major substantive  
570 contributions to all of the errata materials.

---

## 571 Appendix B. Notices

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

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

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

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

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

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