

1

---

# Errata Working Document for SAML V2.0

2

3

## Working Draft 50

4

5 **31 May 2009**

6 **Document identifier:**

7 sstc-saml-errata-2.0-draft-50

8 **This Version:**

9 (See the SSTC document repository: [http://www.oasis-](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)  
10 [open.org/committees/documents.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security))

11 **Previous Version:**

12 (See the SSTC document repository: [http://www.oasis-](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)  
13 [open.org/committees/documents.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security))

14 **Technical Committee:**

15 OASIS Security Services TC

16 **Chairs:**

17 Hal Lockhart, Oracle Corporation  
18 Thomas Hardjono, MIT

19 **Editors:**

20 Abbie Barbir, Nortel, <[abbieb@nortel.com](mailto:abbieb@nortel.com)>  
21 Eve Maler, Sun Microsystems <[eve.maler@sun.com](mailto:eve.maler@sun.com)>  
22 Scott Cantor, Internet2 <[cantor.2@osu.edu](mailto:cantor.2@osu.edu)>

23 **Related Work:**

24 This specification is related to:  
25 Security Assertion Markup Language (SAML) Version 2.0

26 **Abstract:**

27 This document lists the proposed errata against the OASIS SAML V2.0 Committee  
28 Specifications and details about their disposition. Each item describes options for  
29 resolving the issue and the resolution decided on by the SSTC, if any.

30 **Status:**

31 This document is work in progress and will be updated over time to reflect newly  
32 proposed errata. This is meant to be the working document that records the history of  
33 each item; there is a separate document for approved errata that is on a formal approval  
34 track, which summarizes only the errata with resolutions that prescribe specification  
35 changes.

36 Technical Committee members should send comments on this specification and proposed errata  
37 to [security-services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org). Others should send comments to the Technical  
38 Committee by using the “Send A Comment” button on the Technical Committee’s web page at  
39 [http://www.oasis-open.org/committees/comments/index.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/comments/index.php?wg_abbrev=security).

40 For information on whether any patents have been disclosed that may be essential to  
41 implementing this specification, and any offers of patent licensing terms, please refer to the  
42 Intellectual Property Rights section of the Technical Committee web page at [http://www.oasis-](http://www.oasis-open.org/committees/security/ipr.php)  
43 [open.org/committees/security/ipr.php](http://www.oasis-open.org/committees/security/ipr.php).

---

## 44 Notices

45 Copyright © OASIS® 1993–2009. All Rights Reserved. OASIS trademark, IPR and other policies apply.

46 All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual  
47 Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

48 This document and translations of it may be copied and furnished to others, and derivative works that  
49 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published,  
50 and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice  
51 and this section are included on all such copies and derivative works. However, this document itself may  
52 not be modified in any way, including by removing the copyright notice or references to OASIS, except as  
53 needed for the purpose of developing any document or deliverable produced by an OASIS Technical  
54 Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must  
55 be followed) or as required to translate it into languages other than English.

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

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

63 OASIS requests that any OASIS Party or any other party that believes it has patent claims that would  
64 necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard,  
65 to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to  
66 such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that  
67 produced this specification.

68 OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of  
69 any patent claims that would necessarily be infringed by implementations of this specification by a patent  
70 holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR  
71 Mode of the OASIS Technical Committee that produced this specification. OASIS may include such  
72 claims on its website, but disclaims any obligation to do so.

73 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that  
74 might be claimed to pertain to the implementation or use of the technology described in this document or  
75 the extent to which any license under such rights might or might not be available; neither does it represent  
76 that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to  
77 rights in any document or deliverable produced by an OASIS Technical Committee can be found on the  
78 OASIS website. Copies of claims of rights made available for publication and any assurances of licenses  
79 to be made available, or the result of an attempt made to obtain a general license or permission for the  
80 use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS  
81 Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any  
82 information or list of intellectual property rights will at any time be complete, or that any claims in such list  
83 are, in fact, Essential Claims.

84 The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be  
85 used only to refer to the organization and its official outputs. OASIS welcomes reference to, and  
86 implementation and use of, specifications, while reserving the right to enforce its marks against  
87 misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

## Table of Contents

89	1 Introduction.....	7
90	2 Errata.....	7
91	E0: Incorrect section reference .....	7
92	E1: Relay State for HTTP Redirect.....	7
93	E2: Metadata clarifications.....	7
94	E4: SAML 1.1 Artifacts.....	8
95	E6: Encrypted NameID .....	8
96	E7: Metadata attributes WantAuthnRequestsSigned and AuthnRequestsSigned .....	8
97	E8: SLO and NameID termination .....	9
98	E10: Logout Request reason Mismatch with Schema .....	10
99	E11: Improperly Labeled Feature .....	10
100	E12: Clarification on ManageNameIDRequest.....	10
101	E13: Inaccurate description of Authorization Decision .....	11
102	E14: AllowCreate .....	11
103	E17: Authentication Response IssuerName vs. Assertion IssuerName.....	13
104	E18: reference to identity provider discovery service in ECP Profile.....	13
105	E19: Clarification on Error Processing.....	13
106	E20: ECP SSO Profile and Metadata.....	14
107	E21: PAOS Version.....	14
108	E22: Error in Profile/ECP.....	14
109	E24: HTTPS in URI Binding.....	15
110	E25: Metadata Structures Feature in Conformance.....	15
111	E26: Ambiguities around Multiple Assertions and Statements in the SSO Profile.....	16
112	E27: Error in ECP Profile.....	17
113	E28: Conformance Table 1.....	17
114	E29: Conformance Table 2.....	18
115	E30: Considerations for key replacement.....	18
116	E31: Various minor errors in Binding.....	18
117	E32: Missing section in Profiles.....	19
118	E33: References to Assertion Request Protocol.....	19
119	E34: Section Heading.....	19
120	E35: Example in Profiles.....	20
121	E36: Clarification on Action Element.....	20
122	E37: Clarification in Metadata on Indexed Endpoints.....	20
123	E38: Clarification regarding index on <LogoutRequest>.....	21
124	E39: Error in SAML profile example.....	21
125	E40: Holder of Key.....	21
126	E41: EndpointType ResponseLocation clarification in Metadata.....	22
127	E42: Conformance Table 4.....	22
128	E43: Key location in saml:EncryptedData.....	22
129	E45: AuthnContext comparison clarifications .....	25

130	E46: AudienceRestriction clarifications.....	26
131	E47: Clarification on SubjectConfirmation.....	26
132	E48: Clarification on encoding for binary values in LDAP profile.....	27
133	E49: Clarification on attribute name format .....	27
134	E50: Clarification SSL Ciphersuites .....	28
135	E51: Schema type of contents of <AttributeValue> .....	28
136	E52: Clarification on <NotOnOrAfter> attribute .....	29
137	E53: Correction to LDAP/X.500 profile attribute .....	29
138	E54: Correction to ECP URN .....	30
139	E55: Various Language Cleanups.....	30
140	E56: Typo in Profiles.....	30
141	E57: SAML Mime Reference.....	31
142	E58: Typos in Profiles.....	31
143	E59: SSO Response when using HTTP-Artifact.....	31
144	E60: Incorrect URI .....	32
145	E61 Reference to non-existent element.....	32
146	E62: TLS Keys in KeyDescriptor.....	32
147	E63: IdP Discovery Cookie Interpretation.....	33
148	E64: Liberty Moniker Used Inappropriately.....	33
149	E65: Second-level StatusCode.....	33
150	E66: Metadata and DNSSEC.....	34
151	E68: Use of Multiple <KeyDescriptor> Elements.....	34
152	E69: Semantics of <ds:KeyInfo> in <KeyDescriptor>.....	35
153	E70: Obsolete reference to UUID URN namespace.....	35
154	E71: Missing namespace definition in Profiles.....	35
155	E74: Update XML Signature Reference.....	35
156	E75: Clarify Handling of SubjectConfirmation in AuthnRequest.....	36
157	E76: Clarify nested validUntil/cacheDuration.....	36
158	E77: Generalize scope of Metadata specification.....	37
159	E78: Reassignment of persistent identifiers.....	37
160	E79: Clarification of SessionNotOnOrAfter.....	37
161	3 Proposed Errata.....	38
162	PE3: Supported URL Encoding.....	38
163	PE15: NameID Policy (Reopened).....	38
164	PE23: Metadata for <ArtifactResolutionService>.....	39
165	PE67: Absence of elements in metadata (Open).....	39
166	PE73: No definition of Statement in the Glossary (Open).....	39
167	PE80: Error in permissible root elements for MIME type (Open).....	39
168	PE81: Algorithm statement in XML Signature profile (Open).....	40
169	PE82: Empty <ContactPerson> element (Open).....	40
170	PE83: Weaken claim made about Exclusive C14N (Open).....	40
171	Appendix A. Revision History.....	42
172	Appendix B. Summary of Disposition.....	46
173	Appendix C. Acknowledgments.....	50

174

175

---

---

## 1 Introduction

176

177 This document lists the proposed errata against the OASIS SAML 2.0 Committee Specifications and  
178 details about their disposition. It is a working document that may change over time. See also the formally  
179 approved SAML V2.0 Errata document and its associated “errata composite” documents, whose latest  
180 revisions are listed and linked at the SSTC web page ([http://www.oasis-](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)  
181 [open.org/committees/tc\\_home.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)).

---

## 2 Errata

182

183 The SSTC has determined that these reported problems have a solution that can be applied in erratum  
184 form. Their original number designations have changed from “PE*nn*” to “E*nn*” to reflect this status.

---

### E0: Incorrect section reference

185

186 **First reported by:** Rob Philpot, RSA

187 **Message:** <http://lists.oasis-open.org/archives/security-services/200503/msg00080.html>

188 **Document:** Core

189 **Description:** Line 2660 refers back to section “3.6.3” for Reason codes. This should refer to section  
190 “3.7.3”.

191 **Options:**

192 **Disposition:** During the conference call of March 28 the TC unanimously agreed to make this correction.  
193 (Note that this entry was originally number “E1” when there were separate “E” (agreed errata) and “PE”  
194 (potential errata) lists, where the “E” list had only this one entry in it. It has been renamed “E0” so that the  
195 two lists could be merged and a single number would suffice for unique identification across them.)

---

### E1: Relay State for HTTP Redirect

196

197 **First reported by:** Ari Kermaier, Oracle

198 **Message:** <http://lists.oasis-open.org/archives/security-services/200502/msg00003.html>

199 **Document:** Bindings and Profiles

200 **Description:** Section 3.4.3 (Relay State for HTTP Redirect) lines 551-553 read

201 “Signing is not realistic given the space limitation, but because the value is exposed to third-party  
202 tampering, the entity SHOULD insure that the value has not been tampered with by using a checksum, a  
203 pseudo-random value, or similar means.”

204 This language should probably be deleted or modified, as the RelayState parameter \*is\* covered by the  
205 query string signature described in 3.4.4.1 (DEFLATE Encoding).

206 The same language is correctly present in 3.5.3 (Relay State for HTTP POST), as no means of signing  
207 the POST form control data is defined.

208 **Options:** Replace first paragraph of section 3.4.3 at line 545 with: “RelayState data MAY be included with  
209 a SAML protocol message transmitted with this binding. The value MUST NOT exceed 80 bytes in length  
210 and SHOULD be integrity protected by the entity creating the message, either via a digital signature (see  
211 section [3.4.4.1]) or by some independent means.”

212 **Disposition:** During the conference call of April 12 the TC accepted this option.

---

## 213 E2: Metadata clarifications

214 **First reported by:** Scott Cantor, OSU

215 **Message:** <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

216 **Document:** Bindings and Profiles

217 **Description:** Clarify metadata requirements in the various profiles. For example, it's required by  
218 implication that if you support the Artifact binding for some profile that your role descriptor also needs an  
219 ArtifactResolutionService element, but this isn't stated anywhere.

220 **Options:** In [SAMLBind] replace paragraph in section 3.6.7 at lines 1188-1191 with:

221 "Support for receiving messages using the HTTP Artifact binding SHOULD be reflected by indicating URL  
222 endpoints at which requests and responses for a particular protocol or profile should be sent. Either a  
223 single endpoint or distinct request and response endpoints MAY be supplied. Support for sending  
224 messages using this binding SHOULD be accompanied by one or more indexed  
225 <md:ArtifactResolutionService> endpoints for processing <samlp:ArtifactResolve> messages."

226 **Disposition:** A thorough disposition requires a fairly careful review of Metadata and Profiles so that the  
227 requirements can be documented in various places. This work is deferred to SAML 2.x. However, during  
228 the conference call of April 12 the TC accepted the above text as clarification for SAML 2.0.

---

## 229 E4: SAML 1.1 Artifacts

230 **First reported by:** Scott Cantor, OSU

231 **Message:** <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

232 **Document:** Bindings and Profiles

233 **Description:** Clarifying that SAML 1.1 artifacts have no place or use in SAML 2.0

234 **Options:** In [SAMLBind] add to line 1067:

235 "Although the general artifact structure resembles that used in prior versions of SAML and the type code  
236 of the single format described below does not conflict with previously defined formats, there is explicitly no  
237 correspondence between SAML 2.0 artifacts and those found in any previous specifications, and artifact  
238 formats not defined specifically for use with SAML 2.0 MUST NOT be used with this binding."

239 **Disposition:** During the conference call of April 12 the TC accepted this option.

---

## 240 E6: Encrypted NameID

241 **First reported by:** Rob Philpott, RSA

242 **Message:** Communicated during TC conference call of February 1, 2005.

243 **Document:** Core

244 **Description:** When using the nameid-format:encrypted type of name identifier in SAML assertions and  
245 protocol messages, it is not possible to communicate the format of the unencrypted identifier as part of  
246 the assertion or message. This concept was derived from Liberty which only used it for persistent  
247 identifiers. Since we also support other formats in SAML 2.0, the agreement on the unencrypted form  
248 (prior to encryption/after decryption) must be done out of band.

249 **Options:** In [SAMLCore] append to paragraph ending on line 2139:

250 "It is not possible for the service provider to specifically request that a particular kind of identifier be  
251 returned if it asks for encryption. The <md:NameIDFormat> metadata element (see [SAMLMeta]) or other  
252 out-of-band means MAY be used to determine what kind of identifier to encrypt and return."

253 **Disposition:** During the conference call of April 12 the TC accepted this option.

---

## E7: Metadata attributes WantAuthnRequestsSigned and AuthnRequestsSigned

254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296

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

**Message:** <http://lists.oasis-open.org/archives/security-services/200502/msg00017.html>

**Document:** Metadata

**Description:** In Metadata, the IDPSSODescriptor has the setting called “WantAuthnRequestsSigned” and the SPSSODescriptor has the setting called “AuthnRequestsSigned”. But it’s ambiguous about “how” this signing is to be done.

Note that the SP can also define “WantAssertionsSigned”, where it means that the SP wants the IDP to sign the Assertion XML element by including a <ds:Signature> element in the assertion. That is, I do NOT believe it means that the assertion can also be “signed by inclusion” by putting it (unsigned) inside a <samlp:Response> element and signing that element. It is the Assertion XML element itself that is signed. I don’t believe the same approach is what folks expect for the AuthnRequest settings however. I think it is ambiguous and needs to be clarified.

At the interop, folks were using a true setting for [Want]AuthnRequestsSigned to mean that the AuthnRequest message is signed only in the context of the HTTP Redirect Binding where the total URL with parameters is signed using the mechanism specified in that binding. The AuthnRequest XML element is NOT expected to contain a <ds:Signature> element. Now I don’t think this interpretation would necessarily be the same if the message was carried in the POST or Artifact bindings. I assume that in those cases, the XML element itself would be signed and include the ds:Signature> element.

So the interpretation of the setting appears to be dependent on which binding is being used. This is clearly not the case for the WantAssertionsSigned setting. So we should at least clarify this for folks. That is, unless folks have a different interpretation of what the settings mean.

**Options:** Combine this with PE9 and in [SAMLMetadata] add text before line 710:

“The WantAuthnRequestsSigned attribute is intended to indicate to service providers whether or not they can expect an unsigned <AuthnRequest> message to be accepted by the identity provider. The identity provider is not obligated to reject unsigned requests nor is a service provider obligated to sign its requests, although it might reasonably expect an unsigned request will be rejected. In some cases, a service provider may not even know which identity provider will ultimately receive and respond to its requests, so the use of this attribute in such a case cannot be strictly defined.

Furthermore, note that the specific method of signing that would be expected is binding dependent. The HTTP Redirect binding (see [SAMLBind] sec XX) requires the signature be applied to the URL-encoded value rather than placed within the XML message, while other bindings generally permit the signature to be within the message in the usual fashion.”

Add text to paragraph at lines 741-742:

“A value of false (or omission of this attribute) does not imply that the service provider will never sign its requests or that a signed request should be considered an error. However, an identity provider that receives an unsigned <samlp:AuthnRequest> message from a service provider whose metadata contains this attribute with a value of true MUST return a SAML error response and MUST not fulfill the request.”

Add text to paragraph at lines 744-747:

“Note that an enclosing signature at the SAML binding or protocol layer does not suffice to meet this requirement, for example signing a <samlp:Response> containing the assertion(s) or a TLS connection.”

**Disposition:** During the conference call of September 27 the TC accepted this option.

---

## E8: SLO and NameID termination

297  
298  
299  
300

**First reported by:** Thomas Wisniewski, Entrust

**Message:** <http://lists.oasis-open.org/archives/security-services/200503/msg00034.html>

**Document:** Core

301 **Description:** Combining SLO with NameID termination, we should clarify whether it's explicitly not  
302 required for the SP to continue to expect or process SLO messages for an active session following  
303 NameID termination. The spec implies pretty strongly that you don't because you can terminate your local  
304 session.

305 **Options:** Replace the last sentence in 2479-2480 (section 3.6.3) with:

306 "In general it SHOULD NOT invalidate any active session(s) of the principal for whom the relationship has  
307 been terminated. If the receiving provider is an identity provider, it SHOULD NOT invalidate any active  
308 session(s) of the principal established with other service providers. A requesting provider MAY send a  
309 <LogoutRequest> message prior to initiating a name identifier termination by sending a  
310 <ManageNameIDRequest> message if that is the requesting provider's intent (e.g., the name identifier  
311 termination is initiated via an administrator who wished to terminate all user activity). The requesting  
312 provider MUST NOT send a <LogoutRequest> message after the <ManageNameIDRequest> message is  
313 sent."

314 **Disposition:** During the conference call of April 12 the TC accepted this option.

---

## 315 **E10: Logout Request reason Mismatch with Schema**

316 **First reported by:** Rob Philpott, RSA

317 **Message:** <http://lists.oasis-open.org/archives/security-services/200503/msg00080.html>

318 **Document:** Core

319 **Description:** In core line 2540 it says that "Reason" on the LogoutRequest is "in the form of a URI  
320 reference". However, in the schema, the Reason attribute is type="string", not type="anyURI". All of the  
321 reason codes that we define (in section 3.7.3 and 3.7.3.2) are actually URI's. But, since the schema  
322 defines it as a string, the text should be changed to match the schema.

323 **Options:** Change line 2540 of core as follows: The Reason attribute is specified as a string in the  
324 schema. This specification further restricts the schema by requiring that the Reason attribute MUST be in  
325 the form of a URI reference.

326 **Disposition:** During the conference call of February 14, 2006 the TC accepted the text as stated here.

---

## 327 **E11: Improperly Labeled Feature**

328 **First reported by:** Rob Philpott, RSA

329 **Message:** <http://lists.oasis-open.org/archives/security-services/200503/msg00080.html>

330 **Document:** Conformance

331 **Description:** In table 2 of the conformance spec, the feature in the 8<sup>th</sup> row is improperly labeled. It  
332 currently says "Name Identifier Management, HTTP Redirect". It should say "Name Identifier  
333 Management, HTTP Redirect (SP-initiated)".

334 There are also minor inconsistencies in the labels since the parenthetical (xP-initiated) are listed with the  
335 binding in some, but with the profile in others. I suggest always listing it with the profile name.

336 **Options:** Correct the label as suggested in the description of the erratum above.

337 **Disposition:** During the conference call of June 7 the TC accepted this option.

---

## 338 **E12: Clarification on ManageNameIDRequest**

339 **First reported by:** Scott Cantor, OSU/Brian Campbell, Ping Identity

340 **Message:** <http://lists.oasis-open.org/archives/security-services/200504/msg00107.html> and :  
341 <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

342 **Document:** Bindings and Profiles

343 **Description:** The schema defines the <NewID> element of a <ManageNameIDRequest> as a string.  
344 The implication of that is that a NIM request message from IDP to SP can only be used to inform the SP

345 of a change in identifier value (not format – format is immutable once established). There are a few  
346 places in the spec where the text implies that the format can be changed. Additionally, the text about  
347 <NewEncryptedID> should be expanded to clarify that the encrypted element is just the encrypted  
348 <NewID> element and not a full <NameID> as in the more typical <EncryptedID> element used  
349 elsewhere

350 **Options:**

351 Change the schema to allow format and potentially qualifiers to be changed and make all necessary  
352 cascading changes to the spec.

353 Update the wording in the spec to bring it inline with the schema as is and clarify that only the value of the  
354 identifier can be managed with the Name Identifier Management profile.

355 Given the complexity and scope of change involved in option 1 and the consensus that option 2 is  
356 sufficient and not too limiting, text changes consistent with option 2 are proposed below.

357 In Profiles change the text on lines 1320-21 from “Subsequently, the identity provider may wish to notify  
358 the service provider of a change in the format and/or value that it will use to identify the same principal in  
359 the future” to “Subsequently, the identity provider may wish to notify the service provider of a change in  
360 the value that it will use to identify the same principal in the future”

361 In Core change the text on lines 2412-13 from “After establishing a name identifier for a principal, an  
362 identity provider wishing to change the value and/or format of the identifier that it will use when referring to  
363 the principal,...” to “After establishing a name identifier for a principal, an identity provider wishing to  
364 change the value of the identifier that it will use when referring to the principal,...”

365 In Core add the following text after line 2438, “In either case, if the <NewEncryptedID> is used, its  
366 encrypted content is just a <NewID> element containing only the new value for the identifier (format and  
367 qualifiers cannot be changed once established).”

368 **Disposition:** During the conference call of June 7 the TC approved option 2.

---

## 369 **E13: Inaccurate description of Authorization Decision**

370 **First reported by:** Jahan Moreh, Sigaba

371 **Message:** <http://lists.oasis-open.org/archives/security-services/200504/msg0125.html>

372 **Document:** Core

373 **Description:** Core 357-358 currently reads:

374 Authorization Decision: A request to allow the assertion subject to access the specified resource has  
375 been granted or denied.

376 It should say:

377 Authorization Decision: A request to allow the assertion subject to access the specified resource has  
378 been granted, denied, or is indeterminate.

379 **Options:** Make correction as described above.

380 **Disposition:** During the conference call of June 7 the TC approved the change as proposed here.

---

## 381 **E14: AllowCreate**

382 **First reported by:** Brian Campbell, Ping Identity

383 **Message:** <http://lists.oasis-open.org/archives/security-services/200505/msg00014.html>

384 **Document:** Core and Profiles

385 **Description:** AllowCreate needs more clear definition.

386 **Options:** Make the following corrections

387 **In Profiles replace the current text there about AllowCreate with a statement that** “this profile does  
388 not provide additional guidelines for the use of AllowCreate” and reference this text in core as governing.

389 **In Core, replace definition of AllowCreate, lines 2123-2129:**

390 "A Boolean value used to indicate whether the requester grants to the identity provider, in the course of  
391 fulfilling the request, permission to create a new identifier or to associate an existing identifier  
392 representing the principal with the relying party. Defaults to "false" if not present or the entire element is  
393 omitted."

394 **In Core, replace lines 2143-2147 and insert new text at line 2130 (beginning of the explanatory  
395 text):**

396 "The AllowCreate attribute may be used by some deployments to influence the creation of state  
397 maintained by the identity provider pertaining to the use of a name identifier (or any other persistent,  
398 uniquely identifying attributes) by a particular relying party, for purposes such as dynamic identifier or  
399 attribute creation, tracking of consent, subsequent use of the Name Identifier Management protocol (see  
400 section XX), or other related purposes.

401 When "false", the requester tries to constrain the identity provider to issue an assertion only if such state  
402 has already been established or is not deemed applicable by the identity provider to the use of an  
403 identifier. Thus, this does not prevent the identity provider from assuming such information exists outside  
404 the context of this specific request (for example, establishing it in advance for a large number of  
405 principals).

406 A value of "true" permits the identity provider to take any related actions it wishes to fulfill the request,  
407 subject to any other constraints imposed by the request and policy (the IsPassive attribute, for example).

408 Generally, requesters cannot assume specific behavior from identity providers regarding the initial  
409 creation or association of identifiers on their behalf, as these are details left to implementations or  
410 deployments. Absent specific profiles governing the use of this attribute, it might be used as a hint to  
411 identity providers about the requester's intention to store the identifier or link it to a local value.

412 A value of "false" might be used to indicate that the requester is not prepared or able to do so and save  
413 the identity provider wasted effort.

414 Requesters that do not make specific use of this attribute SHOULD generally set it to "true" to maximize  
415 interoperability.

416 The use of the AllowCreate attribute MUST NOT be used and SHOULD be ignored in conjunction with  
417 requests for or assertions issued with name identifiers

418 with a Format of urn:oasis:names:tc:SAML:2.0:nameid-format:transient (they preclude any such state in  
419 and of themselves)."

420 In Core, change lines 2419-2420 to:

421 "This protocol MUST NOT be used in conjunction with the  
422 urn:oasis:names:tc:SAML:2.0:nameidformat:transient <NameID> Format."

423 **In Core, replace lines 2475-2479 with:**

424 "If the <Terminate> element is included in the request, the requesting provider is indicating that (in the  
425 case of a service provider) it will no longer accept assertions from the identity provider or (in the case of  
426 an identity provider) it will no longer issue assertions to the service provider about the principal.

427 If the receiving provider is maintaining state associated with the name identifier, such as the value of the  
428 identifier itself (in the case of a pair-wise identifier), an SPProvidedID value, the sender's consent to the  
429 identifier's creation/use, etc., then the receiver can perform any maintenance with the knowledge that the  
430 relationship represented by the name identifier has been terminated.

431 Any subsequent operations performed by the receiver on behalf of the sender regarding the principal (for  
432 example, a subsequent <AuthnRequest>) SHOULD be carried out in a manner consistent with the  
433 absence of any previous state.

434 Termination is potentially the cleanup step for any state management behavior triggered by the use of the  
435 AllowCreate attribute in the Authentication Request protocol (see section XX). Deployments that do not  
436 make use of that attribute are likely to avoid the use of the <Terminate> element or would treat it as a  
437 purely advisory matter.

438 Note that in most cases (a notable exception being the rules surrounding the SPProvidedID attribute),  
439 there are no requirements on either identity providers or service providers regarding the creation or use of  
440 persistent state. Therefore, no explicit behavior is mandated when the <Terminate> element is received.  
441 However, if persistent state is present pertaining to the use of an identifier (such as if an SPProvidedID  
442 attribute was attached), the <Terminate> element provides a clear indication that this state SHOULD be  
443 deleted (or marked as obsolete in some fashion).”

444 **Disposition:** During the conference call of June 21 the TC approved the change as proposed here.

---

## 445 **E17: Authentication Response IssuerName vs. Assertion** 446 **IssuerName**

447 **First reported by:** Thomas Wisniewski, Entrust

448 **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200506/msg00072.html>

449 **Document:** Profiles

450 **Description:** Profiles document says issuer (for an AuthnRequest Response) MAY be omitted. “the  
451 <Issuer> element MUST be present and MUST contain the unique identifier of the” The main reason is  
452 that Issuer should be a MUST in the SSO Response protocol.

453 **Options:** Change lines 541-543 of profiles to:

454 If the <Response> message is signed or if an enclosed assertion is encrypted, then the <Issuer> element  
455 MUST be present. Otherwise it MAY be omitted. If present it MUST contain the unique identifier of the  
456 issuing identity provider; the Format attribute MUST be omitted or have a value of  
457 urn:oasis:names:tc:SAML:2.0:nameid-format:entity.”

458 **Disposition:** During the conference call of July 5 the TC approved to make the changes as stated here.

---

## 459 **E18: reference to identity provider discovery service in ECP** 460 **Profile**

461 **First reported by:** Prateek Mishra, Principal Identity

462 **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00000.html>

463 **Document:** Profiles

464 **Description:** The ECP does not directly interact with the identity provider discovery service, it may act as  
465 an intermediary for an IdP or SP that plan to utilize the service. Current text gives the impression that it is  
466 a direct participant in the identity provider discovery service. Instead, the main issue is that it should not  
467 impede service interactions with an SP or IdP.

468 **Options:** Delete lines 725 and 726 from saml-profiles-2.0-os, starting at “The ECP MAY use...”.

469 **Disposition:** During the conference call of July 19 the TC approved to make the changes as stated here.

---

## 470 **E19: Clarification on Error Processing**

471 **First reported by:** Connor P. Cahill, AOL

472 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00008.html>

473 **Document:** Bindings

474 **Description:** Clarification on error processing

475 **Options:** The section numbers and line numbers are all from "saml-bindings-2.0-os.pdf"  
476 Section 3.2.2.1, lines 310-317:

- 477 • Change the first sentence to read:
  - 478 ○ The SAML responder SHOULD return a SOAP message containing either a SAML  
479 response element in the body or a SOAP fault.

- 480 • Delete the 3rd sentence (If a SAML responder cannot, for some reason, process....). SOAP  
481 defines when a SOAP fault is required and SAML goes into detail about what we should return  
482 when in section 3.2.3.3 "Error Reporting".
- 483 • Change the 4th sentence to soften the "MUST NOT" and make it a "SHOULD NOT" as there can  
484 be sufficient security through obscurity reasons to do so in some cases.
- 485 • Add a new sentence at the end of the paragraph noting that details about error handling are  
486 covered in section 3.2.3.3 "Error Reporting" or something to that effect.

487 Section 3.2.3.3, lines 370-383: Change the MUST on line 378 to a SHOULD.

488 **Disposition:** During the conference call of August 2 the TC approved the changes as stated here.

---

## 489 E20: ECP SSO Profile and Metadata

490 **First reported by:** Thomas Wisniewski, Entrust

491 **Message:** <http://lists.oasis-open.org/archives/security-services/200506/msg00106.html>

492 **Document:** Profiles

493 **Description:** There is no metadata consideration in ECP profile

494 **Options:** In SAML Profiles specification add new section 4.2.6 as follows:

495 The rules specified in the browser SSO profile in Section 4.1.6 apply here as well. Specifically, the  
496 indexed endpoint element <md:AssertionConsumerService> with a binding of  
497 urn:oasis:names:tc:SAML:2.0:bindings:PAOS, MAY be used to describe the supported binding and  
498 location(s) to which an identity provider may send responses to a service provider using this profile. And,  
499 the endpoint <md:SingleSignOnService> with a binding of urn:oasis:names:tc:SAML:2.0:bindings:SOAP,  
500 MAY be used to describe the supported binding and location(s) to which an service provider may send  
501 requests to an identity provider using this profile

502 **Disposition:** During the conference call of July 19 the TC approved to make the changes as stated here.

---

## 503 E21: PAOS Version

504 **First reported by:** Thomas Wisniewski, Entrust

505 **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00028.html>

506 **Document:** Bindings

507 **Description:** It's unclear what the word minimum implies in the line '... PAOS version with  
508 "urn:liberty:paos:2003-08" at a minimum."

509 **Options:** Strike the words "at a minimum"

510 **Disposition:** During the conference call of July 19 the TC approved to make the changes as stated here.

---

## 511 E22: Error in Profile/ECP

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

513 **Message:** <http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00040.html>

514 **Document:** Profiles

515 **Description:** Line 907 of Profiles says the responseConsumerURL must be the same as the  
516 "AssertionServiceConsumerURL" in an <AuthnRequest> message. The attribute's name should be  
517 "AssertionConsumerServiceURL".

518 **Options:** Make changes as specified.

519 **Disposition:** During the conference call of August 2 the TC approved the changes as stated here.

---

## 520 **E24: HTTPS in URI Binding**

521 **First reported by:** Nick Ragouzis, Enosis Group

522 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00037.html>

523 **Document:** Bindings

524 **Description:** Section 3.7, starting at line 1349 the text states:

525 "Like SOAP, URI resolution can occur over multiple underlying transports. This binding has transport-  
526 independent aspects, but also calls out the use of HTTP with SSL3.0 [SSL3] or TLS 1.0 [RFC2246] as  
527 REQUIRED (mandatory to implement)"

528 **Options:** Replace the current text with the following:

529 "Like SOAP, URI resolution can occur over multiple underlying transports. This binding has protocol-  
530 independent aspects, but also calls out as mandatory the implementation of HTTP URIs."

531 **Disposition:** During the conference call of August 2 the TC approved the changes as stated here.

532

---

## 533 **E25: Metadata Structures Feature in Conformance**

534 **First reported by:** Nick Ragouzis, Enosis Group

535 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00038.html>

536 **Document:** Conformance

537 **Description:** Conformance document does not specify any requirements with respect to metadata.

538 Change to Table 2: Feature Matrix

539

540

	IdP	IdPLite	SP	SPLite	ECP
--	-----	---------	----	--------	-----

541 FEATURE

542 Metadata Structures OPT OPT OPT OPT N/A

543 Metadata Interoperation OPT OPT OPT OPT N/A

544 Change to Table 4: SAML Authority and Requester Matrix

545

	AuthnAuth	AttribAuth	AuthZDcsnAuth	Requester
--	-----------	------------	---------------	-----------

546 FEATURE

547 Metadata Structures OPT OPT OPT OPT

548 Metadata Interoperation OPT OPT OPT OPT

549 New sub-sections to Section 3 (Conformance):

550 3.6 Metadata Structures

551 Implementations claiming conformance to SAMLv2.0 may declare each operational mode's conformance  
552 to SAMLv2.0 Metadata [SAMLMeta] through election of the Metadata Structures option.

553 With respect to each operational mode, such conformance entails the following:

554 \* Implementing SAML metadata according to the extensible SAMLv2.0 Metadata format in all cases  
555 where an interoperating peer has the option, as stated in SAMLv2.0 specifications, of depending on the  
556 existence of SAMLv2.0 Metadata. Electing the Metadata Structures option has the effect of requiring such

557 metadata be available to the interoperating peer. The Metadata Interoperation feature, described below,  
558 provides a means of satisfying this requirement.

559 \* Referencing, consuming, and adherence to the SAML metadata, according to [SAMLMeta], of an  
560 interoperating peer when the known metadata relevant to that peer and the particular operation, and the  
561 current exchange, has expired or is no longer valid in cache, provided the metadata is available and is not  
562 prohibited by policy or the particular operation and that specific exchange.

### 563 3.7 Metadata Interoperation

564 Election of the Metadata Interoperation option requires the implementation offer, in addition to any other  
565 mechanism, the well-known location publication and resolution mechanism described in SAML metadata  
566 [SAMLMeta].

567 **Options:** Make changes as suggested here

568 **Disposition:** During the TC conference call on 9/27 the TC accepted the changes as suggested here.

---

## 569 **E26: Ambiguities around Multiple Assertions and Statements in** 570 **the SSO Profile**

571 **First reported by:** Scott Cantor, OSU

572 **Message:** <http://lists.oasis-open.org/archives/security-services/200508/msg00056.html>

573 **Document:** Profiles

574 **Description:** SSO Profile need clarifications.

575 Section 4.1.4.2, <Response> Usage, replace the list at lines 541-572, with the following list:

- 576 • If the response is unsigned, the <Issuer> element MAY be omitted, but if present (or if the  
577 response is signed) it MUST contain the unique identifier of the issuing identity provider; the  
578 Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-  
579 format:entity
- 580 • It MUST contain at least one <Assertion>. Each assertion's <Issuer> element MUST contain the  
581 unique identifier of the responding identity provider; the Format attribute MUST be omitted or  
582 have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity. Note that this profile  
583 assumes a single responding identity provider, and all assertions in a response MUST be issued  
584 by the same entity.
- 585 • If multiple assertions are included, then each assertion's <Subject> element MUST refer to the  
586 same principal. It is allowable for the content of the <Subject> elements to differ (e.g. using  
587 different <NameID> or alternative <SubjectConfirmation> elements).
- 588 • Any assertion issued for consumption using this profile MUST contain a <Subject> element with  
589 at least one <SubjectConfirmation> element containing a Method of  
590 urn:oasis:names:tc:SAML:2.0:cm:bearer. Such an assertion is termed a bearer assertion. Bearer  
591 assertions MAY contain additional <SubjectConfirmation> elements.
- 592 • Assertions without a bearer <SubjectConfirmation> MAY also be included; processing of  
593 additional assertions or <SubjectConfirmation> elements is outside the scope of this profile.
- 594 • At least one bearer <SubjectConfirmation> element MUST contain a <SubjectConfirmationData>  
595 element that itself MUST contain a Recipient attribute containing the service provider's assertion  
596 consumer service URL and a NotOnOrAfter attribute that limits the window during which the  
597 assertion can be delivered. It MAY also contain an Address attribute limiting the client address  
598 from which the assertion can be delivered. It MUST NOT contain a NotBefore attribute. If the  
599 containing message is in response to an <AuthnRequest>, then the InResponseTo attribute  
600 MUST match the request's ID.
- 601 • The set of one or more bearer assertions MUST contain at least one <AuthnStatement> that  
602 reflects the authentication of the principal to the identity provider. Multiple <AuthnStatement>  
603 elements MAY be included, but the semantics of multiple statements is not defined by this profile.

- 604 • If the identity provider supports the Single Logout profile, defined in Section 4.4, any  
605 authentication statements MUST include a SessionIndex attribute to enable per-session logout  
606 requests by the service provider
- 607 • Other statements MAY be included in the bearer assertion(s) at the discretion of the identity  
608 provider. In particular, <AttributeStatement> elements MAY be included. The <AuthnRequest>  
609 MAY contain an AttributeConsumingServiceIndex XML attribute referencing information about  
610 desired or required attributes in [SAMLMeta]. The identity provider MAY ignore this, or send other  
611 attributes at its discretion.
- 612 • Each bearer assertion MUST contain an <AudienceRestriction> including the service provider's  
613 unique identifier as an <Audience>
- 614 • Other conditions (and other <Audience> elements) MAY be included as requested by the service  
615 provider or at the discretion of the identity provider. (Of course, all such conditions MUST be  
616 understood by and accepted by the service provider in order for the assertion to be considered  
617 valid.
- 618 • The identity provider is NOT obligated to honor the requested set of <Conditions> in the  
619 <AuthnRequest>, if any.

620 In Section 4.1.4.3, <Response> Message Processing Rules:

- 621 • Line 576, change "any bearer" to "the bearer"
- 622 • Line 578, change "any bearer" to "the bearer"
- 623 • Line 583, change to: "Verify that any assertions relied upon are valid in other respects. Note that  
624 while multiple bearer <SubjectConfirmation> elements may be present, the successful evaluation  
625 of a single such element in accordance with this profile is sufficient to confirm an assertion.  
626 However, each assertion, if more than one is present, MUST be evaluated independently."
- 627 • Line 584, change "any bearer" to "the bearer"
- 628 • Append to paragraph ending on line 591: "Note that if multiple <AuthnStatement> elements are  
629 present, the SessionNotOnOrAfter value closest to the present time SHOULD be honored."

630 Section 4.1.4.5, POST-Specific Processing Rules:

- 631 • Replace lines 600-601 with: "If the HTTP POST binding is used to deliver the <Response>, each  
632 assertion MUST be protected by a digital signature. This can be accomplished by signing each  
633 individual <Assertion> element or by signing the <Response> element."

634 **Options:**

635 **Disposition:** During the conference call of August 30 the TC approved the changes as stated here.

---

## 636 **E27: Error in ECP Profile**

637 **First reported by:** Scott Cantor, OSU

638 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00001.html>

639 **Document:** Profiles

640 **Description:** Profiles, line 947, the ECP RelayState header definition refers to step 5 as the one in which  
641 the response is issued to the SP. It should be step 7.

642 **Options:**

644 **Disposition:** During the conference call of September 13 the TC approved the changes as stated here

---

## 645 **E28: Conformance Table 1**

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

647 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>  
648 **Document:** Conformance  
649 **Description:** The first column is labeled “Profile”, yet several of the entries are technically not “profiles”.  
650 The same applies to the section title and the paragraph above the table.  
651 **Options:**  
652 Column 1:  
653 Combine Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query entries  
654 into a single entry labeled:  
655  
656 Assertion Query/Request  
657  
658 Column 2  
659  
660 Label each set of message flows with relevant protocol description:  
661 Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query  
662  
663 Column 3  
664  
665 No change  
666  
667 (2) Remove the following rows from the table:  
668  
669 SAML URI binding  
670 Metadata  
671 **Disposition:** During the conference call of September 27 the TC approved the changes as stated here

---

## 672 **E29: Conformance Table 2**

673 **First reported by:** Rob Philpott, RSA Security  
674 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>  
675 **Document:** Conformance  
676 **Description:** The table is missing feature rows for performing a “Request for Assertion by Identifier” over  
677 SOAP and for “SAML URI Binding”. These features are clearly permissible for IDP’s, since the  
678 IDPSSODescriptor includes an element for zero or more <AssertionIDRequestService> elements.  
679 **Options:** Add two rows table 2; row #1 is labeled Request for Assertion Identifier; row #2 is labeled SAML  
680 URI binding; both are optional for IdP row and N/A for all the rest.  
  
682 **Disposition:** During the conference call of September 27 the TC as stated here.

---

## 683 **E30: Considerations for key replacement**

684 **First reported by:** Rob Philpott, RSA Security  
685 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>  
686 **Document:** Core  
687 **Description:** Line 3110 states: “optionally one or more encrypted keys...”  
688  
689 **Options:** Replace “optionally one or more” with “zero or more”.  
  
691 **Disposition:** During the conference call of September 13 the TC approved the changes as stated here

---

## 692 E31: Various minor errors in Binding

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

694 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

695 **Document:** Bindings

696 **Description:**

- 697 1. Line 511: “security at the SOAP message layer is recommended.” It should be capitalized as in  
698 “RECOMMENDED”.
- 699 2. Line 785: “If no such value is included with a SAML request message” – “value” is ambiguous.  
700 It’s referring to the RelayState parameter, which itself is a name/value pair. This should be  
701 changed to “If no RelayState parameter is included...”
- 702 3. Line 1136: “using a direct SAML binding”. There is no definition for what a “direct” SAML binding  
703 is. Other documents have referred to the SOAP binding as a “synchronous” binding.
- 704 4. Line 1397: “Note that use of wildcards is not allowed on such ID queries”. This should be  
705 changed to: “Note that the URI syntax does not support the use of wildcards in such queries.”

706 **Options:**

708 **Disposition:** During the conference call of September 13 the TC approved the changes for items 2 and  
709 3. During the conference call of September 27 the TC approved the changes for items 1 and 4.

---

## 710 E32: Missing section in Profiles

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

712 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

713 **Document:** Profiles

714 **Description:** Section 4.3. This profile is missing a subsection for “Required Information”, which is present  
715 in all other profiles.  
716

717 **Options:** Beginning at line 1092, insert the following text:

718 4.3.1 Required Information

719 **Identification:** urn:oasis:names:tc:SAML:2.0:profiles:SSO:idp-discovery

720 **Contact information:** [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org)

721 **Description:** Given below.

722 **Updates:** None.

724 **Disposition:** During the conference call of December 5 the TC approved the changes.

---

## 725 E33: References to Assertion Request Protocol

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

727 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

728 **Document:** Metadata

729 **Description:** Lines 700, 871, and 904 state: “profile of the Assertion Request protocol defined in  
730 [SAMLProf]”. References to “Assertion Request” should be changed to “Assertion Query/Request”.

731 **Options:**

733 **Disposition:** During the conference call of September 13 the TC approved the changes.

---

## 734 E34: Section Heading

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

736 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00002.html>

737 **Document:** Metadata

738 **Description:** Line 809: the section 2.4.4.2 should be indented so that it is 2.4.4.1.1 since  
739 <RequestedAttribute> is part of the <AttributeConsumingService> defined in section 2.4.4.1.

740 .  
741

742 **Options:**

744 **Disposition:** During the conference call of September 13 the TC approved the change.

---

## 745 E35: Example in Profiles

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

747 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00023.html> and  
748 <http://www.oasis-open.org/archives/security-services/200602/msg00008.html>

749 **Document:** Profiles

750 **Description:** The example on page 29 line 964 uses a ResponseConsumerURL of [http://identity-](http://identity-service.example.com/abc)  
751 [service.example.com/abc](http://identity-service.example.com/abc). Since this value must be an AssertionConsumerService at the SP and must  
752 match (according to the rules in 4.2.4.4) the value of the responseConsumerURL, the example would result  
753 in an error condition.

754 **Options:** Change the value of the responseConsumerURL in the example on page 29 line 964 to  
755 [https://ServiceProvider.example.com/ecp\\_assertion\\_consumer](https://ServiceProvider.example.com/ecp_assertion_consumer).

756 Change the sentence on page 27 lines 906-908 to: "This value MUST be the same as the  
757 AssertionServiceConsumerURL (or the URL referenced in metadata) conveyed in the <AuthnRequest>  
758 and SHOULD NOT be a relative URL."

759 **Disposition:** During the conference call of February 28 TC approved the change as stated here.

---

## 760 E36: Clarification on Action Element

761 **First reported by:** Emily Xu, Sun Microsystems

762 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00053.html>

763 **Document:** Core

764 **Description:**

765 In section 2.7.4.2 of core spec, Namespace is marked as "Optional". It says: "If this element is absent, the  
766 namespace urn:oasis:names:tx:SAML:1.0:action:rwedc-negation specified in Section 8.1.2 is in effect."  
767 But in the following schema definition, attribute Namespace is marked as required:  
768 <attribute name="Namespace" type="anyURI" use="required"/>  
769

770 A clarification is needed to resolve this apparent conflict.

771 **Options:** In line 1359 change "Optional" to "Required" and strike the sentence starting at line 1361-1363  
772 ("If this element is absent....")

774 **Disposition:** During the conference call of October 25 the TC approved the change.

---

## 775 **E37: Clarification in Metadata on Indexed Endpoints**

776 **First reported by:** Rob Philpot, RSA Security

777 **Message:** <http://lists.oasis-open.org/archives/security-services/200510/msg00025.html>

778 **Document:** Metadata

779 **Description:** Metadata line 272 says "In any such sequence of like endpoints based on this type, the  
780 default...". It is a bit ambiguous what "of like endpoints" means. Are two endpoints alike if they are of the  
781 same binding type (e.g. SOAP)? Or are they alike because they are assigned to the same service  
782 endpoint.

783 **Options:** Modify Metadata, line 272 as follows:

784 "In any such sequence of indexed endpoints that share a common element name and namespace (i.e. all  
785 instances of <md:AssertionConsumerService> within a role), the default endpoint is..."

786 **Disposition:** During the conference call of November 22 the TC approved the changes as stated here

---

## 787 **E38: Clarification regarding index on <LogoutRequest>**

788 **First reported by:** Conor P. Cahill, AOL

789 **Message:** <http://lists.oasis-open.org/archives/security-services/200511/msg00000.html>

790 **Document:** Core, Profiles

791 **Description:** The language surrounding session index on the <LogoutRequest> (line 2546) is unclear.

792 **Options:** The following two changes are suggested:

793 1. Change Core, line 2546 as follows:

794 The index of the session between the principal identified by the <saml:BaseID>, <saml:NameID>, or  
795 <saml:EncryptedID> element, and the session authority. This must correlate to the SessionIndex  
796 attribute, if any, in the <saml:AuthnStatement> of the assertion used to establish the session that is  
797 being terminated."

798 2. Change Profiles, line 1302-1304 to:

799 "If the requester is a session participant, it MUST include at least one <SessionIndex> element in the  
800 request. (Note that the session participant always receives a SessionIndex attribute in the  
801 <saml:AuthnStatement> elements that it receives to initiate the session, per section 4.1.4.2 of the  
802 Web Browser SSO Profile.) If the requester is a session authority (or acting on its behalf), then it MAY  
803 omit any such elements to indicate the termination of all of the principal's applicable sessions."

804 **Disposition:** During the conference call of November 22 the TC approved the changes as stated here

---

## 805 **E39: Error in SAML profile example**

806 **First reported by:** Greg Whitehead, HP

807 **Message:** <http://www.oasis-open.org/archives/security-services/200601/msg00015.html>

808 **Document:** Profiles

809 **Description** In section 8.5.6 of the SAML 2.0 profiles doc the Idaprof:Encoding="LDAP" attribute  
810 should be AttributeValue not Attribute, according to section 8.2.4 of the spec.

811 **Options:**

812 **Disposition:** During the conference call of 1/17/2006 the TC approved the clarification as stated here.

---

## 813 **E40: Holder of Key**

814 **First reported by:** Prateek Mishra, Oracle

815 **Message:** <http://www.oasis-open.org/archives/security-services/200601/msg00027.html>

816 **Document:** Core

817 **Description:** HoK described a key that required proof of possession by a attesting entity vs. being held  
818 by the subject, Appropriate text does appear in lines 781-783 of saml2-core. However,  
819 lines 335-337 of saml2-profiles reads:  
820 "As described in [XMLSig], each <ds:KeyInfo> element holds a key or information that enables an  
821 application to obtain a key. The holder of a specified key is considered to be the subject of the assertion  
822 by the asserting party"  
823 The last sentence should be replaced by:  
824 "The holder of a specified key is considered to be an acceptable attesting entity for the assertion by the  
825 asserting party"  
826 **Options:**  
827 **Disposition:** During the conference call of February 28th the TC approved the change as stated here.

---

## 828 **E41: EndpointType ResponseLocation clarification in Metadata**

829 **First reported by:** Eric Tiffany, Project Liberty  
830 **Message:** <http://www.oasis-open.org/archives/security-services/200601/msg00034.html>  
831 **Document:** Metadata  
832 **Description** Implementer interpreted the metadata spec to mean that ResponseLocation should only be  
833 omitted for the SOAP binding, and that the ResponseLocation be specified in metadata for other bindings.  
834 **Options:** Proposed text to resolve this:  
835 At line 238 in Metadata we have now:  
836 "The ResponseLocation attribute is used to enable different endpoints to be specified for receiving  
837 request and response messages associated with a protocol or profile, not as a means of load-balancing  
838 or redundancy (multiple elements of this type can be included for this purpose). When a role contains an  
839 element of this type pertaining to a protocol or profile for which only a single type of message (request or  
840 response) is applicable, then the ResponseLocation attribute is unused.  
841 The proposal is to add the following:  
842 "If the ResponseLocation attribute is omitted, any response messages associated with a protocol or  
843 profile may be assumed to be handled at the URI indicated by the Location attribute."  
844 **Disposition:** During the conference call of 1/31/06 TC voted to approve changes as stated here.

---

## 845 **E42: Conformance Table 4**

846 **First reported by:** Thomas Wisniewski, Entrust  
847 **Message:** <http://lists.oasis-open.org/archives/security-services/200601/msg00041.html>  
848 **Document:** Conformance  
849 **Description:** Table 4 has a cell for SAML <x> Authority responding to an <y> Query. That is, an Attribute  
850 Authority responding to an Authentication or Authorization Decision Query. This doesn't seem to make  
851 sense as authorities should respond to their respective queries. So the OPTIONAL items under the  
852 authorities should be N/A."  
853 **Options:** Change the reference from "OPTIONAL" to "N/A" under the columns SAML Authentication  
854 Authority, SAML Attribute Authority, and SAML Authorization Decision Authority in Table 4: SAML  
855 Authority and Requester Matrix.  
856 **Disposition:** During the conference call of 1/31/06 TC voted to approve changes as stated here.

---

## 857 **E43: Key location in saml:EncryptedData**

858 **First reported by:** Heather Hinton, IBM

859 **Message:**

860 **Document:** Core

861 **Description:** The specification in core does not properly follow XML Encryption standards with respect to  
862 key location.

863 **Options:** Replace section 6 of core with the following text:  
864

## 865 **6.1 General Considerations**

866 Encryption of the <Assertion>, <BaseID>, <NameID> and <Attribute> elements is provided  
867 by use of XML Encryption [XMLEnc]. Encrypted data and optionally one or more encrypted keys  
868 MUST replace the plaintext information in the same location within the XML instance. The  
869 <xenc:EncryptedData> element's Type attribute SHOULD be used and, if it is present, MUST  
870 have the value <http://www.w3.org/2001/04/xmlenc#Element>.

871 Any of the algorithms defined for use with XML Encryption MAY be used to perform the  
872 encryption. The SAML schema is defined so that the inclusion of the encrypted data yields a  
873 valid instance.

## 874 **6.2 Key and Data Referencing Guidelines**

875 If an encrypted key is NOT included in the XML instance, then the relying party must be able to  
876 locally determine the decryption key, per [XMLEnc].

877 Implementations of SAML MAY implicitly associate keys with the corresponding data they are  
878 used to encrypt, through the positioning of <xenc:EncryptedKey> elements next to the  
879 associated <xenc:EncryptedData> element, within the enclosing SAML parent element.  
880 However, the following set of explicit referencing guidelines are suggested to facilitate  
881 interoperability.

882 If the encrypted key is included in the XML instance, then it SHOULD be referenced within the  
883 associated <xenc:EncryptedData> element, or alternatively embedded within the  
884 <xenc:EncryptedData> element. When an <xenc:EncryptedKey> element is used, the  
885 <ds:KeyInfo> element within <xenc:EncryptedData> SHOULD reference the  
886 <xenc:EncryptedKey> element using a <ds:RetrievalMethod> element of Type  
887 <http://www.w3.org/2001/04/xmlenc#EncryptedKey>.

888 In addition, an <xenc:EncryptedKey> element SHOULD contain an <xenc:ReferenceList>  
889 element containing a <xenc:DataReference> that references the corresponding  
890 <xenc:EncryptedData> element(s) that the key was used to encrypt.

891 In scenarios where the encrypted element is being "multicast" to multiple recipients, and the key  
892 used to encrypt the message must be in turn encrypted individually and independently for each  
893 of the multiple recipients, the <xenc:CarriedKeyName> element SHOULD be used to assign a  
894 common name to each of the <xenc:EncryptedKey> elements so that a <ds:KeyName> can be  
895 used from within the <xenc:EncryptedData> element's <ds:KeyInfo> element.

896 Within the <xenc:EncryptedData> element, the <ds:KeyName> can be thought of as an "alias"  
897 that is used for backwards referencing from the <xenc:CarriedKeyName> element in each  
898 individual <xenc:EncryptedKey> element. While this accommodates a "multicast" approach,  
899 each recipient must be able to understand (at least one) <ds:KeyName>. The Recipient  
900 attribute is used to provide a hint as to which key is meant for which recipient.  
901

902 The SAML implementation has the discretion to accept or reject a message where multiple  
903 Recipient attributes or <ds:KeyName> elements are understood. It is RECOMMENDED that  
904 implementations simply use the first key they understand and ignore any additional keys.  
905

### 906 6.3 Examples

907 In the following example, the parent element (<EncryptedID>) contains  
908 <xenc:EncryptedData> and (referenced) <xenc:EncryptedKey> elements as siblings (note  
909 that the key can in fact be anywhere in the same instance, and the key references the  
910 <xenc:EncryptedData> element) :

```
911 <saml:EncryptedID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">  
912   <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"   
913     Id="Encrypted_DATA_ID"   
914     Type="http://www.w3.org/2001/04/xmlenc#Element">  
915     <xenc:EncryptionMethod   
916       Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-  
917 cbc"/>  
918     <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
919       <ds:RetrievalMethod URI="#Encrypted_KEY_ID"   
920   
921       Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>  
922     </ds:KeyInfo>  
923     <xenc:CipherData>  
924       <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>  
925     </xenc:CipherData>  
926   </xenc:EncryptedData>  
927   
928   <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"   
929     Id="Encrypted_KEY_ID">  
930     <xenc:EncryptionMethod   
931 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>  
932     <xenc:CipherData>  
933 <xenc:CipherValue>PzA5X...</xenc:CipherValue>  
934 </xenc:CipherData>  
935     <xenc:ReferenceList>  
936       <xenc:DataReference URI="#Encrypted_DATA_ID"/>  
937     </xenc:ReferenceList>  
938   </xenc:EncryptedKey>  
939 </saml:EncryptedID>
```

940

941 In the following <EncryptedAttribute> example, the <xenc:EncryptedKey> element is contained within the  
942 <xenc:EncryptedData> element, so there is no explicit referencing:

```
943 <saml:EncryptedAttribute   
944 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">  
945   <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"   
946     Id="Encrypted_DATA_ID"   
947     Type="http://www.w3.org/2001/04/xmlenc#Element">  
948     <xenc:EncryptionMethod   
949 Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>  
950     <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
951       <xenc:EncryptedKey Id="Encrypted_KEY_ID">  
952         <xenc:EncryptionMethod   
953 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>  
954         <xenc:CipherData>  
955         <xenc:CipherValue>SDFSDF... </xenc:CipherValue>  
956       </xenc:CipherData>  
957     </xenc:EncryptedKey>  
958   </ds:KeyInfo>  
959   <xenc:CipherData>
```

```
960 <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
961 </xenc:CipherData>
962 </xenc:EncryptedData>
963 </saml:EncryptedAttribute>
```

964 The final example shows an assertion encrypted for multiple recipients, using the <xenc:CarriedKeyName>  
965 approach:

```
966 <saml:EncryptedAssertion
967 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
968 <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
969 Id="Encrypted_DATA_ID"
970 Type="http://www.w3.org/2001/04/xmlenc#Element">
971 <xenc:EncryptionMethod
972 Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
973 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
974 <ds:KeyName>MULTICAST_KEY_NAME</ds:KeyName>
975 </ds:KeyInfo>
976 <xenc:CipherData>
977 <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
978 </xenc:CipherData>
979 </xenc:EncryptedData>
980
981 <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
982 Id="Encrypted_KEY_ID_1" Recipient="https://spl.org">
983 <xenc:EncryptionMethod
984 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
985 1_5"/>
986 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
987 <ds:KeyName>KEY_NAME_1</ds:KeyName>
988 </ds:KeyInfo>
989 <xenc:CipherData>
990 <xenc:CipherValue>xyzABC...</xenc:CipherValue>
991 </xenc:CipherData>
992 <xenc:ReferenceList>
993 <xenc:DataReference URI="#Encrypted_DATA_ID"/>
994 </xenc:ReferenceList>
995
996 <xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
997 </xenc:EncryptedKey>
998
999 <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
1000 Id="Encrypted_KEY_ID_2" Recipient="https://sp2.org">
1001 <xenc:EncryptionMethod
1002 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
1003 1_5"/>
1004 <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
1005 <ds:KeyName>KEY_NAME_2</ds:KeyName>
1006 </ds:KeyInfo>
1007 <xenc:CipherData>
1008 <xenc:CipherValue>abcXYZ...</xenc:CipherValue>
1009 </xenc:CipherData>
1010 <xenc:ReferenceList>
1011 <xenc:DataReference URI="#Encrypted_DATA_ID"/>
1012 </xenc:ReferenceList>
1013
1014 <xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
1015 </xenc:EncryptedKey>
1016 </saml:EncryptedAssertion>
```

1017 **Disposition:** During the TC conference call on 5/23/06, the TC approved the changes as stated here.

1018

---

## E45: AuthnContext comparison clarifications

1019 **First reported by:** Scott Cantor, OSU

1020 **Message:** <http://www.oasis-open.org/archives/security-services/200602/msg00024.html>

1021 **Document:** Core

1022 **Description:** In section 3.3.2.2.1 contexts are not necessarily a fully ordered set. This should be noted to  
1023 aid in the interpretation of the comparison types.

1024 **Options:**

1025 **Replace the paragraph at 1815-1819 with:**

1026 Either a set of class references or a set of declaration references can be used. If ordering is relevant to  
1027 the evaluation of the request, then the set of supplied elements MUST be evaluated as an ordered set,  
1028 where the first element is the most preferred authentication context class or declaration. For example,  
1029 ordering is significant when using this element in an

1030 <AuthnRequest> message but not in an <AuthnQuery> message.

1031 If none of the specified classes or declarations can be satisfied in accordance with the rules below, then  
1032 the responder MUST return a <Response> message with a second-level <StatusCode> of  
1033 urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext."

1034 **Change current lines 1825-1827 to:**

1035 If Comparison is set to "better", then the resulting authentication context in the authentication statement  
1036 MUST be stronger (as deemed by the responder) than one of the authentication contexts specified."

1037 **Disposition:** During the conference call of 3/28/06 TC voted to approve changes as stated here

---

1038

## E46: AudienceRestriction clarifications

1039 **First reported by:** Connor P. Cahill, Intel

1040 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00001.html>

1041 **Document:** Core

1042 **Description:** On lines 922-925 in the core specification for 2.0, the sentence states:

1043 The effect of this requirement and the preceding definition is that within a given condition, the audiences  
1044 form a disjunction (an "OR") while multiple conditions form a conjunction (an "AND")

1045 **Options:** Clarify by modifying these lines to read as follows:

1046 The effect of this requirement and the preceding definition is that within a given <AudienceRestrictions>,  
1047 the <Audience>s form a disjunction (an "OR") while multiple <AudienceRestrictions> form a conjunction  
1048 (an "AND").

1049 **Disposition:** During the conference call of 5/9/06 the TC approved the change as proposed here.

---

1050

## E47: Clarification on SubjectConfirmation

1051 **First reported by:** Scott Cantor, OSU

1052 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00008.html>

1053 **Document:** Core and profiles

1054 **Description:** The language on Subject Confirmation element and the intent of the embedded secondary  
1055 identifier requires clarification.

1056 **Options:**

1057 **Insert the following at line 698 of core**

1058 If the <SubjectConfirmation> element in an assertion subject contains an identifier the issuer authorizes  
1059 the attesting entity to wield the assertion on behalf of that subject. A relying party MAY apply additional

1060 constraints on the use of such an assertion at its discretion, based upon the identities of both the subject  
1061 and the attesting entity.

1062 If an assertion is issued for use by an entity other than the subject, then that entity SHOULD be identified  
1063 in the <SubjectConfirmation> element."

1064 **Replace lines 335-337 in Profiles with:**

1065 As described in [XMLSig], each <ds:KeyInfo> element holds a key or information that enables an  
1066 application to obtain a key. The holder of one or more of the specified keys is considered to be an  
1067 acceptable attesting entity for the assertion by the asserting party.

1068

1069 **Insert the following at line 341 of Profiles**

1070 "If the keys contained in the <SubjectConfirmationData> element belong to an entity other than the  
1071 subject, then the asserting party SHOULD identify that entity to the relying party by including a SAML  
1072 identifier representing it in the enclosing <SubjectConfirmation> element.

1073 Note that a given <SubjectConfirmation> element using the Holder of Key method SHOULD include keys  
1074 belonging to only a single attesting entity. If multiple attesting entities are to be permitted to use the  
1075 assertion, then multiple <SubjectConfirmation> elements SHOULD be included.

1076 **Replace lines 361-363 in Profiles with:**

1077 The bearer of the assertion is considered to be an acceptable attesting entity for the assertion by the  
1078 asserting party, subject to any optional constraints on confirmation using the attributes that MAY be  
1079 present in the <SubjectConfirmationData> element, as defined by [SAMLCore].

1080 If the intended bearer is known by the asserting party to be an entity other than the subject, then the  
1081 asserting party SHOULD identify that entity to the relying party by including a SAML identifier  
1082 representing it in the enclosing <SubjectConfirmation> element.

1083 If multiple attesting entities are to be permitted to use the assertion based on bearer semantics, then  
1084 multiple <SubjectConfirmation> elements SHOULD be included."

1085 **Disposition:** During the conference call of 3/28/06 TC voted to approve changes as stated here

---

## 1086 **E48: Clarification on encoding for binary values in LDAP profile**

1087 **First reported by:** Greg Whitehead, HP

1088 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00034.html>

1089 **Document:** Profiles

1090 **Description:** In describing the encoding for binary values, the LDAP profile text is ambiguous about  
1091 whether the ASN.1 OCTET STRING wrapper should be included or not.

1092 **Options:**

1093 Change line 1762 of Profiles to:

1094 ... by base64-encoding [RFC2045] the contents of the ASN.1 OCTET STRING-encoded LDAP attribute  
1095 value (not including the ASN.1 OCTET STRING wrapper)

1096 **Disposition:** During the conference call of 5/09/06 TC voted to approve changes as stated here

---

## 1097 **E49: Clarification on attribute name format**

1098 **First reported by:** Greg Whitehead, HP

1099 **Message:** <http://www.oasis-open.org/archives/security-services/200603/msg00034.html>

1100 **Document:** Core

1101 **Description:** The relationship between an attribute's `NameFormat` and its syntax is not clear.

1102 **Options:**

1103

1104 **Add the following text after line 1217 of core:**

1105 Attributes are identified/named by the combination of the NameFormat and Name XML attributes  
1106 described above. Neither one in isolation can be assumed to be unique, but taken together, they ought to  
1107 be unambiguous within a given deployment.  
1108 The SAML profiles specification [SAMLProf] includes a number of attribute profiles designed to improve  
1109 the interoperability of attribute usage in some identified scenarios. Such profiles typically include  
1110 constraints on attribute naming and value syntax. There is no explicit indicator when an attribute profile is  
1111 in use, and it is assumed that deployments can establish this out of band, based on the combination of  
1112 NameFormat and Name.  
1113 **Disposition:** During the TC conference call on 7/18 the TC approved the changes as stated here

---

## 1114 **E50: Clarification SSL Ciphersuites**

1115 **First reported by:** Eric Tiffany, Liberty Alliance

1116 **Message:** <http://www.oasis-open.org/archives/security-services/200604/msg00030.html>

1117 **Document:** Conformance

1118 **Description:** The text needs to be clarified based on ciphersuites that were explicitly called out in the text.  
1119 This is required to make it clear that:

- 1120 1. these are not the only ones that are supported, and
- 1121 2. this is not a minimal set that needs to be supported.

1122 **Options:**

1123 Change the following in the Conformance document:

- 1124 1. In the intro of section 4 (XML Digital Signature and XML Encryption) after line 235, add:
  - 1125 • The algorithms listed below as being required for SAML 2.0 conformance are based on
  - 1126 the mandated algorithms in the W3C recommendations for XML Signature and for XML
  - 1127 Encryption, but modified by the SSTC to ensure interoperability of conformant SAML
  - 1128 implementations. While the SAML-defined set of algorithms is a minimal set for
  - 1129 conformance, additional algorithms supported by XML Signature and XML Encryption
  - 1130 MAY be used. Note, however, that the use of non-mandated algorithms may introduce
  - 1131 interoperability issues if those algorithms are not widely implemented. As additional
  - 1132 algorithms become mandated for use in XML Signature and XML Encryption, the set
  - 1133 required for SAML conformance may be extended. [RSP: not sure about including the
  - 1134 last sentence... opinions?]
- 1135 1. In the intro of section 5 (Use of SSL 3.0 and TLS 1.0) after line 257, add:
  - 1136 • The set up algorithms required for SAML 2.0 conformance is equivalent to that defined in
  - 1137 SAML 1.0 and SAML 1.1. These mandated algorithms were chosen by the SSTC
  - 1138 because of their wide implementation support in the industry. While the algorithms
  - 1139 defined below are the minimal set for SAML conformance, additional algorithms
  - 1140 supported by SSL 3.0 and TLS 1.0 MAY be used.

1141 **Disposition:** During the conference call of 5/23/06 TC voted to approve changes as stated here

---

## 1142 **E51: Schema type of contents of <AttributeValue>**

1143 **First reported by:** Prateek Mishra, Oracle

1144 **Message:** <http://lists.oasis-open.org/archives/security-services/200605/msg00001.html>

1145 **Document:** Profiles

1146 **Description:** Section 8.1 of SAML 2 Profiles state:

1147 The Basic attribute profile specifies simplified, but non-unique, naming of SAML attributes together with  
1148 attribute values based on the built-in XML Schema data types, eliminating the need for extension  
1149 schemas to validate syntax.

1150

1151 Further in the document, lines (1699-70) it states:

1152 The schema type of the contents of the <AttributeValue> element MUST be drawn from one of the types  
1153 defined in Section 3.3 of [Schema2].

1154 This appears to be in error. Section 3 of [Schema2] defines the "Built-in Datatypes" and Section 3.3 is one  
1155 specific sub-section within it (defines "Derived Datatypes"). With the current language both "Date" and  
1156 "anyURI" are excluded; I somehow do not believe this was the original intent.

1157 **Options:** Replace lines 1699-70 with:

1158 The schema type of the contents of the <AttributeValue> element MUST be drawn from one of the types  
1159 defined in Section 3 of [Schema 2].

1160 **Disposition:** During the TC conference call on 5/9 the TC approved the changes as proposed here

---

## 1161 **E52: Clarification on <NotOnOrAfter> attribute**

1162 **First reported by:** Rob Philpott, RSA Security

1163 **Message:** <http://lists.oasis-open.org/archives/security-services/200605/msg00007.html>

1164 **Document:** Profiles

1165 **Description:** Line 556-7: "a NotOnOrAfter attribute that limits the window during which the assertion  
1166 can be delivered."

1167 The NotOnOrAfter in a ConfirmationData element isn't about a window when the assertion can be  
1168 delivered. Core defines it as being the time after which the subject cannot be confirmed. That's  
1169 independent of assertion delivery

1170 **Options:**

1171 Changes Profiles lines 556-7 from:

1172 "a NotOnOrAfter attribute that limits the window during which the assertion can be delivered"

1173 to:

1174 "a NotOnOrAfter attribute that limits the window during which the recipient can perform a confirmation  
1175 of the assertion <Subject>".

1176 **Disposition:** During the TC conference call on 15 Aug 2006 the TC modified the wording to read  
1177 "...during which the assertion can be confirmed by the relying party" and approved the change.

---

## 1178 **E53: Correction to LDAP/X.500 profile attribute**

1179 **First reported by:** Scott Cantor, OSU

1180 **Message:** <http://lists.oasis-open.org/archives/security-services/200605/msg00004.html>

1181 **Document:** Profiles

1182 **Description:** The X.500/LDAP attribute profile is schema-invalid right now because we tell people to  
1183 specify xsi:type="xsd:string" but then add our own X500:Encoding attribute into the AttributeValue  
1184 element. That's illegal. Any fix would be a normative change to the profile, so either it has to be fixed or  
1185 create a new profile and deprecate the original.

1186 **Options:**

- 1187 1. Remove the xsi:type requirement.  
1188 Forces implementations to recognize string vs base64 encoding based on Attribute Name.  
1189
- 1190 2. Remove the x500:Encoding attribute.  
1191 Forces implementations to trigger profile behavior based on Attribute Namespace and Name,  
1192 encoding rules are implied.
- 1193 3. Move the x500:Encoding attribute to the Attribute element.  
1194 Suggests that future encoding rules will be uniform across all values of an attribute, but otherwise  
1195 fully consistent with intent of profile.  
1196

- 1197 4. Define an extended schema type that extends string and base64Binary with the x500:Encoding  
1198 attribute and change the mandated xsi:type values to the extended types. Least change to existing  
1199 profile behavior, but requires publishing and approving an additional schema document.
- 1200 5. Deprecate the existing profile and define a new one incorporation whatever input can be gleaned  
1201 from implementers.
- 1202 6. A variation on 2 and 3, which is to:
- 1203 a. remove the x500:Encoding attribute and document that the LDAP encoding uses xsi:type  
1204 string and base64Binary
- 1205 b. document that other encodings should define new types
- 1206 **Disposition:** During the TC conference call on 6/20 the TC approved option 3 (which subsumes option 5)  
1207 but subsequently decided that this would be a substantive change, such that the profile would have to be  
1208 deprecated once a replacement profile could be specified. At the 16 January 2007 TC telecon we agreed  
1209 it's now safe to mention the (still-draft) new profile and do the deprecation.

---

## 1210 E54: Correction to ECP URN

1211 **First reported by:** Thomas Wisniewski, Entrust

1212 **Message:** <http://lists.oasis-open.org/archives/security-services/200606/msg00019.html>

1213 **Document:** Profiles

1214 **Description:**

1215 Line 757: The reference to the ecp urn should be in double quotes.

1216 Lines 763 - 764: In the example, the reference to the ecp urn and the PAOS version should be in double  
1217 quotes instead of single quotes.

1218 Both of these seem incorrect based on the PAOS specification lines 95 - 100.

1219 **Disposition:** During the TC conference call on 6/20 the TC approved to make the changes as stated  
1220 here.

---

## 1221 E55: Various Language Cleanups

1222 **First reported by:** Scott Cantor, OSU

1223 **Message:** <http://lists.oasis-open.org/archives/security-services/200606/msg00026.html>

1224 **Document:** Core and Profiles

1225 **Description:** This erratum attempts to capture all language cleanup in light of repeated questions. The  
1226 goal here is to clarify these fundamental issues:

- 1227 • NameIDMgmt applies to most of the formats
- 1228 • NameIDMgmt affects only a given identifier for a principal, not every possible identifier that might  
1229 exist for a principal (this is intended as a simplification)

1230 Profiles, line 1319, change "some form of persistent identifier" to "some form of long-term identifier  
1231 (including but not limited to identifiers with the Format urn....persistent)"

1232 Profiles, line 1323, change "about the principal" to "using that identifier".

1233 Core, lines 3337-3339, I'm inclined to say that text should be struck.

1234 Core, line 2477, change "it will no longer issue assertions to the SP about the principal" to "it will no  
1235 longer issue assertions to the SP using that identifier". This does step on an errata, but is a separate  
1236 change from it.

1237 Core, line 2483, change "regarding this principal" to "using the primary identifier".

1238 Core, line 2487-8, change "regarding this principal" to "in any case where the identifier being changed  
1239 would have been used".

1240 **Disposition:** During the TC conference call on 8/15 the TC approved the changes as proposed here

1241

---

## E56: Typo in Profiles

1242 **First reported by:** Eric Tiffany, Liberty Alliance

1243 **Message:** <http://lists.oasis-open.org/archives/security-services/200606/msg00021.html>

1244 **Document:** Profiles

1245 **Description:** Line 326 of profiles states:

1246 "It is anticipated that profiles will define and use several different values for <ConfirmationMethod>"  
1247 The last atom should be "Method" as there is not any<ConfirmationMethod> element in the SAML  
1248 schema.

1249 **Disposition:** During the conference call on 7/18 the TC approved to making the changes as stated here.

---

1250

## E57: SAMLmime Reference

1251 **First reported by:** Jeff Hodges, Nustar

1252 **Message:** <http://lists.oasis-open.org/archives/security-services/200606/msg00036.html>

1253 **Document:** Bindings

1254 **Description:** The [SAMLmime] reference in saml-bindings-2.0-os lines 1468-1469 reads as:

1255 [SAMLmime] application/saml+xml Media Type Registration, IETF Internet-Draft,  
1256 <http://www.ietf.org/internet-drafts/draft-hodges-saml-mediatype-01.txt>.

1257 The document draft-hodges-saml-mediatype-01 expired (and thus was deleted from the I-D repository),  
1258 since we ended up using the new "fast track" MIME Media Type registration process rather than  
1259 publishing an RFC.

1260 **Options:** The reference should be replaced with a reference similar to

1261 [SAMLmime] OASIS Security Services Technical Committee (SSTC), "application/samlassertion+xml  
1262 MIME Media Type Registration", IANA MIME Media Types Registry application/samlassertion+xml,  
1263 December 2004. <http://www.iana.org/assignments/media-types/application/samlassertion+xml>

1264 **Disposition:** During the TC conference call on 7/18 the TC approved the changes as stated here

---

1265

## E58: Typos in Profiles

1266 **First reported by:** Tom Scavo, NCSA/University of Illinois

1267 **Message:** <http://www.oasis-open.org/archives/security-services/200607/msg00049.html>

1268 **Document:** Profiles

1269 **Description:** There are two minor errors in the profiles document on lines 626 and 627.

1270 **Options:**

1271 On line 626 change "sign" to "signing"

1272 On line 627 change "encrypt" to "encryption"

1273 **Disposition:** During the TC conference call on 8/15 the TC approved the changes as proposed here

---

1274

## E59: SSO Response when using HTTP-Artifact

1275 **First reported by:** Rob Phillpot, RSA Security

1276 **Message:** <http://www.oasis-open.org/archives/security-services/200509/msg00019.html>

1277 **Document:** Bindings

1278 **Description:** The specification mandates support for the HTTP Artifact binding for a Web SSO  
1279 <Response> in full and Lite versions of IDP's and SP's. However, the spec does not indicate what  
1280 mechanisms (HTTP Redirect or HTTP POST) are mandated for delivery of the artifact.

1281 **Options:**  
1282 Insert a clarifying paragraph after line 1173 of Bindings:  
1283 "Finally, note that the use of the Destination attribute in the root SAML element of the protocol message is  
1284 unspecified by this binding, because of the message indirection involved."  
1285 **Disposition:** During the TC conference call on 8/15 the TC approved the changes as proposed here

---

## 1286 **E60: Incorrect URI**

1287 **First reported by:** Tom Scavo, NCSA/University of Illinois  
1288 **Message:** <http://lists.oasis-open.org/archives/security-services/200608/msg00069.html>  
1289 **Document:** Core  
1290 **Description:** Line 460 references the URI

1291 `urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified.`  
1292 This is incorrect and should be replaced with

1293 `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

1294 **Options:**  
1295 **Disposition:** During the TC conference call on 8/29, the TC approved the changes as proposed here.

---

## 1296 **E61 Reference to non-existent element**

1297 **First reported by:** Tom Scavo, NCSA/University of Illinois  
1298 **Message:** <http://lists.oasis-open.org/archives/security-services/200608/msg00075.html>  
1299 **Document:** Core  
1300 **Description:** Line 3160 of core refers to the <Request> element. This is a non-existent element.  
1301 **Options:** Delete line 3160  
1302 **Disposition:** During the TC conference call on 8/29 the TC approved the changes as proposed here.  
1303 (Additional edits proposed, in order to make sense of the text that remains. Scheduled to be brought up in  
1304 13 Feb 2007 telecon again for final approval.)  
1305

---

## 1306 **E62: TLS Keys in KeyDescriptor**

1307 **First reported by:** Scott Cantor on security-services list  
1308 **Message:** <http://lists.oasis-open.org/archives/security-services/200612/msg00034.html>  
1309 **Document:** Metadata  
1310 **Description:** The Metadata specification is underspecified with regard to how to interpret the  
1311 KeyDescriptor element's "use" attribute and how TLS keys are expressed.  
1312 **Options:** Scott proposes one solution: Insert text after line 624 of Metadata:  
1313 A use value of "signing" means that the contained key information is applicable to both  
1314 signing and TLS/SSL operations performed by the entity when acting in the enclosing role.  
  
1315 A use value of "encryption" means that the contained key information is suitable for use in  
1316 wrapping encryption keys for use by the entity when acting in the enclosing role.  
  
1317 If the use attribute is omitted, then the contained key information is applicable to both of the  
1318 above uses.

1319 He further comments: "If "wrapping encryption keys" isn't a precise enough term, please find some crypto  
1320 experts to clarify it... It's worth noting to the TC that this doesn't even scratch the surface of the problems  
1321 with KeyInfo interop, and spec and product users are starting to notice..."  
1322

1323 **Disposition:** During the TC conference call on [16 January 2007](#) the TC approved the changes as  
1324 proposed here.

---

## 1325 **E63: IdP Discovery Cookie Interpretation**

1326 **First reported by:** Scott Cantor on security-services list

1327 **Message:** <http://lists.oasis-open.org/archives/security-services/200612/msg00035.html>

1328 **Document:** Profiles

1329 **Description:** There is confusion over how the contents of an IdP Discovery cookie are meant to be  
1330 interpreted because of the allowance for specifying either persistent or session lifetime.

1331 **Options:** Scott proposes one solution: In Profiles Section 4.3, insert the following paragraph after line  
1332 1105:

1333 Note that while a session-only cookie can be used, the intent of this profile is not to provide a  
1334 means of determining whether a user actually has an active session with one or more of the  
1335 identity providers stored in the cookie. The cookie merely identifies identity providers known  
1336 to have been used in the past. Service providers MAY instead rely on the IsPassive attribute  
1337 in their samlp:AuthnRequest message to probe for active sessions.

1338 **Disposition:** During the TC conference call on [16 January 2007](#) the TC approved the changes as  
1339 proposed here.

---

## 1340 **E64: Liberty Moniker Used Inappropriately**

1341 **First reported by:** Jeff Hodges on security-services list

1342 **Message:** <http://lists.oasis-open.org/archives/security-services/200702/msg00047.html>

1343 **Document:** SecConsider

1344 **Description:** Section 7.1.1.9, Impersonation without Reauthentication, contains the following text:

1345 Cookies posted by identity providers MAY be used to support this validation process, though  
1346 **Liberty** does not mandate a cookie-based approach.

1347 **Options:** The reference to Liberty should be changed to a reference to SAML V2.0, as follows:

1348

1349 Cookies posted by identity providers MAY be used to support this validation process, though  
1350 **SAML V2.0** does not mandate a cookie-based approach.

1351 **Disposition:** During the [TC conference call on 27 Feb 2007](#), the TC approved the changes as proposed  
1352 here.

---

## 1353 **E65: Second-level StatusCode**

1354 **First reported by:** Philpott, Robert, EMC

1355 **Message:** <http://lists.oasis-open.org/archives/security-services/200708/msg00053.html>

1356 **Document::** SAML Core

1357 **Description:** There are several places in SAML Core that are currently mandating the return of second-  
1358 level <StatusCode> elements, which for security reasons are assumed to be optional.

1359 **Options:** Reword the relevant sections to indicate that use of a second-level code is optional, but if  
1360 present, the value is constrained.

1361 Change section 3.3.2.2.1 Element `<RequestedAuthnContext>`, lines 1817-1819, to:

1362       If none of the specified classes or declarations can be satisfied in accordance with the rules  
1363       below, then the responder **MUST** return a `<Response>` message with a top-level  
1364       `<StatusCode>` value of `urn:oasis:names:tc:SAML:2.0:status:Responder` and **MAY**  
1365       return a second-level `<StatusCode>` value of  
1366       `urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext`.

1367 Change section 3.4.1.2, lines 2172-2173, to:

1368       In profiles specifying an active intermediary, the intermediary **MAY** examine the list and return a  
1369       `<Response>` message with an error `<Status>` and optionally a second-level `<StatusCode>` of

1370 Change section 3.4.1.5.1 Proxy Processing Rules, lines 2282-2285, to:

1371       Unless the identity provider can directly authenticate the presenter, it **MUST** return a  
1372       `<Response>` message with a top-level `<StatusCode>` value of  
1373       `urn:oasis:names:tc:SAML:2.0:status:Responder` and **MAY** return a second-level  
1374       `<StatusCode>` value of  
1375       `urn:oasis:names:tc:SAML:2.0:status:ProxyCountExceeded`.

1376 Change section 3.8.3, lines 2729-2731:

1377       If the responder does not recognize the principal identified in the request, it **MAY** respond with an  
1378       error `<Status>`, optionally containing a second-level `<StatusCode>` of  
1379       `urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal`.

1380 **Disposition:** During the TC conference call on [11 March 2008](#) the TC approved the changes as  
1381 proposed here.

---

## E66: Metadata and DNSSEC

1382

1383 **First reported by:** Peter Davis, Neustar

1384 **Message:** <http://lists.oasis-open.org/archives/security-services/200709/msg00014.html>

1385 **Document:** SAML Metadata

1386 **Description:** The metadata specification references RFC 2535, which has been obsoleted by RFC 4035.

1387 **Options:** Make the following changes:

1388 Change line 1253 to the following:

1389       It is RECOMMENDED that entities publish their resource records in signed zone files using  
1390       [RFC4035]

1391 Substitute the following for lines 1447-1448:

1392       [RFC4035] R. Arends et al. Protocol Modifications for the DNS Security Extensions. IETF RFC  
1393       4035, March 2005. See <http://www.ietf.org/rfc/rfc4035.txt>.

1394 **Disposition:** During the TC conference call on [11 March 2008](#) the TC approved the changes as proposed  
1395 here.

---

## E68: Use of Multiple `<KeyDescriptor>` Elements

1396

1397 **First reported by:** Scott Cantor, Internet2

1398 **Message:** <http://lists.oasis-open.org/archives/security-services/200802/msg00066.html>

1399 **Document:** SAML Metadata

1400 **Description:** The metadata specification is silent about the meaning of multiple `<KeyDescriptor>`  
1401 elements with the same use attribute.

1402 **Options:** Insert text before line 625:

1403       The inclusion of multiple `<KeyDescriptor>` elements with the same `use` attribute (or no such  
1404       attribute) indicates that any of the included keys may be used by the containing role or affiliation.  
1405       A relying party SHOULD allow for the use of any of the included keys. When possible the signing  
1406       or encrypting party SHOULD indicate as specifically as possible which key it used to enable more  
1407       efficient processing.

1408 **Disposition:** During the TC conference call on 11 March 2008 the TC approved the changes as proposed  
1409 here.

---

## E69: Semantics of `<ds:KeyInfo>` in `<KeyDescriptor>`

1410  
1411 **First reported by:** Scott Cantor, Internet2

1412 **Message:** <http://lists.oasis-open.org/archives/security-services/200802/msg00066.html>

1413 **Document:** SAML Metadata

1414 **Description:** The metadata specification is silent about the semantic interpretation of the `<ds:KeyInfo>`  
1415 element as it pertains to communicating keys that may be wielded by an entity.

1416 **Options:** Insert text before line 625:

1417       The `<ds:KeyInfo>` element is a highly generic and extensible means of communicating key  
1418       material. This specification takes no position on the allowable or suggested content of this  
1419       element, nor on its meaning to a relying party. As a concrete example, no implications of  
1420       including an X.509 certificate by value or reference are to be assumed. Its validity period,  
1421       extensions, revocation status, and other relevant content may or may not be enforced, at the  
1422       discretion of the relying party. The details of such processing, and their security implications, are  
1423       out of scope; they may, however, be addressed by other SAML profiles.

1424 **Disposition:** During the TC conference call on 11 March 2008 the TC approved the changes as proposed  
1425 here.

---

## E70: Obsolete reference to UUID URN namespace

1426  
1427 **First reported by:** Tom Scavo, NCSA

1428 **Message:** <http://lists.oasis-open.org/archives/security-services/200801/msg00001.html>

1429 **Document:** SAML Profiles

1430 **Description:** The normative reference to an I-D at lines 2111-2112 of the profiles specification is obsolete  
1431 and was replaced by an actual RFC.

1432 **Options:** Replace the reference at lines 2111-2112 with a reference to:

1433       P. Leach et al. *A Universally Unique Identifier (UUID) URN Namespace*. IETF RFC 4122, July  
1434       2005. See <http://www.ietf.org/rfc/rfc4122.txt>.

1435       Also adjust the references to same at lines 1836 and 1885, which currently include the entire URL  
1436       rather than a shorthand ref name.

1437 **Disposition:** During the TC conference call on 25 March 2008 the TC approved the changes as proposed  
1438 here.

---

## E71: Missing namespace definition in Profiles

1439  
1440 **First reported by:** Tom Scavo, NCSA

1441 **Message:** <http://lists.oasis-open.org/archives/security-services/200802/msg00000.html>

1442 **Document:** SAML Profiles

1443 **Description:** The namespace prefix `xs:`, used repeatedly in section 8 of [SAML2Prof], is not defined in  
1444 section 1 of the same document.

1445 **Options:** Add the namespace definition to the table in section 1.  
1446 **Disposition:** During the TC conference call on [25 March 2008](#) the TC approved the changes as proposed  
1447 here.

---

## 1448 **E74: Update XML Signature Reference**

1449 **First reported by:** Frederick Hirsch, Nokia

1450 **Message:** <http://lists.oasis-open.org/archives/security-services/200808/msg00087.html>

1451 **Document:** SAML Core, Bindings, Profiles, Metadata, AuthnCtx, Conformance, SecConsider

1452 **Description:** The XML Signature specification was updated with a "Second Edition" that clarifies issues,  
1453 updates references, and so forth. Update normative SAML references to rely on the Second Edition spec,  
1454 and remove a stale non-normative reference in SAML Core to the IETF RFC version of the original spec.

1455 **Options:**

1456 Remove lines 3439-3440 of Core.

1457 Change Core at lines 3415-3416, Bindings at lines 1489-1491, Profiles at lines 2205-2206, Metadata at  
1458 lines 1490-1491, AuthnCtx at lines 3926-3928, Conformance at lines 410-412, SecConsider at lines 1078-  
1459 1079 to:

1460 D. Eastlake et al. *XML Signature Syntax and Processing, Second Edition*. World Wide Web  
1461 Consortium, June 2008. See <http://www.w3.org/TR/xmlsig-core/>.

1462 **Disposition:** During the TC conference call on [2 December 2008](#) the TC approved the changes as  
1463 proposed here.

---

## 1464 **E75: Clarify Handling of SubjectConfirmation in AuthnRequest**

1465 **First reported by:** Tom Scavo, NCSA

1466 **Message:** <http://lists.oasis-open.org/archives/security-services/200811/msg00027.html>

1467 **Document:** SAML Core

1468 **Description:** Section 3.4.1.4 discusses the identity provider's obligation to ensure that if a  
1469 `<samlp:AuthnRequest>` contains a `<saml:Subject>`, then the assertions it returns must strongly  
1470 match that subject. However, it doesn't explicitly state that if it can't do this, an error should be returned.

1471 **Options:**

1472 Add text at line 2247 at the end of the existing paragraph:

1473 If the identity provider cannot or will not produce assertions with a strongly matching subject, then  
1474 it **MUST** return a `<Response>` with an error `<Status>`, and **MAY** return a second-level  
1475 `<StatusCode>` that reflects the reason for the failure.

1476 **Disposition:** During the TC conference call on [13 January 2009](#) the TC approved the changes as  
1477 proposed here.

---

## 1478 **E76: Clarify nested validUntil/cacheDuration**

1479 **First reported by:** Tom Scavo, NCSA

1480 **Message:** <http://lists.oasis-open.org/archives/security-services/200810/msg00010.html>

1481 **Document:** SAML Metadata

1482 **Description:** It's implied, but not stated outright until section 4.3, that nested expiration information is  
1483 interpreted relative to any information in the parent element, and even there it isn't clearly explained. The  
1484 logical intent is that nested information can be more strict, but not less strict, than the parent, and that a  
1485 given element is only valid if both its own and its inherited attributes say it is.

1486 **Options:**

1487 Insert text at lines 336 and 409

1488           When not used as the root element of a metadata instance, a `validUntil` or `cacheDuration`  
1489           attribute MAY be used to impose a shorter expiration or cache duration than that of the parent or  
1490           root element, but never a longer one; the smaller value takes precedence.

1491 Insert text at lines 589 and 972:

1492           A `validUntil` or `cacheDuration` attribute MAY be used to impose a shorter expiration or  
1493           cache duration than that of the parent or root element, but never a longer one; the smaller value  
1494           takes precedence.

1495 **Disposition:** During the TC conference call on [13 January 2009](#) the TC approved the changes as  
1496 proposed here.

---

## 1497 **E77: Generalize scope of Metadata specification**

1498 **First reported by:** Don Schmidt, Microsoft

1499 **Document:** SAML Metadata

1500 **Description:** During the analysis of the applicability of SAML metadata to WS-Federation, it was noted  
1501 that language in the Metadata specification seems to limit its scope to SAML only. This should be  
1502 broadened to match the actual extensibility of the specification and its existing and future uses.

1503 **Options:**

1504 Add text at line 137:

1505           A variety of extension points are also included to allow for the use of SAML metadata in non-  
1506           SAML specifications, profiles, and deployments, and such use is encouraged.

1507 Change text at lines 153-154 to:

1508           SAML metadata is organized around an extensible collection of roles representing common  
1509           combinations of SAML (and potentially non-SAML) protocols and profiles supported by system  
1510           entities.

1511 Remove the word "SAML" from the following lines:

1512           226, 230, 311, 323, 332, 360, 372, 397, 403, 444, 478, 531, 940

1513 **Disposition:** During the TC conference call on [13 January 2009](#) the TC approved the changes as  
1514 proposed here.

---

## 1515 **E78: Reassignment of persistent identifiers**

1516 **First reported by:** Tom Scavo, NCSA

1517 **Message:** <http://marc.info/?l=shibboleth-users&m=122290050427432&w=2>

1518 **Document:** SAML Core

1519 **Description:** A discussion on a Shibboleth list noted that the persistent NameID format in SAML isn't  
1520 explicitly defined as non-reassignable (meaning that a given identifier can never be associated with a  
1521 different principal at a later point in time).

1522 This is a very useful property, and there are no good reasons why an opaque identifier should ever need  
1523 to be reassigned, so the original intent should be clarified if possible.

1524 **Options:**

1525 1. Make non-reassignment a recommendation, adding text at line 3325:

1526           A given value, once associated with a principal, SHOULD NOT be assigned to a different  
1527           principal at any time in the future.

1528 2. Make non-reassignment a requirement, adding text at line 3325:

1529           A given value, once associated with a principal, MUST NOT be assigned to a different principal at  
1530           any time in the future.

1531 **Disposition:** During the TC conference call on [13 January 2009](#) the TC approved option 2 as proposed  
1532 here.

---

## 1533 **E79: Clarification of SessionNotOnOrAfter**

1534 **First reported by:** Rob Philpott, EMC

1535 **Message:** <http://lists.oasis-open.org/archives/security-services/200901/msg00034.html>

1536 **Document:** SAML Core

1537 **Description:** The core specification description of the SessionNotOnOrAfter attribute may be overly  
1538 descriptive rather than deferential to profile-specific guidance.

1539 **Options:** Replace lines 1062-1065 with the following text:

1540       Indicates an upper bound on sessions with the subject derived from the enclosing assertion. The  
1541       time value is encoded in UTC, as described in Section 1.3.3. There is no required relationship  
1542       between this attribute and a `NotOnOrAfter` condition attribute that may be present in the  
1543       assertion. It's left to profiles to provide specific processing rules for relying parties based on this  
1544       attribute.

1545 **Disposition:** During the TC conference call on [10 March 2009](#) the TC approved the changes as proposed  
1546 here.

---

## 1547 **3 Proposed Errata**

1548 These proposed errata, given a “PE $n$ ” number designation, have either been determined by the SSTC  
1549 not to be resolvable with a “non-substantive” change or, in the case of PEs with “[OPEN]” in the title, have  
1550 not been considered by the SSTC yet.

---

### 1551 **PE3: Supported URL Encoding**

1552 **First reported by:** Scott Cantor, OSU

1553 **Message:** <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

1554 **Document:** Metadata

1555 **Description:** Specify the URL encoding supported by an HTTP Redirect binding endpoint.

1556 **Options:** This isn't actually an erratum, it's a missing piece that doesn't currently break anything but could  
1557 in the future if alternate URL encodings for the Redirect binding emerge (for example a binary XML  
1558 representation). We need an extension attribute to indicate non-default encoding support, it can just be  
1559 added to our new “2.0 metadata extension schema”. This should be moved to the issues list.

1560 **Disposition:** During the conference call of April 12 the TC agreed to move this to the issues list.

---

### 1561 **PE15: NameID Policy (Reopened)**

1562 **First reported by:** Thomas Wisniewski, Entrust

1563 **Message:** <http://lists.oasis-open.org/archives/security-services/200506/msg00030.html>

1564 **Document:** Core

1565 **Description:** The returned assertion subject's NameID format and/or SPNameQualifier may be different  
1566 from the ones suggested in the authentication request's NameIDPolicy. I.e., the spec does not explicitly  
1567 forbid these from being different (which it should).

1568 **Options:** Insert the following text between lines 2139 and 2140 in core

1569 When a `Format` defined in Section 8.3.7 is used other than

1570 `urn:oasis:names:TC:SAML:1.1:nameid-format:unspecified` or

1571 urn:oasis:names:TC:SAML:2.0:nameid-format:encrypted, then if the identity provider returns  
1572 any assertions:

- 1573 • the Format value of the <NameID> within the <Subject> of any <Assertion> MUST be  
1574 identical to the Format value supplied in the <NameIDPolicy>, and
- 1575 • if SPNameQualifier is not omitted in <NameIDPolicy>, the SPNameQualifier value of the  
1576 <NameID> within the <Subject> of any <Assertion> MUST be identical to the  
1577 SPNameQualifier value supplied in the <NameIDPolicy>.”

1578 **Disposition:** Open

---

## 1579 **PE23: Metadata for <ArtifactResolutionService>**

1580 **First reported by:** Nick Ragouzis, Enosis Group

1581 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00036.html>

1582 **Document:** Profiles

1583 **Description:** The text is not as clear as it should be. In Section 4.1.6 (Web Browser SSO Profile), at Line  
1584 639 change “MUST” to “SHOULD”. Also, add the following text:

1585 If the request or response message is delivered using the HTTP Artifact binding, the artifact issuer  
1586 SHOULD provide at least one <md:ArtifactResolutionService> endpoint element in its metadata.

1587 **Options:** Accept changes as suggested here.

1588 **Disposition:** During the call on 2/28 the TC moved to close with no resolution

---

## 1589 **PE67: Absence of elements in metadata (Open)**

1590 **First reported by:** Scott Cantor, Internet2

1591 **Message:** <http://lists.oasis-open.org/archives/security-services/200802/msg00066.html>

1592 **Document:** SAML Metadata

1593 **Description:** The metadata specification is ambiguous about the meaning of omission of the  
1594 <NameIDFormat> element and many other elements such as <AttributeProfile>, <KeyDescriptor>, and  
1595 generally anything that's optional.

1596 **Options:** Supplement the note at lines 165-172 with a new paragraph:

1597 In the absence of other sources of information, implementations SHOULD generally view the  
1598 absence of particular elements as implying that any values supported by the consuming  
1599 implementation are acceptable, with the obvious exception of metadata elements representing  
1600 roles, endpoints, keys, etc. (elements that cannot be "defaulted" or that would be security-  
1601 sensitive if assumed). Alternatively, the presence of particular elements SHOULD generally  
1602 constrain the choices made by the consuming implementation.

1603 Of course, if other sources of information are available, implementations are free to combine it  
1604 with, or override, the information found in metadata, as appropriate to that implementation and  
1605 deployment.

1606 **Disposition:** Open. Scott to supply reworked text.

---

## 1607 **PE73: No definition of Statement in the Glossary (Open)**

1608 **First reported by:** Josh Howlett, JANET

1609 **Message:** <http://lists.oasis-open.org/archives/saml-dev/200809/msg00006.html>

1610 **Document:** SAML Glossary

1611 **Description:** The glossary doesn't have a definition of "Statement", as it pertains to SAML.

1612 **Options:** Provide a definition.

1613 **Disposition:** Open.

---

## 1614 **PE80: Error in permissible root elements for MIME type (Open)**

1615 **First reported by:** Ian Young, EDINA, University of Edinburgh

1616 **Message:** <http://lists.oasis-open.org/archives/saml-dev/200906/msg00000.html>

1617 **Document:** Metadata

1618 **Description:** The metadata specification includes a MIME type registration that allows for  
1619 `<md:AffiliationDescriptor>` as the root element of an XML instance, which was not meant to be  
1620 permitted. Affiliations are a role, and don't carry their own entityID, for example.

1621 **Options:** We can remove line 1555, but this would also require resubmitting the registration to IANA, I  
1622 think?

1623 **Disposition:** Open.

---

## 1624 **PE81: Algorithm statement in XML Signature profile (Open)**

1625 **First reported by:** Bob Morgan, Internet2

1626 **Message:** <http://lists.oasis-open.org/archives/security-services/200907/msg00042.html>

1627 **Document:** Core, Metadata

1628 **Description:** The XML Signature profile in SAML indicates implementations SHOULD support the RSA-  
1629 SHA1 algorithm, but this is more properly a conformance requirement (and is already addressed there  
1630 with stronger MUST language). The statement in the profile has misled some readers to believe SAML  
1631 itself precludes other algorithms.

1632 **Options:**

1633 Change lines 2926-2927 in Core, and lines 1182-1183 in Metadata, to the following:

1634 Any algorithm defined for use with the XML Signature specification MAY be used.

1635 **Disposition:** Open.

---

## 1636 **PE82: Empty <ContactPerson> element (Open)**

1637 **First reported by:** Scott Cantor, Internet2

1638 **Message:** <http://lists.oasis-open.org/archives/security-services/200908/msg00004.html>

1639 **Document:** Metadata

1640 **Description:** The `<md:ContactPerson>` element is defined as a sequence of several optional child  
1641 elements, because it was intended to permit a number of alternate ways of defining a contact without  
1642 requiring any particular child element. The lack of co-constraints in XSD make it impractical to define this  
1643 kind of content model without allowing for an empty element. Since an empty contact has no meaning, it  
1644 should have been precluded in the text.

1645 **Options:**

1646 Insert the following before line 500:

1647 At least one child element SHOULD be present in a `<ContactPerson>` element.

1648 **Disposition:** Open.

---

## 1649 **PE83: Weaken claim made about Exclusive C14N (Open)**

1650 **First reported by:** Kyle Meadors, Drummond Group

1651 **Message:** <http://lists.oasis-open.org/archives/security-services/200907/msg00022.html>

1652 **Document:** Core, Metadata

1653 **Description:** The text recommending the use of Exclusive Canonicalization implies that it alone is  
1654 sufficient to ensure context-independent validity of an object.

1655 **Options:**

1656 Change lines 2939-2940 of Core, and lines 1196-1197 of Metadata, to the following:

1657       Use of Exclusive Canonicalization facilitates the verification of signatures created over SAML  
1658       messages when placed into a different XML context than present during signing.

1659       Note that use of this algorithm alone does not guarantee that a particular signed object can be  
1660       moved from one context to another safely, nor is that a requirement of signed SAML objects in  
1661       general, though it MAY be required by particular profiles.

1662 **Disposition:** Open.

## Appendix A.Revision History

<i>Rev</i>	<i>Date</i>	<i>By Whom</i>	<i>What</i>
Draft-00	2005-01-31	Jahan Moreh	Initial version based on emails to the list
Draft-01	2005-02-14	Jahan Moreh	Removed E5 as it is related to the Technical Overview document, which is work in progress. Relabeled all items as Potential Errata (PE). Added PE4 and PE5. Added E1.
Draft-02	2005-03-27	Jahan Moreh	Moved E1 to PE section. Added E2,E3 and E4. Added PE7
Draft-03	2005-03-29	Jahan Moreh	Rearranged E and PE items. The E items now are those which have been resolved and have proposed text, where required. PE items will be moved to E as they meet these requirements.
Draft-04	2005-04-11	Jahan Moreh	Incorporated proposes text all Pes based on emails to the list:
Draft-05	2005-04-12	Jahan Moreh	Minor corrections to PE5 and PE8. Accepted disposition of all items except PE5, PE7 and PE10. Decided to keep disposed Pes in the PE section (and not move them to the E section)
Draft-06	2005-04-25	Jahan Moreh	Added PE11, PE12 and PE13
Draft-07	2005-05-27	Jahan Moreh	Added PE14
Draft-08	2005-06-03	Jahan Moreh	Added PE15
Draft-09	2005-06-20	Jahan Moreh	Added PE16. Disposed PE11, PE12, PE13, and PE16 and PE17.
Draft 10	2005-07-04	Jahan Moreh	Added PE18
Draft 11	2005-07-18	Jahan Moreh	Disposed PE17, added PE19 and PE20
Draft 12	2005-08-01	Jahan Moreh	Disposed PE18, PE19 and PE20. Added PE21-PE25.
Draft 13	2005-08-15	Jahan Moreh	Closed PE19, PE22, PE24. Added PE26.
Draft 14	2005-08-29	Jahan Moreh	Updated PE26

<i>Rev</i>	<i>Date</i>	<i>By Whom</i>	<i>What</i>
Draft 15	2005-09-12	Jahan Moreh	Closed PE26, added PE27-34
Draft 16	2005-09-26	Jahan Moreh	Added PE35. Closed PE30, PE33 and PE34
Draft 17	2005-10-10	Jahan Moreh	Closed PE7, PE25, PE27-29, PE31, PE35.
Draft 18	2005-10-24	Jahan Moreh	Added PE36
Draft 19	2005-11-07	Jahan Moreh	Closed PE36
Draft 20	2005-11-21	Jahan Moreh	Added PE37 and PE38
Draft 21	2005-12-05	Jahan Moreh	Closed PE37 and PE38. Added text for PE32.
Draft 22	2006-01-30	Jahan Moreh	Added PE39, PE40, PE41, PE42 and 43
Draft 23	2006-02-13	Jahan Moreh	Closed PE39, PE41. Added PE44.
Draft 24	2006-02-27	Jahan Moreh	Closed PE10 and added PE45. Modified description and option for correcting PE 35.
Draft 24	2006-02-27	Jahan Moreh	Closed PE10 and added PE45. Modified description and option for correcting PE 35.
Draft 25	2006-03-27	Jahan Moreh	Closed PE23, PE35, PE40. Added PE46 and PE47.
Draft 26	2006-04-10	Jahan Moreh	Closed PE44, PE45 and PE47. Added PE48.
Draft 27	2006-04-24	Jahan Moreh	Split PE48 into two PEs (48 and 49).
Draft 28	2006-05-05	Jahan Moreh	Added PE50 and PE51
Draft 29	2006-05-22	Jahan Moreh	Closed PE46, PE48 and PE51. Added PE52 and PE53
Draft 30	2006-06-05	Jahan Moreh	Closed PE43 and PE50. Updated PE53
Draft 31	2006-06-19	Jahan Moreh	Added PE54
Draft 32	2006-07-17	Jahan Moreh	Added PE55, PE56, PE57 and PE58. Updated PE49
Draft 33	2006-07-31	Jahan Moreh	Replaced PE58. Closed PE49, PE56, PE57. Added PE59.
Draft 34	2006-08-28	Eve Maler and Jahan	Reformatting and clean up.

<b>Rev</b>	<b>Date</b>	<b>By Whom</b>	<b>What</b>
		Moreh	
Draft 35	2006-09-11	Jahan Moreh	Closed PE52, PE55, PE58, and PE59. Added and closed PE60 and PE61.
Draft 36	2006-09-21	Jahan Moreh	Renamed all approved PEs as Es keeping the original numbers. Renamed E1 to E0. Changed Summary of Disposition table to reflect new E #'s.
Draft 37	2006-12-19	Eve Maler	Added PE62 and PE63.
Draft 38	2007-01-14	Eve Maler	Cleanup in accordance with final decisions made by TC (verified by review of the errata composite documents and the creation of the standards-track errata document) and to prepare for eventual final publication of the whole set of documents.
Draft 39	2007-02-12	Eve Maler	Closed PE62 (->E62) and PE63 (->E63). Did a little more editorial distinction around this document vs. the other errata-related documents.
Draft 40	2007-03-04	Eve Maler	Opened (and immediately closed) E64.
Draft 41	2007-10-12	Abbie Barbir	Added PE64 and PE65
Draft 42	2008-02-29	Scott Cantor	Cleaned up PE65 and PE66. Removed any PE that was disposed of as part of an approved errata item but left in the document. Added (Open) to title of undisposed PE items. Added PE67, PE68, PE69.
Draft 43	2008-03-24	Scott Cantor	Closed PE65, PE66, PE68, P69. Added PE70, PE71, PE72. Reworded PE67.
Draft 44	2008-05-06	Scott Cantor	Closed PE70, PE71. Reopened E15 in place of PE72.
Draft 45	2008-11-20	Scott Cantor	Added PE73, PE74, PE75, PE76, PE77.
Draft 46	2008-11-23	Scott Cantor	Added PE78.
Draft 47	2009-01-26	Scott Cantor	Closed PE74, PE75, PE76, PE77, PE78.
Draft 48	2009-03-08	Scott Cantor	Added PE79.
Draft 49	2009-05-31	Scott Cantor	Closed PE79.

<i>Rev</i>	<i>Date</i>	<i>By Whom</i>	<i>What</i>
Draft 50		Scott Cantor	Added PE80, PE81, PE82, PE83.

1664

## Appendix B. Summary of Disposition

<i>Erratum #</i>	<i>Status</i>	<i>Document</i>
E0	Closed	Core
E1	Closed	Bindings
E2	Closed	Bindings
PE3	Closed	Metadata
E4	Closed	Binding
PE5	Closed	Binding/Profiles
E6	Closed	Core
E7	Closed	Metadata
E8	Closed	Core
PE9	Closed – combined with PE7	Metadata
E10	Closed	Core
E11	Closed	Conformance
E12	Closed	Core/Profiles
E13	Closed	Core
E14	Closed	Core/Profiles
E15	Closed	Core
PE16	Closed	Conformance
E17	Closed	Profiles
E18	Closed	Profiles
E19	Closed	Bindings
E20	Closed	Profiles
E21	Closed	Bindings
E22	Closed	Profiles
PE23	Closed	Profiles
E24	Closed	Bindings

<b>Erratum #</b>	<b>Status</b>	<b>Document</b>
E25	Closed	Conformance
E26	Closed	Profiles
E27	Closed	Profiles
E28	Closed	Conformance
E29	Closed	Conformance
E30	Closed	Core
E31	Closed	Bindings
E32	Closed	Profiles
E33	Closed	Metadata
E34	Closed	Metadata
E35	Closed	Profiles
E36	Closed	Core
E37	Closed	Metadata
E38	Closed	Core/Profiles
E39	Closed	Profiles
E40	Closed	Profiles
E41	Closed	Metadata
E42	Closed	Conformance
E43	Closed	Core
PE44	Closed – combined with PE47	Placeholder for Constrained Delegation
E45	Closed	Core
E46	Closed	Core
E47	Closed	Core/Profiles
E48	Closed	Profiles
E49	Closed	Core
E50	Closed	Conformance
E51	Closed	Profiles
E52	Closed	Profiles

<b>Erratum #</b>	<b>Status</b>	<b>Document</b>
E53	Closed	Profiles
E54	Closed	Profiles
E55	Closed	Core/Profiles
E56	Closed	Profiles
E57	Closed	Bindings
E58	Closed	Profiles
E59	Closed	Bindings
E60	Closed	Core
E61	Closed	Core
E62	Closed	Metadata
E63	Closed	Profiles
E64	Closed, not incorporated in the Errata	SecConsider
E65	Closed	Core
E66	Closed	Metadata
PE67	Open	Metadata
E68	Closed	Metadata
E69	Closed	Metadata
E70	Closed	Profiles
E71	Closed	Profiles
PE72	Closed, reopened as change to PE15.	Core
PE73	Open	Glossary
E74	Closed	Core/Profiles/Conf/AuthnCtx/SecConsider
E75	Closed	Core
E76	Closed	Metadata
E77	Closed	Metadata
E78	Closed	Core
E79	Closed	Core
PE80	Open	Metadata

<b><i>Erratum #</i></b>	<b><i>Status</i></b>	<b><i>Document</i></b>
PE81	Open	Core/Metadata
PE82	Open	Metadata
PE83	Open	Core/Metadata

---

1666 **Appendix C. Acknowledgments**

1667 The editors would like to acknowledge the contributions of the OASIS Security Services Technical  
1668 Committee, whose voting members at the time of publication were:

- 1669     • TBD

1670 The editors also would like to gratefully acknowledge Jahan Moreh of Sigaba, who during his tenure on  
1671 the SSTC was the primary editor of this errata document and who made major substantive contributions  
1672 to all of the errata materials.