



1

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

5 **Working Draft 14, 30 June 2003**

6 **Document identifier:**

7 sstc-saml-errata-1.1-draft-14

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 time as
17 the specifications are frozen against editorial changes and sent to the OASIS membership for
18 voting.

19 Comments on issues with the SAML specifications are welcome. If you are on the [security-](mailto:security-services@lists.oasis-open.org)
20 services@lists.oasis-open.org list for committee members, send comments there. If you are not
21 on that list, subscribe to the security-services-comment@lists.oasis-open.org list and send
22 comments there. To subscribe, send an email message to [security-services-comment-](mailto:security-services-comment-request@lists.oasis-open.org)
23 request@lists.oasis-open.org with the word "subscribe" as the body of the message. If you have
24 questions or comments on implementation issues, subscribe to the [saml-dev@lists.oasis-](mailto:saml-dev@lists.oasis-open.org)
25 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>.....	8
51	3.11	PE11: Processing rules for AssertionIDReference.....	9
52	3.12	PE12: Miscellaneous additions and clarifications.....	9
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>.....	11
57	3.17	PE17: Non-normative clarification of status code.....	12
58	3.18	PE18: SAML Versioning.....	12
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	3.21	PE21: Description of the AuthenticationMethod attribute in <AuthenticationQuery>.....	14
62	3.22	PE22: Clarification of AuthenticationMethod attribute.....	14
63	3.23	PE23: Clarification of <Statement>, <SubjectStatement> and Nested Assertions.....	15
64		Appendix A. Revision History.....	16
65		Appendix B. Summary of Disposition.....	17
66		Appendix C. Notices.....	18

67

68 1 Introduction

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

71 2 Errata

72 2.1 E1: Section number inconsistencies

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

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

75 **Document:** Bindings and Profiles

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

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

80 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
81 01 of SAML 1.1 Bindings and Profiles.

82 2.2 E2: Typo

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

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

85 **Document:** Bindings and Profiles

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

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

88 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
89 01 of SAML 1.1 Bindings and Profiles.

90 2.3 E3: Section Formatting

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

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

93 **Document:** Bindings and Profiles

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

95 **Options:** Change formatting

96 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
97 01 of SAML 1.1 Bindings and Profiles.

98 2.4 E4: Font Inconsistencies

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

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

101 **Document:** Assertions and Protocols

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

104 **Options:** Change formatting of line 714
105 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
106 **02 of SAML 1.1 Assertions and Protocols.**

107 **2.5 E5: Spelling errors**

108 **First reported by:** Rob Philpott, RSA Security
109 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>
110 **Document:** Assertions and Protocols
111 **Description:** Line 887: “interger” should be “integer”
112 **Options:** Correct spelling error
113 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
114 **02 of SAML 1.1 Assertions and Protocols.**

115 **2.6 E6: Spelling errors**

116 **First reported by:** Prateek Mishra, Netegrity
117 **Message:** <http://lists.oasis-open.org/archives/security-services/200302/msg00022.html>
118 **Document:** Assertions and Protocols
119 **Description:** Line 1441 is in error and should be removed from this list.
120 Lines 1439-1444 state:
121
122 The following elements are intended specifically for use as extension points
123 in an extension schema; their 1439
124 types are set to abstract, so that the use of an xsi:type attribute with
125 these elements is REQUIRED: 1440
126 * <Assertion> 1441
127 * <Condition> 1442
128 * <Statement> 1443
129 * <SubjectStatement> 1444
130
131 An examination of the schema reveals that <Assertion> is of type <AssertionType> which is a
132 concrete type. Thus, there is no requirement that an xsi:type attribute must be used with
133 assertions.
134 **Options:** Correct error
135 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
136 **02 of SAML 1.1 Assertions and Protocols.**

137 **2.7 E7: Normative use of MAY NOT**

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

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

149 **2.8 E8: Extension types for <RespondWith>**

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

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

152 **Document:** Assertions and Protocols

153 **Description:** In core 1.0 lines 971-973, it says: “To specify extension types, the <RespondWith>
154 element MUST contain exactly the extension element type as specified in the xsi:type attribute
155 on the corresponding element.”

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

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

164

165 **Options:** Fix the almost-ambiguity in V1.1 by saying “**element’s** type” rather than “**element** type”,
166 and treat this as an editorial correction.

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

169 **2.9 E9: Incorrect identifier for alternative SAML Artifact Format**

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

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

172 **Document:** Bindings and Profiles

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

177 **Options:** Make editorial correction.

178 **Disposition:** Make editorial correction as stated above. Incorporated in Draft 03 of SAML
179 **1.1 Bindings and Profiles.**

180 **3 Potential Errata**

181 **3.1 PE1: HTTPS for inter-site transfer service and artifact** 182 **transmission**

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

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

185 **Document:** Bindings and Profiles

186 **Description:** Since SSL/TLS is recommended for inter-site transfer and artifact transmission,
187 perhaps https should be shown in the examples at line [443], [483].
188 **Options:** Use https in the examples.
189 **Disposition:** Agreed to change it at TC meeting 2/18/03. Incorporated in Draft 01 of SAML
190 1.1 Bindings and Profiles.

191 **3.2 PE2: Clarify the expectations of SubjectConfirmationData**

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

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

194 **Document:** Bindings and Profiles

195 **Description:** It might be helpful to clarify the expectations of SubjectConfirmationData and
196 ds:KeyInfo usage for the different ConfirmationMethods in this profile. \

197

198 **Options:**

- 199 1. Reject. The Holder-of-Key case is not involved in any of the web browser profiles. The
200 Browser/Artifact profile does not require the use of SubjectConfirmationData or
201 ds:KeyInfo.
- 202 2. 2/18/03: Add supplementary text to explain use of <SubjectConfirmationData>

203 **Disposition:** April 01 TC meeting: TC voted to choose option 1.

204 **3.3 PE3: Bearer and Holder of Key in POST profile**

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

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

207 **Document:** Bindings and Profiles

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

210 **Options:**

- 211 1. Reject. While there is a requirement that the SAML response message must be signed (694-
212 695) there is no implication that the included assertions contain ds:KeyInfo element
- 213 2. 2/18/03: Add supplementary text to explain use of <SubjectConfirmationData>

214 **Disposition:** April 01 TC meeting: TC voted to choose option 1.

215 **3.4 PE4: Encoding of URI in “Alternative SAML Artifact Format”**

216 **First reported by:** Yuji Sakata, and Juergen Kremp, SAP

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

218 **Document:** Bindings and Profiles

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

221 TypeCode := 0x0002

222 RemainingArtifact := AssertionHandle SourceLocation

223 AssertionHandle := 20-byte_sequence

224 SourceLocation := URI

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

227 **Options:**
228 1. Specify UTF-8 as default character set
229 2. Text proposed by Prateek on 18 April 2003: Insert at end of sentence on line 951:
230 The SourceLocation URI is mapped to a sequence of bytes based on use of the UTF-8
231 [RFC2279] encoding. Add to reference list: RFC 2279 UTF-8, a transformation
232 format of ISO 10646.
233 **Disposition: 2/18/03 – during meeting of TC it was decided to correct this. Prateek to**
234 **propose text changes. During TC meeting of April 22, 2003 SSTC accepted text as**
235 **proposed by Prateek (option 2 above). Incorporated in Draft 02 of SAML 1.1 Bindings and**
236 **Profiles.**

237 **3.5 PE5: Signing Assertions**

238 **First reported by:** Ronald Monzillo, Sun Microsystems
239 **Message:** <http://lists.oasis-open.org/archives/security-services/200212/msg00003.html>
240 **Document:** Assertions and Protocols
241 **Description:** Section 5, lines [1382-1387] indicate that a SAML assertion MUST be signed. The
242 intent here is to strongly advocate the use of signature when assertions are passing through
243 intermediaries. The use of "MUST" here is inappropriate, this is really only advice for profile
244 developers.
245 **Options:**
246 1. Change the specification to read "MAY"
247 2. Change the specification to read "SHOULD"
248 **Disposition: 2/18/03 – during meeting of TC it was decided to correct this to "SHOULD".**
249 **Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.**

250 **3.6 PE6: Artifact and corresponding confirmation method**

251 **First reported by:** Rob Philpott, RSA Security
252 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00016.html>
253 **Document:** Bindings and Profiles
254 **Description:** Section 5.3: Even though it isn't explicitly stated, one would assume that the
255 "...:cm:artifact-01" refers to a type 1 artifact. If so, doesn't there need to be a corresponding
256 confirmation method identifier for "...:cm:artifact-02"? Is there really a need to distinguish the
257 artifact types (i.e. "just use "...:cm:artifact")? We should also be explicit as to whether providing
258 the actual artifact in the ConfirmationData is required, optional, or not permitted – Which is it?
259 **Options:**
260 1. Strike artifact-01
261 2. Add confirmation method identifier "...:cm:artifact-02"
262 3. Add a confirmation method ID (artifact) and indicate that either one can be used for 01, 03, or
263 any other future.
264 **Disposition: 2/18/03 – during meeting of TC it was decided to choose option 3.**
265 **Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.**
266 **4/29/03 – It was decided that to deprecate artifact-01 and simply use artifact. After line 528**
267 **of protocols and bindings add a brief normative note: SAML authorities SHOULD NOT**

268 include SAML artifact in a Confirmation Data. Incorporated in Draft 03 of Binding and
269 Profiles.

270 3.7 PE7: Normative Language

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

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

273 **Document:** Assertions and Protocols

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

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

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

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

278 **Options:**

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

281 Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.

282 3.8 PE8: non-Normative Language

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

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

285 **Document:** Assertions and Protocols

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

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

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

289 **Options:**

290 **Disposition:** 2/18/03 – during meeting of TC it was decided to choose correct 967 and 1219.
291 Keep 1417 as is. Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.

292 3.9 PE9: Reference to AuthorityKind

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

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

295 **Document:** Assertions and Protocols

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

303 **Options:**

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

307 3.10 PE10: Guidance on Element <RespondWith>

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

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

310 **Document:** Assertions and Protocols

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

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

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

326 **3.11 PE11: Processing rules for AssertionIDReference**

327 **First reported by:** Rob Philpott

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

329 **Document:** Assertions and Protocols

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

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

341 3.2.2.1 Requests for Assertions by Reference

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

344 3. Element <AssertionArtifact>

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

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

352 **3.12 PE12: Miscellaneous additions and clarifications**

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

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

355 **Document:** Assertions and Protocols

356 **Description:**
357 1. Lines 1061-1065: In addition to subject and authn method matching rules, we should indicate
358 that the assertion processing rules are also impacted by the presence of RespondWith elements
359 in the Query.
360 2. Section 3.3.4 AttributeQuery – Should also mention the subject-matching rules as described in
361 section 3.3.3
362 3. Line 1085: “the start of the current document” – In a query, the samlp:Request is the
363 ****current**** document, so what does it mean to use a Resource with an empty URI?
364 4. Section 3.3.5 AuthorizationDecisionQuery – Should also mention the subject-matching rules as
365 described in section 3.3.3
366 **Options:** for (1) , (2), (4) add cross reference in the respective sections to clarify. For (3) add text
367 to strongly discourage use of empty URIs.
368 **Disposition: April 01 TC meeting: Eve will make editorial changes. Incorporated in Draft 03**
369 **of SAML 1.1 Assertions and Protocols..**

370 **3.13 PE13: Miscellaneous additions and clarifications**

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

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

373 **Document:** Assertions and Protocols

374 **Description:**

375 1. Section 3.4.4 (Responses to <AuthnQuery> and <AttrQuery>) – Don't the saml:Subject
376 matching rules described in this section also apply to <AuthzQuery>? In fact, one could assume
377 that the rules should apply to all <SubjectQuery> requests, including and extensions. Therefore,
378 the section should be more general.

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

381 **Options:**

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

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

386 **3.14 PE14: Requestor vs. Requester and glossary definition for** 387 **Responder**

388 **First reported by:** Rob Philpott

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

390 **Document:** Assertions and Protocols

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

398
399 Also – we need to add a definition for “Responder” to the glossary. We use it in the specs. The
400 definition for Responder could be:

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

405 **Options:**

406 **Disposition: April 01 TC meeting:** Use “Requester” throughout. Add “SAML Requester and
407 SAML Responder”. **Incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.**

408 Also reviewed SOAP definitions for “Requester” and “Responder” and modified as appropriate.
409 **Incorporated in Draft 01 of SAML 1.1 Glossary**

410 **3.15 PE15: Browser POST profile does not explicitly call out**
411 **encoding**

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

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

414 **Document:** Bindings and Profiles

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

421 **Options:**

- 422 1. Explicitly call-out UTF-8 encoding
- 423 2. Reject based on the following reason. On reviewing the XML specification, it turns out
424 that the issue of specifying and determining the character encoding of XML
425 documents has been completely addressed therein. [http://www.w3.org/TR/REC-](http://www.w3.org/TR/REC-xml#charencoding)
426 [xml#charencoding](http://www.w3.org/TR/REC-xml#charencoding). My reading of this text suggests that SAML does not need to take a
427 position on this issue and no additional text is required in the Browser/POST profile.
- 428 3. Adopt the following text as proposed by Scott: On line 692, replace the current sentence
429 with this text:
- 430 The notation B64(<response>) stands for the result of applying the Base64 Content-
431 Transfer-Encoding to the response, as defined by RFC 1521, section 5.2, and SHOULD
432 consist of lines of encoded data of up to 76 characters. The first encoded line begins after
433 the opening quote signifying the “value” attribute of the SAMLResponse form element.
- 434 The character set used to represent the encoded data is determined by the “charset”
435 attribute of the Content-Type of the HTML document containing the form. The character
436 set of the XML document resulting from decoding the data is determined in the normal
437 fashion, and defaults to UTF-8 if no character set is indicated.

438

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

442 **3.16 PE16: Use of Qnames in <AuthorityKind> and**
443 **<RespondWith>**

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

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

446 **Document:** Assertions and Protocols
447 **Description:** Near lines 716 (all line references in this message are to core 1.0) for
448 AuthorityKind, and 968 for RespondWith, the text gives an example of a QName in use
449 and unfortunately implies (rather more strongly in the latter case) that the prefix must
450 read “saml” when a natively defined construct is being referenced. But the prefix of a
451 namespaced value is never fixed, and we don’t clarify that the appropriate namespace
452 must have been defined in the scope of the relevant element where the QName appears.
453

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

456
457 For AuthorityKind: “For example, an attribute authority would be identified by
458 AuthorityKind=”samlp:AttributeQuery”, where there is a namespace declaration in the
459 scope of this attribute that binds the samlp: prefix to the SAML protocol namespace_.”
460

461 For RespondWith: “For example, a requestor that wishes to receive assertions containing
462 only attribute statements would_ [this was a lowercase “must”] specify
463 <RespondWith>saml:AttributeStatement</RespondWith>, where the prefix is
464 bound to the SAML assertion namespace in a namespace declaration that is
465 in the scope of this element_.”

466 **Options:** Incorporate changes as described.

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

469 **3.17 PE17: Non-normative clarification of status code**

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

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

472 **Document:** Bindings and profiles

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

475 “In the case of a SAML processing error, the SOAP HTTP server MUST respond with “200 OK”
476 and include a SAML-specified error description as the only child of the <SOAP-ENV:Body>
477 element.”
478

479 Should we be putting Major Version etc. attributes on StatusCode along with Assertion, Request,
480 and Response? If we did, we’d want to make them optional, with default values inherited from
481 the nearest SAML ancestor, if any.
482

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

484 **Disposition:** 4/29/03 – Accepted text by Eve. Deprecated StatusCode as a top element in
485 SOAP response. StatusCode MUST be a child of <samlp:Response>. Incorporated in Draft
486 03 of Bindings and Profiles

487 **3.18 PE18: SAML Versioning**

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

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

490 **Document:** All documents
491 **Description:** The SAML specification is versioned in several, independent ways. This leads to
492 possible confusion. We should have a clear and consistent versioning specification.
493
494 **Options:** Specify a new SAML versioning as detailed in [http://lists.oasis-](http://lists.oasis-open.org/archives/security-services/200304/doc00000.doc)
495 [open.org/archives/security-services/200304/doc00000.doc](http://lists.oasis-open.org/archives/security-services/200304/doc00000.doc)
496 **Disposition:** Accepted during TC meeting on April 15, 2003. Incorporated in Drafts 05 and
497 06 of SAML 1.1 Assertions and Protocols.

498 **3.19 PE19: Clarification of status code for the case of no** 499 **assertion**

500 **First reported by:** Rob Philpott, RSA Security
501 **Message:** <http://www.oasis-open.org/archives/security-services/200304/msg00221.html>
502 **Document:** SAML 1.1 Bindings and Profiles, Draft 02
503 **Description:** Lines 505-507 (section 4.1.1.6) of the -02 draft B&P document states:
504
505 “If the source site is able to find or construct the requested assertions, it responds with a
506 <samlp:Response> message with the requested assertions. Otherwise, it returns an
507 appropriate status code, as defined within the selected SAML binding.” This is not really clear and
508 will probably be construed by the reader to mean either that a SAML error status code should be
509 returned in a samlp:Response or that a SOAP fault error should be returned (assuming the
510 “selected SAML binding” is SOAP over HTTPS).
511 We should clarify this as follows:
512 “If the source site is able to find or construct the requested assertions, it responds with a
513 <samlp:Response> message with the requested assertions. Otherwise, it responds with a
514 <samlp:Response> message with no assertions and a <samlp:StatusCode> element with
515 the value Success.”
516 **Options:** Make editorial change to clarify
517 **Disposition:** Adopted editorial change as suggested. Incorporated in Draft 03 of Bindings
518 and Profiles

519 **3.20 PE20: Clarification of <ConfirmationData> in Browser/POST**

520 **First reported by:** Rob Philpott, RSA Security
521 **Message:** <http://www.oasis-open.org/archives/security-services/200304/msg00225.html>
522 **Document:** Bindings and Profiles
523 **Description:** Section 4.1.2.5 states that:
524 The <saml:ConfirmationMethod> element of each assertion MUST be set to
525 urn:oasis:names:tc:SAML:1.0:cm:bearer. This absence of text regarding
526 <saml:confirmationData> may lead to confusion.
527 We should clarify as follows:
528 Every subject-based statement in the assertion(s) returned to the destination site MUST
529 contain a <saml:SubjectConfirmation> element. The <ConfirmationMethod> element in
530 the <SubjectConfirmation> MUST be set to urn:oasis:names:tc:SAML:1.0:cm:bearer.
531

532 Additionally, section 4.1.1.6 should also be updated to reflect the same change for the
533 Browser/Artifact, as follows:
534 Every subject-based statement in the assertion(s) returned to the destination site MUST contain a
535 <saml:SubjectConfirmation> element as follows:
536 • The <saml:ConfirmationMethod> element MUST be set to either
537 urn:oasis:names:tc:SAML:1.0:cm:artifact-01 (deprecated) or
538 urn:oasis:names:tc:SAML:1.0:cm:artifact (RECOMMENDED).
539 • The <SubjectConfirmationData> element SHOULD NOT be specified.
540 **Options:** Make editorial change to clarify.
541 **Disposition: Editorial change incorporated in Draft 03 of Bindings and Profiles. TC**
542 **approval is expected at next available opportunity.**

543 **3.21 PE21: Description of the AuthenticationMethod attribute in** 544 **<AuthenticationQuery>**

545 **First reported by:** Rob Philpott, RSA Security
546 **Message:** <http://lists.oasis-open.org/archives/security-services/200305/msg00104.html>
547 **Document:** Assertions and Protocols
548 **Description:** Draft 10 of Assertions and Protocols, lines 1114-1118 describing
549 AuthenticationQuery states:
550 "This element is of type **AuthenticationQueryType**, which extends **SubjectQueryAbstractType**
551 with the addition of the following element:
552 <AuthenticationMethod> [Optional]
553 A filter for possible responses. If it is present, the query made is "What assertions containing
554 authentication statements do you have for this subject with the supplied authentication method?"
555
556 Lines 1123-1125 state:
557 If the <AuthenticationMethod> element is present in the query, at least one
558 <AuthenticationMethod> element in the set of returned assertions MUST match. It is
559 OPTIONAL for the complete set of all such matching assertions to be returned in the response.
560
561 The problem is that the schema for AuthenticationQueryType defines "AuthenticationQuery" as
562 an XML attribute of type anyURI. It is not defined as an element.

563
564 **Options:**
565 1. Make editorial change to state that <AuthenticationMethod> is an attribute not an element.
566 2. Make <AuthenticationMethod> an element and allow multiple occurrences of it in
567 <AuthenticationQuery>.

568
569 **Disposition: SSTC chose option 1 during its weekly conference call of 5/13. The SSTC**
570 **concluded that this option is consistent with the usage of <AuthenticationMethod> in the**
571 **rest of the specification. Change incorporated in draft 11 of Assertion and Protocols.**

572 **3.22 PE22: Clarification of AuthenticationMethod attribute**

573 **First reported by:** Rob Philpott, RSA Security
574 **Message:** <http://lists.oasis-open.org/archives/security-services/200305/msg00106.html>

575 **Document:** Assertions and Protocols

576 **Description:** Draft 10 of Assertions and Protocols, section 7.1 uses the form
577 <AuthenticationMethod>, which leads to it being interpreted as an element. We should modify the
578 text to clearly indicate that AuthenticationMethod is an attribute. The proposed text is as follows:

579 The AuthenticationMethod attribute of an <AuthenticationStatement> and the
580 <SubjectConfirmationMethod> element of a SAML subject perform different functions, although
581 both can refer to the same underlying mechanisms. An authentication statement with an
582 AuthenticationMethod attribute describes an authentication act that occurred in the past. The
583 AuthenticationMethod attribute indicates how that authentication was done. Note that the
584 authentication statement does not provide the means to perform that authentication, such as a
585 password, key, or certificate.

586 **Options:** Make editorial change.

587 **Disposition:** Based on the disposition of PE21, the SSTC approved this editorial change
588 via email exchanges. Incorporated in Draft 11.

589 **3.23 PE23: Clarification of <Statement>, <SubjectStatement> and** 590 **Nested Assertions**

591 **First reported by:** John Kemp, Project Liberty

592 **Message:** <http://lists.oasis-open.org/archives/security-services/200305/msg00150.html>

593 **Document:** Assertions and Protocols

594 **Description:**

595 Lines 324-326 note that three kinds of assertion are specified by SAML. When reading the
596 schema, <Statement> and <SubjectStatement> are treated as if they might appear independently
597 of these three kinds of assertion, which is not in fact the case - they are for extensions that
598 specify additional kinds of assertion. It is recommend that this distinction be made clear in this
599 introductory text.

600 2. Line 331 states that "Assertions have a nested structure". 'Nesting' implies that one assertion
601 may be contained within another, which as far as I can tell from the schema is not possible. It is
602 recommended that this sentence be changed to note that an "assertion acts as a container for a
603 number of assertion statements" or some similar text.

604 **Options:** Make editorial change.

605 **Disposition:** During the SSTC conference call of 6/10, the co-chairs were directed to make
606 editorial changes to the document to clarify as suggested. These changes were made to
607 final version of core before submitting the document as OASIS standard.

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	2003-05-02	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.
Draft-12	2003-05-13	Jahan Moreh	Added PE21, PE22 and their disposition.
Draft 13	2003-06-13	Jahan Moreh	Added PE23
Draft 14	2003-06-30	Jahan Moreh	Recorded final disposition of PE23

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
PE14	Disposed	Assertions and Protocols	03
		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
PE21	Disposed	Assertions and Protocols	11
PE22	Disposed	Assertions and Protocols	11
PE23	Disposed	Assertions and Protocols	sstc-saml-core-1.1-cs-02

612 Appendix C. Notices

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

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

625 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]
626 2002 and 2003. All Rights Reserved.

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

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

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