



# Errata for the OASIS Security Assertion Markup Language (SAML) V2.0

Working Draft 28, 8 May 2006

**Document identifier:**

sstc-saml-errata-2.0-draft-28

**Location:**

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

**Editor:**

Jahan Moreh, Sigaba <[jmoreh@sigaba.com](mailto:jmoreh@sigaba.com)>

**Abstract:**

This document lists the reported errata and potential errata against the OASIS SAML 2.0 Committee Specifications and their status.

**Status:**

This document is work in progress and will be updated to reflect reported errata.

Comments on issues with the SAML specifications are welcome. If you are on the [security-services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org) list for committee members, send comments there. If you are not on that list, subscribe to the [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org) list and send comments there. To subscribe, send an email message to [security-services-comment-request@lists.oasis-open.org](mailto:security-services-comment-request@lists.oasis-open.org) with the word "subscribe" as the body of the message. If you have questions or comments on implementation issues, subscribe to the [saml-dev@lists.oasis-open.org](mailto:saml-dev@lists.oasis-open.org) list and send comments there.

Copyright © 2005 and 2006 The Organization for the Advancement of Structured Information Standards [OASIS]

## 26 Table of Contents

27	1	Introduction .....	4
28	2	Errata .....	4
29	2.1	E1: Incorrect section reference .....	4
30	3	Potential Errata .....	4
31	3.1	PE1: Relay State for HTTP Redirect.....	4
32	3.2	PE2: Metadata clarifications.....	5
33	3.3	PE3: Supported URL Encoding.....	5
34	3.4	PE4: SAML 1.1 Artifacts.....	5
35	3.5	PE5: Rules for NameIDPolicy .....	6
36	3.6	PE6: Encrypted NameID .....	6
37	3.7	PE7: Metadata attributes WantAuthnRequestsSigned and AuthnRequestsSigned .....	7
38	3.8	PE8: SLO and NameID termination .....	8
39	3.9	PE9: Clarification on SP AuthnRequestsSigned and the IdP	
40		WantAuthnRequestsSigned SP metadata flags .....	8
41	3.10	PE10: Logout Request <i>reason</i> Mismatch with Schema.....	8
42	3.11	PE11: Improperly Labeled Feature .....	9
43	3.12	PE12: Clarification on ManageNameIDRequest.....	9
44	3.13	PE13: Inaccurate description of Authorization Decision .....	10
45	3.14	PE14: AllowCreate .....	11
46	3.15	PE15: NameID Policy.....	13
47	3.16	PE16: Inaccurate data in Feature Matrix .....	14
48	3.17	PE17: Authentication Response IssuerName vs. Assertion IssuerName.....	14
49	3.18	PE18: reference to identity provider discovery service in ECP Profile .....	15
50	3.19	PE19: Clarification on Error Processing.....	15
51	3.20	PE20: ECP SSO Profile and Metadata .....	16
52	3.21	PE21: PAOS Version .....	16
53	3.22	PE22: Error in Profile/ECP .....	16
54	3.23	PE23: Metadata for <ArtifactResolutionService>.....	17
55	3.24	PE24: HTTPS in URI Binding.....	17
56	3.25	PE25: Metadata Structures Feature in Conformance .....	17
57	3.26	PE26: Ambiguities around Multiple Assertions and Statements in the SSO Profile .....	19
58	3.27	PE27: Error in ECP Profile .....	21
59	3.28	PE28: Conformance Table 1 .....	21
60	3.29	PE29: Conformance Table 2.....	22
61	3.30	PE30: Considerations for key replacement.....	22
62	3.31	PE31: Various minor errors in Binding.....	22
63	3.32	PE32: Missing section in Profiles .....	23
64	4.3.1	Required Information .....	23
65	3.33	PE33: References to Assertion Request Protocol .....	23

66	3.34 PE34: Section Heading .....	23
67	3.35 PE35: Example in Profiles.....	24
68	3.36 PE36: Clarification on Action Element .....	24
69	3.37 PE37: Clarification in Metadata on Indexed Endpoints.....	25
70	3.38 PE38: Clarification regarding index on <LogoutRequest> .....	25
71	3.39 PE39: Error in SAML profile example .....	26
72	3.40 PE40: Holder of Key.....	26
73	3.41 PE41: EndpointType ResponseLocation clarification in Metadata .....	26
74	3.42 PE42: Conformance Table 4.....	27
75	3.43 PE43: Key location in saml:EncryptedData .....	27
76	3.44 PE44: Constrained Delegation.....	28
77	3.45 PE45: AuthnContext comparison clarifications .....	28
78	3.46 PE46: AudienceRestriction clarifications .....	29
79	3.47 PE47: Clarification on SubjectConfirmation .....	29
80	3.48 PE48: Clarification on encoding for binary values in LDAP profile .....	30
81	3.49 PE49: Clarification on attribute name format .....	31
82	3.50 PE50: Clarification SSL Ciphersuites.....	31
83	3.51 PE51: Schema type of contents of <AttributeValue>.....	32
84	Appendix A. Revision History .....	33
85	Appendix B. Summary of Disposition .....	35
86	Appendix C. Notices .....	37

87

---

## 88 1 Introduction

89 This document lists the reported errata and potential errata against the OASIS SAML 2.0  
90 Committee Specifications and their status.

---

## 91 2 Errata

### 92 2.1 E1: Incorrect section reference

93 First reported by: Rob Philpot, RSA

94 Message: <http://lists.oasis-open.org/archives/security-services/200503/msg00080.html>

95 Document: Core

96

97 **Description:** Line 2660 refers back to section “3.6.3” for Reason codes. This should refer to  
98 section “3.7.3”.

99 **Options:**

100 **Disposition:** During the conference call of March 28 the TC unanimously agreed to make this  
101 correction.

---

## 102 3 Potential Errata

### 103 3.1 PE1: Relay State for HTTP Redirect

104 **First reported by:** Ari Kermaier, Oracle

105 Message: <http://lists.oasis-open.org/archives/security-services/200502/msg00003.html>

106 **Document:** Bindings and Profiles

107 **Description:** Section 3.4.3 (Relay State for HTTP Redirect) lines 551-553 read

108 “Signing is not realistic given the space limitation, but because the value is exposed to third-party  
109 tampering, the entity SHOULD insure that the value has not been tampered with by using a  
110 checksum, a pseudo-random value, or similar means.”

111

112 This language should probably be deleted or modified, as the RelayState parameter \*is\* covered  
113 by the query string signature described in 3.4.4.1 (DEFLATE Encoding).

114

115 The same language is correctly present in 3.5.3 (Relay State for HTTP POST), as no means of  
116 signing the POST form control data is defined.

117

118 **Options:** Replace first paragraph of section 3.4.3 at line 545 with: “RelayState data MAY be  
119 included with a SAML protocol message transmitted with this binding. The value MUST NOT  
120 exceed 80 bytes in length and SHOULD be integrity protected by the entity creating the message,  
121 either via a digital signature (see section [3.4.4.1]) or by some independent means.”

122

123 **Disposition:** During the conference call of April 12 the TC accepted this option.

### 124 **3.2 PE2: Metadata clarifications**

125 First reported by: Scott Cantor, OSU

126 Message: <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

127 **Document:** Bindings and Profiles

128 **Description:** Clarify metadata requirements in the various profiles. For example, it's required by  
129 implication that if you support the Artifact binding for some profile that your role descriptor also  
130 needs an ArtifactResolutionService element, but this isn't stated anywhere.

131 **Options:** In [SAMLBind] replace paragraph in section 3.6.7 at lines 1188-1191 with:

132 "Support for receiving messages using the HTTP Artifact binding SHOULD be reflected by  
133 indicating URL endpoints at which requests and responses for a particular protocol or profile  
134 should be sent. Either a single endpoint or distinct request and response endpoints MAY be  
135 supplied. Support for sending messages using this binding SHOULD be accompanied by one or  
136 more indexed <md:ArtifactResolutionService> endpoints for processing <samlp:ArtifactResolve>  
137 messages."

138

139 **Disposition:** A thorough disposition requires a fairly careful review of Metadata and Profiles so  
140 that the requirements can be documented in various places. This work is deferred to SAML 2.x.  
141 However, during the conference call of April 12 the TC accepted the above text as clarification for  
142 SAML 2.0.

### 143 **3.3 PE3: Supported URL Encoding**

144 First reported by: Scott Cantor, OSU

145 Message: <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

146 Document: Metadata

147 **Description:** Specify the URL encoding supported by an HTTP Redirect binding endpoint.

148 **Options:** This isn't actually an erratum, it's a missing piece that doesn't currently break anything  
149 but could in the future if alternate URL encodings for the Redirect binding emerge (for example a  
150 binary XML representation). We need an extension attribute to indicate non-default encoding  
151 support, it can just be added to our new "2.0 metadata extension schema". This should be moved  
152 to the issues list.

153

154 **Disposition:** During the conference call of April 12 the TC agreed to move this to the issues list.

### 155 **3.4 PE4: SAML 1.1 Artifacts**

156 First reported by: Scott Cantor, OSU

157 Message: <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

158 **Document:** Bindings and Profiles

159 **Description:** Clarifying that SAML 1.1 artifacts have no place or use in SAML 2.0

160 **Options:** In [SAMLBind] add to line 1067:

161 "Although the general artifact structure resembles that used in prior versions of SAML and the  
162 type code of the single format described below does not conflict with previously defined formats,

163 there is explicitly no correspondence between SAML 2.0 artifacts and those found in any previous  
164 specifications, and artifact formats not defined specifically for use with SAML 2.0 MUST NOT  
165 be used with this binding.”

166

167 **Disposition:** During the conference call of April 12 the TC accepted this option.

## 168 **3.5 PE5: Rules for NameIDPolicy**

169 **First reported by:** Brian Campbell, Ping Identity

170 Message: <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

171 **Document:** Binding and Profiles

172 **Description:** A *transient* nameid-format of a <NameIDPolicy> in an <AuthRequest> with  
173 *allowCreate* is meaningless.

174 **Options:** There are two options. Both involve adding text after line 2147 of [SAMLCore].

175

### 176 **1. Strict option:**

177 “Finally, note that since the urn:oasis:names:tc:SAML:2.0:nameid-format:transient Format value  
178 (see Section 8.3.8) implicitly results in a new identifier being created during the handling of most  
179 requests, the AllowCreate attribute MUST be set to true in order for such a value to be returned.”

180

### 181 **2. Optimized option:**

182 “Finally, note that since them urn:oasis:names:tc:SAML:2.0:nameid-format:transient Format value  
183 (see Section 8.3.8) implicitly results in a new identifier being created during the handling of most  
184 requests, the AllowCreate attribute MUST be ignored by the identity provider when such an  
185 identifier is requested or issued.”

186

187 **Disposition:** During the conference call of June 21 the TC agreed that PE14 addresses this  
188 erratum and approved to dispose of this erratum as such.

189

## 190 **3.6 PE6: Encrypted NameID**

191 First reported by: Rob Philpott, RSA

192 Message: Communicated during TC conference call of February 1, 2005.

193 Document: Core

194 **Description:** When using the nameid-format:encrypted type of name identifier in SAML  
195 assertions and protocol messages, it is not possible to communicate the format of the  
196 unencrypted identifier as part of the assertion or message. This concept was derived from Liberty  
197 which only used it for persistent identifiers. Since we also support other formats in SAML 2.0, the  
198 agreement on the unencrypted form (prior to encryption/after decryption) must be done out of  
199 band.

200 **Options:** In [SAMLCore] append to paragraph ending on line 2139:

201 “It is not possible for the service provider to specifically request that a particular kind of identifier  
202 be returned if it asks for encryption. The <md:NameIDFormat> metadata element (see  
203 [SAMLMeta]) or other out-of-band means MAY be used to determine what kind of identifier to  
204 encrypt and return.”

205

206 **Disposition:** During the conference call of April 12 the TC accepted this option.

### 207 **3.7 PE7: Metadata attributes WantAuthnRequestsSigned and** 208 **AuthnRequestsSigned**

209 First reported by: Rob Philpott, RSA

210 Message: <http://lists.oasis-open.org/archives/security-services/200502/msg00017.html>

211 Document: Metadata

212 **Description:** In Metadata, the IDPSSODescriptor has the setting called  
213 "WantAuthnRequestsSigned" and the SPSSODescriptor has the setting called  
214 "AuthnRequestsSigned". But it's ambiguous about "how" this signing is to be done.

215

216 Note that the SP can also define "WantAssertionsSigned", where it means that the SP wants the  
217 IDP to sign the Assertion XML element by including a <ds:Signature> element in the assertion.  
218 That is, I do NOT believe it means that the assertion can also be "signed by inclusion" by putting  
219 it (unsigned) inside a <samlp:Response> element and signing that element. It is the Assertion  
220 XML element itself that is signed. I don't believe the same approach is what folks expect for the  
221 AuthnRequest settings however. I think it is ambiguous and needs to be clarified.

222 At the interop, folks were using a true setting for [Want]AuthnRequestsSigned to mean that the  
223 AuthnRequest message is signed only in the context of the HTTP Redirect Binding where the  
224 total URL with parameters is signed using the mechanism specified in that binding. The  
225 AuthnRequest XML element is NOT expected to contain a <ds:Signature> element. Now I don't  
226 think this interpretation would necessarily be the same if the message was carried in the POST or  
227 Artifact bindings. I assume that in those cases, the XML element itself would be signed and  
228 include the ds:Signature> element.

229 So the interpretation of the setting appears to be dependent on which binding is being used. This  
230 is clearly not the case for the WantAssertionsSigned setting. So we should at least clarify this for  
231 folks. That is, unless folks have a different interpretation of what the settings mean.

232 **Options:** Combine this with PE9 and in [SAMLMetadata] add text before line 710:

233 "The WantAuthnRequestsSigned attribute is intended to indicate to service providers whether or  
234 not they can expect an unsigned <AuthnRequest> message to be accepted by the identity  
235 provider. The identity provider is not obligated to reject unsigned requests nor is a service  
236 provider obligated to sign its requests, although it might reasonably expect an unsigned request  
237 will be rejected. In some cases, a service provider may not even know which identity provider will  
238 ultimately receive and respond to its requests, so the use of this attribute in such a case cannot  
239 be strictly defined.

240 Furthermore, note that the specific method of signing that would be expected is binding  
241 dependent. The HTTP Redirect binding (see [SAMLBind] sec XX) requires the signature be  
242 applied to the URL-encoded value rather than placed within the XML message, while other  
243 bindings generally permit the signature to be within the message in the usual fashion."

244

245 Add text to paragraph at lines 741-742:

246 "A value of false (or omission of this attribute) does not imply that the service provider will never  
247 sign its requests or that a signed request should be considered an error. However, an identity  
248 provider that receives an unsigned <samlp:AuthnRequest> message from a service provider  
249 whose metadata contains this attribute with a value of true MUST return a SAML error response  
250 and MUST not fulfill the request."

251

252 Add text to paragraph at lines 744-747:

253 "Note that an enclosing signature at the SAML binding or protocol layer does not suffice to meet  
254 this requirement, for example signing a <samlp:Response> containing the assertion(s) or a TLS  
255 connection."

256 **Disposition:** During the conference call of September 27 the TC accepted this option.

257

### 258 **3.8 PE8: SLO and NameID termination**

259 **First reported by:** Thomas Wisniewski, Entrust

260 **Message:** <http://lists.oasis-open.org/archives/security-services/200503/msg00034.html>

261 **Document:** Core

262

263 **Description:** Combining SLO with NameID termination, we should clarify whether it's explicitly  
264 not required for the SP to continue to expect or process SLO messages for an active session  
265 following NameID termination. The spec implies pretty strongly that you don't because you can  
266 terminate your local session.

267 **Options:** Replace the last sentence in 2479-2480 (section 3.6.3) with:

268 "In general it SHOULD NOT invalidate any active session(s) of the principal for whom the  
269 relationship has been terminated. If the receiving provider is an identity provider, it SHOULD NOT  
270 invalidate any active session(s) of the principal established with other service providers. A  
271 requesting provider MAY send a <LogoutRequest> message prior to initiating a name  
272 identifier termination by sending a <ManageNameIDRequest> message if that is the requesting  
273 provider's intent (e.g., the name identifier termination is initiated via an administrator who wished  
274 to terminate all user activity). The requesting provider MUST NOT send a <LogoutRequest>  
275 message after the <ManageNameIDRequest> message is sent."

276

277 **Disposition:** During the conference call of April 12 the TC accepted this option.

### 278 **3.9 PE9: Clarification on SP AuthnRequestsSigned and the IdP 279 ~~WantAuthnRequestSigned~~ SP metadata flags**

280 **First reported by:** Greg Whitehead, Trustgenix

281 **Message:** <http://lists.oasis-open.org/archives/security-services/200503/msg00005.html>.

282 **Document:** Metadata

283 **Description:** The lack of a flag at an SP was not intended to imply that an SP would never sign if  
284 it had a reason to, and the IdP flag was not intended to somehow create a conflict. One can't  
285 resolve the situation policy-wise if an SP and IdP disagree about whether to sign, the metadata  
286 simply might reflect this.

287 **Options:** See PE7

288 **Disposition:** During the conference call of April 12 the TC accepted the option of combining this  
289 with PE7 and disposing of it accordingly.

### 290 **3.10 PE10: Logout Request *reason* Mismatch with Schema**

291 **First reported by:** Rob Philpott, RSA

292 Message: <http://lists.oasis-open.org/archives/security-services/200503/msg00080.html>

293 Document: Core

294

295 **Description:** In core line 2540 it says that “Reason” on the LogoutRequest is “in the form of a  
296 URI reference”. However, in the schema, the Reason attribute is type=“string”, not  
297 type=“anyURI”. All of the reason codes that we define (in section 3.7.3 and 3.7.3.2) are actually  
298 URI’s. But, since the schema defines it as a string, the text should be changed to match the  
299 schema.

300 **Options:** Change line 2540 of core as follows: The Reason attribute is specified as a string in the  
301 schema. This specification further restricts the schema by requiring that the Reason attribute  
302 MUST be in the form of a URI reference.

303 **Disposition:** During the conference call of February 14, 2006 the TC accepted the text as stated  
304 here.

### 305 **3.11 PE11: Improperly Labeled Feature**

306 First reported by: Rob Philpott, RSA

307 Message: <http://lists.oasis-open.org/archives/security-services/200503/msg00080.html>

308 **Document:** Conformance

309

310 **Description:** In table 2 of the conformance spec, the feature in the 8<sup>th</sup> row is improperly labeled.  
311 It currently says “Name Identifier Management, HTTP Redirect”. It should say “Name Identifier  
312 Management, HTTP Redirect (SP-initiated)”.

313

314 There are also minor inconsistencies in the labels since the parenthetical (xP-initiated) are listed  
315 with the binding in some, but with the profile in others. I suggest always listing it with the profile  
316 name.

317

318 **Options:** Correct the label as suggested in the description of the erratum above.

319 **Disposition:** During the conference call of June 7 the TC accepted this option.

320

### 321 **3.12 PE12: Clarification on ManageNameIDRequest**

322 **First reported by:** Scott Cantor, OSU/Brian Campbell, Ping Identity

323 **Message:** <http://lists.oasis-open.org/archives/security-services/200504/msg00107.html> and :  
324 <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

325

326 **Document:** Bindings and Profiles

327

328 **Description:** The schema defines the <NewID> element of a <ManageNameIDRequest> as a  
329 string. The implication of that is that a NIM request message from IDP to SP can only be used to  
330 inform the SP of a change in identifier value (not format – format is immutable once established).  
331 There are a few places in the spec where the text implies that the format can be changed.  
332 Additionally, the text about <NewEncryptedID> should be expanded to clarify that the encrypted

333 element is just the encrypted <NewID> element and not a full <NameID> as in the more typical  
334 <EncryptedID> element used elsewhere

335

336 Options:

337 Change the schema to allow format and potentially qualifiers to be changed and make all  
338 necessary cascading changes to the spec.

339 Update the wording in the spec to bring it inline with the schema as is and clarify that only the  
340 value of the identifier can be managed with the Name Identifier Management profile.

341

342 Given the complexity and scope of change involved in option 1 and the consensus that option 2 is  
343 sufficient and not too limiting, text changes consistent with option 2 are proposed below.

344 In Profiles change the text on lines 1320-21 from “Subsequently, the identity provider may wish to  
345 notify the service provider of a change in the format and/or value that it will use to identify the  
346 same principal in the future” to “Subsequently, the identity provider may wish to notify the service  
347 provider of a change in the value that it will use to identify the same principal in the future”

348 In Core change the text on lines 2412-13 from “After establishing a name identifier for a principal,  
349 an identity provider wishing to change the value and/or format of the identifier that it will use when  
350 referring to the principal,...” to “After establishing a name identifier for a principal, an identity  
351 provider wishing to change the value of the identifier that it will use when referring to the  
352 principal,...”

353 In Core add the following text after line 2438, “In either case, if the <NewEncryptedID> is used, its  
354 encrypted content is just a <NewID> element containing only the new value for the identifier  
355 (format and qualifiers cannot be changed once established).”

356

357 **Disposition:** During the conference call of June 7 the TC approved option 2.

### 358 **3.13 PE13: Inaccurate description of Authorization Decision**

359 **First reported by:** Jahan Moreh, Sigaba

360 **Message:** <http://lists.oasis-open.org/archives/security-services/200504/msg0125.html>

361 Document: Core

362

363 **Description:** Core 357-358 currently reads:

364 Authorization Decision: A request to allow the assertion subject to access the specified resource  
365 has been granted or denied.

366

367 It should say:

368 Authorization Decision: A request to allow the assertion subject to access the specified resource  
369 has been granted, denied, or is indeterminate.

370

371 **Options:** Make correction as described above.

372 **Disposition:** During the conference call of June 7 the TC approved the change as proposed  
373 here.

374 **3.14 PE14: AllowCreate**

375 **First reported by:** Brian Campbell, Ping Identity

376 **Message:** <http://lists.oasis-open.org/archives/security-services/200505/msg00014.html>

377 **Document:** Core and Profiles

378

379 **Description:** AllowCreate needs more clear definition.

380 **Author's note:** this may be the same as/related to PE5

381

382 **Options:** Make the following corrections

383

384 **In Profiles replace the current text there about AllowCreate with a statement that** “this  
385 profile does not provide additional guidelines for the use of AllowCreate” and reference this text in  
386 core as governing.

387

388 **In Core, replace definition of AllowCreate, lines 2123-2129:**

389 “A Boolean value used to indicate whether the requester grants to the identity provider, in the  
390 course of fulfilling the request, permission to create a new identifier or to associate an existing  
391 identifier representing the principal with the relying party. Defaults to “false” if not present or the  
392 entire element is omitted.”

393

394 **In Core, replace lines 2143-2147 and insert new text at line 2130 (beginning of the explanatory  
395 text):**

396

397 “The AllowCreate attribute may be used by some deployments to influence the creation of state  
398 maintained by the identity provider pertaining to the use of a name identifier (or any other  
399 persistent, uniquely identifying attributes) by a particular relying party, for purposes such as  
400 dynamic identifier or attribute creation, tracking of consent, subsequent use of the Name Identifier  
401 Management protocol (see section XX), or other related purposes.

402

403 When “false”, the requester tries to constrain the identity provider to issue an assertion only if  
404 such state has already been established or is not deemed applicable by the identity provider to  
405 the use of an identifier. Thus, this does not prevent the identity provider from assuming such  
406 information exists outside the context of this specific request (for example, establishing it in  
407 advance for a large number of principals).

408

409 A value of “true” permits the identity provider to take any related actions it wishes to fulfill the  
410 request, subject to any other constraints imposed by the request and policy (the IsPassive  
411 attribute, for example).

412

413 Generally, requesters cannot assume specific behavior from identity providers regarding the initial  
414 creation or association of identifiers on their behalf, as these are details left to implementations or  
415 deployments. Absent specific profiles governing the use of this attribute, it might be used as a hint  
416 to identity providers about the requester’s intention to store the identifier or link it to a local value.

417 A value of “false” might be used to indicate that the requester is not prepared or able to do so and  
418 save the identity provider wasted effort.

419

420 Requesters that do not make specific use of this attribute SHOULD generally set it to “true” to  
421 maximize interoperability.

422

423 The use of the AllowCreate attribute MUST NOT be used and SHOULD be ignored in conjunction  
424 with requests for or assertions issued with name identifiers  
425 with a Format of urn:oasis:names:tc:SAML:2.0:nameid-format:transient (they preclude any such  
426 state in and of themselves).”

427

428 **In Core, change lines 2419-2420 to:**

429 “This protocol MUST NOT be used in conjunction with the  
430 urn:oasis:names:tc:SAML:2.0:nameidformat:transient <NameID> Format.”

431

432 **In Core, replace lines 2475-2479 with:**

433

434 “If the <Terminate> element is included in the request, the requesting provider is indicating that  
435 (in the case of a service provider) it will no longer accept assertions from the identity provider or  
436 (in the case of an identity provider) it will no longer issue assertions to the service provider about  
437 the principal.

438

439 If the receiving provider is maintaining state associated with the name identifier, such as the value  
440 of the identifier itself (in the case of a pair-wise identifier), an SPProvidedID value, the sender’s  
441 consent to the identifier’s creation/use, etc., then the receiver can perform any maintenance with  
442 the knowledge that the relationship represented by the name identifier has been terminated.

443

444 Any subsequent operations performed by the receiver on behalf of the sender regarding the  
445 principal (for example, a subsequent <AuthnRequest>) SHOULD be carried out in a manner  
446 consistent with the absence of any previous state.

447

448 Termination is potentially the cleanup step for any state management behavior triggered by the  
449 use of the AllowCreate attribute in the Authentication Request protocol (see section XX).

450 Deployments that do not make use of that attribute are likely to avoid the use of the <Terminate>  
451 element or would treat it as a purely advisory matter.

452

453 Note that in most cases (a notable exception being the rules surrounding the SPProvidedID  
454 attribute), there are no requirements on either identity providers or service providers regarding the  
455 creation or use of persistent state. Therefore, no explicit behavior is mandated when the  
456 <Terminate> element is received. However, if persistent state is present pertaining to the use of  
457 an identifier (such as if an SPProvidedID attribute was attached), the <Terminate> element  
458 provides a clear indication that this state SHOULD be deleted (or marked as obsolete in some  
459 fashion).”

460

461 **Disposition:** During the conference call of June 21 the TC approved the change as proposed  
462 here.

### 463 **3.15 PE15: NameID Policy**

464 **First reported by:** Thomas Wisniewski, Entrust

465 Message: <http://lists.oasis-open.org/archives/security-services/200506/maillist.html> - 00030

466 **Document:** Core

467

468 **Description:** The returned assertion subject's NameID format and/or SPNameQualifier may be  
469 different from the ones suggested in the authentication request's NameIDPolicy. I.e., the spec  
470 does not explicitly forbid these from being different (which it should).

471

472 **Options:** Insert the following text between lines 2139 and 2140 in core

473 When a Format defined in Section 8.3.7 is used other than

474 urn:oasis:names:TC:SAML:2.0:nameid-format:unspecified or

475 urn:oasis:names:TC:SAML:2.0:nameid-format:encrypted, then if the identity provider returns any  
476 assertions:

- 477 • the Format value of the <NameID> within the <Subject> of any <Assertion> MUST be  
478 identical to the Format value supplied in the <NameIDPolicy>, and

- 479       • if SPNameQualifier is not omitted in <NameIDPolicy>, the SPNameQualifier value of the  
480       <NameID> within the <Subject> of any <Assertion> **MUST** be identical to the  
481       SPNameQualifier value supplied in the <NameIDPolicy>.”

482       **Disposition:** During the conference call of June 7 the TC approved to make the addition as  
483       stated here.

### 484       **3.16 PE16: Inaccurate data in Feature Matrix**

485       **First reported by:** Eric Tiffany, Liberty Alliance

486       **Message:** <http://lists.oasis-open.org/archives/security-services-comment/200506/msg00000.html>

487       **Document:** Conformance

488

489       **Description:** The Feature Matrix (Table 2), last row, lists Identity Provider Discovery as N/A in  
490       the ECP column. However, the Profiles spec (line 725) notes that “The ECP MAY use the SAML  
491       identity provider discovery profile” to determine the IdP.”

492

493       **Options:** Change the cell to say OPTIONAL instead of N/A

494       **Disposition:** During the conference call of June 21 the TC approved to make no changes to the  
495       conformance document. A new erratum will be proposed to correct the Profile document to  
496       address this issue (see PE18).

### 497       **3.17 PE17: Authentication Response IssuerName vs. Assertion 498       IssuerName**

499       **First reported by:** Thomas Wisniewski, Entrust

500       **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200506/msg00072.html>

501       **Document:** Profiles

502

503       **Description:** Profiles document says issuer (for an AuthnRequest Response) MAY be omitted.

504       “the <Issuer> element **MUST** be present and **MUST** contain the unique identifier of the” The

505       main reason is that Issuer should be a **MUST** in the SSO Response protocol.

506       **Options:** Change lines 541-543 of profiles to:

507       If the <Response> message is signed or if an enclosed assertion is encrypted, then the <Issuer>

508       element **MUST** be present. Otherwise it **MAY** be omitted. If present it **MUST** contain the unique

509       identifier of the issuing identity provider; the Format attribute **MUST** be omitted or have a value of

510       urn:oasis:names:tc:SAML:2.0:nameid-format:entity.”

511

512       **Disposition:** During the conference call of July 5 the TC approved to make the changes as  
513       stated here.

514 **3.18 PE18: reference to identity provider discovery service in**  
515 **ECP Profile**

516 **First reported by:** Prateek Mishra, Principal Identity

517 **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00000.html>

518 **Document:** Profiles

519 **Description:** The ECP does not directly interact with the identity provider discovery service, it  
520 may act as an intermediary for an IdP or SP that plan to utilize the service. Current text gives the  
521 impression that it is a direct participant in the identity provider discovery service. Instead, the  
522 main issue is that it should not impede service interactions with an SP or IdP.

523 **Options:** Delete lines 725 and 726 from saml-profiles-2.0-os, starting at "The ECP MAY use...".

524 **Disposition:** During the conference call of July 19 the TC approved to make the changes as  
525 stated here.

526 **3.19 PE19: Clarification on Error Processing**

527 **First reported by:** Connor P. Cahill, AOL

528 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00008.html>

529 **Document:** Bindings

530

531 **Description:** Clarification on error processing

532

533 **Options:** The section numbers and line numbers are all from "saml-bindings-2.0-os.pdf"

534

535 Section 3.2.2.1, lines 310-317:

- 536
- 537 • Change the first sentence to read:
    - 538 ○ The SAML responder SHOULD return a SOAP message containing either a  
539 SAML response element in the body or a SOAP fault.
  - 540 • Delete the 3rd sentence (If a SAML responder cannot, for some reason, process....).  
541 SOAP defines when a SOAP fault is required and SAML goes into detail about what we  
542 should return when in section 3.2.3.3 "Error Reporting".
  - 543 • Change the 4th sentence to soften the "MUST NOT" and make it a "SHOULD NOT" as  
544 there can be sufficient security through obscurity reasons to do so in some cases.
  - 545 • Add a new sentence at the end of the paragraph noting that details about error handling  
are covered in section 3.2.3.3 "Error Reporting" or something to that effect.

546 Section 3.2.3.3, lines 370-383: Change the MUST on line 378 to a SHOULD.

547 **Disposition:** During the conference call of August 2 the TC approved the changes as stated  
548 here.

## 549 **3.20 PE20: ECP SSO Profile and Metadata**

550 **First reported by:** Thomas Wisniewski, Entrust

551 **Message:** <http://lists.oasis-open.org/archives/security-services/200506/msg00106.html>

552 **Document:** Profiles

553 **Description:** There is no metadata consideration in ECP profile

554 **Options:** In SAML Profiles specification add new section 4.2.6 as follows:

555 The rules specified in the browser SSO profile in Section 4.1.6 apply here as well. Specifically,  
556 the indexed endpoint element <md:AssertionConsumerService> with a binding of  
557 urn:oasis:names:tc:SAML:2.0:bindings:PAOS, MAY be used to describe the supported binding  
558 and location(s) to which an identity provider may send responses to a service provider using this  
559 profile. And, the endpoint <md:SingleSignOnService> with a binding  
560 of urn:oasis:names:tc:SAML:2.0:bindings:SOAP, MAY be used to describe the supported  
561 binding and location(s) to which an service provider may send requests to an identity provider  
562 using this profile

563

564 **Disposition:** During the conference call of July 19 the TC approved to make the changes as  
565 stated here.

566

## 567 **3.21 PE21: PAOS Version**

568 **First reported by:** Thomas Wisniewski, Entrust

569 **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00028.html>

570 **Document:** Bindings

571 **Description:** It's unclear what the word minimum implies in the line "... PAOS version  
572 with "urn:liberty:paos:2003-08" at a minimum."

573 **Options:** Strike the words "at a minimum"

574 **Disposition:** During the conference call of July 19 the TC approved to make the changes as  
575 stated here.

## 576 **3.22 PE22: Error in Profile/ECP**

577 **First reported by:** Rob Philpott, RSA Security

578 **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00040.html>

579 **Document:** Profiles

580 **Description:** Line 907 of Profiles says the responseConsumerURL must be the same as the  
581 "AssertionServiceConsumerURL" in an <AuthnRequest> message. The attribute's name should  
582 be "AssertionConsumerServiceURL".

583 **Options:** Make changes as specified.

584 **Disposition:** During the conference call of August 2 the TC approved the changes as stated  
585 here.

### 586 **3.23 PE23: Metadata for <ArtifactResolutionService>**

587 **First reported by:** Nick Ragouzis, Enosis Group

588 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00036.html>

589 **Document:** Profiles

590 **Description:** The text is not as clear as it should be. In Section 4.1.6 (Web Browser SSO Profile),  
591 at Line 639 change “MUST” to “SHOULD”. Also, add the following text:

592 If the request or response message is delivered using the HTTP Artifact binding, the artifact  
593 issuer SHOULD provide at least one <md:ArtifactResolutionService> endpoint element in its  
594 metadata.

595 **Options:** Accept changes as suggested here.

596 **Disposition:** During the call on 2/28 the TC moved to close with no resolution

### 597 **3.24 PE24: HTTPS in URI Binding**

598 **First reported by:** Nick Ragouzis, Enosis Group

599 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00037.html>

600 **Document:** Bindings

601 **Description:** Section 3.7, starting at line 1349 the text states:

602 “Like SOAP, URI resolution can occur over multiple underlying transports. This binding has  
603 transport-independent aspects, but also calls out the use of HTTP with SSL3.0 [SSL3] or TLS 1.0  
604 [RFC2246] as REQUIRED (mandatory to implement)”

605 **Options:** Replace the current text with the following:

606 “Like SOAP, URI resolution can occur over multiple underlying transports. This binding has  
607 protocol-independent aspects, but also calls out as mandatory the implementation of HTTP  
608 URIs.”

609 **Disposition:** During the conference call of August 2 the TC approved the changes as stated  
610 here.

611

### 612 **3.25 PE25: Metadata Structures Feature in Conformance**

613 **First reported by:** Nick Ragouzis, Enosis Group

614 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00038.html>

615 **Document:** Conformance

616 **Description:** Conformance document does not specify any requirements with respect to  
617 metadata.

618

619 Change to Table 2: Feature Matrix

620

621 IdP IdPLite SP SPLite ECP

622 FEATURE

623 Metadata Structures OPT OPT OPT OPT N/A

624 Metadata Interoperation OPT OPT OPT OPT N/A

625

626

627 Change to Table 4: SAML Authority and Requester Matrix

628

629 AuthnAuth AttribAuth AuthZDcsnAuth Requester FEATURE

630 Metadata Structures OPT OPT OPT OPT

631 Metadata Interoperation OPT OPT OPT OPT

632

633

634 New sub-sections to Section 3 (Conformance):

635

636

637 3.6 Metadata Structures

638 Implementations claiming conformance to SAMLv2.0 may declare each operational mode's

639 conformance to SAMLv2.0 Metadata [SAMLMeta] through election of the Metadata Structures

640 option.

641

642 With respect to each operational mode, such conformance entails the following:

643

644 \* Implementing SAML metadata according to the extensible SAMLv2.0 Metadata format in all  
645 cases where an interoperating peer has the option, as stated in SAMLv2.0 specifications, of  
646 depending on the existence of SAMLv2.0 Metadata. Electing the Metadata Structures option has  
647 the effect of requiring such metadata be available to the interoperating peer. The Metadata  
648 Interoperation feature, described below, provides a means of satisfying this requirement.

649

650 \* Referencing, consuming, and adherence to the SAML metadata, according to [SAMLMeta], of  
651 an interoperating peer when the known metadata relevant to that peer and the particular  
652 operation, and the current exchange, has expired or is no longer valid in cache, provided the

653 metadata is available and is not prohibited by policy or the particular operation and that specific  
654 exchange.

655

656

657 3.7 Metadata Interoperation

658 Election of the Metadata Interoperation option requires the implementation offer, in addition to  
659 any other mechanism, the well-known location publication and resolution mechanism described in  
660 SAML metadata [SAMLMeta].

661

662 **Options:** Make changes as suggested here

663 **Disposition:** During the TC conference call on 9/27 the TC accepted the changes as suggested  
664 here.

## 665 3.26 PE26: Ambiguities around Multiple Assertions and 666 Statements in the SSO Profile

667 **First reported by:** Scott Cantor, OSU

668 **Message:** <http://lists.oasis-open.org/archives/security-services/200508/msg00056.html>

669 **Document:** Profiles

670 **Description:** SSO Profile need clarifications.

671

672 Section 4.1.4.2, <Response> Usage, replace the list at lines 541-572, with the following list:

- 673 • If the response is unsigned, the <Issuer> element MAY be omitted, but if present (or if the  
674 response is signed) it MUST contain the unique identifier of the issuing identity provider;  
675 the Format attribute MUST be omitted or have a value of  
676 urn:oasis:names:tc:SAML:2.0:nameid-format:entity
- 677 • It MUST contain at least one <Assertion>. Each assertion's <Issuer> element MUST  
678 contain the unique identifier of the responding identity provider; the Format attribute  
679 MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity.  
680 Note that this profile assumes a single responding identity provider, and all assertions in  
681 a response MUST be issued by the same entity.
- 682 • If multiple assertions are included, then each assertion's <Subject> element MUST refer  
683 to the same principal. It is allowable for the content of the <Subject> elements to differ  
684 (e.g. using different <NameID> or alternative <SubjectConfirmation> elements).
- 685 • Any assertion issued for consumption using this profile MUST contain a <Subject>  
686 element with at least one <SubjectConfirmation> element containing a Method of  
687 urn:oasis:names:tc:SAML:2.0:cm:bearer. Such an assertion is termed a bearer assertion.  
688 Bearer assertions MAY contain additional <SubjectConfirmation> elements.
- 689 • Assertions without a bearer <SubjectConfirmation> MAY also be included; processing of  
690 additional assertions or <SubjectConfirmation> elements is outside the scope of this  
691 profile.
- 692 • At least one bearer <SubjectConfirmation> element MUST contain a  
693 <SubjectConfirmationData> element that itself MUST contain a Recipient attribute  
694 containing the service provider's assertion consumer service URL and a NotOnOrAfter

- 695 attribute that limits the window during which the assertion can be delivered. It MAY also  
 696 contain an Address attribute limiting the client address from which the assertion can be  
 697 delivered. It MUST NOT contain a NotBefore attribute. If the containing message is in  
 698 response to an <AuthnRequest>, then the InResponseTo attribute MUST match the  
 699 request's ID.
- 700 • The set of one or more bearer assertions MUST contain at least one <AuthnStatement>  
 701 that reflects the authentication of the principal to the identity provider. Multiple  
 702 <AuthnStatement> elements MAY be included, but the semantics of multiple statements  
 703 is not defined by this profile.
  - 704 • If the identity provider supports the Single Logout profile, defined in Section 4.4, any  
 705 authentication statements MUST include a SessionIndex attribute to enable per-session  
 706 logout requests by the service provider
  - 707 • Other statements MAY be included in the bearer assertion(s) at the discretion of the  
 708 identity provider. In particular, <AttributeStatement> elements MAY be included. The  
 709 <AuthnRequest> MAY contain an AttributeConsumingServiceIndex XML attribute  
 710 referencing information about desired or required attributes in [SAMLMeta]. The identity  
 711 provider MAY ignore this, or send other attributes at its discretion.
  - 712 • Each bearer assertion MUST contain an <AudienceRestriction> including the service  
 713 provider's unique identifier as an <Audience>
  - 714 • Other conditions (and other <Audience> elements) MAY be included as requested by the  
 715 service provider or at the discretion of the identity provider. (Of course, all such  
 716 conditions MUST be understood by and accepted by the service provider in order for the  
 717 assertion to be considered valid.
  - 718 • The identity provider is NOT obligated to honor the requested set of <Conditions> in the  
 719 <AuthnRequest>, if any.

720

721 In Section 4.1.4.3, <Response> Message Processing Rules:

- 722 • Line 576, change "any bearer" to "the bearer"
- 723 • Line 578, change "any bearer" to "the bearer"
- 724 • Line 583, change to: "Verify that any assertions relied upon are valid in other respects.  
 725 Note that while multiple bearer <SubjectConfirmation> elements may be present, the  
 726 successful evaluation of a single such element in accordance with this profile is sufficient  
 727 to confirm an assertion. However, each assertion, if more than one is present, MUST be  
 728 evaluated independently."
- 729 • Line 584, change "any bearer" to "the bearer"
- 730 • Append to paragraph ending on line 591: "Note that if multiple <AuthnStatement>  
 731 elements are present, the SessionNotOnOrAfter value closest to the present time  
 732 SHOULD be honored."

733

734 Section 4.1.4.5, POST-Specific Processing Rules:

- 735 • Replace lines 600-601 with: "If the HTTP POST binding is used to deliver the  
 736 <Response>, each assertion MUST be protected by a digital signature. This can be  
 737 accomplished by signing each individual <Assertion> element or by signing the  
 738 <Response> element."

739 **Options:**

740 **Disposition:** During the conference call of August 30 the TC approved the changes as stated  
741 here.

742

### 743 **3.27 PE27: Error in ECP Profile**

744 **First reported by:** Scott Cantor, OSU

745 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00001.html>

746 **Document:** Profiles

747

748 **Description:** Profiles, line 947, the ECP RelayState header definition refers to step 5 as the one  
749 in which the response is issued to the SP. It should be step 7.

750

751 **Options:**

752

753 **Disposition:** During the conference call of September 13 the TC approved the changes as  
754 stated here

### 755 **3.28 PE28: Conformance Table 1**

756 **First reported by:** Rob Philpott, RSA Security

757 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

758 **Document:** Conformance

759

760 **Description:** The first column is labeled "Profile", yet several of the entries are technically not  
761 "profiles". The same applies to the section title and the paragraph above the table.

762

763 **Options:** Column 1

764

765 Combine Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query  
766 entries into a single entry labeled:

767

768 Assertion Query/Request

769 Column 2

770

771 Label each set of message flows with relevant protocol description:

772 Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query

773

774 Column 3

775

776 No change

777

778

779 (2) Remove the following rows from the table:

780

781 SAML URI binding

782 Metadata

783

784 **Disposition:** During the conference call of September 27 the TC approved the changes as  
785 stated here

786

### 787 **3.29 PE29: Conformance Table 2**

788 **First reported by:** Rob Philpott, RSA Security

789 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

790 **Document:** Conformance

791

792 **Description:** The table is missing feature rows for performing a “Request for Assertion by  
793 Identifier” over SOAP and for “SAML URI Binding”. These features are clearly permissible for  
794 IDP’s, since the IDPSSODescriptor includes an element for zero or more  
795 <AssertionIDRequestService> elements. .

796

797 **Options:** Add two rows table 2; row #1 is labeled Request for Assertion Identifier; row #2 is  
798 labeled SAML URI binding; both are optional for IdP row and N/A for all the rest.

799

800 **Disposition:** During the conference call of September 27 the TC as stated here.

801

### 802 **3.30 PE30: Considerations for key replacement**

803 **First reported by:** Rob Philpott, RSA Security

804 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

805 **Document:** Core

806

807 **Description:** Line 3110 states: “optionally one or more encrypted keys...”

808

809 **Options:** Replace “optionally one or more” with “zero or more”.

810

811 **Disposition:** During the conference call of September 13 the TC approved the changes as  
812 stated here

### 813 **3.31 PE31: Various minor errors in Binding**

814 **First reported by:** Rob Philpott, RSA Security

815 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

816 **Document:** Bindings

817

818 **Description:**

- 819 1. Line 511: “security at the SOAP message layer is recommended.” It should be capitalized  
820 as in “RECOMMENDED”.
- 821 2. Line 785: “If no such value is included with a SAML request message” – “value” is  
822 ambiguous. It’s referring to the RelayState parameter, which itself is a name/value pair.  
823 This should be changed to “If no RelayState parameter is included...”
- 824 3. Line 1136: “using a direct SAML binding”. There is no definition for what a “direct” SAML  
825 binding is. Other documents have referred to the SOAP binding as a “synchronous”  
826 binding.

827 4. Line 1397: "Note that use of wildcards is not allowed on such ID queries". This should be  
828 changed to: "Note that the URI syntax does not support the use of wildcards in such  
829 queries."

830 **Options:**  
831

832 **Disposition:** During the conference call of September 13 the TC approved the changes for items  
833 2 and 3. During the conference call of September 27 the TC approved the changes for items 1  
834 and 4.

### 835 **3.32 PE32: Missing section in Profiles**

836 **First reported by:** Rob Philpott, RSA Security

837 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

838 **Document:** Profiles

839  
840 **Description:** Section 4.3. This profile is missing a subsection for "Required Information", which is  
841 present in all other profiles.  
842

843 **Options:** Beginning at line 1092, insert the following text:

#### 844 **4.3.1 Required Information**

845 **Identification:** urn:oasis:names:tc:SAML:2.0:profiles:SSO:idp-discovery

846 **Contact information:** [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org)

847 **Description:** Given below.

848 **Updates:** None.

849  
850

851 **Disposition:** During the conference call of December 5 the TC approved the changes.

### 852 **3.33 PE33: References to Assertion Request Protocol**

853 **First reported by:** Rob Philpott, RSA Security

854 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

855 **Document:** Metadata

856  
857 **Description:** Lines 700, 871, and 904 state: "profile of the Assertion Request protocol defined in  
858 [SAMLProf]". References to "Assertion Request" should be changed to "Assertion  
859 Query/Request".

860  
861 **Options:**  
862

863 **Disposition:** During the conference call of September 13 the TC approved the changes.

864

### 865 **3.34 PE34: Section Heading**

866 **First reported by:** Rob Philpott, RSA Security

867 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

868 **Document:** Metadata

869

870 **Description:** Line 809: the section 2.4.4.2 should be indented so that it is 2.4.4.1.1 since  
871 <RequestedAttribute> is part of the <AttributeConsumingService> defined in section 2.4.4.1.

872 .

873

874 **Options:**

875

876 **Disposition:** During the conference call of September 13 the TC approved the change.

### 877 **3.35 PE35: Example in Profiles**

878 **First reported by:** Rob Philpott, RSA Security

879 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00023.html> and

880 <http://www.oasis-open.org/archives/security-services/200602/msg00008.html>

881 **Document:** Profiles

882

883 **Description:** The example on page 29 line 964 uses a ResponseConsumerURL of [http://identity-](http://identity-service.example.com/abc)  
884 [service.example.com/abc](http://identity-service.example.com/abc). Since this value must be an AssertionConsumerService at the SP and  
885 must match (according to the rules in 4.2.4.4) the value of the responseConsumerURL, the  
886 example would result in an error condition.

887

888 **Options:** Change the value of the responseConsumerURL in the example on page 29 line 964 to  
889 [https://ServiceProvider.example.com/ecp\\_assertion\\_consumer](https://ServiceProvider.example.com/ecp_assertion_consumer).

890 Change the sentence on page 27 lines 906-908 to: "This value MUST be the same as the  
891 AssertionServiceConsumerURL (or the URL referenced in metadata) conveyed in the  
892 <AuthnRequest> and SHOULD NOT be a relative URL."

893

894 **Disposition:** During the conference call of February 28 TC approved the change as stated here.

895

896

### 897 **3.36 PE36: Clarification on Action Element**

898 **First reported by:** Emily Xu, Sun Microsystems

899 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00053.html>

900 **Document:** Core

901

902 **Description:**

903 In section 2.7.4.2 of core spec, Namespace is marked as "Optional". It says: "If this element is  
904 absent, the namespace urn:oasis:names:tx:SAML:1.0:action:rwdc-negation specified in Section  
905 8.1.2 is in effect." But in the following schema definition, attribute Namespace is marked as  
906 required:

907 <attribute name="Namespace" type="anyURI" use="required"/>

908  
909 A clarification is needed to resolve this apparent conflict.  
910  
911 **Options:** In line 1359 change "Optional" to "Required" and strike the sentence starting at line  
912 1361-1363 ("If this element is absent....")  
913  
914 **Disposition:** During the conference call of October 25 the TC approved the change.

### 915 **3.37 PE37: Clarification in Metadata on Indexed Endpoints**

916 **First reported by:** Rob Philpot, RSA Security

917 **Message:** <http://lists.oasis-open.org/archives/security-services/200510/msg00025.html>

918 **Document:** Metadata

919  
920 **Description:** Metadata line 272 says "In any such sequence of like endpoints based on this type,  
921 the default...". It is a bit ambiguous what "of like endpoints" means. Are two endpoints alike if  
922 they are of the same binding type (e.g. SOAP)? Or are they alike because they are assigned to  
923 the same service endpoint.  
924

925 **Options:** Modify Metadata, line 272 as follows:  
926 "In any such sequence of indexed endpoints that share a common element name and  
927 namespace (i.e. all instances of <md:AssertionConsumerService> within a role), the default  
928 endpoint is..."  
929

930 **Disposition:** During the conference call of November 22 the TC approved the changes as stated  
931 here

### 932 **3.38 PE38: Clarification regarding index on <LogoutRequest>**

933 **First reported by:** Conor P. Cahill, AOL

934 **Message:** <http://lists.oasis-open.org/archives/security-services/200511/msg00000.html>

935 **Document:** Core, Profiles

936  
937 **Description:** The language surrounding session index on the <LogoutRequest> (line 2546) is  
938 unclear.  
939

940 **Options:** The following two changes are suggested:

941 1. Change Core, line 2546 as follows:

942 The index of the session between the principal identified by the <saml:BaseID>,  
943 <saml:NameID>, or <saml:EncryptedID> element, and the session authority. This must  
944 correlate to the SessionIndex attribute, if any, in the <saml:AuthnStatement> of the assertion  
945 used to establish the session that is being terminated."

946 2. Change Profiles, line 1302-1304 to:

947 "If the requester is a session participant, it MUST include at least one <SessionIndex>  
948 element in the request. (Note that the session participant always receives a SessionIndex  
949 attribute in the <saml:AuthnStatement> elements that it receives to initiate the session, per  
950 section 4.1.4.2 of the Web Browser SSO Profile.) If the requester is a session authority (or  
951 acting on its behalf), then it MAY omit any such elements to indicate the termination of all of  
952 the principal's applicable sessions."

953

954 **Disposition:** During the conference call of November 22 the TC approved the changes as stated  
955 here

### 956 **3.39 PE39: Error in SAML profile example**

957 **First reported by:** Greg Whitehead, HP

958 **Message:** <http://www.oasis-open.org/archives/security-services/200601/msg00015.html>

959 **Document:** Profiles

960

961 **Description** In section 8.5.6 of the SAML 2.0 profiles doc the Idaprof:Encoding="LDAP"  
962 attribute should be AttributeValue not Attribute, according to section 8.2.4 of the spec.

963

964 **Options:**

965

966 **Disposition:** During the conference call of 1/17/2006 the TC approved the clarification as stated  
967 here.

### 968 **3.40 PE40: Holder of Key**

969 **First reported by:** Prateek Mishra, Oracle

970 **Message:** <http://www.oasis-open.org/archives/security-services/200601/msg00027.html>

971 **Document:** Core

972

973 **Description** HoK described a key that required proof of possession by a attesting entity vs. being  
974 held by the subject, Appropriate text does appear in lines 781-783 of saml2-core. However,  
975 lines 335-337 of saml2-profiles reads:  
976 "As described in [XMLSig], each <ds:KeyInfo> element holds a key or information that enables  
977 an application to obtain a key. The holder of a specified key is considered to be the subject of the  
978 assertion by the asserting party"

979

980 The last sentence should be replaced by:

981 "The holder of a specified key is considered to be an acceptable attesting entity for the assertion  
982 by the asserting party"

983

984 **Options:**

985

986 **Disposition:** During the conference call of February 28th the TC approved the change as stated  
987 here.

988

### 989 **3.41 PE41: EndpointType ResponseLocation clarification in** 990 **Metadata**

991 **First reported by:** Eric Tiffany, Project Liberty

992 **Message:** <http://www.oasis-open.org/archives/security-services/200601/msg00034.html>

993 **Document:** Metadata

994

995 **Description** Implementer interpreted the metadata spec to mean that ResponseLocation should  
996 only be omitted for the SOAP binding, and that the ResponseLocation be specified in metadata  
997 for other bindings.

998 **Options:** Proposed text to resolve this:

999

1000 At line 238 in Metadata we have now:

1001 "The ResponseLocation attribute is used to enable different endpoints to be specified for  
1002 receiving request and response messages associated with a protocol or profile, not as a means  
1003 of load-balancing or redundancy (multiple elements of this type can be included for this purpose).  
1004 When a role contains an element of this type pertaining to a protocol or profile for which only a  
1005 single type of message (request or response) is applicable, then the ResponseLocation attribute  
1006 is unused.

1007

1008 The proposal is to add the following:

1009 "If the ResponseLocation attribute is omitted, any response messages associated with a protocol  
1010 or profile may be assumed to be handled at the URI indicated by the Location attribute."

1011

1012 **Disposition:** During the conference call of 1/31/06 TC voted to approve changes as stated here.

1013

### 1014 **3.42 PE42: Conformance Table 4**

1015 **First reported by:** Thomas Wisniewski, Entrust

1016 **Message:** <http://lists.oasis-open.org/archives/security-services/200601/msg00041.html>

1017 **Document:** Conformance

1018

1019 **Description:** Table 4 has a cell for SAML <x> Authority responding to an <y> Query. That is, an  
1020 Attribute Authority responding to an Authentication or Authorization Decision Query. This doesn't  
1021 seem to make sense as authorities should respond to their respective queries. So the OPTIONAL  
1022 items under the authorities should be N/A."

1023

1024 **Options:** Change the reference from "OPTIONAL" to "N/A" under the columns SAML  
1025 Authentication Authority, SAML Attribute Authority, and SAML Authorization Decision Authority in  
1026 Table 4: SAML Authority and Requester Matrix.

1027

1028 **Disposition:** During the conference call of 1/31/06 TC voted to approve changes as stated here.

1029

### 1030 **3.43 PE43: Key location in saml:EncryptedData**

1031 **First reported by:** Heather Hinton, IBM

1032 **Message:**

1033 **Document:** Core

1034

1035 **Description:** The specification in core does not properly follow XML Encryption standards with  
1036 respect to key location.

1037

1038 **Options:**

1039

1040 **Disposition:**

### 1041 **3.44 PE44: Constrained Delegation**

1042 **First reported by:** Place holder for possible erratum. Scott will provide text as necessary.

1043 **Message:**

1044 **Document:**

1045

1046 **Description:**

1047

1048 **Options:**

1049

1050 **Disposition:** Deactivated. Rolled into PE47.

### 1051 **3.45 PE45: AuthnContext comparison clarifications**

1052 **First reported by:** Scott Cantor, OSU

1053 **Message:** <http://www.oasis-open.org/archives/security-services/200602/msg00024.html>

1054 **Document:** Core

1055

1056 **Description:** In section 3.3.2.2.1 contexts are not necessarily a fully ordered set. This should be  
1057 noted to aid in the interpretation of the comparison types.

1058

1059 **Options:**

1060 **Replace the paragraph at 1815-1819 with:**

1061

1062 Either a set of class references or a set of declaration references can be used. If ordering is  
1063 relevant to the evaluation of the request, then the set of supplied elements MUST be evaluated  
1064 as an ordered set, where the first element is the most preferred authentication context class or  
1065 declaration. For example, ordering is significant when using this element in an  
1066 <AuthnRequest> message but not in an <AuthnQuery> message.

1067

1068 If none of the specified classes or declarations can be satisfied in accordance with the rules  
1069 below, then the responder MUST return a <Response> message with a second-level  
1070 <StatusCode> of urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext."

1071

1072 **Change current lines 1825-1827 to:**

1073

1074 If Comparison is set to "better", then the resulting authentication context in the authentication  
1075 statement MUST be stronger (as deemed by the responder) than one of the authentication  
1076 contexts specified."

1077

1078 **Disposition:** During the conference call of 3/28/06 TC voted to approve changes as stated here

### 1079 **3.46 PE46: AudienceRestriction clarifications**

1080 **First reported by:** Connor P. Cahill, Intel

1081 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00001.html>

1082 **Document:** Core

1083

1084 **Description:** On lines 922-925 in the core specification for 2.0, the sentence states:

1085 The effect of this requirement and the preceding definition is that within a given condition, the  
1086 audiences form a disjunction (an "OR") while multiple conditions form a conjunction (an "AND")

1087

1088

1089 **Options:** Clarify by modifying these lines to read as follows:

1090 The effect of this requirement and the preceding definition is that within a given  
1091 <AudienceRestriction, the <Audience>s form a disjunction (an "OR") while multiple  
1092 <AudienceRestrictions> form a conjunction (an "AND").

1093

1094

1095 **Disposition:**

1096

### 1097 **3.47 PE47: Clarification on SubjectConfirmation**

1098 **First reported by:** Scott Cantor, OSU

1099 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00008.html>

1100 **Document:** Core and profiles

1101

1102 **Description**

1103 The language on Subject Confirmation element and the intent of the embedded secondary  
1104 identifier requires clarification.

1105

1106

1107 **Options:**

1108 **Insert the following at line 698 of core**

1109

1110 If the <SubjectConfirmation> element in an assertion subject contains an identifier the issuer  
1111 authorizes the attesting entity to wield the assertion on behalf of that subject. A relying party MAY  
1112 apply additional constraints on the use of such an assertion at its discretion, based upon the  
1113 identities of both the subject and the attesting entity.

1114

1115 If an assertion is issued for use by an entity other than the subject, then that entity SHOULD be  
1116 identified in the <SubjectConfirmation> element."

1117

1118 **Replace lines 335-337 in Profiles with:**

1119

1120 As described in [XMLSig], each <ds:KeyInfo> element holds a key or information that enables an  
1121 application to obtain a key. The holder of one or more of the specified keys is considered to be an  
1122 acceptable attesting entity for the assertion by the asserting party.

1123

1124 **Insert the following at line 341 of Profiles**

1125

1126 "If the keys contained in the <SubjectConfirmationData> element belong to an entity other than  
1127 the subject, then the asserting party SHOULD identify that entity to the relying party by including  
1128 a SAML identifier representing it in the enclosing <SubjectConfirmation> element.

1129

1130 Note that a given <SubjectConfirmation> element using the Holder of Key method SHOULD  
1131 include keys belonging to only a single attesting entity. If multiple attesting entities are to be  
1132 permitted to use the assertion, then multiple <SubjectConfirmation> elements SHOULD be  
1133 included.

1134

1135 **Replace lines 361-363 in Profiles with:**

1136

1137 The bearer of the assertion is considered to be an acceptable attesting entity for the assertion by  
1138 the asserting party, subject to any optional constraints on confirmation using the attributes that  
1139 MAY be present in the <SubjectConfirmationData> element, as defined by [SAMLCore].

1140 If the intended bearer is known by the asserting party to be an entity other than the subject, then  
1141 the asserting party SHOULD identify that entity to the relying party by including a SAML identifier  
1142 representing it in the enclosing <SubjectConfirmation> element.

1143

1144 If multiple attesting entities are to be permitted to use the assertion based on bearer semantics,  
1145 then multiple <SubjectConfirmation> elements SHOULD be included."

1146

1147 **Disposition:** During the conference call of 3/28/06 TC voted to approve changes as stated here

## 1148 **3.48 PE48: Clarification on encoding for binary values in LDAP** 1149 **profile**

1150 **First reported by:** Greg Whitehead, HP

1151 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00034.html>

1152 **Document:** Profiles

1153

1154 **Description:** In describing the encoding for binary values, the LDAP profile text is ambiguous  
1155 about whether the ASN.1 OCTET STRING wrapper should be included or not.

1156  
1157 **Options:**  
1158 **Change line 1762 of Profiles to:**  
1159  
1160 ... by base64-encoding [RFC2045] the contents of the ASN.1 OCTET STRING-encoded LDAP  
1161 attribute value (not including the ASN.1 OCTET STRING wrapper)  
1162  
1163

1164 **Disposition:**

### 1165 **3.49 PE49: Clarification on attribute name format**

1166 **First reported by:** Greg Whitehead, HP

1167 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00034.html>

1168 **Document:** Core

1169

1170 **Description:** The relationship between an attribute's `NameFormat` and its syntax is not clear.

1171

1172 **Options:**

1173

1174 **Add the following text after line 1217 of core:**

1175 Note that nothing can be inferred from an `Attribute's NameFormat` about the syntax of its  
1176 attribute values. That is, attribute name formats may be re-used across multiple attribute profiles  
1177 and so the use of a particular name format in an `Attribute` cannot be used to infer the use of a  
1178 particular attribute profile. The implication of this is that deployments **MUST** agree out-of-band on  
1179 which attribute profile to use for each attribute name (where an attribute name is identified by a  
1180 unique combination of `Name` and `NameFormat`).

1181

1182 **Disposition:**

### 1183 **3.50 PE50: Clarification SSL Ciphersuites**

1184 **First reported by:** Eric Tiffany, Liberty Alliance

1185 **Message:** <http://www.oasis-open.org/archives/security-services/200604/msg00030.html>

1186 **Document:** Conformance

1187

1188 **Description:** The text needs to be clarified based on ciphersuites that were explicitly called out in  
1189 the text. This is required to make it clear that:

- 1190 1. these are not the only ones that are supported, and  
1191 2. this is not a minimal set that needs to be supported.

1192 **Options:**

1193

1194 Change the following in the Conformance document:

- 1195 1. In the intro of section 4 (XML Digital Signature and XML Encryption) after line 235, add:  
1196 • The algorithms listed below as being required for SAML 2.0 conformance are  
1197 based on the mandated algorithms in the W3C recommendations for XML  
1198 Signature and for XML Encryption, but modified by the SSTC to ensure

1199 interoperability of conformant SAML implementations. While the SAML-defined  
1200 set of algorithms is a minimal set for conformance, additional algorithms  
1201 supported by XML Signature and XML Encryption MAY be used. Note, however,  
1202 that the use of non-mandated algorithms may introduce interoperability issues if  
1203 those algorithms are not widely implemented. As additional algorithms become  
1204 mandated for use in XML Signature and XML Encryption, the set required for  
1205 SAML conformance may be extended. [RSP: not sure about including the last  
1206 sentence... opinions?]

1207 2. In the intro of section 5 (Use of SSL 3.0 and TLS 1.0) after line 257, add:

- 1208 • The set up algorithms required for SAML 2.0 conformance is equivalent to that  
1209 defined in SAML 1.0 and SAML 1.1. These mandated algorithms were chosen by  
1210 the SSTC because of their wide implementation support in the industry. While the  
1211 algorithms defined below are the minimal set for SAML conformance, additional  
1212 algorithms supported by SSL 3.0 and TLS 1.0 MAY be used.  
1213

1214

1215 **Disposition:**

### 1216 **3.51 PE51: Schema type of contents of <AttributeValue>**

1217 **First reported by:** Prateek Mishra, Oracle

1218 **Message:** <http://lists.oasis-open.org/archives/security-services/200605/msg00001.html>

1219 **Document:** Profiles

1220

1221 **Description:** Section 8.1 of SAML 2 Profiles state:

1222 The Basic attribute profile specifies simplified, but non-unique, naming of SAML attributes  
1223 together with attribute values based on the built-in XML Schema data types, eliminating the need  
1224 for extension schemas to validate syntax.

1225

1226 Further in the document, lines (1699-70) it states:

1227 The schema type of the contents of the <AttributeValue> element MUST be drawn from one of  
1228 the types defined in Section 3.3 of [Schema2].

1229

1230 This appears to be in error. Section 3 of [Schema2] defines the "Built-in Datatypes" and Section  
1231 3.3 is one specific sub-section within it (defines "Derived Datatypes"). With the current language  
1232 both "Date" and "anyURI" are excluded; I somehow do not believe this was the original intent.

1233

1234 **Options:**

1235

1236 Replace lines 1699-70 with:

1237 The schema type of the contents of the <AttributeValue> element MUST be drawn from one of  
1238 the types defined in Section 3 of [Schema2].

1239

1240 **Disposition:**

1241

## Appendix A. Revision History

Rev	Date	By Whom	What
Draft-00	2005-01-31	Jahan Moreh	Initial version based on emails to the list
Draft-01	2005-02-14	Jahan Moreh	Removed E5 as it is related to the Technical Overview document, which is work in progress. Relabeled all items as Potential Errata (PE). Added PE4 and PE5. Added E1.
Draft-02	2005-03-27	Jahan Moreh	Moved E1 to PE section. Added E2,E3 and E4. Added PE7
Draft-03	2005-03-29	Jahan Moreh	Rearranged E and PE items. The E items now are those which have been resolved and have proposed text, where required. PE items will be moved to E as they meet these requirements.
Draft-04	2005-04-11	Jahan Moreh	Incorporated proposes text all PEs based on emails to the list:
Draft-05	2005-04-12	Jahan Moreh	Minor corrections to PE5 and PE8. Accepted disposition of all items except PE5, PE7 and PE10. Decided to keep disposed Pes in the PE section (and not move them to the E section)
Draft-06	2005-04-25	Jahan Moreh	Added PE11, PE12 and PE13
Draft-07	2005-05-27	Jahan Moreh	Added PE14
Draft-08	2005-06-03	Jahan Moreh	Added PE15
Draft-09	2005-06-20	Jahan Moreh	Added PE16. Disposed PE11, PE12, PE13, and PE16 and PE17.
Draft 10	2005-07-04	Jahan Moreh	Added PE18
Draft 11	2005-07-18	Jahan Moreh	Disposed PE17, added PE19 and PE20
Draft 12	2005-08-01	Jahan Moreh	Disposed PE18, PE19 and PE20. Added PE21-PE25.
Draft 13	2005-08-15	Jahan Moreh	Closed PE19, PE22, PE24. Added PE26.
Draft 14	2005-08-29	Jahan Moreh	Updated PE26

Rev	Date	By Whom	What
Draft 15	2005-09-12	Jahan Moreh	Closed PE26, added PE27-34
Draft 16	2005-09-26	Jahan Moreh	Added PE35. Closed PE30, PE33 and PE34
Draft 17	2005-10-10	Jahan Moreh	Closed PE7, PE25, PE27-29, PE31, PE35.
Draft 18	2005-10-24	Jahan Moreh	Added PE36
Draft 19	2005-11-07	Jahan Moreh	Closed PE36
Draft 20	2005-11-21	Jahan Moreh	Added PE37 and PE38
Draft 21	2005-12-05	Jahan Moreh	Closed PE37 and PE38. Added text for PE32.
Draft 22	2006-01-30	Jahan Moreh	Added PE39, PE40, PE41, PE42 and 43
Draft 23	2006-02-13	Jahan Moreh	Closed PE39, PE41. Added PE44.
Draft 24	2006-02-27	Jahan Moreh	Closed PE10 and added PE45. Modified description and option for correcting PE 35.
Draft 24	2006-02-27	Jahan Moreh	Closed PE10 and added PE45. Modified description and option for correcting PE 35.
Draft 25	2006-03-27	Jahan Moreh	Closed PE23, PE35, PE40. Added PE46 and PE47.
Draft 26	2006-04-10	Jahan Moreh	Closed PE44, PE45 and PE47. Added PE48.
Draft 27	2006-04-24	Jahan Moreh	Split PE48 into two PEs (48 and 49).
Draft 28	2006-05-05	Jahan Moreh	Added PE50 and PE51

1243

## Appendix B. Summary of Disposition

Erratum #	Status	Document
E1	Closed	Core
PE1	Closed	Binding/Profiles
PE2	Closed	Binding/Profiles
PE3	Closed	Metadata
PE4	Closed	Binding/Profiles
PE5	Closed	Binding/Profiles
PE6	Closed	Core
PE7	Closed	Metadata
PE8	Closed	Binding
PE9	Closed – combined with PE7	Metadata
PE10	Closed	Core
PE11	Closed	Conformance
PE12	Closed	Bindings/Profiles
PE13	Closed	Core
PE14	Closed	Core and Profiles
PE15	Closed	Core
PE16	Closed	Conformance
PE17	Closed	Profiles
PE18	Closed	Profiles
PE19	Closed	Bindings
PE20	Closed	Profiles
PE21	Closed	Bindings
PE22	Closed	Profiles
PE23	Closed	Profiles
PE24	Closed	Bindings
PE25	Closed	Conformance
PE26	Closed	Profiles

PE27	Closed	Profiles
PE28	Closed	Conformance
PE29	Closed	Conformance
PE30	Closed	Core
PE31	Closed	Bindings
PE32	Closed	Profiles
PE33	Closed	Metadata
PE34	Closed	Metadata
PE35	Closed	Profiles
PE36	Closed	Core
PE37	Closed	Metadata
PE38	Closed	Core, Profiles
PE39	Closed	Profiles
PE40	Closed	Core
PE41	Closed	Metadata
PE42	Closed	Conformance
<b>PE43</b>	<b>Active</b>	<b>Core</b>
PE44	Closed	Place holder for Constrained Delegation
PE45	Closed	Core
<b>PE46</b>	<b>Active</b>	<b>Core</b>
PE47	Closed	Core and Profiles
<b>PE48</b>	<b>Active</b>	<b>Profiles</b>
<b>PE49</b>	<b>Active</b>	<b>Core</b>
<b>PE50</b>	<b>Active</b>	<b>Conformance</b>
<b>PE51</b>	<b>Active</b>	<b>Profiles</b>

1245  
1246

---

1247

## Appendix C. Notices

1248 OASIS takes no position regarding the validity or scope of any intellectual property or other rights  
1249 that might be claimed to pertain to the implementation or use of the technology described in this  
1250 document or the extent to which any license under such rights might or might not be available;  
1251 neither does it represent that it has made any effort to identify any such rights. Information on  
1252 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS  
1253 website. Copies of claims of rights made available for publication and any assurances of licenses  
1254 to be made available, or the result of an attempt made to obtain a general license or permission  
1255 for the use of such proprietary rights by implementors or users of this specification, can be  
1256 obtained from the OASIS Executive Director.

1257 OASIS invites any interested party to bring to its attention any copyrights, patents or patent  
1258 applications, or other proprietary rights which may cover technology that may be required to  
1259 implement this specification. Please address the information to the OASIS Executive Director.

1260 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]  
1261 2005. All Rights Reserved.

1262 This document and translations of it may be copied and furnished to others, and derivative works  
1263 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,  
1264 published and distributed, in whole or in part, without restriction of any kind, provided that the  
1265 above copyright notice and this paragraph are included on all such copies and derivative works.  
1266 However, this document itself does not be modified in any way, such as by removing the  
1267 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS  
1268 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual  
1269 Property Rights document must be followed, or as required to translate it into languages other  
1270 than English.

1271 The limited permissions granted above are perpetual and will not be revoked by OASIS or its  
1272 successors or assigns.

1273 This document and the information contained herein is provided on an "AS IS" basis and OASIS  
1274 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO  
1275 ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE  
1276 ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A  
1277 PARTICULAR PURPOSE.