



Errata Working Document for SAML V2.0

Working Draft 39, 12 February 2007

Document identifier:

sstc-saml-errata-2.0-draft-39

Location:

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

Editor:

Eve Maler, Sun Microsystems <eve.maler@sun.com>

Abstract:

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

Status:

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

Committee members should send comments and potential errata to security-services@lists.oasis-open.org. Others should submit them by following the instructions at http://www.oasis-open.org/committees/comments/index.php?wg_abbrev=security.

Table of Contents

24	1 Introduction.....	4
25	2 Errata.....	4
26	E0: Incorrect section reference	4
27	E1: Relay State for HTTP Redirect.....	4
28	E2: Metadata clarifications.....	5
29	E4: SAML 1.1 Artifacts.....	5
30	E6: Encrypted NameID	5
31	E7: Metadata attributes WantAuthnRequestsSigned and AuthnRequestsSigned	6
32	E8: SLO and NameID termination	7
33	E10: Logout Request reason Mismatch with Schema	7
34	E11: Improperly Labeled Feature	7
35	E12: Clarification on ManageNameIDRequest.....	8
36	E13: Inaccurate description of Authorization Decision	8
37	E14: AllowCreate	9
38	E15: NameID Policy	10
39	E17: Authentication Response IssuerName vs. Assertion IssuerName	10
40	E18: reference to identity provider discovery service in ECP Profile.....	11
41	E19: Clarification on Error Processing.....	11
42	E20: ECP SSO Profile and Metadata.....	12
43	E21: PAOS Version.....	12
44	E22: Error in Profile/ECP.....	12
45	E24: HTTPS in URI Binding.....	13
46	E25: Metadata Structures Feature in Conformance.....	13
47	E26: Ambiguities around Multiple Assertions and Statements in the SSO Profile.....	14
48	E27: Error in ECP Profile.....	15
49	E28: Conformance Table 1.....	16
50	E29: Conformance Table 2.....	16
51	E30: Considerations for key replacement.....	17
52	E31: Various minor errors in Binding.....	17
53	E32: Missing section in Profiles.....	17
54	E33: References to Assertion Request Protocol.....	18
55	E34: Section Heading.....	18
56	E35: Example in Profiles.....	18
57	E36: Clarification on Action Element.....	19
58	E37: Clarification in Metadata on Indexed Endpoints.....	19
59	E38: Clarification regarding index on <LogoutRequest>.....	19
60	E39: Error in SAML profile example.....	20
61	E40: Holder of Key.....	20
62	E41: EndpointType ResponseLocation clarification in Metadata.....	20
63	E42: Conformance Table 4.....	21
64	E43: Key location in saml:EncryptedData.....	21

65	E45: AuthnContext comparison clarifications	24
66	E46: AudienceRestriction clarifications.....	25
67	E47: Clarification on SubjectConfirmation.....	25
68	E48: Clarification on encoding for binary values in LDAP profile.....	26
69	E49: Clarification on attribute name format	26
70	E50: Clarification SSL Ciphersuites	27
71	E51: Schema type of contents of <AttributeValue>	27
72	E52: Clarification on <NotOnOrAfter> attribute	28
73	E53: Correction to LDAP/X.500 profile attribute	28
74	E54: Correction to ECP URN	29
75	E55: Various Language Cleanups.....	29
76	E56: Typo in Profiles.....	29
77	E57: SAML Mime Reference.....	30
78	E58: Typos in Profiles.....	30
79	E59: SSO Response when using HTTP-Artifact.....	30
80	E60: Incorrect URI	31
81	E61 Reference to non-existent element.....	31
82	E62: TLS Keys in KeyDescriptor.....	31
83	E63: IdP Discovery Cookie Interpretation.....	32
84	3 Proposed Errata.....	32
85	PE3: Supported URL Encoding.....	32
86	PE5: Rules for NameIDPolicy	32
87	PE9: Clarification on SP AuthnRequestsSigned and the IdP WantAuthnRequestsSigned SP	
88	metadata flags.....	33
89	PE16: Inaccurate data in Feature Matrix	33
90	PE23: Metadata for <ArtifactResolutionService>.....	33
91	PE44: Constrained Delegation.....	34
92	Appendix A. Revision History.....	35
93	Appendix B. Summary of Disposition.....	38
94	Appendix C. Acknowledgments.....	41
95	Appendix D. Notices.....	42
96		
97		

98

1 Introduction

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

100

2 Errata

101 The SSTC has determined that these reported problems have a solution that can be applied in
102 erratum form. Their original number designations have changed from “PE_{nn}” to “E_{nn}” to reflect
103 this status.

102

E0: Incorrect section reference

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

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

105 **Document:** Core

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

107 **Options:**

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

109

E1: Relay State for HTTP Redirect

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

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

112 **Document:** Bindings and Profiles

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

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

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

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

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

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

119 E2: Metadata clarifications

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

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

122 **Document:** Bindings and Profiles

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

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

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

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

127 E4: SAML 1.1 Artifacts

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

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

130 **Document:** Bindings and Profiles

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

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

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

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

135 E6: Encrypted NameID

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

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

138 **Document:** Core

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

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

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

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

143 **E7: Metadata attributes WantAuthnRequestsSigned and**
144 **AuthnRequestsSigned**

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

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

146 **Document:** Metadata

147 **Description:** In Metadata, the IDPSSODescriptor has the setting called
148 "WantAuthnRequestsSigned" and the SPSSODescriptor has the setting called
149 "AuthnRequestsSigned". But it's ambiguous about "how" this signing is to be done.

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

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

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

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

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

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

154 Add text to paragraph at lines 741-742:

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

156 Add text to paragraph at lines 744-747:

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

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

159 E8: SLO and NameID termination

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

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

162 **Document:** Core

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

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

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

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

167 E10: Logout Request *reason* Mismatch with Schema

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

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

170 **Document:** Core

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

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

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

174 E11: Improperly Labeled Feature

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

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

177 **Document:** Conformance

178 **Description:** In table 2 of the conformance spec, the feature in the 8th row is improperly labeled.
179 It currently says "Name Identifier Management, HTTP Redirect". It should say "Name Identifier
180 Management, HTTP Redirect (SP-initiated)".

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

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

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

182 E12: Clarification on ManageNameIDRequest

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

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

185 **Document:** Bindings and Profiles

186 **Description:** The schema defines the <NewID> element of a <ManageNameIDRequest> as a
187 string. The implication of that is that a NIM request message from IDP to SP can only be used to
188 inform the SP of a change in identifier value (not format – format is immutable once established).
189 There are a few places in the spec where the text implies that the format can be changed.
190 Additionally, the text about <NewEncryptedID> should be expanded to clarify that the encrypted
191 element is just the encrypted <NewID> element and not a full <NameID> as in the more typical
192 <EncryptedID> element used elsewhere

187 **Options:**

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

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

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

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

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

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

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

195 E13: Inaccurate description of Authorization Decision

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

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

198 **Document:** Core

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

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

201 It should say:

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

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

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

205 **E14: AllowCreate**

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

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

208 **Document:** Core and Profiles

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

210 **Options:** Make the following corrections

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

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

213 “A Boolean value used to indicate whether the requester grants to the identity provider, in the
214 course of fulfilling the request, permission to create a new identifier or to associate an existing
215 identifier representing the principal with the relying party. Defaults to “false” if not present or the
216 entire element is omitted.”

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

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

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

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

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

219 A value of “false” might be used to indicate that the requester is not prepared or able to do so and
220 save the identity provider wasted effort.

220 Requesters that do not make specific use of this attribute SHOULD generally set it to “true” to
221 maximize interoperability.

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

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

226 In Core, change lines 2419-2420 to:

227 “This protocol MUST NOT be used in conjunction with the
228 urn:oasis:names:tc:SAML:2.0:nameidformat:transient <NameID> Format.”

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

230 “If the <Terminate> element is included in the request, the requesting provider is indicating that
231 (in the case of a service provider) it will no longer accept assertions from the identity provider or

232 (in the case of an identity provider) it will no longer issue assertions to the service provider about
233 the principal.

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

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

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

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

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

254 E15: NameID Policy

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

256 **Message:** <http://lists.oasis-open.org/archives/security-services/200506/maillist.html - 00030>

257 **Document:** Core

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

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

262 When a Format defined in Section 8.3.7 is used other than
263 urn:oasis:names:TC:SAML:2.0:nameid-format:unspecified or
264 urn:oasis:names:TC:SAML:2.0:nameid-format:encrypted, then if the identity provider returns any
265 assertions:

- 266 • the Format value of the <NameID> within the <Subject> of any <Assertion> MUST be
267 identical to the Format value supplied in the <NameIDPolicy>, and
- 268 • if SPNameQualifier is not omitted in <NameIDPolicy>, the SPNameQualifier value of the
269 <NameID> within the <Subject> of any <Assertion> **MUST** be identical to the
270 SPNameQualifier value supplied in the <NameIDPolicy>."

271 **Disposition:** During the conference call of June 7 the TC approved to make the addition as
272 stated here.

273 E17: Authentication Response IssuerName vs. Assertion 274 IssuerName

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

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

277 **Document:** Profiles

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

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

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

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

288 E18: reference to identity provider discovery service in ECP 289 Profile

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

291 **Message:** [http://www.oasis-](http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00000.html)
292 [open.org/apps/org/workgroup/security/email/archives/200507/msg00000.html](http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00000.html)

293 **Document:** Profiles

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

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

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

301 E19: Clarification on Error Processing

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

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

304 **Document:** Bindings

305 **Description:** Clarification on error processing

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

- 308 • Change the first sentence to read:
 - 309 ○ The SAML responder SHOULD return a SOAP message containing either a
 - 310 SAML response element in the body or a SOAP fault.
- 311 • Delete the 3rd sentence (If a SAML responder cannot, for some reason, process...).
- 312 SOAP defines when a SOAP fault is required and SAML goes into detail about what we
- 313 should return when in section 3.2.3.3 "Error Reporting".
- 314 • Change the 4th sentence to soften the "MUST NOT" and make it a "SHOULD NOT" as
- 315 there can be sufficient security through obscurity reasons to do so in some cases.
- 316 • Add a new sentence at the end of the paragraph noting that details about error handling
- 317 are covered in section 3.2.3.3 "Error Reporting" or something to that effect.

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

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

321 **E20: ECP SSO Profile and Metadata**

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

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

324 **Document:** Profiles

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

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

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

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

329 **E21: PAOS Version**

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

331 **Message:** [http://www.oasis-
332 open.org/apps/org/workgroup/security/email/archives/200507/msg00028.html](http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00028.html)

332 **Document:** Bindings

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

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

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

336 **E22: Error in Profile/ECP**

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

338 **Message:** [http://www.oasis-
339 open.org/apps/org/workgroup/security/email/archives/200507/msg00040.html](http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00040.html)

339 **Document:** Profiles

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

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

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

343 **E24: HTTPS in URI Binding**

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

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

346 **Document:** Bindings

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

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

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

350 “Like SOAP, URI resolution can occur over multiple underlying transports. This binding has
351 protocol-independent aspects, but also calls out as mandatory the implementation of HTTP
352 URIs.”

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

352

353 **E25: Metadata Structures Feature in Conformance**

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

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

356 **Document:** Conformance

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

358 Change to Table 2: Feature Matrix

359

360

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

361 FEATURE

362 Metadata Structures OPT OPT OPT OPT N/A

363 Metadata Interoperation OPT OPT OPT OPT N/A

364 Change to Table 4: SAML Authority and Requester Matrix

365

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

366 FEATURE

367 Metadata Structures OPT OPT OPT OPT

368 Metadata Interoperation OPT OPT OPT OPT

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

370 3.6 Metadata Structures

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

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

373 * Implementing SAML metadata according to the extensible SAMLv2.0 Metadata format in all
374 cases where an interoperating peer has the option, as stated in SAMLv2.0 specifications, of
375 depending on the existence of SAMLv2.0 Metadata. Electing the Metadata Structures option has

374 the effect of requiring such metadata be available to the interoperating peer. The Metadata
375 Interoperation feature, described below, provides a means of satisfying this requirement.

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

376 3.7 Metadata Interoperation

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

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

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

380 E26: Ambiguities around Multiple Assertions and Statements in 381 the SSO Profile

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

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

383 **Document:** Profiles

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

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

- 386 • If the response is unsigned, the <Issuer> element MAY be omitted, but if present (or if the
387 response is signed) it MUST contain the unique identifier of the issuing identity provider;
388 the Format attribute MUST be omitted or have a value of
389 urn:oasis:names:tc:SAML:2.0:nameid-format:entity
- 387 • It MUST contain at least one <Assertion>. Each assertion's <Issuer> element MUST
388 contain the unique identifier of the responding identity provider; the Format attribute
389 MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
390 Note that this profile assumes a single responding identity provider, and all assertions in
391 a response MUST be issued by the same entity.
- 388 • If multiple assertions are included, then each assertion's <Subject> element MUST refer
389 to the same principal. It is allowable for the content of the <Subject> elements to differ
390 (e.g. using different <NameID> or alternative <SubjectConfirmation> elements).
- 389 • Any assertion issued for consumption using this profile MUST contain a <Subject>
390 element with at least one <SubjectConfirmation> element containing a Method of
391 urn:oasis:names:tc:SAML:2.0:cm:bearer. Such an assertion is termed a bearer assertion.
392 Bearer assertions MAY contain additional <SubjectConfirmation> elements.
- 390 • Assertions without a bearer <SubjectConfirmation> MAY also be included; processing of
391 additional assertions or <SubjectConfirmation> elements is outside the scope of this
392 profile.
- 391 • At least one bearer <SubjectConfirmation> element MUST contain a
392 <SubjectConfirmationData> element that itself MUST contain a Recipient attribute
393 containing the service provider's assertion consumer service URL and a NotOnOrAfter
394 attribute that limits the window during which the assertion can be delivered. It MAY also
395 contain an Address attribute limiting the client address from which the assertion can be
396 delivered. It MUST NOT contain a NotBefore attribute. If the containing message is in
397 response to an <AuthnRequest>, then the InResponseTo attribute MUST match the
398 request's ID.

- 392 • The set of one or more bearer assertions MUST contain at least one <AuthnStatement>
393 that reflects the authentication of the principal to the identity provider. Multiple
394 <AuthnStatement> elements MAY be included, but the semantics of multiple statements
395 is not defined by this profile.
- 393 • If the identity provider supports the Single Logout profile, defined in Section 4.4, any
394 authentication statements MUST include a SessionIndex attribute to enable per-session
395 logout requests by the service provider
- 394 • Other statements MAY be included in the bearer assertion(s) at the discretion of the
395 identity provider. In particular, <AttributeStatement> elements MAY be included. The
396 <AuthnRequest> MAY contain an AttributeConsumingServiceIndex XML attribute
397 referencing information about desired or required attributes in [SAMLMeta]. The identity
398 provider MAY ignore this, or send other attributes at its discretion.
- 395 • Each bearer assertion MUST contain an <AudienceRestriction> including the service
396 provider's unique identifier as an <Audience>
- 396 • Other conditions (and other <Audience> elements) MAY be included as requested by the
397 service provider or at the discretion of the identity provider. (Of course, all such
398 conditions MUST be understood by and accepted by the service provider in order for the
399 assertion to be considered valid.
- 397 • The identity provider is NOT obligated to honor the requested set of <Conditions> in the
398 <AuthnRequest>, if any.

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

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

404 Section 4.1.4.5, POST-Specific Processing Rules:

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

406 **Options:**

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

408 **E27: Error in ECP Profile**

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

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

411 **Document:** Profiles

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

413 **Options:**

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

415 **E28: Conformance Table 1**

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

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

418 **Document:** Conformance

419 **Description:** The first column is labeled “Profile”, yet several of the entries are technically not
420 “profiles”. The same applies to the section title and the paragraph above the table.

420 **Options:**

421 Column 1:

422 Combine Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query
423 entries into a single entry labeled:

424 Assertion Query/Request

425

426 Column 2

427

428 Label each set of message flows with relevant protocol description:

429 Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query

430

431 Column 3

432

433 No change

434

435 (2) Remove the following rows from the table:

436

437 SAML URI binding

438 Metadata

439 **Disposition:** During the conference call of September 27 the TC approved the changes as
440 stated here

440 **E29: Conformance Table 2**

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

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

443 **Document:** Conformance

444 **Description:** The table is missing feature rows for performing a “Request for Assertion by
445 Identifier” over SOAP and for “SAML URI Binding”. These features are clearly permissible for
446 IDP’s, since the IDPSSODescriptor includes an element for zero or more
447 <AssertionIDRequestService> elements.

445 **Options:** Add two rows table 2; row #1 is labeled Request for Assertion Identifier; row #2 is
446 labeled SAML URI binding; both are optional for IdP row and N/A for all the rest.

446 **Disposition:** During the conference call of September 27 the TC as stated here.

447 **E30: Considerations for key replacement**

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

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

450 **Document:** Core

451 **Description:** Line 3110 states: “optionally one or more encrypted keys...”

452

453 **Options:** Replace “optionally one or more” with “zero or more”.

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

455 **E31: Various minor errors in Binding**

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

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

458 **Document:** Bindings

459 **Description:**

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

464 **Options:**

465 **Disposition:** During the conference call of September 13 the TC approved the changes for items
466 2 and 3. During the conference call of September 27 the TC approved the changes for items 1
467 and 4.

466 **E32: Missing section in Profiles**

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

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

469 **Document:** Profiles

470 **Description:** Section 4.3. This profile is missing a subsection for “Required Information”, which is
471 present in all other profiles.
471

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

473 4.3.1 Required Information

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

475 **Contact information:** security-services-comment@lists.oasis-open.org

476 **Description:** Given below.

477 **Updates:** None.

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

479 **E33: References to Assertion Request Protocol**

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

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

482 **Document:** Metadata

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

484 **Options:**

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

486 **E34: Section Heading**

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

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

489 **Document:** Metadata

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

491 .

492

493 **Options:**

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

495 **E35: Example in Profiles**

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

497 **Message:** <http://lists.oasis-open.org/archives/security-services/200509/msg00023.html> and

498 <http://www.oasis-open.org/archives/security-services/200602/msg00008.html>

499 **Document:** Profiles

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

501 **Options:** Change the value of the responseConsumerURL in the example on page 29 line 964 to
502 https://ServiceProvider.example.com/ecp_assertion_consumer.

502 Change the sentence on page 27 lines 906-908 to: “This value **MUST** be the same as the
503 AssertionServiceConsumerURL (or the URL referenced in metadata) conveyed in the
504 <AuthnRequest> and **SHOULD NOT** be a relative URL.”

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

504 E36: Clarification on Action Element

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

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

507 **Document:** Core

508 **Description:**

509 In section 2.7.4.2 of core spec, Namespace is marked as "Optional". It says: "If this element is
510 absent, the namespace urn:oasis:names:tx:SAML:1.0:action:rwedc-negation specified in Section
511 8.1.2 is in effect." But in the following schema definition, attribute Namespace is marked as
512 required:

```
510 <attribute name="Namespace" type="anyURI" use="required"/>
```

511
512 A clarification is needed to resolve this apparent conflict.

513 **Options:** In line 1359 change "Optional" to "Required" and strike the sentence starting at line
514 1361-1363 ("If this element is absent....")

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

515 E37: Clarification in Metadata on Indexed Endpoints

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

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

518 **Document:** Metadata

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

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

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

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

523 E38: Clarification regarding index on <LogoutRequest>

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

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

526 **Document:** Core, Profiles

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

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

529 1. Change Core, line 2546 as follows:

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

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

532 "If the requester is a session participant, it MUST include at least one <SessionIndex>
533 element in the request. (Note that the session participant always receives a SessionIndex

534 attribute in the <saml:AuthnStatement> elements that it receives to initiate the session, per
535 section 4.1.4.2 of the Web Browser SSO Profile.) If the requester is a session authority (or
536 acting on its behalf), then it MAY omit any such elements to indicate the termination of all of
537 the principal's applicable sessions."

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

540 **E39: Error in SAML profile example**

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

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

543 **Document:** Profiles

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

546 **Options:**

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

549 **E40: Holder of Key**

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

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

552 **Document:** Core

553 **Description:** HoK described a key that required proof of possession by a attesting entity vs. being
554 held by the subject, Appropriate text does appear in lines 781-783 of saml2-core. However,
555 lines 335-337 of saml2-profiles reads:

556 "As described in [XMLSig], each <ds:KeyInfo> element holds a key or information that enables
557 an application to obtain a key. The holder of a specified key is considered to be the subject of the
558 assertion by the asserting party"

559 The last sentence should be replaced by:

560 "The holder of a specified key is considered to be an acceptable attesting entity for the assertion
561 by the asserting party"

562 **Options:**

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

565 **E41: EndpointType ResponseLocation clarification in Metadata**

566 **First reported by:** Eric Tiffany, Project Liberty

567 **Message:** <http://www.oasis-open.org/archives/security-services/200601/msg00034.html>

568 **Document:** Metadata

569 **Description** Implementer interpreted the metadata spec to mean that ResponseLocation should
570 only be omitted for the SOAP binding, and that the ResponseLocation be specified in metadata
571 for other bindings.

572 **Options:** Proposed text to resolve this:

573 At line 238 in Metadata we have now:

574 "The ResponseLocation attribute is used to enable different endpoints to be specified for
575 receiving request and response messages associated with a protocol or profile, not as a means

576 of load-balancing or redundancy (multiple elements of this type can be included for this purpose).
577 When a role contains an element of this type pertaining to a protocol or profile for which only a
578 single type of message (request or response) is applicable, then the ResponseLocation attribute
579 is unused.

580 The proposal is to add the following:

581 "If the ResponseLocation attribute is omitted, any response messages associated with a protocol
582 or profile may be assumed to be handled at the URI indicated by the Location attribute."

583 **Disposition:** During the conference call of 1/31/06 TC voted to approve changes as stated here.

584 E42: Conformance Table 4

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

586 **Message:** <http://lists.oasis-open.org/archives/security-services/200601/msg00041.html>

587 **Document:** Conformance

588 **Description:** Table 4 has a cell for SAML <x> Authority responding to an <y> Query. That is, an
589 Attribute Authority responding to an Authentication or Authorization Decision Query. This doesn't
590 seem to make sense as authorities should respond to their respective queries. So the OPTIONAL
591 items under the authorities should be N/A."

592 **Options:** Change the reference from "OPTIONAL" to "N/A" under the columns SAML
593 Authentication Authority, SAML Attribute Authority, and SAML Authorization Decision Authority in
594 Table 4: SAML Authority and Requester Matrix.

595 **Disposition:** During the conference call of 1/31/06 TC voted to approve changes as stated here.

596 E43: Key location in saml:EncryptedData

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

598 **Message:**

599 **Document:** Core

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

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

603

604 6.1 General Considerations

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

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

614 6.2 Key and Data Referencing Guidelines

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

617 Implementations of SAML MAY implicitly associate keys with the corresponding data
618 they are used to encrypt, through the positioning of <xenc:EncryptedKey> elements

619 next to the associated `<xenc:EncryptedData>` element, within the enclosing SAML
620 parent element. However, the following set of explicit referencing guidelines are
621 suggested to facilitate interoperability.

622 If the encrypted key is included in the XML instance, then it SHOULD be referenced
623 within the associated `<xenc:EncryptedData>` element, or alternatively embedded within
624 the `<xenc:EncryptedData>` element. When an `<xenc:EncryptedKey>` element is used,
625 the `<ds:KeyInfo>` element within `<xenc:EncryptedData>` SHOULD reference the
626 `<xenc:EncryptedKey>` element using a `<ds:RetrievalMethod>` element of Type
627 <http://www.w3.org/2001/04/xmlenc#EncryptedKey>.

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

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

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

643

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

648

649 6.3 Examples

650 In the following example, the parent element (`<EncryptedID>`) contains
651 `<xenc:EncryptedData>` and (referenced) `<xenc:EncryptedKey>` elements as siblings
652 (note that the key can in fact be anywhere in the same instance, and the key references
653 the `<xenc:EncryptedData>` element) :

```
654 <saml:EncryptedID
655     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
656     <xenc:EncryptedData
657     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
658         Id="Encrypted_DATA_ID"
659         Type="http://www.w3.org/2001/04/xmlenc#Element">
660         <xenc:EncryptionMethod
661
662             Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
663         <ds:KeyInfo
664     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
665         <ds:RetrievalMethod URI="#Encrypted_KEY_ID"
666
667             Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
```

```

668         </ds:KeyInfo>
669         <xenc:CipherData>
670
671         <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
672         </xenc:CipherData>
673     </xenc:EncryptedData>
674
675     <xenc:EncryptedKey
676 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
677         Id="Encrypted_KEY_ID">
678         <xenc:EncryptionMethod
679 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
680         <xenc:CipherData>
681 <xenc:CipherValue>PzA5X...</xenc:CipherValue>
682 </xenc:CipherData>
683         <xenc:ReferenceList>
684             <xenc:DataReference URI="#Encrypted_DATA_ID"/>
685         </xenc:ReferenceList>
686     </xenc:EncryptedKey>
687 </saml:EncryptedID>

```

688

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

```

691 <saml:EncryptedAttribute
692 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
693     <xenc:EncryptedData
694 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
695         Id="Encrypted_DATA_ID"
696         Type="http://www.w3.org/2001/04/xmlenc#Element">
697         <xenc:EncryptionMethod
698 Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
699         <ds:KeyInfo
700 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
701             <xenc:EncryptedKey Id="Encrypted_KEY_ID">
702                 <xenc:EncryptionMethod
703 Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
704                 <xenc:CipherData>
705 <xenc:CipherValue>SDFSDF... </xenc:CipherValue>
706 </xenc:CipherData>
707             </xenc:EncryptedKey>
708         </ds:KeyInfo>
709         <xenc:CipherData>
710 <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
711 </xenc:CipherData>
712     </xenc:EncryptedData>
713 </saml:EncryptedAttribute>

```

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

```

716 <saml:EncryptedAssertion
717 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
718     <xenc:EncryptedData
719 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
720         Id="Encrypted_DATA_ID"
721         Type="http://www.w3.org/2001/04/xmlenc#Element">
722         <xenc:EncryptionMethod
723 Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
724         <ds:KeyInfo
725 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
726 <ds:KeyName>MULTICAST_KEY_NAME</ds:KeyName>
727         </ds:KeyInfo>
728     </xenc:EncryptedData>

```

```

729     <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
730     </xenc:CipherData>
731 </xenc:EncryptedData>
732
733     <xenc:EncryptedKey
734 xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
735     Id="Encrypted_KEY_ID_1" Recipient="https://spl.org">
736     <xenc:EncryptionMethod
737
738         Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
739     <ds:KeyInfo
740 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
741 <ds:KeyName>KEY_NAME_1</ds:KeyName>
742 </ds:KeyInfo>
743     <xenc:CipherData>
744 <xenc:CipherValue>xyzABC...</xenc:CipherValue>
745 </xenc:CipherData>
746     <xenc:ReferenceList>
747     <xenc:DataReference URI="#Encrypted_DATA_ID"/>
748 </xenc:ReferenceList>
749
750 <xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
751 </xenc:EncryptedKey>
752
753 <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
754 Id="Encrypted_KEY_ID_2" Recipient="https://sp2.org">
755 <xenc:EncryptionMethod
756
757     Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
758 <ds:KeyInfo
759 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
760 <ds:KeyName>KEY_NAME_2</ds:KeyName>
761 </ds:KeyInfo>
762     <xenc:CipherData>
763 <xenc:CipherValue>abcXYZ...</xenc:CipherValue>
764 </xenc:CipherData>
765     <xenc:ReferenceList>
766     <xenc:DataReference URI="#Encrypted_DATA_ID"/>
767 </xenc:ReferenceList>
768
769 <xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
770 </xenc:EncryptedKey>
771 </saml:EncryptedAssertion>

```

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

777 **E45: AuthnContext comparison clarifications**

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

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

780 **Document:** Core

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

783 **Options:**

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

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

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

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

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

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

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

798 **E46: AudienceRestriction clarifications**

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

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

801 **Document:** Core

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

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

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

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

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

810 **E47: Clarification on SubjectConfirmation**

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

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

813 **Document:** Core and profiles

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

816 **Options:**

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

818 If the <SubjectConfirmation> element in an assertion subject contains an identifier the issuer
819 authorizes the attesting entity to wield the assertion on behalf of that subject. A relying party MAY
820 apply additional constraints on the use of such an assertion at its discretion, based upon the
821 identities of both the subject and the attesting entity.

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

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

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

828

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

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

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

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

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

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

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

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

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

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

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

850 **Document:** Profiles

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

853 **Options:**

854 Change line 1762 of Profiles to:

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

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

858 **E49: Clarification on attribute name format**

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

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

861 **Document:** Core

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

863 **Options:**

864

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

866 Attributes are identified/named by the combination of the `NameFormat` and `Name` XML attributes
867 described above. Neither one in isolation can be assumed to be unique, but taken together, they
868 ought to be unambiguous within a given deployment.

869 The SAML profiles specification [SAMLProf] includes a number of attribute profiles designed to
870 improve the interoperability of attribute usage in some identified scenarios. Such profiles typically
871 include constraints on attribute naming and value syntax. There is no explicit indicator when an
872 attribute profile is in use, and it is assumed that deployments can establish this out of band,
873 based on the combination of `NameFormat` and `Name`.

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

875 E50: Clarification SSL Ciphersuites

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

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

878 **Document:** Conformance

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

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

883 **Options:**

884 Change the following in the Conformance document:

- 885 1. In the intro of section 4 (XML Digital Signature and XML Encryption) after line 235, add:
 - 886 • The algorithms listed below as being required for SAML 2.0 conformance are
887 based on the mandated algorithms in the W3C recommendations for XML
888 Signature and for XML Encryption, but modified by the SSTC to ensure
889 interoperability of conformant SAML implementations. While the SAML-defined
890 set of algorithms is a minimal set for conformance, additional algorithms
891 supported by XML Signature and XML Encryption MAY be used. Note, however,
892 that the use of non-mandated algorithms may introduce interoperability issues if
893 those algorithms are not widely implemented. As additional algorithms become
894 mandated for use in XML Signature and XML Encryption, the set required for
895 SAML conformance may be extended. [RSP: not sure about including the last
896 sentence... opinions?]
- 897 1. In the intro of section 5 (Use of SSL 3.0 and TLS 1.0) after line 257, add:
 - 898 • The set up algorithms required for SAML 2.0 conformance is equivalent to that
899 defined in SAML 1.0 and SAML 1.1. These mandated algorithms were chosen by
900 the SSTC because of their wide implementation support in the industry. While the
901 algorithms defined below are the minimal set for SAML conformance, additional
902 algorithms supported by SSL 3.0 and TLS 1.0 MAY be used.

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

904 E51: Schema type of contents of <AttributeValue>

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

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

907 **Document:** Profiles

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

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

912

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

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

916 This appears to be in error. Section 3 of [Schema2] defines the "Built-in Datatypes" and Section
917 3.3 is one specific sub-section within it (defines "Derived Datatypes"). With the current language
918 both "Date" and "anyURI" are excluded; I somehow do not believe this was the original intent.

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

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

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

924 **E52: Clarification on <NotOnOrAfter> attribute**

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

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

927 **Document:** Profiles

928 **Description:** Line 556-7: “a `NotOnOrAfter` attribute that limits the window during which the
929 assertion can be delivered.”

930 The `NotOnOrAfter` in a `ConfirmationData` element isn’t about a window when the assertion can be
931 delivered. Core defines it as being the time after which the subject cannot be confirmed. That’s
932 independent of assertion delivery

933 **Options:**

934 Changes Profiles lines 556-7 from:

935 “a `NotOnOrAfter` attribute that limits the window during which the assertion can be delivered”
936 to:

937 “a `NotOnOrAfter` attribute that limits the window during which the recipient can perform a
938 confirmation of the assertion <Subject>”.

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

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

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

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

944 **Document:** Profiles

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

949 **Options:**

- 950 1. Remove the `xsi:type` requirement.
951 Forces implementations to recognize string vs base64 encoding based on Attribute Name.
952
- 953 2. Remove the `x500:Encoding` attribute.
954 Forces implementations to trigger profile behavior based on Attribute Namespace and Name,
955 encoding rules are implied.
- 956 3. Move the `x500:Encoding` attribute to the Attribute element.
957 Suggests that future encoding rules will be uniform across all values of an attribute, but
958 otherwise fully consistent with intent of profile.
959
- 960 4. Define an extended schema type that extends string and base64Binary with the
961 `x500:Encoding` attribute and change the mandated `xsi:type` values to the extended types.
962 Least change to existing profile behavior, but requires publishing and approving an additional
963 schema document.
- 964 5. Deprecate the existing profile and define a new one incorporation whatever input can be
965 gleaned from implementers.
- 966 6. A variation on 2 and 3, which is to:
967 a. remove the `x500:Encoding` attribute and document that the LDAP encoding uses
968 `xsi:type` string and base64Binary

969 b. document that other encodings should define new types
970 **Disposition:** During the TC conference call on 6/20 the TC approved option 3 (which subsumes
971 option 5) but subsequently decided that this would be a substantive change, such that the profile
972 would have to be deprecated once a replacement profile could be specified. At the 16 January
973 2007 TC telecon we agreed it's now safe to mention the (still-draft) new profile and do the
974 deprecation.

975 **E54: Correction to ECP URN**

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

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

978 **Document:** Profiles

979 **Description:**

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

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

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

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

986 **E55: Various Language Cleanups**

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

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

989 **Document:** Core and Profiles

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

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

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

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

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

999 Core, line 2477, change "it will no longer issue assertions to the SP about the principal" to "it will
1000 no longer issue assertions to the SP using that identifier". This does step on an errata, but is a
1001 separate change from it.

1002 Core, line 2483, change "regarding this principal" to "using the primary identifier".

1003 Core, line 2487-8, change "regarding this principal" to "in any case where the identifier being
1004 changed would have been used".

1005 **Disposition:** During the TC conference call on 8/15 the TC approved the changes as proposed
1006 here

1007 **E56: Typo in Profiles**

1008 **First reported by:** Eric Tiffany, Liberty Alliance

1009 **Message:** <http://lists.oasis-open.org/archives/security-services/200606/msg00021.html>

1010 **Document:** Profiles

1011 **Description:** Line 326 of profiles states:
1012 "It is anticipated that profiles will define and use several different values for
1013 <ConfirmationMethod>"
1014 The last atom should be "Method" as there is not any<ConfirmationMethod> element in the SAML
1015 schema.
1016 **Disposition:** During the conference call on 7/18 the TC approved to making the changes as
1017 stated here.

1018 **E57: SAMLmime Reference**

1019 **First reported by:** Jeff Hodges, Nustar
1020 **Message:** <http://lists.oasis-open.org/archives/security-services/200606/msg00036.html>
1021 **Document:** Bindings
1022 **Description:** The [SAMLmime] reference in saml-bindings-2.0-os lines 1468-1469 reads as:
1023 [SAMLmime] application/saml+xml Media Type Registration, IETF Internet-Draft,
1024 <http://www.ietf.org/internet-drafts/draft-hodges-saml-mediatype-01.txt>.
1025 The document draft-hodges-saml-mediatype-01 expired (and thus was deleted from the I-D
1026 repository), since we ended up using the new "fast track" MIME Media Type registration process
1027 rather than publishing an RFC.
1028 **Options:** The reference should be replaced with a reference similar to
1029 [SAMLmime] OASIS Security Services Technical Committee (SSTC),
1030 "application/samlassertion+xml MIME Media Type Registration", IANA MIME Media Types
1031 Registry application/samlassertion+xml, December 2004.
1032 <http://www.iana.org/assignments/media-types/application/samlassertion+xml>
1033 **Disposition:** During the TC conference call on 7/18 the TC approved the changes as stated here

1034 **E58: Typos in Profiles**

1035 **First reported by:** Tom Scavo, NCSA/University of Illinois
1036 **Message:** <http://www.oasis-open.org/archives/security-services/200607/msg00049.html>
1037 **Document:** Profiles
1038 **Description:** There are two minor errors in the profiles document on lines 626 and 627.
1039 **Options:**
1040 On line 626 change "sign" to "signing"
1041 On line 627 change "encrypt" to "encryption"
1042 **Disposition:** During the TC conference call on 8/15 the TC approved the changes as proposed
1043 here

1044 **E59: SSO Response when using HTTP-Artifact**

1045 **First reported by:** Rob Phillipot, RSA Security
1046 **Message:** <http://www.oasis-open.org/archives/security-services/200509/msg00019.html>
1047 **Document:** Bindings
1048 **Description:** The specification mandates support for the HTTP Artifact binding for a Web SSO
1049 <Response> in full and Lite versions of IDP's and SP's. However, the spec does not indicate
1050 what mechanisms (HTTP Redirect or HTTP POST) are mandated for delivery of the artifact.
1051 **Options:**
1052 Insert a clarifying paragraph after line 1173 of Bindings:

1053 "Finally, note that the use of the Destination attribute in the root SAML element of the protocol
1054 message is unspecified by this binding, because of the message indirection involved."
1055 **Disposition:** During the TC conference call on 8/15 the TC approved the changes as proposed
1056 here

1057 **E60: Incorrect URI**

1058 **First reported by:** Tom Scavo, NCSA/University of Illinois

1059 **Message:** <http://lists.oasis-open.org/archives/security-services/200608/msg00069.html>

1060 **Document:** Core

1061 **Description:** Line 460 references the URI

1062 `urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified.`

1063 This is incorrect and should be replaced with

1064 `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`

1065 **Options:**

1066 **Disposition:** During the TC conference call on 8/29 the TC approved the changes as proposed
1067 here.

1068 **E61 Reference to non-existent element**

1069 **First reported by:** Tom Scavo, NCSA/University of Illinois

1070 **Message:** <http://lists.oasis-open.org/archives/security-services/200608/msg00075tml>

1071 **Document:** Core

1072 **Description:** Line 3160 of core refers to the <Request> element. This is a non-existent element.

1073 **Options:** Delete line 3160

1074 **Disposition:** During the TC conference call on 8/29 the TC approved the changes as proposed
1075 here. (Additional edits proposed, in order to make sense of the text that remains. Scheduled to be
1076 brought up in 13 Feb 2007 telecon again for final approval.)

1077

1078 **E62: TLS Keys in KeyDescriptor**

1079 **First reported by:** Scott Cantor on security-services list

1080 **Message:** <http://lists.oasis-open.org/archives/security-services/200612/msg00034.html>

1081 **Document:** Metadata

1082 **Description:** The Metadata specification is underspecified with regard to how to interpret the
1083 KeyDescriptor element's "use" attribute and how TLS keys are expressed.

1084 **Options:** Scott proposes one solution: Insert text after line 624 of Metadata:

1085 A use value of "signing" means that the contained key information is applicable to
1086 both signing and TLS/SSL operations performed by the entity when acting in the
1087 enclosing role.

1088 A use value of "encryption" means that the contained key information is suitable for
1089 use in wrapping encryption keys for use by the entity when acting in the enclosing
1090 role.

1091 If the use attribute is omitted, then the contained key information is applicable to both
1092 of the above uses.

1093 He further comments: "If "wrapping encryption keys" isn't a precise enough term, please find
1094 some crypto experts to clarify it... It's worth noting to the TC that this doesn't even scratch the
1095 surface of the problems with KeyInfo interop, and spec and product users are starting to notice..."
1096
1097 **Disposition:** During the TC conference call on [16 January 2007](#) the TC approved the changes as
1098 proposed here.

1099 **E63: IdP Discovery Cookie Interpretation**

1100 **First reported by:** Scott Cantor on security-services list

1101 **Message:** <http://lists.oasis-open.org/archives/security-services/200612/msg00035.html>

1102 **Document:** Profiles

1103 **Description:** There is confusion over how the contents of an IdP Discovery cookie are meant to
1104 be interpreted because of the allowance for specifying either persistent or session lifetime.

1105 **Options:** Scott proposes one solution: In Profiles Section 4.3, insert the following paragraph after
1106 line 1105:

1107 Note that while a session-only cookie can be used, the intent of this profile is not to
1108 provide a means of determining whether a user actually has an active session with
1109 one or more of the identity providers stored in the cookie. The cookie merely
1110 identifies identity providers known to have been used in the past. Service providers
1111 MAY instead rely on the IsPassive attribute in their samlp:AuthnRequest message to
1112 probe for active sessions.

1113 **Disposition:** During the TC conference call on [16 January 2007](#) the TC approved the changes as
1114 proposed here.

1115 **3 Proposed Errata**

1116 These proposed errata, given a "PE n " number designation, have either been determined by the
1117 SSTC not to be resolvable with a "non-substantive" change or, in the case of PEs with "[OPEN]"
1118 in the title, have not been considered by the SSTC yet.

1119 **PE3: Supported URL Encoding**

1120 **First reported by:** Scott Cantor, OSU

1121 **Message:** <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

1122 **Document:** Metadata

1123 **Description:** Specify the URL encoding supported by an HTTP Redirect binding endpoint.

1124 **Options:** This isn't actually an erratum, it's a missing piece that doesn't currently break anything
1125 but could in the future if alternate URL encodings for the Redirect binding emerge (for example a
1126 binary XML representation). We need an extension attribute to indicate non-default encoding
1127 support, it can just be added to our new "2.0 metadata extension schema". This should be moved
1128 to the issues list.

1129 **Disposition:** During the conference call of April 12 the TC agreed to move this to the issues list.

1130 **PE5: Rules for NameIDPolicy**

1131 **First reported by:** Brian Campbell, Ping Identity

1132 **Message:** <http://lists.oasis-open.org/archives/security-services/200501/msg00058.html>

1133 **Document:** Binding and Profiles

1134 **Description:** A *transient* nameid-format of a <NameIDPolicy> in an <AuthRequest> with
1135 *allowCreate* is meaningless.

1136 **Options:** There are two options. Both involve adding text after line 2147 of [SAMLCore].

1137 **1. Strict option:**

1138 “Finally, note that since the urn:oasis:names:tc:SAML:2.0:nameid-format:transient Format value
1139 (see Section 8.3.8) implicitly results in a new identifier being created during the handling of most
1140 requests, the AllowCreate attribute MUST be set to true in order for such a value to be returned.”

1141 **2. Optimized option:**

1142 “Finally, note that since them urn:oasis:names:tc:SAML:2.0:nameid-format:transient Format value
1143 (see Section 8.3.8) implicitly results in a new identifier being created during the handling of most
1144 requests, the AllowCreate attribute MUST be ignored by the identity provider when such an
1145 identifier is requested or issued.”

1146 **Disposition:** During the conference call of June 21 the TC agreed that E14 addresses this
1147 erratum and approved to dispose of this erratum as such.
1148

1149 **PE9: Clarification on SP AuthnRequestsSigned and the IdP** 1150 **WantAuthnRequestsSigned SP metadata flags**

1151 **First reported by:** Greg Whitehead, Trustgenix

1152 **Message:** <http://lists.oasis-open.org/archives/security-services/200503/msg00005.html>.

1153 **Document:** Metadata

1154 **Description:** The lack of a flag at an SP was not intended to imply that an SP would never sign if
1155 it had a reason to, and the IdP flag was not intended to somehow create a conflict. One can't
1156 resolve the situation policy-wise if an SP and IdP disagree about whether to sign, the metadata
1157 simply might reflect this.

1158 **Options:** See PE7

1159 **Disposition:** During the conference call of April 12 the TC accepted the option of combining this
1160 with E7 and disposing of it accordingly.

1161 **PE16: Inaccurate data in Feature Matrix**

1162 **First reported by:** Eric Tiffany, Liberty Alliance

1163 **Message:** <http://lists.oasis-open.org/archives/security-services-comment/200506/msg00000.html>

1164 **Document:** Conformance

1165 **Description:** The Feature Matrix (Table 2), last row, lists Identity Provider Discovery as N/A in
1166 the ECP column. However, the Profiles spec (line 725) notes that “The ECP MAY use the SAML
1167 identity provider discovery profile” to determine the IdP.”

1168 **Options:** Change the cell to say OPTIONAL instead of N/A

1169 **Disposition:** During the conference call of June 21 the TC approved to make no changes to the
1170 conformance document. A new erratum will be proposed to correct the Profile document to
1171 address this issue (see E18).

1172 **PE23: Metadata for <ArtifactResolutionService>**

1173 **First reported by:** Nick Ragouzis, Enosis Group

1174 **Message:** <http://lists.oasis-open.org/archives/security-services/200507/msg00036.html>

1175 **Document:** Profiles

1176 **Description:** The text is not as clear as it should be. In Section 4.1.6 (Web Browser SSO Profile),
1177 at Line 639 change “MUST” to “SHOULD”. Also, add the following text:

1178 If the request or response message is delivered using the HTTP Artifact binding, the artifact
1179 issuer SHOULD provide at least one <md:ArtifactResolutionService> endpoint element in its
1180 metadata.

1181 **Options:** Accept changes as suggested here.

1182 **Disposition:** During the call on 2/28 the TC moved to close with no resolution

1183 **PE44: Constrained Delegation**

1184 **First reported by:** Place holder for possible erratum. Scott will provide text as necessary.

1185 **Message:**

1186 **Document:**

1187 **Description:**

1188 **Options:**

1189 **Disposition:** Deactivated. Rolled into E47.

1190

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.

<i>Rev</i>	<i>Date</i>	<i>By Whom</i>	<i>What</i>
		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.

1192

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

Erratum #	Status	Document
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

<i>Erratum #</i>	<i>Status</i>	<i>Document</i>
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
PE62	Closed	Metadata
PE63	Closed	Profiles

1194 **Appendix C. Acknowledgments**

1195 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
1196 Committee, whose voting members at the time of publication were:

1197 • TBS

1198 The editors also would like to gratefully acknowledge Jahan Moreh of Sigaba, who during his
1199 tenure on the SSTC was the primary editor of this errata document and who made major
1200 substantive contributions to all of the errata materials.

Appendix D. Notices

1201

1202 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
1203 that might be claimed to pertain to the implementation or use of the technology described in this
1204 document or the extent to which any license under such rights might or might not be available;
1205 neither does it represent that it has made any effort to identify any such rights. Information on
1206 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
1207 website. Copies of claims of rights made available for publication and any assurances of licenses
1208 to be made available, or the result of an attempt made to obtain a general license or permission
1209 for the use of such proprietary rights by implementers or users of this specification, can be
1210 obtained from the OASIS Executive Director.

1211 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
1212 applications, or other proprietary rights which may cover technology that may be required to
1213 implement this specification. Please address the information to the OASIS Executive Director.

1214 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS]
1215 2007. All Rights Reserved.

1216 This document and translations of it may be copied and furnished to others, and derivative works
1217 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
1218 published and distributed, in whole or in part, without restriction of any kind, provided that the
1219 above copyright notice and this paragraph are included on all such copies and derivative works.
1220 However, this document itself does not be modified in any way, such as by removing the
1221 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS
1222 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual
1223 Property Rights document must be followed, or as required to translate it into languages other
1224 than English.

1225 The limited permissions granted above are perpetual and will not be revoked by OASIS or its
1226 successors or assigns.

1227 This document and the information contained herein is provided on an "AS IS" basis and OASIS
1228 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO
1229 ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE
1230 ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A
1231 PARTICULAR PURPOSE.