



1

2 Errata for the OASIS SAML 1.1 3 Committee Specifications

4 Working Draft 04, 18 March 2003

5 **Document identifier:**

6 TBD

7 **Location:**

8 <http://www.oasis-open.org/committees/security/docs/>

9 **Editor:**

10 Jahan Moreh, Sigaba <jmoreh@sigaba.com>

11 **Abstract:**

12 This document lists the reported potential errata against the OASIS SAML 1.1 Committee
13 Specifications and their status.

14 **Status:**

15 This document will be updated alongside the SAML Committee Specifications until such
16 time as the specifications are frozen against editorial changes and sent to the OASIS
17 membership for voting.

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

25 Copyright © 2002 and 2003 The Organization for the Advancement of Structured Information
26 Standards [OASIS]

27 Table of Contents

28	1	Introduction.....	3
29	2	Errata.....	3
30	2.1	E1: Section number inconsistencies.....	3
31	2.2	E2: Typo.....	3
32	2.3	E3: Section Formatting.....	3
33	2.4	E4: Font Inconsistencies.....	3
34	2.5	E5: Spelling errors.....	4
35	2.6	E6: Spelling errors.....	4
36	3	Potential Errata.....	4
37	3.1	PE1: HTTPS for inter-site transfer service and artifact transmission.....	5
38	3.2	PE2: clarify the expectations of SubjectConfirmationData.....	5
39	3.3	PE3: Bearer and Holder of Key in POST profile.....	5
40	3.4	PE4: Encoding of URI in “Alternative SAML Artifact Format”.....	5
41	3.5	PE5: Signing Assertions.....	6
42	3.6	PE6: Artifact and corresponding confirmation method.....	6
43	3.7	PE7: Normative Language.....	7
44	3.8	PE8: non-Normative Language.....	7
45	3.9	PE9: Reference to AuthorityKind.....	7
46	3.10	PE10: Guidance on Element <RespondWith>.....	8
47	3.11	PE11: Processing rules for AssertionIDReference.....	8
48	3.12	PE12: Miscellaneous additions and clarifications.....	8
49	3.13	PE13: Miscellaneous additions and clarifications.....	9
50	3.14	PE14: Requestor vs. Requester and glossary definition for Responder.....	9
51	3.15	PE15: Browser POST profile does not explicitly call out encoding.....	9
52		Appendix A. Revision History.....	11
53		Appendix B. Notices.....	12
54			

55 1 Introduction

56 This document lists the reported errata against the OASIS SAML V1.1 release 00 Committee
57 Specifications and their status..

58 2 Errata

59 2.1 E1: Section number inconsistencies

60 **First reported by:** Fredrick Hirsch, Nokia

61 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00000.html>

62 **Document:** Bindings and Profiles

63 **Description:** section numbers for the SOAP over HTTP need to be updated, namely 3.1.3.2 on
64 line [258] for authentication, 3.1.3.3 on line [263] for integrity and 3.1.3.4 on line [267] for
65 confidentiality

66 **Options:**

67 **Disposition:** Accepted for correction during TC meeting on 2/18/03.

68 2.2 E2: Typo

69 **First reported by:** Fredrick Hirsch

70 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00000.html>

71 **Document:** Bindings and Profiles

72 **Description:** There is an extra backslash on line 831.

73 **Options:**

74 **Disposition:** Accepted for correction during TC meeting on 2/18/03.

75

76 2.3 E3: Section Formatting

77 **First reported by:** Rob Philpott

78 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00016.html>

79 **Document:** Bindings and Profiles

80 **Description:** Line 291: The section number is not bolded as are all other section numbers.

81 **Options:**

82 1. Change formatting

83 **Disposition:** Accepted for correction during TC meeting on 2/18/03.

84 2.4 E4: Font Inconsistencies

85 **First reported by:** Rob Philpott

86 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

87 **Document:** Assertions and Protocols
88 **Description:** Lines 722, 726: The font for the “Location” and “Binding” attributes is different from
89 “AuthorityKind” on line 714.
90 **Options:**
91 1. Change formatting of line 714
92 **Disposition:** Accepted for correction during TC meeting on 2/18/03.

93 **2.5 E5: Spelling errors**

94 **First reported by:** Rob Philpott
95 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>
96 **Document:** Assertions and Protocols
97 **Description:** Line 887: interger should be integer
98 **Options:**
99 Correct spelling error
100 **Disposition:** Accepted for correction during TC meeting on 2/18/03.

101 **2.6 E6: Spelling errors**

102 **First reported by:** Prateek Mishra
103 **Message:** <http://lists.oasis-open.org/archives/security-services/200302/msg00022.html>
104 **Document:** Assertions and Protocols
105 **Description:** Line 1441 is in error and should be removed from this list.
106 Lines 1439-1444 state:
107
108 The following elements are intended specifically for use as extension points
109 in an extension schema; their 1439
110 types are set to abstract, so that the use of an xsi:type attribute with
111 these elements is REQUIRED: 1440
112 * <Assertion> 1441
113 * <Condition> 1442
114 * <Statement> 1443
115 * <SubjectStatement> 1444
116
117 An examination of the schema reveals that <Assertion> is of type
118 <AssertionType> which is a concrete type. Thus there is no requirement
119 that an xsi:type attribute must be used with assertions.
120 **Options:**
121 Correct error
122 **Disposition:** Accepted for correction during TC meeting on 2/18/03.
123

124 **3 Potential Errata**

125 .

126 **3.1 PE1: HTTPS for inter-site transfer service and artifact**
127 **transmission**

128 **First reported by:** Fredrick Hirsch, Nokia

129 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00000.html>

130 **Document:** Bindings and Profiles

131 **Description:** Since SSL/TLS is recommended for inter-site transfer and artifact transmission,
132 perhaps https should be shown in the examples at line [443], [483].

133 **Options:**

134 **Disposition:** Agreed to change it at TC meeting 2/18/03

135 **3.2 PE2: clarify the expectations of SubjectConfirmationData**

136 **First reported by:** Fredrick Hirsch

137 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00000.html>

138 **Document:** Bindings and Profiles

139 **Description:** It might be helpful to clarify the expectations of SubjectConfirmationData and
140 ds:KeyInfo usage for the different ConfirmationMethods in this profile. Is it true that only
141 holder-of-key would be expected to have a ds:KeyInfo SubjectConfirmation element (For
142 the assertion subject), and none would have SubjectConfirmationData?

143 **Options:**

- 144 1. Reject. The Holder-of-Key case is not involved in any of the web browser profiles. The
145 Browser/Artifact profile does not require the use of SubjectConfirmationData or
146 ds:KeyInfo.
- 147 2. 2/18/03: Add supplementary text to explain use of <SubjectConfirmationData>

148 **Disposition:**

149 **3.3 PE3: Bearer and Holder of Key in POST profile**

150 **First reported by:** Fredrick Hirsch

151 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00000.html>

152 **Document:** Bindings and Profiles

153 **Description:** Presumably the Bearer method would have a ds:KeyInfo element as part of the
154 SAML response signature, but this is separate from ConfirmationMethod.

155

156 **Options:**

- 157 1. Reject. While there is a requirement that the SAML response message must be signed (694-
158 695) there is no implication that the included assertions contain ds:KeyInfo element
- 159 2. 2/18/03: Add supplementary text to explain use of <SubjectConfirmationData>

160 **Disposition:**

161 **3.4 PE4: Encoding of URI in “Alternative SAML Artifact Format”**

162 **First reported by:** Yuji Sakata and Juergen Kremp

163 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00002.html>

164 **Document:** Bindings and Profiles

165 **Description:** chapter 9 of the Bindings document introduces an alternative format for the
166 Assertion Artifact:

167 TypeCode := 0x0002

168 RemainingArtifact := AssertionHandle SourceLocation

169 AssertionHandle := 20-byte_sequence

170 SourceLocation := URI

171 To create the artifact, Base64 is to be applied to the concatenation of TypeCode and
172 RemainingArtifact. Base64 uses Bytes as input.

173 **Options:**

174 1. Specify UTF-8 as default character set

175 2. ??

176 **Disposition: 2/18/03 – during meeting of TC it was decided to correct this. Prateek to**
177 **propose text changes.**

178 **3.5 PE5: Signing Assertions**

179 **First reported by:** Ronald Monzillo

180 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00003.html>

181 **Document:** Assertions and Protocols

182 **Description:** Section 5, lines [1382-1387] indicate that a SAML assertion MUST be signed. The
183 intent here is to strongly advocate the use of signature when assertions are passing through
184 intermediaries. The use of “MUST” here is inappropriate, this is really only advice for profile
185 developers.

186 **Options:**

187 1. Change the specification to read “MAY”

188 2. Change the specification to read “SHOULD”

189 3. ??

190 **Disposition: 2/18/03 – during meeting of TC it was decided to correct this to “SHOULD”.**

191

192 **3.6 PE6: Artifact and corresponding confirmation method**

193 **First reported by:** Rob Philpott

194 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00016.html>

195 **Document:** Profiles and Bindings

196 **Description:** Section 5.3: Even though it isn’t explicitly stated, I have been assuming that the
197 “...:cm:artifact-01” refers to a type 1 artifact. If so, doesn’t there need to be a corresponding
198 confirmation method identifier for “...:cm:artifact-02”? Is there really a need to distinguish the
199 artifact types (i.e. “just use “...:cm:artifact”)? We should also be explicit as to whether providing
200 the actual artifact in the ConfirmationData is required, optional, or not permitted – Which is it?

201 **Options:**

202 1. Strike artifact-01

203 2. Add confirmation method identifier “...:cm:artifact-02”

204 3. Add a confirmation method ID (artifact) and indicate that either one can be used for 01, 03, or
205 any other future.

206 **Disposition: 2/18/03 – during meeting of TC it was decided to choose option 3**

207

208 **3.7 PE7: Normative Language**

209 **First reported by:** Rob Philpott

210 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

211 **Document:** Assertions and Protocols

212 **Description:** Line 961: change “may” to “MAY”.

213 Line 966: change “success would normally” to “Success MUST”.

214 Line 971: Change “must” to “MUST”.

215 Line 1237: Change subcodes MAY be to “subcodes may be”

216 **Options:**

217 **Disposition: 2/18/03 – during meeting of TC it was decided to choose correct 966. Line 971**
218 **remains as is because it was an example. Line 1237 also remains unchanged.**

219 **3.8 PE8: non-Normative Language**

220 **First reported by:** Rob Philpott

221 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

222 **Document:** Assertions and Protocols

223 **Description:** Line 967: change “to be found therein” to “will be included” .

224 Line 1219: Change “request. Top-most” to “request. The top-most”

225 Line 1417: Change “REQUIRES” to “requires”

226 **Options:**

227 **Disposition: 2/18/03 – during meeting of TC it was decided to choose correct 967 and 1219.**
228 **Keep 1417 as is.**

229 **3.9 PE9: Reference to AuthorityKind**

230 **First reported by:** Rob Philpott

231 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

232 **Document:** Assertions and Protocols

233 **Description:** Lines 969-970: “exactly as for saml:AuthorityKind attribute; see Section 2.4.3.2” –
234 The AuthorityKind section is referring to sampl:Query references not saml:Statement references.
235 Folks read the reference to AuthorityKind and sometime try to figure out a relationship between
236 RespondWith and AuthorityKind, which of course does not exist. The section reference is
237 intended to highlight the use of saml and sampl Qnames. Also, AuthorityKind is an attribute, while
238 RespondWith is an element, so the methods for specifying the values are different. I recommend
239 removing the section reference and simply insert similar text inline.

240 **Options:**

241 **Disposition: 2/18/03 – during meeting of TC it was decided to dispose of this PE as**
242 **suggested. Rob to propose replacement text.**

243 **3.10 PE10: Guidance on Element <RespondWith>**

244 **First reported by:** Rob Philpott

245 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

246 **Document:** Assertions and Protocols

247 **Description:** Should provide better guidance on rationalizing use of RespondWith elements in a
248 query and the associated Query type. I know there's been some discussion on this topic on the
249 list, but I don't think the current text here is very clear. For example, we should be explicit about
250 what happens on an AuthenticationQuery that includes a RespondWith for a
251 saml:AttributeStatement. Another example is when an authority has an existing Web SSO
252 assertion that contains both AuthenticationStatements and an AttributeStatement (e.g. what we
253 used in the Interop). Now if a later AuthenticationQuery arrives for the SAML Subject with a
254 RespondWith of saml:AuthenticationStatement, this Web SSO assertion should NOT be returned
255 according to lines 963-964. So we should be explicit that if an assertion contains multiple
256 statement types, there must be a RespondWith in the query for every statement type in the
257 assertion (assuming at least one RespondWith is specified).

258 **Options:**

259 **Disposition:** 2/18/03 – during meeting of TC it was decided to send an email to the list to
260 discuss this. Jahan will send email to the list starting the discussion.

261

262 **3.11 PE11: Processing rules for AssertionIDReference**

263 **First reported by:** Rob Philpott

264 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

265 **Document:** Assertions and Protocols

266 **Description:** Section 3.2 (Requests) – Section 3.3 (Queries) provides not only definitions of
267 query elements, it also provides processing rules and interpretation info for the Queries. But we
268 don't do that for the <AssertionArtifact> or <AssertionIDReference> request types. Section 3.2.3
269 defines the <AssertionArtifact> element but doesn't say how it is used (of course this is discussed
270 in the Profiles). There is no section describing the RequestType "saml:AssertionIDReference"
271 here since the element is defined in section 2.3.1. When someone asked me why
272 AssertionIDReference wasn't described, I at first thought it was an omission since all of the other
273 request and query types are discussed in 3.2 and 3.3. Then I realized the saml/samlp distinction.
274 But it might be clearer and avoid questions if there was a brief mention of processing rules for
275 AssertionIDReference.

276 **Options:**

277 **Disposition:**

278 **3.12 PE12: Miscellaneous additions and clarifications**

279 **First reported by:** Rob Philpott

280 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

281 **Document:** Assertions and Protocols

282 **Description:**

283 Lines 1061-1065: In addition to subject and authn method matching rules, we should indicate that
284 the assertion processing rules are also impacted by the presence of RespondWith elements in
285 the Query.

286 Section 3.3.4 AttributeQuery – Should also mention the subject-matching rules as described in
287 section 3.3.3
288 Line 1085: “the start of the current document” – In a query, the samlp:Request is the ****current****
289 document, so what does it mean to use a Resource with an empty URI?
290 Section 3.3.5 AuthorizationDecisionQuery – Should also mention the subject-matching rules as
291 described in section 3.3.3

292 **3.13 PE13: Miscellaneous additions and clarifications**

293

294 **First reported by:** Rob Philpott

295 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>

296 **Document:** Assertions and Protocols

297 **Description:**

298 Section 3.4.4 (Responses to <AuthnQuery> and <AttrQuery>) – Don't the saml:Subject matching
299 rules described in this section also apply to <AuthzQuery>? In fact, I assume the rules should
300 apply to all <SubjectQuery> requests, including and extensions. So I think the section should be
301 more general.

302 Section 5.4.2 (C14n) – We should mention the preference for Exclusive C14N and refer to the
303 external Dsig Guidelines document.

304 **3.14 PE14: Requestor vs. Requester and glossary definition for** 305 **Responder**

306 **First reported by:** Rob Philpott

307 **Message:** <http://lists.oasis-open.org/archives/security-services/200302/msg00014.html>

308 **Document:** Assertions and Protocols

309 **Description:** In core, we use both spellings. The only normative use is in the definition of
310 <Status> where it the “requester” spelling is used. I recommend we change all “requestor”
311 spellings to “requester”. If folks want to use the “requestor” spelling, then it would be an issue
312 since it introduces a compatibility issue with the current spec. Note that the glossary uses the
313 “Requester” spelling”. There are about 15 uses of “requestor” in core, although one of them is in
314 the references section pointing to “*The Kerberos Network Authentication Requestor (V5)*” that we
315 wouldn't want to change.

316

317 Also – we need to add a definition for “Responder” to the glossary. We use it in the specs. I'll
318 provide a first shot at it (based on Requester):
319

320 Responder – A *system entity* that utilizes a protocol to respond to a request for services from
321 another system entity. The term “server” for this notion is not used because many system entities
322 simultaneously or serially act as both clients and servers.

323 **Options:**

324 **Disposition:**

325 **3.15 PE15: Browser POST profile does not explicitly call out** 326 **encoding**

327 **First reported by:** Jon Westbrook, Emerson Process Management

328 **Message:** sent to saml-dev list

329 **Document:** Profiles and Bindings

330 **Description:** In step 2 of this profile, the base64 encoding of a SAML response is embedded in a
331 HTML form. In order to do this you must first serialize the SAML response to a sequence of
332 octets, which can then be base64 encoded. What character encoding is supposed to be used to
333 serialize the SAML response to a sequence of octets? [lines 692-694 of the bindings document](#) it
334 appears that we haven't explicitly called out the use of UTF-8. This seems to be standard
335 technique used, for example, in c14n canonicalization.

336 **Options:** Explicitly call-out UTF-8 encoding

337 **Disposition:**

338

Appendix A. Revision History

Rev	Date	By Whom	What
Draft-00	2002-12-10	Jahan Moreh	Initial version based on emails to the list
Draft-01	2003-01-22	Jahan Moreh	Additions from Rob Philpott
Draft-02	2003-02-14	Jahan Moreh	Additions from Prateek Mishra
Draft-03	2003-02-18	Jahan Moreh	Updated based on discussions during SSTC meeting of 2/18/03.
Draft-04	2003-03-18	Jahan Moreh	Updated based on a message from Jon Westbrook and Prateek's response to that message

341 **Appendix B. Notices**

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

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

354 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]
355 2002 and 2003. All Rights Reserved.

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

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

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