



Issues List for Security Assertion Markup Language (SAML) V1.1

Working Draft 01, 25 June 2003

Document identifier:

sstc-saml-1.1-issues-draft-01

Location:

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

Editor:

Rob Philpott, RSA Security <rphilpott@rsasecurity.com>

Contributors:

Hal Lockhart, BEA Systems (former editor)

Abstract:

This document catalogs issues for the Security Assertions Markup Language (SAML) V1.1, developed by the OASIS Security Services Technical Committee. It lists those issues deferred during work on the SAML V1.0 standard and any new issues raised during the SAML V1.1 effort.

Status:

This document is a draft working document of the OASIS Security Services Technical Committee. This document is updated periodically on no particular schedule. Send comments to the editor.

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should subscribe to and send comments to the security-services-comment@lists.oasis-open.org list. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (<http://www.oasis-open.org/committees/security/>).

31 Table of Contents

32	Introduction	5
33	1.1 Notation	5
34	2 Use Case Issues	6
35	2.0 Group 0: Document Format & Strategy	6
36	2.1 Group 1: Single Sign-on Push and Pull Variations	6
37	2.1.1 ISSUE:[UC-1-05:FirstContact]	6
38	2.1.2 DEFERRED ISSUE:[UC-1-14: NoPassThruAuthnImpactsPEP2PDP]	6
39	2.2 Group 2: B2B Scenario Variations	7
40	2.2.1 DEFERRED ISSUE:[UC-2-05:EMarketplace]	7
41	2.3 Group 3: Sessions	7
42	2.3.1 DEFERRED ISSUE:[UC-3-01:UserSession]	7
43	2.3.2 DEFERRED ISSUE:[UC-3-02:ConversationSession]	8
44	2.3.3 DEFERRED ISSUE:[UC-3-03:Logout]	8
45	2.3.4 DEFERRED ISSUE:[UC-3-05:SessionTermination]	8
46	2.3.5 DEFERRED ISSUE:[UC-3-06:DestinationLogout]	9
47	2.3.6 DEFERRED ISSUE:[UC-3-07:Logout Extent]	9
48	2.3.7 DEFERRED ISSUE:[UC-3-08:DestinationSessionTermination]	9
49	2.3.8 DEFERRED ISSUE:[UC-3-09:Destination-Time-In]	10
50	2.4 Group 4: Security Services	10
51	2.5 Group 5: AuthN Protocols	10
52	2.5.1 DEFERRED ISSUE:[UC-5-02:SASL]	10
53	2.6 Group 6: Protocol Bindings	11
54	2.7 Group 7: Enveloping vs. Enveloped	11
55	2.8 Group 8: Intermediaries	11
56	2.8.1 DEFERRED ISSUE:[UC-8-02:IntermediaryAdd]	11
57	2.8.2 DEFERRED ISSUE:[UC-8-03:IntermediaryDelete]	11
58	2.8.3 DEFERRED ISSUE:[UC-8-04:IntermediaryEdit]	11
59	2.9 Group 9: Privacy	12
60	2.9.1 DEFERRED ISSUE:[UC-9-01:RuntimePrivacy]	12
61	2.10 Group 10: Framework	12
62	2.11 Group 11: AuthZ Use Case	12
63	2.12 Group 12: Encryption	13
64	2.12.1 DEFERRED ISSUE:[UC-12-04:EncryptionMethod]	13
65	2.13 Group 13: Business Requirements	13
66	2.13.1 DEFERRED ISSUE [UC-13-07: Hailstorm Interoperability]	13
67	2.14 Group 14: Domain Model	13
68	2.14.1 DEFERRED ISSUE:[UC-14-01:UMLCardinalities]	13
69	3 Design Issues	15
70	3.1 Group 1: Naming Subjects	15
71	3.1.1 DEFERRED ISSUE:[DS-1-02: Anonymity Technique]	15

72	3.2 Group 2: Naming Objects.....	15
73	3.3 Group 3: Assertion Validity.....	15
74	3.3.1 CLOSED ISSUE:[DS-3-01: DoNotCache]	15
75	3.4 Group 4: Assertion Style	16
76	3.4.1 DEFERRED ISSUE:[DS-4-06: Final Types]	16
77	3.4.2 DEFERRED ISSUE:[DS-4-15: Common XML Attributes]	16
78	3.5 Group 5: Reference Other Assertions.....	16
79	3.5.1 DEFERRED ISSUE:[DS-5-01: Dependency Audit]	16
80	3.6 Group 6: Attributes	17
81	3.6.1 DEFERRED ISSUE:[DS-6-01: Nested Attributes]	17
82	3.6.2 DEFERRED ISSUE:[DS-6-04: Negative Roles]	17
83	3.7 Group 7: Authentication Assertions.....	18
84	3.7.1 DEFERRED ISSUE:[DS-7-06: DiscoverAuthNProtocols].....	18
85	3.8 Group 8: Authorities and Domains	18
86	3.9 Group 9: Request Handling.....	18
87	3.9.1 DEFERRED ISSUE:[DS-9-02: MultipleRequest]	18
88	3.9.2 DEFERRED ISSUE:[DS-9-03: IDandAttribQuery]	19
89	3.9.3 DEFERRED ISSUE:[DS-9-05: RequestAttributes]	19
90	3.10 Group 10: Assertion Binding	19
91	3.11 Group 11: Authorization Decision Assertions	19
92	3.11.1 DEFERRED ISSUE:[DS-11-01: MultipleSubjectAssertions]	19
93	3.12 Group 12: Attribute Assertions	20
94	3.12.1 DEFERRED ISSUE:[DS-12-03: AttrSchemaReqs]	20
95	3.12.2 DEFERRED ISSUE:[DS-12-04: AttrNameReqs]	20
96	3.12.3 DEFERRED ISSUE:[DS-12-08: Delegation]	21
97	3.13 Group 13: Dynamic Sessions.....	21
98	3.13.1 DEFERRED ISSUE:[DS-13-01: SessionsinEffect]	21
99	3.14 Group 14:General – Multiple Message Types	21
100	3.14.1 DEFERRED ISSUE:[DS-14-04: Aggregation]	21
101	3.14.2 DEFERRED ISSUE:[DS-14-14: ErrMsg in Multiple Languages].....	22
102	3.14.3 CLOSED ISSUE:[DS-14-15: Version Synchronization].....	24
103	3.14.4 DEFERRED ISSUE:[DS-14-16: Version Positive].....	25
104	3.15 Group 15: Elements Expressing Time Instants.....	25
105	4 Miscellaneous Issues.....	26
106	4.1 Group 1: Terminology	26
107	4.2 Group 2: Administrative.....	26
108	4.3 Group 3: Conformance.....	26
109	4.4 Group 4: XMLDSIG	26
110	4.5 Group 5: Bindings.....	26
111	4.5.1 DEFERRED ISSUE:[MS-5-08: Publish WSDL]	26
112	5 References.....	27
113	5.1 Normative	27
114	Appendix A. Acknowledgments	28

115 Appendix B. Revision History 29
116 Appendix C. Notices 30
117

118 Introduction

119 This document describes all issues deferred during work on the SAML V1.0 standard and any
120 new issues that were raised during the SAML V1.1 effort. These issues have been raised on the
121 SSTC mailing lists, in conference calls, and in other venues. The SAML V1.0 issues list is
122 available at [ISSUES-1.0]. All issues in this document are deferred or closed. All deferred issues
123 will be reviewed during the SAML V2.0 effort.

124 1.1 Notation

125 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”,
126 “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be
127 interpreted as described in [RFC2119].

128 Each issue includes the following information:

- 129 • **ISSUE:** [Category-Issue Number: Short name]
- 130 • **Source:** Location where the issue was initially raised (e.g. V1.0 Deferred Issue)
- 131 • **Champion:** None
- 132 • **Status:** Date - Decision
- 133 • **Description:** Long description of the issue
- 134 • **Resolution Alternatives:** With optional editor resolution

135 The following “Category” codes are defined for the issues:

- 136 • UC – Use Case issues
- 137 • DS – Design issues
- 138 • MS – Miscellaneous issues

139 The issues within each category are grouped according to general areas of concern. The "Issue
140 Number" is thus specified as "group-*nn*", where “group” identifies the area group, and “*nn*” is the
141 issue # within the group. To avoid reusing issue numbers from V1.0 issues that were closed and
142 thus don't appear in this document, the highest issue number used within each group in the V1.0
143 Issues List [ISSUES-1.0] is listed at the beginning of the group section in this document.

144 To make reading this document easier, the following convention has been adopted for shading
145 sections in various colors. Modified text in updated sections of the current document revision is
146 displayed in **red font**.

147 Gray sections indicate issues closed or deferred in previous revisions of this document.

148 Blue sections indicate issues closed or deferred in the current revision of this document.

149 Yellow sections indicate issues recently created or modified or that are actively being
150 debated.

151 Other open issues are not marked, i.e. left white.

152 2 Use Case Issues

153 2.0 Group 0: Document Format & Strategy

154 **Highest V1.0 Issue Number:** UC-0-03

155 No deferred or new issues.

156 2.1 Group 1: Single Sign-on Push and Pull Variations

157 **Highest V1.0 Issue Number:** UC-1-14

158 2.1.1 ISSUE:[UC-1-05:FirstContact]

159 **Source:** V1.0 Deferred Issue

160 **Champion:** None

161 **Status:** 25-Jun-2003 – Propose closing this issue.

162 **Status:** 29-Jan-2002 – Deferred by vote. Discussions at F2F#4 established that SAML 1.0
163 partially meets this requirement, but does not provide everything TC members could envisage.

164 **Status:** F2F #2 – Closed by explicit vote, Option 2 carries, however see UC-1-14

165 **Description:** A variation on the single sign on use case that has been proposed is one where the
166 Web user goes directly to the destination Web site without authenticating with a definitive
167 authority first.

168 [25-Jun-2003] Destination Site First use cases were again explored during V1.1. The Liberty
169 Alliance's Liberty 1.1 ID Federation Framework provides use cases for this area. Now that the
170 Liberty 1.1 ID-FF specifications have been contributed to the SSTC for our V2.0 effort, the
171 committee should use the Liberty use cases and thus this issue can be closed.

172 [Text Removed to Archive]

173 **Resolution Alternatives:**

- 174 1. Add this use case scenario to the use case document.
175 2. Do not add this use case scenario to the use case document.
176 3. Address this issue using the Liberty use cases.

177 2.1.2 DEFERRED ISSUE:[UC-1-14: 178 NoPassThruAuthnImpactsPEP2PDP]

179 **Source:** V1.0 Deferred Issue

180 **Champion:** None

181 **Status:** 5-Feb-2002 – Deferred by vote – Previously closed on 15-May-2002 telcon. Option 2
182 carries

183 **Description:** Stephen Farrell has argued that dropping PassThruAuthN prevents standardization
184 of important functionality in a commonly used configuration.

185 The counter argument is the technical difficulty of implementing this capability, especially when
186 both username/password and PKI AuthN must be supported.

187 **Resolution Alternatives:**

- 188 1. Add this requirement to SAML 1.0
189 2. authorize a subgroup/task force to evaluate a suitable pass-through authN solution for
190 eventual inclusion in V.next of SAML. If the TC likes the design once it is presented, it
191 may choose to open up its scope to once again include pass-through authN in V1.0.
192 Stephen is willing to champion this."
193 3. Do not add this requirement.

194 2.2 Group 2: B2B Scenario Variations

195 **Highest V1.0 Issue Number:** UC-2-08

196 2.2.1 DEFERRED ISSUE:[UC-2-05:EMarketplace]

197 **Source:** V1.0 Deferred Issue

198 **Champion:** None

199 **Status:** 29-Jan-2002 – Deferred by vote. This functionality is not directly supported by SAML 1.0
200 Bindings and Profiles, but could be constructed using the current core.

201 **Description:** Zahid Ahmed proposes the following additional use case scenario for inclusion in
202 the use case and requirements document.

203 Scenario X: E-Marketplace

204 **[Text Removed to Archive]**

205 **Resolution Alternatives:**

- 206 1. The above scenario should be added to the use cases document.
207 2. The above scenario should not be added to the document.

208 2.3 Group 3: Sessions

209 **Highest V1.0 Issue Number:** UC-3-09

210 [At F2F #2, it was agreed to charter a sub group to “do the prep work to ensure that logout,
211 timeout, and timeout will not be precluded from working with SAML later; commit to doing these
212 other pieces "next" after 1.0.” Therefore all the items in this section have been closed with the
213 notation “referred to sub group.”]

214 [25-Jun-2003] Some of the session requirements discussed in this group have been addressed
215 by the Liberty Alliance’s Liberty 1.1 ID Federation Framework. Now that the Liberty 1.1 ID-FF
216 specifications have been contributed to the SSTC for our V2.0 effort, the committee should
217 determine whether these issues need to be carried forward to V2.0.

218 The purpose of the issues/resolutions in this group is to provide guidance to the rest of the TC as
219 to the functionality required related to sessions. Some of the scenarios contain some detail about
220 the messages which are transferred between parties, but the intention is not to require a
221 particular protocol. Instead, these details are offered as a way of describing the functionality
222 required. It would be perfectly acceptable if the resulting specification used different messages to
223 accomplish the same functionality.

224 2.3.1 DEFERRED ISSUE:[UC-3-01:UserSession]

225 **Source:** V1.0 Deferred Issue

226 **Champion:** None

227 **Status:** 5-Feb-2002 – Deferred by vote.

228 **Description:** Should the use cases of log-off and timeout be supported

229 [Text Removed to Archive].

230 **Resolution Alternatives:**

231 1. Add this requirement and/or use cases to SAML.

232 2. Do not add this requirement and/or use cases.

233 **2.3.2 DEFERRED ISSUE:[UC-3-02:ConversationSession]**

234 **Source:** V1.0 Deferred Issue

235 **Champion:** None

236 **Status:** 5-Feb-2002 – Deferred by vote.

237 **Description:** Is the concept of a session between security authorities separate from the concept
238 of a user session? If so, should use case scenarios or requirements supporting security system
239 sessions be supported? [DavidO: I don't understand this issue, but I have left in for backwards
240 compatibility]. [DarrenP: I think this issue arose out of a misunderstanding/miscommunication on
241 the mailing list and has been resolved. This is more of a formality to vote this one to a closed
242 status.]

243 **Resolution Alternatives:**

244 1. Do not pursue this requirement as it is not in scope.

245 2. Do further analysis on this requirement to determine what it is specifically.

246 **2.3.3 DEFERRED ISSUE:[UC-3-03:Logout]**

247 **Source:** V1.0 Deferred Issue

248 **Champion:** None

249 **Status:** 5-Feb-2002 – Deferred by vote.

250 **Description:** Should SAML support transfer of information about application-level logouts (e.g., a
251 principal intentionally ending a session) from the application to the Session Authority ?

252 **Candidate Requirement:**

253 [CR-3-3-Logout] SAML shall support a message format to indicate the end of an
254 application-level session due to logout by the principal.

255 Note that this requirement is implied by Scenario 1-3 (the second scenario 1-3 in straw man 3 -
256 oops). This issue seeks to clarify the document by making the requirement explicit.

257 **Resolution Alternatives:**

258 1. Add this requirement to SAML.

259 2. Do not add this requirement to SAML.

260 **2.3.4 DEFERRED ISSUE:[UC-3-05:SessionTermination]**

261 **Source:** V1.0 Deferred Issue

262 **Champion:** None

263 **Status:** 5-Feb-2002 – Deferred by vote.

264 **Description:** For managing a SAML User Sessions, it may be useful to have a way to indicate
265 that the SAML-level session is no longer valid. The logout requirement would invalidate a session
266 based on user input. This requirement, for termination, would invalidate the SAML-level session
267 based on other factors, such as when the user has not used any of the SAML-level sessions

268 constituent application- level sessions for more than a set amount of time. Timeout would be an
269 example of a session termination.

270 Candidate requirement:

271 [CR-3-5-SessionTermination] SAML shall support a message format for timeout
272 of a SAML-level session. Here, "termination" is defined as the ending of a
273 SAML-level session by a security system not based on user input. For example, if
274 the user has not used any of the application-level sub-sessions for a set amount of
275 time, the session may be considered "timed out."

276 Note that this requirement is implied by Scenario 1-3, figure 6, specifically the last message
277 labeled 'optionally delete/revoke session'. This issue seeks to clarify the document by making the
278 requirement explicit.

279 **Resolution Alternatives:**

- 280 1. Add this requirement to SAML.
- 281 2. Do not add this requirement and/or use cases.

282 **2.3.5 DEFERRED ISSUE:[UC-3-06:DestinationLogout]**

283 **Source:** V1.0 Deferred Issue

284 **Champion:** None

285 **Status:** 5-Feb-2002 – Deferred by vote.

286 **Description:** Should logging out of an individual application-level session be supported?
287 Advantage: allows application Web sites control over their local domain consistent with the model
288 most widely implemented on the web. Disadvantage: potentially more interactions between the
289 application and the Session Authority.

290 **[Text Removed to Archive]**

291 **Resolution Alternatives:**

- 292 1. Add this scenario and requirement to SAML.
- 293 2. Do not add this scenario or requirement.

294 **2.3.6 DEFERRED ISSUE:[UC-3-07:Logout Extent]**

295 **Source:** V1.0 Deferred Issue

296 **Champion:** None

297 **Status:** 5-Feb-2002 – Deferred by vote.

298 **Description:** What is the impact of logging out at a destination web site?

299 **Possible Resolution:**

- 300 1. Logout from destination web site is local to destination [DavidO recommendation]
- 301 2. Logout from destination web site is global, that is destination + source web sites.

302 **2.3.7 DEFERRED ISSUE:[UC-3-08:DestinationSessionTermination]**

303 **Source:** V1.0 Deferred Issue

304 **Champion:** None

305 **Status:** 5-Feb-2002 – Deferred by vote.

306 **Description:** Having the Session Authority determine the timeout of a session is covered under
307 [UC-3-5]. This issue covers the manner and extent to which systems participating in that session
308 can initiate and control the timeout of their own sessions.

309 **[Text Removed to Archive].**

310 **Resolution Alternatives:**

- 311 1. Add this scenario and requirement to SAML.
312 2. Do not add this scenario or requirement.

313 **2.3.8 DEFERRED ISSUE:[UC-3-09:Destination-Time-In]**

314 **Source:** V1.0 Deferred Issue

315 **Champion:** None

316 **Status:** 5-Feb-2002 – Deferred by vote.

317 **Description:** In this scenario, a user has traveled from the source site (site of initial login) to
318 some destination site. The source site has set a maximum idle-time limit for the user session,
319 based on user activity at the source or destination site. The user stays at the destination site for a
320 period longer than the source site idle-time limit; and at that point the user returns to the source
321 site. We do not wish to have the user time-out at the source site and be re-challenged for
322 authentication; instead, the user should continue to enjoy the original session which would
323 somehow be cognizant of user activity at the destination site.

324 **Candidate Requirement:**

325 **[CR-3-9:Destination-TimeIn]** SAML shall support destination system time-in.

326 **Resolution Alternatives:**

- 327 1. Add this scenario and requirement to SAML.
328 2. Do not add this scenario or requirement to SAML.

329 **2.4 Group 4: Security Services**

330 **Highest V1.0 Issue Number:** UC-4-04

331 No deferred or new issues.

332 **2.5 Group 5: AuthN Protocols**

333 **Highest V1.0 Issue Number:** UC-5-03

334 **2.5.1 DEFERRED ISSUE:[UC-5-02:SASL]**

335 **Source:** V1.0 Deferred Issue

336 **Champion:** None

337 **Status:** 5-Feb-2002 – Deferred by vote. Was previously closed per F2F #2, Option 2 carries.

338 **Description:** Is there a need to develop materials within SAML that explore its relationship to
339 SASL [SASL]?

340 **Resolution Alternatives:**

- 341 1. Yes
342 2. No

343 **2.6 Group 6: Protocol Bindings**

344 **Highest V1.0 Issue Number:** UC-6-01

345 No deferred or new issues.

346 **2.7 Group 7: Enveloping vs. Enveloped**

347 **Highest V1.0 Issue Number:** UC-7-02

348 No deferred or new issues.

349 **2.8 Group 8: Intermediaries**

350 **Highest V1.0 Issue Number:** UC-8-05

351 **2.8.1 DEFERRED ISSUE:[UC-8-02:IntermediaryAdd]**

352 **Source:** V1.0 Deferred Issue

353 **Champion:** None

354 **Status:** 29-Jan-2002 – Deferred by vote. There is no support for intermediaries in SAML 1.0. In
355 fact, the SOAP Profile was defined to explicitly omit interactions among more than two parties.

356 **Description:** One question that has been raised is whether intermediaries can make additions to
357 SAML documents. It is possible that intermediaries could add data to assertions, or add new
358 assertions that are bound to the original assertions.

359 **[Text Removed to Archive]**

360 **Resolution Alternatives:**

361 1. Add this use-case scenario to the document.

362 2. Don't add this use-case scenario.

363 **2.8.2 DEFERRED ISSUE:[UC-8-03:IntermediaryDelete]**

364 **Source:** V1.0 Deferred Issue

365 **Champion:** None

366 **Status:** 29-Jan-2002 – Deferred by vote. There is no support for intermediaries in SAML 1.0. In
367 fact, the SOAP Profile was defined to explicitly omit interactions among more than two parties.

368 **Description:** Another issue with intermediaries is whether SAML must support allowing
369 intermediaries to delete data from SAML documents.

370 **[Text Removed to Archive]**

371 **Resolution Alternatives:**

372 1. Add this use-case scenario to the document.

373 2. Don't add this use-case scenario.

374 **2.8.3 DEFERRED ISSUE:[UC-8-04:IntermediaryEdit]**

375 **Source:** V1.0 Deferred Issue

376 **Champion:** None

377 **Status:** 29-Jan-2002 – Deferred by vote. There is no support for intermediaries in SAML 1.0. In
378 fact, the SOAP Profile was defined to explicitly omit interactions among more than two parties.

379 **Description:** Similar to [UC-8-03:IntermediaryDelete] is the issue of whether SAML must support
380 allowing intermediaries to edit or change SAML data as they pass it between parties.

381 **[Text Removed to Archive]**

382 **Resolution Alternatives:**

383 1. Add this use-case scenario to the document.

384 2. Don't add this use-case scenario.

385 **2.9 Group 9: Privacy**

386 **Highest V1.0 Issue Number:** UC-9-02

387 **2.9.1 DEFERRED ISSUE:[UC-9-01:RuntimePrivacy]**

388 **Source:** V1.0 Deferred Issue

389 **Champion:** None

390 **Status:** 29-Jan-2002 – Deferred by vote.

391 **Description:** Should protecting the privacy of the user be part of the SAML conversation? In
392 other words, should user consent to exchange of data be given at run time, or at the time the user
393 establishes a relationship with a security system?

394 An example of runtime privacy configuration would be use case scenario described in [UC-1-
395 04:ARundgrenPush]. Because this scenario has been rejected by the use cases and requirement
396 group, it makes sense to phrase this as a non-goal of SAML, rather than as a requirement.

397 [CR-9-01:RuntimePrivacy] SAML does not provide for subject control of data
398 flow (privacy) at run-time. The determination of privacy policy is between the
399 subject and security authorities and should be determined out-of-band, for
400 example, in a privacy agreement.

401 **Resolution Alternatives:**

402 1. Add this proposed non-goal.

403 2. Do not add this proposed non-goal.

404 **Voting Results:**

Date	27 Mar 2001
Eligible	15
Resolution 1	9
Resolution 2	4

405 **2.10 Group 10: Framework**

406 **Highest V1.0 Issue Number:** UC-10-07

407 No deferred or new issues.

408 **2.11 Group 11: AuthZ Use Case**

409 **Highest V1.0 Issue Number:** UC-11-01

410 No deferred or new issues.

sstc-saml-1.1-issues-draft-01
Copyright © OASIS Open 2003. All Rights Reserved.

Colors: Gray Blue Yellow

411 2.12 Group 12: Encryption

412 Highest V1.0 Issue Number: UC-12-04

413 2.12.1 DEFERRED ISSUE:[UC-12-04:EncryptionMethod]

414 **Source:** V1.0 Deferred Issue

415 **Champion:** None

416 **Status:** 5-Feb-2002 – Deferred by vote. Previously closed per F2F #2, Resolution 3 Carries

417 **Description:** If confidentiality protection is included in the SAML assertion format (that is, you
418 chose option 1 or 2 for [UC-12-02:AssertionConfidentiality]), how should the protection be
419 provided?

420 Note that if option 2 (assertion confidentiality is required) was chosen for UC-12-02, resolution 1
421 of this issue implies that SAML will not be published until after XML Encryption is published.

422 **Resolution Alternatives:**

- 423
- 424 1. Add the requirement: [R-EncryptionMethod] SAML should use XML Encryption.
 - 425 2. Add the requirement: [R-EncryptionMethod] Because there is no currently published
426 standard for encrypting XML, SAML should define its own encryption format. Edit the
existing non-goal of not creating new cryptographic techniques to allow this.
 - 427 3. Add no requirement now, but include a note that this issue must be revisited in a future
428 version of the SAML spec after XML Encryption is published.
 - 429 4. Do not add any of these requirements or notes.

430 2.13 Group 13: Business Requirements

431 Highest V1.0 Issue Number: UC-13-07

432 2.13.1 DEFERRED ISSUE [UC-13-07: Hailstorm Interoperability]

433 **Source:** V1.0 Deferred Issue

434 **Champion:** None

435 **Status:** 29-Jan-2002 – Deferred by vote.

436 **Description:** Should SAML provide interoperability with the Microsoft Hailstorm architecture,
437 including the Passport login system?

438 **Resolution Alternatives:** ???

439 2.14 Group 14: Domain Model

440 Highest V1.0 Issue Number: UC-14-01

441 2.14.1 DEFERRED ISSUE:[UC-14-01:UMLCardinalities]

442 **Source:** V1.0 Deferred Issue

443 **Champion:** None

444 **Status:** 29-Jan-2002 – Deferred by vote.

445 **Description:** The cardinalities in the UML diagrams in the Domain Model are backwards.

446 Frank Seliger comments: The Domain model claims to use the UML notation, but has the
447 multiplicities according to the Coad method. If it were UML, the diagram would state that one
448 Credential could belong to many Principals. I assume that we would rather want to state that one

449 Principal can have many Credentials, similarly for System Entity, the generalization of User. One
450 Principal would belong to several System Entities or Users according to the diagram. I would
451 rather think we want one System Entity or User to have several Principals.

452 My theory how these wrong multiplicities happened is the following: As I can see from the change
453 history, the tool Together has been used to create the initial version of this diagram. Together in
454 its first version used only the Peter Coad notation. Later versions still offered the Coad notation
455 as default. Peter Coad had the cardinalities (UML calls this multiplicities) just swapped compared
456 to the rest of the world. This always caused grief, and it did again here.

457 Dave Orchard agrees this should be fixed.

458 **Resolution Alternatives: ???**

459 3 Design Issues

460 3.1 Group 1: Naming Subjects

461 Highest V1.0 Issue Number: DS-1-13

462 3.1.1 DEFERRED ISSUE:[DS-1-02: Anonymity Technique]

463 Source: V1.0 Deferred Issue

464 Champion: None

465 Status: 29-Jan-2002 – Deferred by vote.

466 Description: How should the requirement of Anonymity of SAML assertions be met?

467 Resolution Alternatives:

- 468 1. Generate a new, random identified to refer to an individual for the lifetime of a session.
469 2. ???

470 3.2 Group 2: Naming Objects

471 Highest V1.0 Issue Number: DS-2-02

472 No deferred or new issues.

473 3.3 Group 3: Assertion Validity

474 Highest V1.0 Issue Number: DS-3-03

475 3.3.1 CLOSED ISSUE:[DS-3-01: DoNotCache]

476 Source: V1.0 Deferred Issue

477 Champion: Hal Lockhart

478 Status: 25-Jun-2003 – This issue was resolved in V1.1 and Resolution Alternative 2 was
479 implemented.

480 Status: 29-Jan-2002 – Deferred by vote.

481 Description: It has been suggested that there should be a way in SAML to specify that an
482 assertion is currently valid, but should not be cached for later use. This should not depend on the
483 particular amount of variation between clocks in the network.

484 For example, a PDP may wish to indicate to a PEP that it should make a new request for every
485 authorization decision. For example, its policy may be subject to change at frequent and
486 unpredictable intervals. It would be desirable to have a SAML specified convention for doing this.
487 This may interact with the position taken on clock skew. For example, if SAML takes no position
488 on clock skew the PDP may have to set the NotAfter value to some time in the future to insure
489 that it is not considered expired by the PEP.

490 Resolution Alternatives:

- 491 1. SAML will specify some combination of settings of the IssueInstant and ValidityInterval to
492 mean that the assertion should not be cached. For example, setting all three datetime
493 fields to the same value could be deemed indicate this.

- 494 2. SAML will add an additional element to either Assertions or Responses to indicate the
495 assertion should not be cached.
496 3. SAML will provide no way to indicate that an Assertion should not be cached.

497 3.4 Group 4: Assertion Style

498 **Highest V1.0 Issue Number:** DS-4-15

499 3.4.1 DEFERRED ISSUE:[DS-4-06: Final Types]

500 **Source:** V1.0 Deferred Issue

501 **Champion:** None

502 **Status:** 5-Feb-2002 – Deferred by vote. Was previously closed by vote on Sept 4. The Schema
503 recommendations proposed by Eve and Phill at F2F#4 have been accepted.

504 **Description:** Does the TC plan to restrict certain types in the SAML schema to be final? If so,
505 which types are to be so restricted?

506 This was identified as CONS-03.

507 **Resolution Alternatives:** ???

508 3.4.2 DEFERRED ISSUE:[DS-4-15: Common XML Attributes]

509 **Source:** V1.0 Deferred Issue

510 **Champion:** Eve Maler

511 **Status:** 19-Mar-2002 – Deferred by vote.

512 **Description:** Factor out various common XML attributes used in various places. This is ELM-1 in:
513 <http://lists.oasis-open.org/archives/security-services/200203/msg00042.html>

514 **Resolution Alternatives:** ???

515 3.5 Group 5: Reference Other Assertions

516 **Highest V1.0 Issue Number:** DS-5-04

517 3.5.1 DEFERRED ISSUE:[DS-5-01: Dependency Audit]

518 **Source:** V1.0 Deferred Issue

519 **Champion:** None

520 **Status:** 29-Jan-2002 – Deferred by vote.

521 **Description:** One issue with draft-sstc-core-07.doc is a lack of support for audit of assertion
522 dependency between co-operating authorities. As one explicit goal of SAML was to support inter-
523 domain security (i.e., each authority may be administered by a separate business entity) this
524 seems to be a serious "gap" in reaching that goal.

525 Consider the following example:

526 (1) User Ravi authenticates in his native security domain and receives

527 Assertion A:

528 <Assertion>

529 <AssertionID><http://www.small-company.com/A></AssertionID>

530 <Issuer>URN:small-company:DivisionB</Issuer>

531 <ValidityInterval> . . . </ValidityInterval>


```
532 <Claims>
533 <subject>"cn=ravi, ou=finance, id=325619"</subject>
534 <attribute>manager</attribute>
535 </Claims>
536 </Assertion>
```

537 (2) User Ravi authenticates to the Widget Marketplace using assertion A and based on the policy:

538 All entities with "ou=finance" authenticated thru small-company.com with attribute
539 manager have purchase limit \$100,000 receives Assertion B from the Widget Marketplace:

```
540 <Assertion>
541 <AssertionID>http://www.WidgetMarket.com/B<AssertionID>
542 <Issuer>URN:WidgetMarket:PartsExchange</Issuer>
543 <ValidityInterval>. . . </ValidityInterval>
544 <Claims>
545 <subject>"cn=ravi, ou=finance, id=325619"</subject>
546 <attribute>max-purchase-limit-$100,000</attribute>
547 </Claims>
548 </Assertion>
```

549 (3) User Ravi purchases farm machinery from a parts provider hosted at the Widget Marketplace.
550 The parts provider authorizes the transaction based on Assertion B.

551 Even though Assertion B has been issued by the Widget Marketplace in response to assertion A
552 (I guess another way to look at this to view assertion A as the subject of B as in [1]) there is no
553 way to represent this information within SAML.

554 If there is a problem with Ravi's purchases at the Widget Marketplace (Ravi wont pay his bills)
555 there is nothing in the SAML flow that ties Assertion B to Assertion A. This appears to be a
556 significant missing piece to me.

557 **Resolution Alternatives: ???**

558 3.6 Group 6: Attributes

559 **Highest V1.0 Issue Number:** DS-6-06

560 3.6.1 DEFERRED ISSUE:[DS-6-01: Nested Attributes]

561 **Source:** V1.0 Deferred Issue

562 **Champion:** None

563 **Status:** 29-Jan-2002 – Deferred by vote.

564 **Description:** Should SAML support nested attributes? This means that for example, a role could
565 be a member of another role. This is one standard way of distinguishing the semantics of roles
566 from groups.

567 There are many issues of semantics and pragmatics related to this. These include:

- 568 1. Limit of levels if any
- 569 2. Circular references
- 570 3. Distributed definition
- 571 4. Mixed attribute types.

572 **Resolution Alternatives: ???**

573 3.6.2 DEFERRED ISSUE:[DS-6-04: Negative Roles]

574 **Source:** V1.0 Deferred Issue

575 **Champion:** None
576 **Status:** 29-Jan-2002 – Deferred by vote.
577 **Description:** Should there be a way to state that someone does not have a role?
578 **Resolution Alternatives:** ???

3.7 Group 7: Authentication Assertions

580 **Highest V1.0 Issue Number:** DS-7-06

3.7.1 DEFERRED ISSUE:[DS-7-06: DiscoverAuthNProtocols]

582 **Source:** V1.0 Deferred Issue
583 **Champion:** None
584 **Status:** 29-Jan-2002 – Deferred by vote.
585 **Description:** Should SAML provide a means to discover supported types of AuthN protocols?
586 Simon Godik has suggested: One way to do it is to use AuthenticationQuery with empty
587 Authenticator subject. Then SAMLRequest will carry AuthenticationAssertion with Authenticator
588 subject listing acceptable protocols.
589 The problem is that Authenticator element does not allow for 0 occurrences of Protocol.
590 Should we specify minOccurs=0 on Protocol element for that purpose?
591 **Resolution Alternatives:**

1. Declare AuthN Protocol discovery out of scope for SAML V1.0.
2. Support it in the way suggested.
3. Support it some other way.

3.8 Group 8: Authorities and Domains

596 **Highest V1.0 Issue Number:** DS-8-06
597 No deferred or new issues.

3.9 Group 9: Request Handling

599 **Highest V1.0 Issue Number:** DS-9-16

3.9.1 DEFERRED ISSUE:[DS-9-02: MultipleRequest]

601 **Source:** V1.0 Deferred Issue
602 **Champion:** None
603 **Status:** 29-Jan-2002 – Deferred by vote.
604 **Description:** Should SAML provide a means of requesting multiple assertion types in a single
605 request? This has been referred to as “boxcaring.” In simplest form this could consist of
606 concatenating several defined requests one message. However there are usecases in which it
607 would convenient to have the second request use data from the results of the first.
608 For example, it would be useful to ask for an AuthN Assertion by ID and for and Attribute
609 Assertion referring to the same subject.
610 **Resolution Alternatives:**

1. Do not specify a way to make requests for multiple assertions types in SAML V1.0.

- 612 2. Allow simple concatenation of requests in one message.
613 3. Provide a more general scheme for multiple requests.

614 **3.9.2 DEFERRED ISSUE:[DS-9-03: IDandAttribQuery]**

615 **Source:** V1.0 Deferred Issue

616 **Champion:** None

617 **Status:** 29-Jan-2002 – Deferred by vote.

618 **Description:** Should SAML allow queries containing both an Assertion ID and Attributes?

619 Tim Moses comments: The need to convey an assertion id and attributes in the same query
620 arises in the following circumstances.

621 **[Text Removed to Archive]**

622 **Resolution Alternatives:**

- 623 1. Allow queries to specify both an Assertion ID and Attributes
624 2. Only allow queries to specify one or the other.

625 **3.9.3 DEFERRED ISSUE:[DS-9-05: RequestAttributes]**

626 **Source:** V1.0 Deferred Issue

627 **Champion:** Simon Godik

628 **Status:** 12-Mar-2002 – Deferred by vote.

629 **Description:** We should be able to pass request attributes to the issuing party.

630 I would like to propose addition to the RequestType:

```
631 <complexType name="RequestType">
632   <complexContent>
633     <extension base="samlp:RequestAbstractType">
634       <sequence>
635         <element ref="saml:Attribute" minOccurs="0" maxOccurs="unbounded"/>
636         <choice>
637           -- same as before --
638         </choice>
639       </sequence>
640     </extension>
641   </complexContent>
642 </complexType>
```

643 **Resolution Alternatives:** ???

644 **3.10 Group 10: Assertion Binding**

645 **Highest V1.0 Issue Number:** DS-10-01

646 No deferred or new issues.

647 **3.11 Group 11: Authorization Decision Assertions**

648 **Highest V1.0 Issue Number:** DS-11-08

649 **3.11.1 DEFERRED ISSUE:[DS-11-01: MultipleSubjectAssertions]**

650 **Source:** V1.0 Deferred Issue

651 **Champion:** None
652 **Status:** 29-Jan-2002 – Deferred by vote.
653 **Description:** It has been proposed (WhiteboardTranscription-01.pdf section 4.0) that an
654 Authorization Decision Assertion Request (and presumably the Assertion sent in response) may
655 contain multiple subject Assertions (or their Ids). Must these assertions all refer to the same
656 subject or may they refer to multiple subjects.
657 One view is that the assertions all provide evidence about a single subject who has requested
658 access to a resource. For example, the request might include a Authentication Assertion and one
659 or more Attribute Assertions about the same person.
660 Another view is that for efficiency or other reasons it is desirable to ask about access to a
661 resource by multiple individuals in a single request. This raises the question of how the PDP
662 should respond if some subjects are allowed and others are not.
663 The PDP might have the freedom to return a single, all encompassing Assertion in response or
664 reduce the request in order to give a positive response or return multiple Assertions with positive
665 and negative indications.
666 Identified as F2F#3-30 and F2F#3-31.
667 **Resolution Alternatives:**
668 1. Require that all the assertions and assertion ids in a request refer to the same subject.
669 2. Treat assertions with different subjects as requesting a decision for each of the subjects
670 mentioned.
671 3. Treat assertions with different subjects and a question about the collective group, i.e. true
672 only if access is allowed for all.
673 4. Allow multiple subjects, but assign some other semantic to such a request.

674 **3.12 Group 12: Attribute Assertions**

675 **Highest V1.0 Issue Number:** DS-12-08

676 **3.12.1 DEFERRED ISSUE:[DS-12-03: AttrSchemaReqs]**

677 **Source:** V1.0 Deferred Issue

678 **Champion:** None

679 **Status:** 29-Jan-2002 – Deferred by vote.

680 **Description:** Should it be possible to request only the Attribute schema?

681 This was identified as F2F#3-22.

682 **Resolution Alternatives:**

- 683 1. Allow Attribute Schema Requests.
684 2. Do not allow Attribute Schema Requests.

685 **3.12.2 DEFERRED ISSUE:[DS-12-04: AttrNameReqs]**

686 **Source:** V1.0 Deferred Issue

687 **Champion:** None

688 **Status:** 29-Jan-2002 – Deferred by vote.

689 **Description:** Should it be possible to request only attribute names and not values? It is not clear
690 whether these would be all the attributes the Attribute Authority knows about or just the ones

691 pertaining to a particular subject. It is not clear what this would be used for. No usecase seems to
692 require it.

693 This was identified as F2F#3-23.

694 This was identified as PRO-04.

695 **Resolution Alternatives:**

- 696 1. Allow Attribute Name Requests.
697 2. Do not allow Attribute Name Requests.

698 **3.12.3 DEFERRED ISSUE:[DS-12-08: Delegation]**

699 **Source:** V1.0 Deferred Issue

700 **Champion:** Hal Lockhart

701 **Status:** Deferred.

702 **Description:** Should SAML provide assertion statements concerning delegation? Proposed by
703 Nell Rehn on the public comment list.

704 <http://lists.oasis-open.org/archives/security-services-comment/200202/msg00009.html>

705 **Resolution Alternatives:** ???

706 **3.13 Group 13: Dynamic Sessions**

707 **Highest V1.0 Issue Number:** DS-13-01

708 **3.13.1 DEFERRED ISSUE:[DS-13-01: SessionsinEffect]**

709 **Source:** V1.0 Deferred Issue

710 **Champion:** None

711 **Status:** 29-Jan-2002 – Deferred by vote.

712 **Description:** How can a relying party determine if dynamic sessions are in effect? If dynamic
713 sessions are in effect it will be necessary to determine if the session has ended, even if the
714 relevant Assertions have not yet expired. However, if dynamic sessions are not in use, attempting
715 to check session state is likely to increase response times unnecessarily.

716 This was identified as F2F#3-3.

717 **Resolution Alternatives:**

- 718 1. Define a field in Assertion Headers to indicate dynamic sessions.
719 2. Configure the implementation based on some out of band information.

720 **3.14 Group 14:General – Multiple Message Types**

721 **Highest V1.0 Issue Number:** DS-14-20

722 **3.14.1 DEFERRED ISSUE:[DS-14-04: Aggregation]**

723 **Source:** V1.0 Deferred Issue

724 **Champion:** None

725 **Status:** 29-Jan-2002 – Deferred by vote.

726 **Description:** Do we need an explicit element for aggregating multiple assertions into a single
727 object as part of the SAML specification? If so, what is the type of this element?

728 This was identified as CONS-01.

729 **Resolution Alternatives:** ???

730 **3.14.2 DEFERRED ISSUE:[DS-14-14: ErrMsg in Multiple Languages]**

731 **Source:** V1.0 Deferred Issue

732 **Champion:** Eve Maler

733 **Status:** 9-Apr-2002 – Deferred by vote.

734 **Description:** Should SAML allow status messages to be in multiple natural languages?

735 In core-25, StatusMessage is defined (Section 3.4.3.3, lines 1183-1187) as being of type string.
736 Its inclusion in the Status element (lines 1114-1115) allows multiple occurrences, that is, zero or
737 more messages per status returned. In the call on Tuesday we discussed the potential need to
738 allow for multiple natural-language versions of status messages.

739 If the StatusMessage element can't contain markup, then it makes it hard for someone to provide,
740 say, both English and Japanese versions of an error message. Here are two obvious different
741 ways to do this, both using the native xml:lang attribute to indicate the language in which the
742 message is written.

743 (See also a possible SEPARATE issue at the bottom of this message.)

744 =====

745 Option 1: Multiple StatusMessage elements, each with language indicated

746 Currently, multiple StatusMessages are already allowed, but we say nothing in the spec to
747 explain how they're supposed to be used or interpreted. The description just says (lines 1105-
748 1106):

749 <StatusMessage> [Any Number]

750 A message which MAY be returned to an operator.

751 (Hmm, not sure what "operator" means here..) This option would place a specific interpretation
752 on the appearance of multiple StatusMessage elements related to language differentiation, and
753 would allow for an optional xml:lang attribute on the element:

754 <StatusMessage> [Zero or more]

755 A natural-language message explaining the status in a human-readable way. If more
756 than one <StatusMessage> element is provided, the messages are natural-language
757 equivalents of each other; in this case, the xml:lang attribute SHOULD be provided on
758 each element.

```
759 <element name="StatusMessage">
760   <complexType>
761     <simpleContent>
762       <extension base="string">
763         <attribute name="xml:lang" type="language"/>
764       </extension>
765     </simpleContent>
766   </complexType>
767 </element>
```

768 I prefer this option because it has less markup overhead, as long as the multiple
769 <StatusMessage> elements already allowed in the schema weren't intended to have some other
770 meaning instead (in which case, that meaning needs to be documented). If they weren't, then if
771 this option *isn't* picked, I think we need to shut down multiple occurrences of <StatusMessage>,
772 changing it to minOccurs="0" and maxOccurs="1".

773 =====

774 Option 2: One StatusMessage element, with partitioned content indicating language
775 This option isn't all that different from option 1. It would invent a new subelement to go into the
776 content of <StatusMessage> like so:

777 <StatusMessage>

778 A natural-language message explaining the status in a human-readable way. It contains
779 one or more <MessageText> elements, each providing different natural-language
780 equivalents of the same message.

781 <element name="StatusMessage" type="StatusMessageType" />

782 <complexType name="StatusMessageType">

783 <sequence>

784 <element ref="MessageText" maxOccurs="unbounded" />

785 </sequence>

786 </complexType>

787 <MessageText>

788 The text of the status message. If more than one <MessageText> element is provided,
789 the messages are natural-language equivalents of each other; in this case, the xml:lang
790 attribute SHOULD be provided on each element.

791 <element name="MessageText">

792 <complexType>

793 <simpleContent>

794 <extension base="string">

795 <attribute name="xml:lang" type="language"/>

796 </extension>

797 </simpleContent>

798 </complexType>

799 </element>

800 I think this option is necessary *if* multiple occurrences of <StatusMessage> were already
801 intended to have some other meaning. If they weren't, then I prefer option 1.

802 =====

803 Digression on xml:lang

804 You can read about this attribute here:

805 Brief description of the xml: namespace:

806 <http://www.w3.org/XML/1998/namespace.html>

807 Section of the XML spec itself that defines xml:lang:

808 <http://www.w3.org/TR/REC-xml#sec-lang-tag>

809 There is also a non-normative but helpful schema module that defines the items in the xml:
810 namespace. You can find it here:

811 <http://www.w3.org/XML/1998/namespace.xsd>

812 This schema module can be useful if you want to slurp those definitions into the SAML schemas
813 to make sure that SAML instances can be fully validated. Alternatively, we can legally cook up
814 our own schema code for this as shown in the two options above, which would avoid importing
815 another schema module into both of ours, with attendant code and documentation. If we do that,
816 note that we'll still need to declare the xml: namespace at the tops of our schema modules.

817 =====

818 Final thoughts

819 Even if the issue of multiple-language support is deferred until a future release, I believe that
820 <StatusMessage> and the fact that it's repeatable is underspecified at the moment. I would like

821 to see it restricted to an optional single occurrence, or alternatively, I would like to have its
822 semantics explained when multiple occurrences are used. This can be listed as a separate issue
823 if you like.

824 <http://lists.oasis-open.org/archives/security-services/200201/msg00265.html>

825 **Resolution Alternatives:** ???

826 **3.14.3 CLOSED ISSUE:[DS-14-15: Version Synchronization]**

827 **Source:** V1.0 Deferred Issue

828 **Champion:** Rob Philpott

829 **Status:** 25-Jun-2003 – This issue was resolved in V1.1

830 **Status:** 9-Apr-2002 – Deferred by vote.

831 **Description:** What is the relationship between the version of the Assertions, Requests and
832 Responses? Should the values always be the same or can they change independently of each
833 other?

834 **Resolution Alternatives:**

- 835 1. Requests and Responses each have Major/Minor version info attributes, which implies that,
836 in theory, they could be upgraded independently (I didn't see where this is explicitly
837 prohibited). If so, Line 1228-1229 should be explicit: "This document defines SAML
838 Assertions 1.0, SAML Request Protocol 1.0, and SAML Response Protocol 1.0".
- 839 2. If the intent is to keep the request and response protocols synchronized with a single SAML
840 protocol version (separate from the assertion version), then the RequestAbstractType type
841 (3.2.1) and the ResponseAbstractType type (3.4.1) should replace the MajorVersion and
842 MinorVersion attributes with a new <ProtocolVersionInfo> element defined something like:

```
843 <element name="ProtocolVersionInfo" type="saml:ProtocolVersionInfoType"/>
```

```
844 <complexType name="ProtocolVersionInfoType">
```

```
845     <attribute name="MajorVersion" type="integer" use="required"/>
```

```
846     <attribute name="MinorVersion" type="integer" use="required"/>
```

```
847 </complexType>
```

- 848 3. If the intent is to keep the version info synchronized for assertions, request protocol, and
849 response protocol, then we could use the following in the <assertion> element (2.3.3) and the
850 request/response abstract types could include the <VersionInfo> element:

```
851 <element name="VersionInfo" type="saml:VersionInfoType"/>
```

```
852 <complexType name="VersionInfoType">
```

```
853     <attribute name="MajorVersion" type="integer" use="required"/>
```

```
854     <attribute name="MinorVersion" type="integer" use="required"/>
```

```
855 </complexType>
```

856 The above alternatives were taken from: <http://lists.oasis-open.org/archives/security-services/200201/msg00163.html>.

858 [25-Jun-2003] The adopted resolution in V1.1 was to clarify via specification text rather than
859 schema changes. The spec now requires Protocol versions in Request and Response messages
860 to be synchronized. Assertion versions may deviate from Protocol versions. See V1.1 spec for
861 details.

862 **3.14.4 DEFERRED ISSUE:[DS-14-16: Version Positive]**

863 **Source:** V1.0 Deferred Issue

864 **Champion:** Eve Maler

865 **Status:** 9-Apr-2002 – Deferred by vote.

866 **Description:** It is intended that Major and Minor version numbers must be positive. It was
867 discussed that this could be enforced by using facets. We would want to make a
868 VersionNumberType simple type for this.

869 This issue was identified as Low Priority Issue - L2 from Sun.

870 <http://lists.oasis-open.org/archives/security-services/200202/msg00012.html>

871 **Resolution Alternatives:** ???

872 **3.15 Group 15: Elements Expressing Time Instants**

873 **Highest V1.0 Issue Number:** DS-15-03

874 No deferred or new issues.

875 **4 Miscellaneous Issues**

876 **4.1 Group 1: Terminology**

877 **Highest V1.0 Issue Number:** MS-1-03

878 No deferred or new issues.

879 **4.2 Group 2: Administrative**

880 **Highest V1.0 Issue Number:** MS-2-02

881 No deferred or new issues.

882 **4.3 Group 3: Conformance**

883 **Highest V1.0 Issue Number:** MS-3-03

884 No deferred or new issues.

885 **4.4 Group 4: XMLDSIG**

886 **Highest V1.0 Issue Number:** MS-4-02

887 No deferred or new issues.

888 **4.5 Group 5: Bindings**

889 **Highest V1.0 Issue Number:** MS-5-08

890 **4.5.1 DEFERRED ISSUE:[MS-5-08: Publish WSDL]**

891 **Source:** V1.0 Deferred Issue

892 **Champion:** Eve Maler

893 **Status:** 19-Mar-2002 – Deferred by vote. Needs more review and a decision where to publish it.

894 **Description:** Publish Irving's WSDL for SAML 1.0, even if it is non-normative. Where? Perhaps in
895 Bindings doc? This is ELM-8 in:

896 <http://lists.oasis-open.org/archives/security-services/200203/msg00042.html>

897 **Resolution Alternatives:** ???

898 **5 References**

899 **5.1 Normative**

- 900 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
901 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 902 **[ISSUES-1.0]** H.Lockhart, *Security Assertions Markup Language Issues List Version*
903 12, <http://www.oasis-open.org/committees/security/>, OASIS, April 16,
904 2002.

905 **Appendix A. Acknowledgments**

906 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
907 Committee, whose voting members at the time of publication were:

- 908 • Frank Siebenlist, Argonne National Laboratory
- 909 • Irving Reid, Baltimore Technologies
- 910 • Hal Lockhart, BEA Systems
- 911 • Steven Lewis, Booz Allen Hamilton
- 912 • John Hughes, Entegriy Solutions
- 913 • Carlisle Adams, Entrust
- 914 • Jason Rouault, HP
- 915 • Maryann Hondo, IBM
- 916 • Anthony Nadalin, IBM
- 917 • Scott Cantor, Individual
- 918 • Bob Morgan, Individual
- 919 • Trevor Perrin, Individual
- 920 • Pdraig Moloney, NASA
- 921 • Prateek Mishra, Netegrity (co-chair)
- 922 • Frederick Hirsch, Nokia
- 923 • Senthil Sengodan, Nokia
- 924 • Timo Skytta, Nokia
- 925 • Charles Knouse, Oblix
- 926 • Steve Anderson, OpenNetwork
- 927 • Simon Godik, OverXeer
- 928 • Rob Philpott, RSA Security (co-chair)
- 929 • Dipak Chopra, SAP
- 930 • Jahan Moreh, Sigaba
- 931 • Bhavna Bhatnagar, Sun Microsystems
- 932 • Jeff Hodges, Sun Microsystems
- 933 • Eve Maler, Sun Microsystems (coordinating editor)
- 934 • Emily Xu, Sun Microsystems
- 935 • Phillip Hallam-Baker, VeriSign

936

Appendix B. Revision History

Rev	Date	By Whom	What
Draft-01	200-06-24	Rob Philpott	Initial draft for SAML V1.1

937

Appendix C. Notices

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

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

951 **Copyright © OASIS Open 2003. All Rights Reserved.**

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

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

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