



# Errata for the OASIS SAML 1.1 Committee Specifications

Working Draft 02, 14 February 2003

**Document identifier:**

TBD

**Location:**

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

**Editor:**

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

**Abstract:**

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

**Status:**

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

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 © 2002 and 2003 The Organization for the Advancement of Structured Information 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: clarify the expectations of SubjectConfirmationData .....            | 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> .....                             | 7  |
| 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 .....                    | 8  |
| 50 | 3.14 | PE14: Requestor vs. Requester and glossary definition for Responder.....  | 9  |
| 51 |      | Appendix A. Revision History .....  | 10 |
| 52 |      | Appendix B. Notices .....   | 11 |
| 53 |      |   |    |

---

## 54 1 Introduction

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

---

## 57 2 Errata

### 58 2.1 E1: Section number inconsistencies

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

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

61 **Document:** Bindings and Profiles

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

65 **Options:**

66 **Disposition:**

### 67 2.2 E2: Typo

68 **First reported by:** Fredrick Hirsch

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

70 **Document:** Bindings and Profiles

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

72 **Options:**

73 **Disposition:**

### 74 2.3 E3: Section Formatting

75 **First reported by:** Rob Philpott

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

77 **Document:** Bindings and Profiles

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

79 **Options:**

80 1. Change formatting

81 **Disposition:**

### 82 2.4 E4: Font Inconsistencies

83 **First reported by:** Rob Philpott

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

85 **Document:** Assertions and Protocols

86 **Description:** Lines 722, 726: The font for the "Location" and "Binding" attributes is different from  
87 "AuthorityKind" on line 714.

88 **Options:**

89 1. Change formatting of line 714

90 **Disposition:**

## 91 **2.5 E5: Spelling errors**

92 **First reported by:** Rob Philpott

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

94 **Document:** Assertions and Protocols

95 **Description:** Line 887: interger should be integer

96 **Options:**

97 Correct spelling error

98 **Disposition:**

## 99 **2.6 E6: Spelling errors**

100 **First reported by:** Prateek Mishra

101 **Message:** <http://lists.oasis-open.org/archives/security-services/200302/msg00022.html>

102 **Document:** Assertions and Protocols

103 **Description:** Line 1441 is in error and should be removed from this list.

104 Lines 1439-1444 state:

105

106 The following elements are intended specifically for use as extension points

107 in an extension schema; their 1439

108 types are set to abstract, so that the use of an xsi:type attribute with

109 these elements is REQUIRED: 1440

110 \* <Assertion> 1441

111 \* <Condition> 1442

112 \* <Statement> 1443

113 \* <SubjectStatement> 1444

114

115 An examination of the schema reveals that <Assertion> is of type

116 <AssertionType> which is a concrete type. Thus there is no requirement

117 that an xsi:type attribute must be used with assertions.

118 **Options:**

119 Correct error

120 **Disposition:**

121

---

## 122 **3 Potential Errata**

123 .

124 **3.1 PE1: HTTPS for inter-site transfer service and artifact**  
125 **transmission**

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

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

128 **Document:** Bindings and Profiles

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

131 **Options:**

132 **Disposition:**

133 **3.2 PE2: clarify the expectations of SubjectConfirmationData**

134 **First reported by:** Fredrick Hirsch

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

136 **Document:** Bindings and Profiles

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

141 **Options:**

142 1. Reject. The Holder-of-Key case is not involved in any of the web browser profiles. The  
143 Browser/Artifact profile does not require the use of SubjectConfirmationData or  
144 ds:KeyInfo.

145 2. ??

146 **Disposition:**

147 **3.3 PE3: clarify the expectations of SubjectConfirmationData**

148 **First reported by:** Fredrick Hirsch

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

150 **Document:** Bindings and Profiles

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

153

154 **Options:**

155 1. Reject. While there is a requirement that the SAML response message must be signed (694-  
156 695) there is no implication that the included assertions contain ds:KeyInfo element

157 2. ??

158

159 **Disposition:**

160 **3.4 PE4: Encoding of URI in "Alternative SAML Artifact Format"**

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

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

163 **Document:** Bindings and Profiles  
164 **Description:** chapter 9 of the Bindings document introduces an alternative format for the  
165 Assertion Artifact:  
166 TypeCode := 0x0002  
167 RemainingArtifact := AssertionHandle SourceLocation  
168 AssertionHandle := 20-byte\_sequence  
169 SourceLocation := URI  
170 To create the artifact, Base64 is to be applied to the concatenation of TypeCode and  
171 RemainingArtifact. Base64 uses Bytes as input.

172 **Options:**

- 173 1. Specify UTF-8 as default character set
- 174 2. ??

175 **Disposition:**

### 176 **3.5 PE5: Signing Assertions**

177 **First reported by:** Ronald Monzillo

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

179 **Document:** Assertions and Protocols

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

184 **Options:**

- 185 1. Change the specification to read "MAY"
- 186 2. Change the specification to read "SHOULD"
- 187 3. ??

188 **Disposition:**

189

### 190 **3.6 PE6: Artifact and corresponding confirmation method**

191 **First reported by:** Rob Philpott

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

193 **Document:** Assertions and Protocols

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

199 **Options:**

- 200 1. ??

201 **Disposition:**

### 202 **3.7 PE7: Normative Language**

203 **First reported by:** Rob Philpott

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

205 **Document:** Assertions and Protocols

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

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

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

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

210 **Options:**

211 **Disposition:**

### 212 **3.8 PE8: non-Normative Language**

213 **First reported by:** Rob Philpott

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

215 **Document:** Assertions and Protocols

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

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

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

219 **Options:**

220 **Disposition:**

### 221 **3.9 PE9: Reference to AuthorityKind**

222 **First reported by:** Rob Philpott

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

224 **Document:** Assertions and Protocols

225 **Description:** Lines 969-970: "exactly as for saml:AuthorityKind attribute; see Section 2.4.3.2" -  
226 The AuthorityKind section is referring to samlp:Query references not saml:Statement references.  
227 Folks read the reference to AuthorityKind and sometime try to figure out a relationship between  
228 RespondWith and AuthorityKind, which of course does not exist. The section reference is  
229 intended to highlight the use of saml and samlp QNames. Also, AuthorityKind is an attribute,  
230 while RespondWith is an element, so the methods for specifying the values are different. I  
231 recommend removing the section reference and simply insert similar text inline.

232 **Options:**

233 **Disposition:**

### 234 **3.10 PE10: Guidance on Element <RespondWith>**

235 **First reported by:** Rob Philpott

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

237 **Document:** Assertions and Protocols

238 **Description:** Should provide better guidance on rationalizing use of RespondWith elements in a  
239 query and the associated Query type. I know there's been some discussion on this topic on the  
240 list, but I don't think the current text here is very clear. For example, we should be explicit about

241 what happens on an AuthenticationQuery that includes a RespondWith for a  
242 saml:AttributeStatement. Another example is when an authority has an existing Web SSO  
243 assertion that contains both AuthenticationStatements and an AttributeStatement (e.g. what we  
244 used in the Interop). Now if a later AuthenticationQuery arrives for the SAML Subject with a  
245 RespondWith of saml:AuthenticationStatement, this Web SSO assertion should NOT be returned  
246 according to lines 963-964. So we should be explicit that if an assertion contains multiple  
247 statement types, there must be a RespondWith in the query for every statement type in the  
248 assertion (assuming at least one RespondWith is specified).

249 **Options:**

250 **Disposition:**

### 251 **3.11 PE11: Processing rules for AssertionIDReference**

252 **First reported by:** Rob Philpott

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

254 **Document:** Assertions and Protocols

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

265 **Options:**

266 **Disposition:**

### 267 **3.12 PE12: Miscellaneous additions and clarifications**

268 **First reported by:** Rob Philpott

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

270 **Document:** Assertions and Protocols

271 **Description:**

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

275 Section 3.3.4 AttributeQuery - Should also mention the subject-matching rules as described in  
276 section 3.3.3

277 Line 1085: "the start of the current document" - In a query, the sampl:Request is the \*\*current\*\*  
278 document, so what does it mean to use a Resource with an empty URI?

279 Section 3.3.5 AuthorizationDecisionQuery - Should also mention the subject-matching rules as  
280 described in section 3.3.3

### 281 **3.13 PE13: Miscellaneous additions and clarifications**

282

283 **First reported by:** Rob Philpott



284 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>  
285 **Document:** Assertions and Protocols  
286 **Description:**  
287 Section 3.4.4 (Responses to <AuthnQuery> and <AttrQuery>) - Don't the saml:Subject matching  
288 rules described in this section also apply to <AuthzQuery>? In fact, I assume the rules should  
289 apply to all <SubjectQuery> requests, including and extensions. So I think the section should be  
290 more general.  
291 Section 5.4.2 (C14n) - We should mention the preference for Exclusive C14N and refer to the  
292 external DSig Guidelines document.

### 293 **3.14 PE14: Requestor vs. Requester and glossary definition for** 294 **Responder**

295 **First reported by:** Rob Philpott

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

297 **Document:** Assertions and Protocols

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

305  
306 Also - we need to add a definition for "Responder" to the glossary. We use it in the specs. I'll  
307 provide a first shot at it (based on Requester):

308  
309 Responder - A *system entity* that utilizes a protocol to respond to a request for services from  
310 another system entity. The term "server" for this notion is not used because many system entities  
311 simultaneously or serially act as both clients and servers.

312

313

314

315

---

## Appendix A. Revision History

| <b>Rev</b> | <b>Date</b> | <b>By Whom</b> | <b>What</b>                                 |
|------------|-------------|----------------|---|
| 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               |

316

---

317

## Appendix B. Notices

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

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

330 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]  
331 2002 and 2003. All Rights Reserved.

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

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

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