



1

2 **Errata for the OASIS Security**
3 **Assertion Markup Language (SAML)**
4 **V1.1**

5 **Working Draft 11, 2 May 2003**

6 **Document identifier:**

7 sstc-saml-errata-1.1-draft-11

8 **Location:**

9 http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

10 **Editor:**

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

12 **Abstract:**

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

15 **Status:**

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

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

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

28 Table of Contents

29	1	Introduction.....	3
30	2	Errata.....	3
31	2.1	E1: Section number inconsistencies.....	3
32	2.2	E2: Typo.....	3
33	2.3	E3: Section Formatting.....	3
34	2.4	E4: Font Inconsistencies.....	3
35	2.5	E5: Spelling errors.....	4
36	2.6	E6: Spelling errors.....	4
37	2.7	E7: Normative use of MAY NOT.....	4
38	2.8	E8: Extension types for <RespondWith>.....	5
39	2.9	E9: Incorrect identifier for alternative SAML Artifact Format.....	5
40	3	Potential Errata.....	5
41	3.1	PE1: HTTPS for inter-site transfer service and artifact transmission.....	5
42	3.2	PE2: clarify the expectations of SubjectConfirmationData.....	6
43	3.3	PE3: Bearer and Holder of Key in POST profile.....	6
44	3.4	PE4: Encoding of URI in "Alternative SAML Artifact Format".....	6
45	3.5	PE5: Signing Assertions.....	7
46	3.6	PE6: Artifact and corresponding confirmation method.....	7
47	3.7	PE7: Normative Language.....	8
48	3.8	PE8: non-Normative Language.....	8
49	3.9	PE9: Reference to AuthorityKind.....	8
50	3.10	PE10: Guidance on Element <RespondWith>.....	9
51	3.11	PE11: Processing rules for AssertionIDReference.....	9
52	3.12	PE12: Miscellaneous additions and clarifications.....	10
53	3.13	PE13: Miscellaneous additions and clarifications.....	10
54	3.14	PE14: Requestor vs. Requester and glossary definition for Responder.....	10
55	3.15	PE15: Browser POST profile does not explicitly call out encoding.....	11
56	3.16	PE16: Use of QNames in <AuthorityKind> and <RespondWith>.....	12
57	3.17	PE17: Non-normative clarification of status code.....	12
58	3.18	PE18: SAML Versioning.....	13
59	3.19	PE19: Clarification of status code for the case of no assertion.....	13
60	3.20	PE20: Clarification of <ConfirmationData> in Browser/POST.....	13
61		Appendix A. Revision History.....	15
62		Appendix B. Summary of Disposition.....	16
63		Appendix C. Notices.....	17
64			

65 1 Introduction

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

68 2 Errata

69 2.1 E1: Section number inconsistencies

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

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

72 **Document:** Bindings and Profiles

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

76 **Options:** Make corrections as suggested.

77 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
78 01 of SAML 1.1 Bindings and Profiles.

79 2.2 E2: Typo

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

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

82 **Document:** Bindings and Profiles

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

84 **Options:** Make corrections as suggested.

85 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
86 01 of SAML 1.1 Bindings and Profiles.

87 2.3 E3: Section Formatting

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

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

90 **Document:** Bindings and Profiles

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

92 **Options:** Change formatting

93 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
94 01 of SAML 1.1 Bindings and Profiles.

95 2.4 E4: Font Inconsistencies

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

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

98 **Document:** Assertions and Protocols

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

101 **Options:** Change formatting of line 714
102 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
103 **02 of SAML 1.1 Assertions and Protocols.**

104 **2.5 E5: Spelling errors**

105 **First reported by:** Rob Philpott, RSA Security
106 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>
107 **Document:** Assertions and Protocols
108 **Description:** Line 887: integer should be integer
109 **Options:** Correct spelling error
110 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
111 **02 of SAML 1.1 Assertions and Protocols.**

112 **2.6 E6: Spelling errors**

113 **First reported by:** Prateek Mishra, Netegrity
114 **Message:** <http://lists.oasis-open.org/archives/security-services/200302/msg00022.html>
115 **Document:** Assertions and Protocols
116 **Description:** Line 1441 is in error and should be removed from this list.
117 Lines 1439-1444 state:
118
119 The following elements are intended specifically for use as extension points
120 in an extension schema; their 1439
121 types are set to abstract, so that the use of an xsi:type attribute with
122 these elements is REQUIRED: 1440
123 * <Assertion> 1441
124 * <Condition> 1442
125 * <Statement> 1443
126 * <SubjectStatement> 1444
127
128 An examination of the schema reveals that <Assertion> is of type
129 <AssertionType> which is a concrete type. Thus there is no requirement
130 that an xsi:type attribute must be used with assertions.
131 **Options:** Correct error
132 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
133 **02 of SAML 1.1 Assertions and Protocols.**

134 **2.7 E7: Normative use of MAY NOT**

135 **First reported by:** Eve Maler, Sun Microsystems
136 **Message:** <http://lists.oasis-open.org/archives/security-services/200304/msg00024.html>
137 **Document:** Assertions and Protocols
138 **Description:** There are two instances of the phrase "MAY NOT" in the core spec (lines 1050 and
139 1258). This phrase is not actually defined by RFC 2119; I believe what was meant was "MUST
140 NOT". For this reason, and because "may not" is a classic ambiguous phrase in technical
141 documentation ("don't do this", as opposed to "you may or may not do this"), I recommend that
142 we change it to "MUST NOT" in both locations.
143 **Options:** Change lines 1050 and 1258 from MAY NOT to MUST NOT.

144 **Disposition:** Accepted during TC meeting of April 08. Incorporated in Draft 04 of SAML 1.1
145 **Assertions and Protocols.**

146 **2.8 E8: Extension types for <RespondWith>**

147 **First reported by:** Eve Maler, Sun Microsystems

148 **Message:** <http://lists.oasis-open.org/archives/security-services/200304/msg00039.html>

149 **Document:** Assertions and Protocols

150 **Description:** In core 1.0 lines 971-973, it says: "To specify extension types, the <RespondWith>
151 element MUST contain exactly the extension element type as specified in the xsi:type attribute
152 on the corresponding element."

153 There is a tiny bit of ambiguity in the sentence as it stands. The phrase "element type", to XML
154 DTD old-timers, means roughly an element declaration -- it's a model for element instances.
155 With the advent of XML Schema and its OO-inspired design, we now have real "types" to which
156 element declarations are bound. The xsi:type reference makes clear that what's meant is the
157 type name, not the element name, but it threw me off.

158 Given this, we have a seemingly inconsistent situation. When the statement is a native SAML
159 element, the content of <RespondWith> is a qualified element name. But when the statement is
160 a foreign extension element, the qualified type name has to be supplied instead.

161

162 **Options:** Fix the almost-ambiguity in V1.1 by saying "element's type" rather than "element type",
163 and treat this as an editorial correction.

164 **Disposition:** Accepted during TC meeting of April 08, 2003. Incorporated in Draft 03 of
165 **SAML 1.1 Assertions and Protocols.**

166 **2.9 E9: Incorrect identifier for alternative SAML Artifact Format**

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

168 **Message:** <http://lists.oasis-open.org/archives/security-services/200304/msg00217.html>

169 **Document:** Bindings and Profiles

170 **Description:** Line 941, lists the identifier for the alternative SAML Artifact Format as
171 "urn:oasis:names:tc:SAML:1.0:draft-sstc-bindings-model-13:profiles:artifact-02". The urn should
172 be "urn:oasis:names:tc:SAML:1.0:profiles:artifact-02" to be consistent with the type 1 artifact
173 profile.

174 **Options:** Make editorial correction.

175 **Disposition:** Make editorial correction as stated above. Incorporated in Draft 03 of SAML
176 **1.1 Bindings and Profiles.**

177 **3 Potential Errata**

178 **3.1 PE1: HTTPS for inter-site transfer service and artifact** 179 **transmission**

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

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

182 **Document:** Bindings and Profiles

183 **Description:** Since SSL/TLS is recommended for inter-site transfer and artifact transmission,
184 perhaps https should be shown in the examples at line [443], [483].
185 **Options:** Use https in the examples.
186 **Disposition:** Agreed to change it at TC meeting 2/18/03. Incorporated in Draft 01 of SAML
187 **1.1 Bindings and Profiles.**

188 **3.2 PE2: clarify the expectations of SubjectConfirmationData**

189 **First reported by:** Fredrick Hirsch, Nokia
190 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00000.html>
191 **Document:** Bindings and Profiles
192 **Description:** It might be helpful to clarify the expectations of SubjectConfirmationData and
193 ds:KeyInfo usage for the different ConfirmationMethods in this profile. Is it true that only
194 holder-of-key would be expected to have a ds:KeyInfo SubjectConfirmation element (For
195 the assertion subject), and none would have SubjectConfirmationData?
196 **Options:**
197 1. Reject. The Holder-of-Key case is not involved in any of the web browser profiles. The
198 Browser/Artifact profile does not require the use of SubjectConfirmationData or
199 ds:KeyInfo.
200 2. 2/18/03: Add supplementary text to explain use of <SubjectConfirmationData>
201 **Disposition:** April 01 TC meeting: TC voted to choose option 1.

202 **3.3 PE3: Bearer and Holder of Key in POST profile**

203 **First reported by:** Fredrick Hirsch, Nokia
204 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00000.html>
205 **Document:** Bindings and Profiles
206 **Description:** Presumably the Bearer method would have a ds:KeyInfo element as part of the
207 SAML response signature, but this is separate from ConfirmationMethod.
208 **Options:**
209 1. Reject. While there is a requirement that the SAML response message must be signed (694-
210 695) there is no implication that the included assertions contain ds:KeyInfo element
211 2. 2/18/03: Add supplementary text to explain use of <SubjectConfirmationData>
212 **Disposition:** April 01 TC meeting: TC voted to choose option 1.

213 **3.4 PE4: Encoding of URI in “Alternative SAML Artifact Format”**

214 **First reported by:** Yuji Sakata, and Juergen Kremp, SAP
215 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00002.html>
216 **Document:** Bindings and Profiles
217 **Description:** chapter 9 of the Bindings document introduces an alternative format for the
218 Assertion Artifact:
219 TypeCode := 0x0002
220 RemainingArtifact := AssertionHandle SourceLocation
221 AssertionHandle := 20-byte_sequence
222 SourceLocation := URI

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

225 **Options:**

- 226 1. Specify UTF-8 as default character set
- 227 2. Text proposed by Prateek on 18 April 2003: Insert at end of sentence on line 951:
228 The SourceLocation URI is mapped to a sequence of bytes based on use of the UTF-8
229 [RFC2279] encoding. Add to reference list: RFC 2279 UTF-8, a transformation
230 format of ISO 10646.

231 **Disposition: 2/18/03 – during meeting of TC it was decided to correct this. Prateek to**
232 **propose text changes. During TC meeting of April 22, 2003 SSTC accepted text as**
233 **proposed by Prateek (option 2 above). Incorporated in Draft 02 of SAML 1.1 Bindings and**
234 **Profiles.**

235 **3.5 PE5: Signing Assertions**

236 **First reported by:** Ronald Monzillo, Sun Microsystems

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

238 **Document:** Assertions and Protocols

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

243 **Options:**

- 244 1. Change the specification to read “MAY”
- 245 2. Change the specification to read “SHOULD”

246 **Disposition: 2/18/03 – during meeting of TC it was decided to correct this to “SHOULD”.**
247 **Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.**

248 **3.6 PE6: Artifact and corresponding confirmation method**

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

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

251 **Document:** Bindings and Profiles

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

257 **Options:**

- 258 1. Strike artifact-01
- 259 2. Add confirmation method identifier “...:artificat-02”
- 260 3. Add a confirmation method ID (artifact) and indicate that either one can be used for 01, 03, or
261 any other future.

262 **Disposition: 2/18/03 – during meeting of TC it was decided to choose option 3.**
263 **Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.**

264 **4/29/03 – It was decided that to deprecate *artifact-01* and simply use *artifact*. After line 528**
265 **of protocols and bindings add a brief normative note: SAML authorities SHOULD NOT**
266 **include SAML artifact in a Confirmation Data.**

267 **3.7 PE7: Normative Language**

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

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

270 **Document:** Assertions and Protocols

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

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

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

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

275 **Options:**

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

278 **Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.**

279 **3.8 PE8: non-Normative Language**

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

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

282 **Document:** Assertions and Protocols

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

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

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

286 **Options:**

287 **Disposition:** 2/18/03 – during meeting of TC it was decided to choose correct 967 and 1219.

288 **Keep 1417 as is. Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.**

289 **3.9 PE9: Reference to AuthorityKind**

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

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

292 **Document:** Assertions and Protocols

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

300 **Options:**

301 **Disposition:** 2/18/03 – during meeting of TC it was decided to dispose of this PE as
302 **suggested. Rob to propose replacement text. Incorporated in Draft 06 of SAML 1.1**
303 **Assertions and Protocols.**

304 **3.10 PE10: Guidance on Element <RespondWith>**

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

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

307 **Document:** Assertions and Protocols

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

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

321 **Disposition:** In light of the decision to deprecate <RespondWith> it was decided to not
322 make any changes.

323 **3.11 PE11: Processing rules for AssertionIDReference**

324 **First reported by:** Rob Philpott

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

326 **Document:** Assertions and Protocols

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

337 **Options:** Provide additional text to clarify as follows:

338 3.2.2.1 Requests for Assertions by Reference

339 In the context of a <Request> element, the <saml:AssertionIDReference> element is used to
340 request an assertion by means of its ID. See Section 2.3.1 for more information on this element.

341 3.2.2.2 Element <AssertionArtifact>

342 The <AssertionArtifact> element is used to specify the assertion artifact that represents an
343 assertion being requested. Its use is governed by the specific profile of SAML that is being used;
344 see the SAML specification for bindings and profiles [SAMLBind] for more information on the use
345 of assertion artifacts in profiles. The following schema fragment defines the <AssertionArtifact>
346 element: <element name="AssertionArtifact" type="string"/>

347 **Disposition:** Accepted during TC meeting of April 08. Already incorporated in Draft 03 of
348 SAML 1.1 Assertions and Protocols.

349 **3.12 PE12: Miscellaneous additions and clarifications**

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

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

352 **Document:** Assertions and Protocols

353 **Description:**

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

357 2. Section 3.3.4 AttributeQuery – Should also mention the subject-matching rules as described in
358 section 3.3.3

359 3. Line 1085: “the start of the current document” – In a query, the samlp:Request is the
360 ****current**** document, so what does it mean to use a Resource with an empty URI?

361 4. Section 3.3.5 AuthorizationDecisionQuery – Should also mention the subject-matching rules as
362 described in section 3.3.3

363 **Options:** for (1) , (2), (4) add cross reference in the respective sections to clarify. For (3) add text
364 to strongly discourage use of empty URIs.

365 **Disposition: April 01 TC meeting: Eve will make editorial changes. Incorporated in Draft 03**
366 **of SAML 1.1 Assertions and Protocols..**

367 **3.13 PE13: Miscellaneous additions and clarifications**

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

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

370 **Document:** Assertions and Protocols

371 **Description:**

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

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

378 **Options:**

379 **Disposition: April 01 TC meeting:** For (1) see items 1,2, and 4 in PE 12 (Eve will make editorial
380 changes). **Incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.**

381 For (2), Scott to propose text. **Incorporated in Draft 06 of SAML 1.1 Assertions and**
382 **Protocols.**

383 **3.14 PE14: Requestor vs. Requester and glossary definition for** 384 **Responder**

385 **First reported by:** Rob Philpott

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

387 **Document:** Assertions and Protocols

388 **Description:** In core, we use both spellings. The only normative use is in the definition of
389 <Status> where it the “requester” spelling is used. I recommend we change all “requestor”
390 spellings to “requester”. If folks want to use the “requestor” spelling, then it would be an issue
391 since it introduces a compatibility issue with the current spec. Note that the glossary uses the

392 "Requester" spelling". There are about 15 uses of "requestor" in core, although one of them is in
393 the references section pointing to "*The Kerberos Network Authentication Requestor (V5)*" that we
394 wouldn't want to change.

395

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

398

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

402 **Options:**

403 **Disposition: April 01 TC meeting:** Use "Requester" throughout. Add "SAML Requester and
404 SAML Responder". **Incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.**

405 Also look at SOAP definitions for "Requester" and "Responder" and add decide if it is appropriate
406 to add as is or modify as appropriate. **Incorporated in Draft 01 of SAML 1.1 Glossary**

407 **3.15 PE15: Browser POST profile does not explicitly call out** 408 **encoding**

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

410 **Message:** <http://lists.oasis-open.org/archives/security-services/200303/msg00000.html>

411 **Document:** Bindings and Profiles

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

418 **Options:**

419 1. Explicitly call-out UTF-8 encoding

420 2. Reject based on the following reason. On reviewing the XML specification, it turns out
421 that the issue of specifying and determining the character encoding of XML
422 documents has been completely addressed therein. [http://www.w3.org/TR/REC-](http://www.w3.org/TR/REC-xml#charencoding)
423 [xml#charencoding](http://www.w3.org/TR/REC-xml#charencoding). My reading of this text suggests that SAML does not need to take a
424 position on this issue and no additional text is required in the Browser/POST profile.

425 3. Adopt the following text as proposed by Scott: On line 692, replace the current sentence
426 with this text:

427 The notation B64(<response>) stands for the result of applying the Base64 Content-
428 Transfer-Encoding to the response, as defined by RFC 1521, section 5.2, and SHOULD
429 consist of lines of encoded data of up to 76 characters. The first encoded line begins after
430 the opening quote signifying the "value" attribute of the SAMLResponse form element.

431 The character set used to represent the encoded data is determined by the "charset"
432 attribute of the Content-Type of the HTML document containing the form. The character
433 set of the XML document resulting from decoding the data is determined in the normal
434 fashion, and defaults to UTF-8 if no character set is indicated.

435

436 **Disposition: April 08 TC meeting:** Review proposal by Scott. **April 22 TC meeting, adopted**
437 **text by Scott as describe in option 3 above. Incorporated in Draft 02 of SAML 1.1 Bindings**
438 **and Profiles.**

439 **3.16 PE16: Use of QNames in <AuthorityKind> and**
440 **<RespondWith>**

441 **First reported by:** Eve Maler, Sun Microsystems

442 **Message:** <http://lists.oasis-open.org/archives/security-services/200304/msg00040.html>

443 **Document:** Assertions and Protocols

444 **Description:** Near lines 716 (all line references in this message are to core 1.0) for
445 AuthorityKind, and 968 for RespondWith, the text gives an example of a QName in use
446 and unfortunately implies (rather more strongly in the latter case) that the prefix must
447 read "saml" when a natively defined construct is being referenced. But the prefix of a
448 namespaced value is never fixed, and we don't clarify that the appropriate namespace
449 must have been defined in the scope of the relevant element where the QName appears.

450

451 It would be better to say something like this (underscores around new or
452 changed material):

453

454 For AuthorityKind: "For example, an attribute authority would be identified by
455 AuthorityKind="samlp:AttributeQuery", _where there is a namespace declaration in the
456 scope of this attribute that binds the samlp: prefix to the SAML protocol namespace_."

457

458 For RespondWith: "For example, a requestor that wishes to receive assertions containing
459 only attribute statements _would_ [this was a lowercase "must"] specify
460 <RespondWith>saml:AttributeStatement</RespondWith>, _where the prefix is
461 bound to the SAML assertion namespace in a namespace declaration that is
462 in the scope of this element_."

463 **Options:**

464 **Disposition:** Accepted during TC meeting on April 08, 2003. Incorporated in Draft 04 of
465 SAML 1.1 Assertions and Protocols.

466 **3.17 PE17: Non-normative clarification of status code**

467 **First reported by:** Eve Maler, Sun Microsystems

468 **Message:** <http://lists.oasis-open.org/archives/security-services/200304/msg00063.html>

469 **Document:** Bindings and profiles

470 **Description:** In reviewing the bindings doc for typographical inconsistencies in the treatment of
471 status code stuff, I found this in Section 3.1.3.6 Error Reporting:

472 "In the case of a SAML processing error, the SOAP HTTP server MUST
473 respond with "200 OK" and include a SAML-specified error description as
474 the only child of the <SOAP-ENV:Body> element."

475

476 Should we be putting Major Version etc. attributes on StatusCode
477 along with Assertion, Request, and Response? If we did, we'd want to
478 make them optional, with default values inherited from the nearest SAML
479 ancestor, if any.

480

481 **Options:** Add text to clarify that a Response is sent with the StatusCode.

482 **Disposition:** 4/29/03 – Accepted text by Eve. Deprecated `StatusCode` as a top element in
483 SOAP response. `StatusCode` MUST be a child of `<samlp:Response>`. Incorporated in Draft
484 03 of Bindings and Profiles

485 **3.18 PE18: SAML Versioning**

486 **First reported by:** Scott Cantor, Ohio State University and Internet 2

487 **Message:** <http://lists.oasis-open.org/archives/security-services/200304/msg00000.html>

488 **Document:** All documents

489 **Description:** The SAML specification is versioned in several, independent ways. This leads to
490 possible confusion. We should have a clear and consistent versioning specification.

491

492 **Options:** Specify a new SAML versioning as detailed in [http://lists.oasis-](http://lists.oasis-open.org/archives/security-services/200304/doc00000.doc)
493 [open.org/archives/security-services/200304/doc00000.doc](http://lists.oasis-open.org/archives/security-services/200304/doc00000.doc)

494 **Disposition:** Accepted during TC meeting on April 15, 2003. Incorporated in Drafts 05 and
495 06 of SAML 1.1 Assertions and Protocols.

496 **3.19 PE19: Clarification of status code for the case of no** 497 **assertion**

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

499 **Message:** <http://www.oasis-open.org/archives/security-services/200304/msg00221.html>

500 **Document:** SAML 1.1 Bindings and Profiles, Draft 02

501 **Description:** Lines 505-507 (section 4.1.1.6) of the -02 draft B&P document states:

502

503 "If the source site is able to find or construct the requested assertions, it responds with a
504 `<samlp:Response>` message with the requested assertions. Otherwise, it returns an
505 appropriate status code, as defined within the selected SAML binding." This is not really clear and
506 will probably be construed by the reader to mean either that a SAML error status code should be
507 returned in a `samlp:Response` or that a SOAP fault error should be returned (assuming the
508 "selected SAML binding" is SOAP over HTTPS).

509 We should clarify this as follows:

510 "If the source site is able to find or construct the requested assertions, it responds with a
511 `<samlp:Response>` message with the requested assertions. Otherwise, it responds with a
512 `<samlp:Response>` message with no assertions and a `<samlp:StatusCode>` element with
513 the value `Success`."

514 **Options:** Make editorial change to clarify

515 **Disposition:** Adopted editorial change as suggested. Incorporated in Draft 03 of Bindings
516 and Profiles

517 **3.20 PE20: Clarification of `<ConfirmationData>` in Browser/POST**

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

519 **Message:** <http://www.oasis-open.org/archives/security-services/200304/msg00225.html>

520 **Document:** Bindings and Profiles

521 **Description:** Section 4.1.2.5 states that:

522 The `<saml:ConfirmationMethod>` element of each assertion MUST be set to

523 urn:oasis:names:tc:SAML:1.0:cm:bearer. This absence of text regarding
524 <saml:confirmationData> may lead to confusion.

525 We should clarify as follows:

526 Every subject-based statement in the assertion(s) returned to the destination site **MUST**
527 contain a <saml:SubjectConfirmation> element. The <ConfirmationMethod> element in
528 the <SubjectConfirmation> **MUST** be set to urn:oasis:names:tc:SAML:1.0:cm:bearer.

529

530 Additionally, section 4.1.1.6 should also be updated to reflect the same change for the
531 Browser/Artifcat, as follows:

532 Every subject-based statement in the assertion(s) returned to the destination site **MUST** contain a
533 <saml:SubjectConfirmation> element as follows:

- 534 • The <saml:ConfirmationMethod> element **MUST** be set to either
535 urn:oasis:names:tc:SAML:1.0:cm:artifact-01 (deprecated) or
536 urn:oasis:names:tc:SAML:1.0:cm:artifact (RECOMMENDED).
- 537 • The <SubjectConfirmationData> element **SHOULD NOT** be specified.

538 **Options:** Make editorial change to clarify.

539 **Disposition: Editorial change incorporated in Draft 03 of Bindings and Profiles. TC**
540 **approval is expected at next available opportunity.**

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
Draft-05	2003-03-31	Jahan Moreh	Added possible resolution to PE 15 per Prateek's email
Draft-06	2003-04-01	Jahan Moreh	Modifications and dispositions based on TC meeting of April 01, 2003
Draft-07	2003-04-07	Jahan Moreh	Added new erratum reported by Eve Maler. Added potential erratum reported by Eve Maler regarding editorial changes to make clear the use of QName in <AuthorityKind> and <RespondWith>. Updated Option's section of PE11 per Eve Maler's suggestion.
Draft-08	2003-04-14	Jahan Moreh	Modifications and dispositions based on TC meeting of April 08, 2003. Added Appendix B, Summary of Dispositions.
Draft-09	2003-04-21	Jahan Moreh	Added PE 17 and PE 18. Updated PE 15.
Draft-10	2003-04-28	Jahan Moreh	Finalized disposition of PE4, PE9, PE13, PE15 and PE18.
Draft-11	2003-02-05	Jahan Moreh	Added E9 and PE 19 and PE20 and their disposition. Recorded disposition of PE6 and PE17. Changed document location for public availability. Changed title to make it consistent with last call working drafts. Fixed hyperlinks to messages.

Appendix B. Summary of Disposition

Erratum #	Status	Document	Draft
E1	Disposed	Bindings and Profiles	01
E2	Disposed	Bindings and Profiles	01
E3	Disposed	Bindings and Profiles	01
E4	Disposed	Assertions and Protocols	02
E5	Disposed	Assertions and Protocols	02
E6	Disposed	Assertions and Protocols	02
E7	Disposed	Assertions and Protocols	04
E8	Disposed	Assertions and Protocols	03
E9	Disposed	Bindings and profiles	03
PE1	Disposed	Bindings and Profiles	01
PE2	Disposed; No action required		
PE3	Disposed; No action required		
PE4	Disposed	Bindings and Profiles	02
PE5	Disposed	Assertions and Protocols	02
PE6	Disposes	Bindings and Profiles	03
PE7	Disposed	Assertions and Protocols	02
PE8	Disposed	Assertions and Protocols	02
PE9	Disposed	Assertions and Protocols	06
PE10	Disposed; No action required		
PE11	Disposed	Assertions and Protocols	03
PE12	Disposed	Assertions and Protocols	03
PE13	Disposed	Assertions and Protocols	03 and 06
		Assertions and Protocols	03
PE14	Disposed	Glossary	01
PE15	Disposed	Bindings and Profiles	02
PE16	Disposed	Assertions and Protocols	04
PE17	Disposed	Bindings and Profiles	03
PE18	Disposed	Assertions and Protocols	05 and 06
PE19	Disposed	Bindings and Profiles	03
PE20	Disposed	Bindings and Profiles	03

545

Appendix C. Notices

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

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

558 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]
559 2002 and 2003. All Rights Reserved.

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

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

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