



1

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

5 **Working Draft 16, 02 September 2003**

6 **Document identifier:**

7 sstc-saml-errata-1.1-draft-16

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	2.10	E10: Incorrect Characterization of Identifier Uniqueness	5
41	3	Potential Errata	6
42	3.1	PE1: HTTPS for inter-site transfer service and artifact transmission.....	6
43	3.2	PE2: Clarify the expectations of SubjectConfirmationData.....	6
44	3.3	PE3: Bearer and Holder of Key in POST profile	6
45	3.4	PE4: Encoding of URI in "Alternative SAML Artifact Format"	7
46	3.5	PE5: Signing Assertions.....	7
47	3.6	PE6: Artifact and corresponding confirmation method.....	7
48	3.7	PE7: Normative Language	8
49	3.8	PE8: non-Normative Language.....	8
50	3.9	PE9: Reference to AuthorityKind	8
51	3.10	PE10: Guidance on Element <RespondWith>	9
52	3.11	PE11: Processing rules for AssertionIDReference	9
53	3.12	PE12: Miscellaneous additions and clarifications	10
54	3.13	PE13: Miscellaneous additions and clarifications	10
55	3.14	PE14: Requestor vs. Requester and glossary definition for Responder.....	11
56	3.15	PE15: Browser POST profile does not explicitly call out encoding.....	11
57	3.16	PE16: Use of Qnames in <AuthorityKind> and <RespondWith>	12
58	3.17	PE17: Non-normative clarification of status code	12
59	3.18	PE18: SAML Versioning.....	13
60	3.19	PE19: Clarification of status code for the case of no assertion	13
61	3.20	PE20: Clarification of <ConfirmationData> in Browser/POST	14
62	3.21	PE21: Description of the AuthenticationMethod attribute in <AuthenticationQuery>	14
63	3.22	PE22: Clarification of AuthenticationMethod attribute.....	15
64	3.23	PE23: Clarification of <Statement>, <SubjectStatement> and Nested Assertions.....	15
65		Appendix A. Revision History	17
66		Appendix B. Summary of Disposition	18
67		Appendix C. Notices	19

68

69 1 Introduction

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

72 2 Errata

73 2.1 E1: Section number inconsistencies

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

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

76 **Document:** Bindings and Profiles

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

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

81 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
82 01 of SAML 1.1 Bindings and Profiles.

83 2.2 E2: Typo

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

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

86 **Document:** Bindings and Profiles

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

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

89 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
90 01 of SAML 1.1 Bindings and Profiles.

91 2.3 E3: Section Formatting

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

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

94 **Document:** Bindings and Profiles

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

96 **Options:** Change formatting

97 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
98 01 of SAML 1.1 Bindings and Profiles.

99 2.4 E4: Font Inconsistencies

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

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

102 **Document:** Assertions and Protocols

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

105 **Options:** Change formatting of line 714
106 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
107 **02 of SAML 1.1 Assertions and Protocols.**

108 **2.5 E5: Spelling errors**

109 **First reported by:** Rob Philpott, RSA Security
110 **Message:** <http://lists.oasis-open.org/archives/security-services/200301/msg00014.html>
111 **Document:** Assertions and Protocols
112 **Description:** Line 887: “interger” should be “integer”
113 **Options:** Correct spelling error
114 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
115 **02 of SAML 1.1 Assertions and Protocols.**

116 **2.6 E6: Spelling errors**

117 **First reported by:** Prateek Mishra, Netegrity
118 **Message:** <http://lists.oasis-open.org/archives/security-services/200302/msg00022.html>
119 **Document:** Assertions and Protocols
120 **Description:** Line 1441 is in error and should be removed from this list.
121 Lines 1439-1444 state:
122
123 The following elements are intended specifically for use as extension points
124 in an extension schema; their 1439
125 types are set to abstract, so that the use of an xsi:type attribute with
126 these elements is REQUIRED: 1440
127 * <Assertion> 1441
128 * <Condition> 1442
129 * <Statement> 1443
130 * <SubjectStatement> 1444
131
132 An examination of the schema reveals that <Assertion> is of type <AssertionType> which is a
133 concrete type. Thus, there is no requirement that an xsi:type attribute must be used with
134 assertions.
135 **Options:** Correct error
136 **Disposition:** Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft
137 **02 of SAML 1.1 Assertions and Protocols.**

138 **2.7 E7: Normative use of MAY NOT**

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

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

150 **2.8 E8: Extension types for <RespondWith>**

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

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

153 **Document:** Assertions and Protocols

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

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

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

165

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

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

170 **2.9 E9: Incorrect identifier for alternative SAML Artifact Format**

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

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

173 **Document:** Bindings and Profiles

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

178 **Options:** Make editorial correction.

179 **Disposition:** Make editorial correction as stated above. Incorporated in Draft 03 of SAML
180 **1.1 Bindings and Profiles.**

181 **2.10 E10: Incorrect Characterization of Identifier Uniqueness**

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

183 **Message:** <http://lists.oasis-open.org/archives/security-services/200307/msg00063.html>

184 **Document:** Assertions and Protocols

185 **Description:** Lines 236 and 237 of sstc-saml-core-1.1-cs-03 state: "the probability of two
186 randomly chosen identifiers being identical MUST be less than 2^{-128} and SHOULD be less than 2^{-160} ".
187 The correct statement is: the probability of two randomly chosen identifiers being identical
188 MUST be less than **or equal to** 2^{-128} and SHOULD be less **or equal to** 2^{-160}

189 **Options:** Make editorial correction.

190 **Disposition:** Incorporated in the final 1.1 committee specification.

192 3 Potential Errata

193 3.1 PE1: HTTPS for inter-site transfer service and artifact 194 transmission

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

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

197 **Document:** Bindings and Profiles

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

200 **Options:** Use https in the examples.

201 **Disposition:** Agreed to change it at TC meeting 2/18/03. Incorporated in Draft 01 of SAML
202 1.1 Bindings and Profiles.

203 3.2 PE2: Clarify the expectations of SubjectConfirmationData

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

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

206 **Document:** Bindings and Profiles

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

209

210 **Options:**

- 211 1. Reject. The Holder-of-Key case is not involved in any of the web browser profiles. The
- 212 Browser/Artifact profile does not require the use of `SubjectConfirmationData` or
- 213 `ds:KeyInfo`.
- 214 2. 2/18/03: Add supplementary text to explain use of `<SubjectConfirmationData>`

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

216 3.3 PE3: Bearer and Holder of Key in POST profile

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

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

219 **Document:** Bindings and Profiles

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

222 **Options:**

- 223 1. Reject. While there is a requirement that the SAML response message must be signed (694-
224 695) there is no implication that the included assertions contain `ds:KeyInfo` element
- 225 2. 2/18/03: Add supplementary text to explain use of `<SubjectConfirmationData>`

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

227 **3.4 PE4: Encoding of URI in “Alternative SAML Artifact Format”**

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

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

230 **Document:** Bindings and Profiles

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

233 TypeCode := 0x0002

234 RemainingArtifact := AssertionHandle SourceLocation

235 AssertionHandle := 20-byte_sequence

236 SourceLocation := URI

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

239 **Options:**

240 1. Specify UTF-8 as default character set

241 2. Text proposed by Prateek on 18 April 2003: Insert at end of sentence on line 951:

242 The SourceLocation URI is mapped to a sequence of bytes based on use of the UTF-8
243 [RFC2279] encoding. Add to reference list: RFC 2279 UTF-8, a transformation
244 format of ISO 10646.

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

249 **3.5 PE5: Signing Assertions**

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

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

252 **Document:** Assertions and Protocols

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

257 **Options:**

258 1. Change the specification to read “MAY”

259 2. Change the specification to read “SHOULD”

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

262 **3.6 PE6: Artifact and corresponding confirmation method**

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

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

265 **Document:** Bindings and Profiles

266 **Description:** Section 5.3: Even though it isn't explicitly stated, one would assume that the
267 "...:cm:artifact-01" refers to a type 1 artifact. If so, doesn't there need to be a corresponding
268 confirmation method identifier for "...:cm:artifact-02"? Is there really a need to distinguish the
269 artifact types (i.e. "just use "...:cm:artifact")? We should also be explicit as to whether providing
270 the actual artifact in the ConfirmationData is required, optional, or not permitted – Which is it?

271 **Options:**

- 272 1. Strike artifact-01
- 273 2. Add confirmation method identifier "...:cm:artifact-02"
- 274 3. Add a confirmation method ID (artifact) and indicate that either one can be used for 01, 03, or
275 any other future.

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

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

278 **4/29/03 – It was decided that to deprecate *artifact-01* and simply use *artifact*. After line 528**
279 **of protocols and bindings add a brief normative note: SAML authorities SHOULD NOT**
280 **include SAML artifact in a Confirmation Data. Incorporated in Draft 03 of Binding and**
281 **Profiles.**

282 3.7 PE7: 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 961: change "may" to "MAY".

287 Line 966: change "success would normally" to "Success MUST".

288 Line 971: Change "must" to "MUST".

289 Line 1237: Change "subcodes MAY be" to "subcodes may be"

290 **Options:**

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

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

294 3.8 PE8: non-Normative Language

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

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

297 **Document:** Assertions and Protocols

298 **Description:** Line 967: change "to be found therein" to "will be included" .

299 Line 1219: Change "request. Top-most" to "request. The top-most"

300 Line 1417: Change "REQUIRES" to "requires"

301 **Options:**

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

304 3.9 PE9: Reference to AuthorityKind

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

315 **Options:**

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

319 **3.10 PE10: Guidance on Element <RespondWith>**

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

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

322 **Document:** Assertions and Protocols

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

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

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

338 **3.11 PE11: Processing rules for AssertionIDReference**

339 **First reported by:** Rob Philpott

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

341 **Document:** Assertions and Protocols

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

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

353 3. Requests for Assertions by Reference

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

356 3. Element <AssertionArtifact>

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

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

364 3.12 PE12: Miscellaneous additions and clarifications

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

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

367 **Document:** Assertions and Protocols

368 **Description:**

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

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

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

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

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

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

382 3.13 PE13: Miscellaneous additions and clarifications

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

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

385 **Document:** Assertions and Protocols

386 **Description:**

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

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

393 **Options:**

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

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

398 **3.14 PE14: Requestor vs. Requester and glossary definition for** 399 **Responder**

400 **First reported by:** Rob Philpott

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

402 **Document:** Assertions and Protocols

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

410

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

413

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

417 **Options:**

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

420 Also reviewed SOAP definitions for “Requester” and “Responder” and modified as appropriate.

421 **Incorporated in Draft 01 of SAML 1.1 Glossary**

422 **3.15 PE15: Browser POST profile does not explicitly call out** 423 **encoding**

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

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

426 **Document:** Bindings and Profiles

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

433 **Options:**

434 1. Explicitly call-out UTF-8 encoding

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

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

442 The notation B64(<response>) stands for the result of applying the Base64 Content-
443 Transfer-Encoding to the response, as defined by RFC 1521, section 5.2, and SHOULD

444 consist of lines of encoded data of up to 76 characters. The first encoded line begins after
445 the opening quote signifying the “value” attribute of the SAMLResponse form element.

446 The character set used to represent the encoded data is determined by the “charset”
447 attribute of the Content-Type of the HTML document containing the form. The character
448 set of the XML document resulting from decoding the data is determined in the normal
449 fashion, and defaults to UTF-8 if no character set is indicated.

450

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

454 **3.16 PE16: Use of Qnames in <AuthorityKind> and** 455 **<RespondWith>**

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

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

458 **Document:** Assertions and Protocols

459 **Description:** Near lines 716 (all line references in this message are to core 1.0) for
460 AuthorityKind, and 968 for RespondWith, the text gives an example of a Qname in use
461 and unfortunately implies (rather more strongly in the latter case) that the prefix must
462 read “saml” when a natively defined construct is being referenced. But the prefix of a
463 namespaced value is never fixed, and we don’t clarify that the appropriate namespace
464 must have been defined in the scope of the relevant element where the Qname appears.

465

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

468

469 For AuthorityKind: “For example, an attribute authority would be identified by
470 AuthorityKind=”samlp:AttributeQuery”, _where there is a namespace declaration in the
471 scope of this attribute that binds the samlp: prefix to the SAML protocol namespace_.”

472

473 For RespondWith: “For example, a requestor that wishes to receive assertions containing
474 only attribute statements _would_ [this was a lowercase “must”] specify
475 <RespondWith>saml:AttributeStatement</RespondWith>, _where the prefix is
476 bound to the SAML assertion namespace in a namespace declaration that is
477 in the scope of this element_.”

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

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

481 **3.17 PE17: Non-normative clarification of status code**

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

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

484 **Document:** Bindings and profiles

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

487 "In the case of a SAML processing error, the SOAP HTTP server MUST respond with "200 OK"
488 and include a SAML-specified error description as the only child of the <SOAP-ENV:Body>
489 element."
490
491 Should we be putting Major Version etc. attributes on StatusCode along with Assertion, Request,
492 and Response? If we did, we'd want to make them optional, with default values inherited from
493 the nearest SAML ancestor, if any.
494
495 **Options:** Add text to clarify that a Response is sent with the StatusCode.
496 **Disposition: 4/29/03 – Accepted text by Eve. Deprecated StatusCode as a top element in**
497 **SOAP response. StatusCode MUST be a child of <samlp:Response>. Incorporated in Draft**
498 **03 of Bindings and Profiles**

499 **3.18 PE18: SAML Versioning**

500 **First reported by:** Scott Cantor, Ohio State University and Internet 2
501 **Message:** <http://lists.oasis-open.org/archives/security-services/200304/msg00000.html>
502 **Document:** All documents
503 **Description:** The SAML specification is versioned in several, independent ways. This leads to
504 possible confusion. We should have a clear and consistent versioning specification.
505
506 **Options:** Specify a new SAML versioning as detailed in [http://lists.oasis-](http://lists.oasis-open.org/archives/security-services/200304/doc00000.doc)
507 [open.org/archives/security-services/200304/doc00000.doc](http://lists.oasis-open.org/archives/security-services/200304/doc00000.doc)
508 **Disposition: Accepted during TC meeting on April 15, 2003. Incorporated in Drafts 05 and**
509 **06 of SAML 1.1 Assertions and Protocols.**

510 **3.19 PE19: Clarification of status code for the case of no** 511 **assertion**

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

531 **3.20 PE20: Clarification of <ConfirmationData> in Browser/POST**

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

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

534 **Document:** Bindings and Profiles

535 **Description:** Section 4.1.2.5 states that:

536 The <saml:ConfirmationMethod> element of each assertion MUST be set to
537 urn:oasis:names:tc:SAML:1.0:cm:bearer. This absence of text regarding
538 <saml:confirmationData> may lead to confusion.

539 We should clarify as follows:

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

543

544 Additionally, section 4.1.1.6 should also be updated to reflect the same change for the
545 Browser/Artifact, as follows:

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

- 548 • The <saml:ConfirmationMethod> element MUST be set to either
549 urn:oasis:names:tc:SAML:1.0:cm:artifact-01 (deprecated) or
550 urn:oasis:names:tc:SAML:1.0:cm:artifact (RECOMMENDED).
- 551 • The <SubjectConfirmationData> element SHOULD NOT be specified.

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

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

555 **3.21 PE21: Description of the AuthenticationMethod attribute in** 556 **<AuthenticationQuery>**

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

558 **Message:** <http://lists.oasis-open.org/archives/security-services/200305/msg00104.html>

559 **Document:** Assertions and Protocols

560 **Description:** Draft 10 of Assertions and Protocols, lines 1114-1118 describing
561 AuthenticationQuery states:

562 "This element is of type **AuthenticationQueryType**, which extends **SubjectQueryAbstractType**
563 with the addition of the following element:

564 <AuthenticationMethod> [Optional]

565 A filter for possible responses. If it is present, the query made is "What assertions containing
566 authentication statements do you have for this subject with the supplied authentication method?"

567

568 Lines 1123-1125 state:

569 If the <AuthenticationMethod> element is present in the query, at least one
570 <AuthenticationMethod> element in the set of returned assertions MUST match. It is
571 OPTIONAL for the complete set of all such matching assertions to be returned in the response.

572

573 The problem is that the schema for AuthenticationQueryType defines "AuthenticationQuery" as
574 an XML attribute of type anyURI. It is not defined as an element.

575

576 **Options:**

577 1. Make editorial change to state that <AutenticationMethod> is an attribute not an element.

578 2. Make <AuthenticationMethod> an element and allow multiple occurrences of it in
579 <AuthenticationQuery>.

580

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

584 **3.22 PE22: Clarification of AuthenticationMethod attribute**

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

586 **Message:** <http://lists.oasis-open.org/archives/security-services/200305/msg00106.html>

587 **Document:** Assertions and Protocols

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

591 The AuthenticationMethod attribute of an <AuthenticationStatement> and the
592 <SubjectConfirmationMethod> element of a SAML subject perform different functions, although
593 both can refer to the same underlying mechanisms. An authentication statement with an
594 AuthenticationMethod attribute describes an authentication act that occurred in the past. The
595 AuthenticationMethod attribute indicates how that authentication was done. Note that the
596 authentication statement does not provide the means to perform that authentication, such as a
597 password, key, or certificate.

598 **Options:** Make editorial change.

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

601 **3.23 PE23: Clarification of <Statement>, <SubjectStatement> and** 602 **Nested Assertions**

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

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

605 **Document:** Assertions and Protocols

606 **Description:**

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

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

616 **Options:** Make editorial change.

617 **Disposition: During the SSTC conference call of 6/10, the co-chairs were directed to make**
618 **editorial changes to the document to clarify as suggested. These changes were made to**
619 **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
Draft 15	2003-08-19	Jahan Moreh	Added E10.

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
E10	Disposed	Assertions and Protocols	Final committee specs.
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

Appendix C. Notices

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

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

637 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]
638 2002 and 2003. All Rights Reserved.

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

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

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