
1 Kantara Initiative 2 eGovernment Profiles of SAML 2.0

3 Version 2.0

4 **Working Draft 01**
5 **February 16, 2010**

6 **Document identifier:**
7 draft-kantara-egov-saml2-profiles-2.0

8 **Location:**
9 TBD

10 **Editors:**
11 Scott Cantor, Internet2

12 **Contributors:**
13 Kantara eGovernment WG
14 Andreas Åkre Solberg, UNINETT

15 **Abstract:**
16 This document contains implementation and deployment profiles for eGovernment use of SAML
17 V2.0, suitable for the purposes of developing a conformance program.

18 **Notice:**
19 This document has been prepared by Participants of Kantara Initiative. Permission is hereby
20 granted to use the document solely for the purpose of implementing the Specification. No rights
21 are granted to prepare derivative works of this Specification. Entities seeking permission to
22 reproduce portions of this document for other uses must contact Kantara Initiative to determine
23 whether an appropriate license for such use is available.

24
25 Implementation or use of certain elements of this document may require licenses under third party
26 intellectual property rights, including without limitation, patent rights. The Participants of and any
27 other contributors to the Specification are not and shall not be held responsible in any manner for
28 identifying or failing to identify any or all such third party intellectual property rights. This
29 Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of
30 any kind, expressed or implied, including any implied warranties of merchantability, non-
31 infringement of third party intellectual property rights, and fitness for a particular purpose.
32 Implementers of this Specification are advised to review Kantara Initiative's website
33 (<http://www.kantarainitiative.org/>) for information concerning any Necessary Claims Disclosure
34 Notices that have been received by the Kantara Initiative Board of Trustees.

35
36 Copyright: The content of this document is copyright of Kantara Initiative. © 2010 Kantara
37 Initiative.

38 Table of Contents

39	1 Introduction.....	4
40	1.1 Notation.....	4
41	1.2 Normative References.....	5
42	2 SAML V2.0 Browser SSO/SLO Implementation Profile.....	6
43	2.1 Required Information.....	6
44	2.2 Metadata and Trust Management.....	6
45	2.2.1 Conformance Assertions.....	7
46	2.3 Identity Provider Discovery.....	7
47	2.3.1 Conformance Assertions.....	7
48	2.4 Name Identifiers.....	7
49	2.4.1 Conformance Assertions.....	7
50	2.5 Attributes.....	7
51	2.5.1 Conformance Assertions.....	8
52	2.6 Single Sign-On.....	8
53	2.6.1 Authentication Requests.....	8
54	2.6.1.1 Binding and Security Requirements.....	8
55	2.6.1.1 Conformance Assertions.....	8
56	2.6.1.2 Message Content.....	8
57	2.6.1.2.1 Conformance Assertions.....	8
58	2.6.2 Responses.....	9
59	2.6.2.1 Binding and Security Requirements.....	9
60	2.6.2.1.1 Conformance Assertions.....	9
61	2.6.2.2 Message Content.....	9
62	2.6.2.2.1 Conformance Assertions.....	9
63	2.7 Single Logout.....	10
64	2.7.1 Logout Requests.....	10
65	2.7.1.1 Binding and Security Requirements.....	10
66	2.7.1.1.1 Conformance Assertions.....	10
67	2.7.1.2 User Interface Behavior.....	10
68	2.7.1.2.1 Conformance Assertions.....	10
69	2.7.2 Logout Responses.....	10
70	2.7.2.1 Binding and Security Requirements.....	10
71	2.7.2.1.1 Conformance Assertions.....	10
72	3 SAML V2.0 Browser SSO/SLO Deployment Profile.....	11
73	3.1 Required Information.....	11
74	3.2 Metadata and Trust Management.....	11
75	3.3 Name Identifiers.....	11
76	3.4 Attributes.....	12
77	3.5 Single Sign-On.....	12
78	3.5.1 Authentication Requests.....	12
79	3.5.1.1 Binding and Security Requirements.....	12
80	3.5.1.2 Message Content.....	12
81	3.5.2 Responses.....	13
82	3.5.2.1 Binding and Security Requirements.....	13
83	3.5.2.2 Message Content.....	13
84	3.6 Single Logout.....	13
85	3.6.1 Logout Requests.....	13
86	3.6.1.1 Binding and Security Requirements.....	13
87	3.6.2 Logout Responses.....	14

88	3.6.2.1 Binding and Security Requirements.....	14
89	Appendix A. Open Issues.....	15
90		

91 1 Introduction

92 SAML V2.0 is a rich and extensible standard that must be profiled to be used interoperably, and the
93 profiles that typically emerge from the broader standardization process usually remain fairly broad and
94 include a number of options and features that increase the burden for implementers and make
95 deployment-time decisions more difficult.

96 The Kantara Initiative eGovernment profiles make up a SAML V2.0 conformance specification for Identity
97 Provider and Service Provider implementations operating in eGovernment federations and deployments.
98 The profiles are based on the SAML V2.0 specifications created by the Security Services Technical
99 Committee (SSTC) of OASIS, and related specifications approved by that body. It constrains and
100 supplements the base SAML V2.0 features, elements, and attributes required for eGovernment
101 federations and deployments.

102 It is divided into *implementation* and *deployment* profiles. Implementation profiles define the features that
103 implementations must support within their product offerings such that deployers can be assured of the
104 ability to meet their own (possibly varied) deployment requirements. Deployment profiles define specific
105 options and constraints to which deployments are required to conform; they guide product configuration
106 and federation operations, and provide criteria against which actual deployments may be tested.

107 1.1 Notation

108 This specification uses normative text to describe the use of SAML capabilities.

109 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
110 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
111 described in [RFC 2119]:

112 ...they MUST only be used where it is actually required for interoperation or to limit behavior
113 which has potential for causing harm (e.g., limiting retransmissions)...

114 These keywords are thus capitalized when used to unambiguously specify requirements over protocol and
115 application features and behavior that affect the interoperability and security of implementations. When
116 these words are not capitalized, they are meant in their natural-language sense.

117 Listings of XML schemas appear like this.

118 Example code listings appear like this.

119 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
120 their respective namespaces as follows, whether or not a namespace declaration is present in the
121 example:

- 123 • The prefix `saml2:` stands for the SAML 2.0 assertion namespace,
124 `urn:oasis:names:tc:SAML:2.0:assertion`
- 125 • The prefix `saml2p:` stands for the SAML 2.0 protocol namespace,
126 `urn:oasis:names:tc:SAML:2.0:protocol`
- 127 • The prefix `md:` stands for the SAML 2.0 metadata namespace,
128 `urn:oasis:names:tc:SAML:2.0:metadata`
- 129 • The prefix `idpdisc:` stands for the Identity Provider Discovery Service Protocol and Profile
130 [`IdPDisco`] namespace, `urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-`
131 `protocol`
- 132 • The prefix `mdattr:` stands for the Metadata Extension for Entity Attributes Version 1.0 [MetaAttr]
133 namespace, `urn:oasis:names:tc:SAML:metadata:attribute`

134 This specification uses the following typographical conventions in text: <ns:Element>, Attribute,
135 **Datatype**, OtherCode.

136 1.2 Normative References

- 137 [RFC 2119] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*,
138 March 1997. <http://www.ietf.org/rfc/rfc2119.txt>
- 139 [RFC2616] IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*, June 1999.
140 <http://www.ietf.org/rfc/rfc2616.txt>
- 141 [RFC2818] IETF RFC 2818, *HTTP Over TLS*, May 2000. <http://www.ietf.org/rfc/rfc2818.txt>
- 142 [IdPDisco] OASIS Committee Specification, *Identity Provider Discovery Service Protocol
and Profile*, March 2008. <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf>
- 143 [MetaAttr] OASIS Committee Specification, *SAML V2.0 Metadata Extension for Entity
Attributes Version 1.0*, August 2009. <http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf>
- 144 [MetaIOP] OASIS Committee Specification, *SAML V2.0 Metadata Interoperability Profile
Version 1.0*, August 2009. <http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf>
- 145 [SAML2Core] OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion
Markup Language (SAML) V2.0*, March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 146 [SAML2Meta] OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language
(SAML) V2.0*, March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>
- 147 [SAML2Bind] OASIS Standard, *Bindings for the OASIS Security Assertion Markup Language
(SAML) V2.0*, March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf>
- 148 [SAML2Prof] OASIS Standard, *Profiles for the OASIS Security Assertion Markup Language
(SAML) V2.0*, March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>
- 149 [SAML2Err] OASIS Approved Errata, *SAML V2.0 Errata*. <http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf>
- 150 [SAML-X500] OASIS Committee Specification, *SAML V2.0 X.500/LDAP Attribute Profile*, March
151 2008. <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf>

168 Non-Normative References

- 169 [eGov15] Kyle Meadors, *Liberty Alliance eGov Profile for SAML 2.0 Version 1.5*.

170 **2 SAML V2.0 Browser SSO/SLO Implementation 171 Profile**

172 This profile specifies behavior and options that implementations of the SAML V2.0 Web Browser SSO and
173 Single Logout Profiles [SAML2Prof] are required to support. The requirements specified are *in addition to*
174 all normative requirements of the original profiles, as modified by the Approved Errata [SAML2Err], and
175 readers should be familiar with all relevant reference documents. Any such requirements are not repeated
176 here except where deemed necessary to highlight a point of discussion or draw attention to an issue
177 addressed in errata, but remain implied.

178 SAML leaves substantial latitude to implementations with regard to how software is architected and
179 combined with authentication and application infrastructure. Where the terms "Identity Provider" and
180 "Service Provider" are used, they should be understood to include the total software footprint intended to
181 provided the desired functionality; no specific assumptions are made as to how the required features are
182 exposed to deployers, only that there is some method for doing so.

183 **2.1 Required Information**

184 **Identification:** TBD

185 **Contact information:** TBD

186 **Description:** Given below

187 **Updates:** Liberty Alliance eGov Profile for SAML 2.0 [eGov15]

188 **2.2 Metadata and Trust Management**

189 Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of
190 SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 Web Browser SSO
191 Profile [SAML2Prof]. Additional expectations around the use of particular metadata elements related to
192 profile behavior may be encountered in subsequent sections.

193 Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetalOP].

194 Implementations MUST support the **TBD: insert profile for PKI here**

195 It is OPTIONAL for implementations to support the generation, publication, or exportation of metadata, but
196 implementations MUST support the following mechanisms for the importation of metadata:

- 197 • local file
- 198 • remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL
199 [RFC2818]

200 In the case of HTTP resolution, implementations MUST support use of the "ETag" header for cache
201 management; other cache control support is OPTIONAL. Implementations SHOULD support the use of
202 more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a
203 single entity's metadata is present in more than one source.

204 In accordance with [MetalOP], importation of multiple entities' metadata contained within an
205 <md:EntitiesDescriptor> element MUST be supported.

206 Verification of metadata, if supported, MUST include XML signature verification at least at the root
207 element level, and SHOULD support the following mechanisms for signature key trust establishment:

- 208 • direct comparison against known keys

- 209 • some form of path-based certificate validation against one or more trusted root certificates and
210 certificate revocation lists
- 211 The latter mechanism does not impose a particular profile for certificate validation, as no such profile has
212 wide enough adoption across tools and libraries to warrant such a requirement, but should be understood
213 as being consistent with the "usual" practices encountered in the implementation of certificate validation.
214 Where possible, implementations SHOULD document known limitations of the mechanisms they employ.
- 215 Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0
216 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension
217 mechanism.
- 218 Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without
219 substantial disruption of services.

220 **2.2.1 Conformance Assertions**

221 TBD

222 **2.3 Identity Provider Discovery**

223 Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery
224 Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].

225 **TBD: Maintain MUST for CDC profile?**

226 **2.3.1 Conformance Assertions**

227 TBD

228 **2.4 Name Identifiers**

229 Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name
230 identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]:

- 231 • urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
232 • urn:oasis:names:tc:SAML:2.0:nameid-format:transient

233 Support for other formats is OPTIONAL.

234 **2.4.1 Conformance Assertions**

235 TBD

236 **2.5 Attributes**

237 Identity Provider and Service Provider implementations MUST support the generation and consumption of
238 <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-
239 X500].

240 **TBD: Should support for more than simple strings be required or recommended?**

241 **2.5.1 Conformance Assertions**

242 TBD

243 **2.6 Single Sign-On**

244 **2.6.1 Authentication Requests**

245 **2.6.1.1 Binding and Security Requirements**

246 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect
247 binding [SAML2Bind] for the transmission of <saml2p:AuthnRequest> messages, including the
248 generation or verification of signatures in conjunction with this binding.

249 Support for other bindings is OPTIONAL.

250 **2.6.1.1.1 Conformance Assertions**

251 TBD

252 **2.6.1.2 Message Content**

253 In addition to standard core- and profile-driven requirements, Service Provider implementations MUST
254 support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes
255 (when appropriate):

- 256 • AssertionConsumerServiceURL
- 257 • ProtocolBinding
- 258 • ForceAuthn
- 259 • IsPassive
- 260 • AttributeConsumingServiceIndex
- 261 • <saml2p:RequestedAuthnContext>
- 262 • <saml2p:NameIDPolicy>

263 Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and
264 attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate
265 errors when confronted by particular request options. However, implementations SHOULD fully support
266 the options enumerated above. Implementations MAY limit their support of the
267 <saml2p:RequestedAuthnContext> element to the value "exact" for the Comparison attribute.

268 **2.6.1.2.1 Conformance Assertions**

269 TBD

270 **2.6.2 Responses**

271 **2.6.2.1 Binding and Security Requirements**

272 Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST binding
273 [SAML2Bind] for the transmission of <saml2p:Response> messages.

274 Support for other bindings is OPTIONAL.

275 Identity Providers and Service Providers MUST support the generation and consumption of unsolicited
276 <saml2p:Response> messages (i.e., responses that are not the result of a <saml2p:AuthnRequest>
277 message).

278 Identity Provider and Service Provider implementations MUST support the signing of
279 <saml2:Assertion> elements in responses; support for signing of the <saml2p:Response> element
280 is OPTIONAL.

281 Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the
282 <saml2:EncryptedAssertion> element; support for the <saml2:EncryptedID> and
283 <saml2:EncryptedAttribute> elements is OPTIONAL.

284 **2.6.2.1.1 Conformance Assertions**

285 TBD

286 **2.6.2.2 Message Content**

287 The Web Browser SSO Profile allows responses to contain any number of assertions and statements.
288 Identity Provider implementations MUST allow the number of <saml2:Assertion>,
289 <saml2:AuthnStatement>, and <saml2:AttributeStatement> elements in the
290 <saml2p:Response> message to be limited to one.

291 In turn, Service Provider implementations MAY limit support to a single instance of those elements when
292 processing <saml2p:Response> messages.

293 Identity Provider implementations MUST support the inclusion of a **Consent** attribute in
294 <saml2p:Response> messages, and a **SessionIndex** attribute in <saml2:AuthnStatement>
295 elements.

296 Service Provider implementations that provide some form of session semantics MUST support the
297 <saml2:AuthnStatement> element's **SessionNotOnOrAfter** attribute.

298 **2.6.2.2.1 Conformance Assertions**

299 TBD

300 **2.7 Single Logout**

301 **2.7.1 Logout Requests**

302 **2.7.1.1 Binding and Security Requirements**

303 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect
304 binding [SAML2Bind] for the transmission of <saml2p:LogoutRequest> messages, including the
305 generation or verification of signatures in conjunction with this binding.

306 Support for other bindings is OPTIONAL.

307 Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the
308 <saml2:EncryptedID> element.

309 **2.7.1.1.1 Conformance Assertions**

310 TBD

311 **2.7.1.2 User Interface Behavior**

312 Identity Provider and Service Provider implementations MUST support "local" logout as well as initiation of
313 Single Logout, subject to deployer and user option.

314 **2.7.1.2.1 Conformance Assertions**

315 TBD

316 **2.7.2 Logout Responses**

317 **2.7.2.1 Binding and Security Requirements**

318 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect
319 binding [SAML2Bind] for the transmission of <saml2p:LogoutResponse> messages, including the
320 generation or verification of signatures in conjunction with this binding.

321 Support for other bindings is OPTIONAL.

322 **2.7.2.1.1 Conformance Assertions**

323 TBD

3 SAML V2.0 Browser SSO/SLO Deployment Profile

This profile specifies behavior and options that deployments of the SAML V2.0 Web Browser SSO Profile [SAML2Prof] are required or permitted to rely on. The requirements specified are *in addition to* all normative requirements of the original profile, as modified by the Approved Errata [SAML2Err], and readers should be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

This profile addresses the content, exchange, and processing of SAML messages only, and does not address deployment details that go beyond that scope. Furthermore, nothing in the profile should be taken to imply that disclosing personally identifiable information, or indeed any information, is *required* from an Identity Provider with respect to any particular Service Provider. That remains at the discretion of applicable settings, user consent, or other appropriate means in accordance with regulations and policies.

Note that SAML features that are optional, or lack mandatory processing rules, are assumed to be optional and out of scope of this profile if not otherwise precluded or given specific processing rules.

3.1 Required Information

Identification: TBD

Contact information: TBD

Description: Given below

Updates: Liberty Alliance eGov Profile for SAML 2.0 [eGov15]

3.2 Metadata and Trust Management

TBD: Any agreement on the profile of metadata IdPs and SPs should supply?

If a Service Provider forgoes the use of TLS/SSL for its Assertion Consumer Service endpoints, then its metadata MUST include a `<md:KeyDescriptor>` suitable for XML Encryption. Note that use of TLS/SSL is RECOMMENDED.

If a Service Provider plans to utilize an external Discovery Service supporting the Identity Provider Discovery Service Protocol Profile [IdPDisco], then its metadata MUST include one or more `<idpdisc:DiscoveryResponse>` elements in the `<md:Extensions>` element of its `<md:SPSSODescriptor>` element.

3.3 Name Identifiers

Identity Providers MUST support the `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` name identifier format [SAML2Core]. They SHOULD support the `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` name identifier format [SAML2Core]. Support for other formats is OPTIONAL.

Service Providers, if they rely at all on particular name identifier formats, MUST support one of the following:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`

Reliance on other formats by Service Providers is NOT RECOMMENDED.

362 Note that these requirements are reflected in additional constraints on message content in subsequent
363 sections.

364 **3.4 Attributes**

365 Any `<saml2:Attribute>` elements exchanged via any SAML 2.0 messages, assertions, or metadata
366 MUST contain a NameFormat of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

367 The use of LDAP/X.500 attributes, and the SAML V2.0 X.500/LDAP Attribute Profile [SAML-X500] is
368 RECOMMENDED where possible.

369 It is RECOMMENDED that the content of `<saml2:AttributeValue>` elements exchanged via any
370 SAML 2.0 messages, assertions, or metadata be limited to a single child text node (i.e., a simple string
371 value).

372 **3.5 Single Sign-On**

373 **3.5.1 Authentication Requests**

374 **3.5.1.1 Binding and Security Requirements**

375 The `<saml2p:AuthnRequest>` message issued by a Service Provider MUST be communicated to the
376 Identity Provider using the HTTP-REDIRECT binding [SAML2Bind].

377 The endpoints at which an Identity Provider receives a `<saml2p:AuthnRequest>` message, and all
378 subsequent exchanges with the user agent, SHOULD be protected by TLS/SSL.

379 **3.5.1.2 Message Content**

380 The `<saml2p:AuthnRequest>` message issued by a Service Provider MUST contain an
381 AssertionConsumerServiceURL attribute identifying the desired response location. The
382 ProtocolBinding attribute, if present, MUST be set to
383 `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.

384 The `<saml2p:AuthnRequest>` message MUST NOT contain a `<saml2:Subject>` element.

385 The `<saml2p:AuthnRequest>` message SHOULD contain a `<saml2p:NameIDPolicy>` element with
386 an AllowCreate attribute of "true". Its Format attribute, if present, SHOULD be set to one of the
387 following values:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`

388 The `<saml2p:AuthnRequest>` message MAY contain a `<saml2p:RequestedAuthnContext>`
389 element, but SHOULD do so only in the presence of an arrangement between the Identity and Service
390 Providers regarding the Authentication Context definitions in use. The Comparison attribute SHOULD be
393 omitted or be set to "exact".

394 **3.5.2 Responses**

395 **3.5.2.1 Binding and Security Requirements**

396 The `<saml2p:Response>` message issued by an Identity Provider MUST be communicated to the
397 Service Provider using the HTTP-POST binding [SAML2Bind].

398 The endpoint(s) at which a Service Provider receives a `<saml2p:Response>` message SHOULD be
399 protected by TLS/SSL. If this is not the case, then Identity Providers MUST utilize XML Encryption and
400 return a `<saml2:EncryptedAssertion>` element in the `<saml2p:Response>` message. The
401 `<saml2:EncryptedID>` and `<saml2:EncryptedAttribute>` elements MUST NOT be used.

402 Whether encrypted or not, the `<saml2:Assertion>` element issued by the Identity Provider MUST itself
403 be signed directly using a `<ds:Signature>` element within the `<saml2:Assertion>`.

404 Service Providers MUST support unsolicited `<saml2p:Response>` messages (i.e., responses that are
405 not the result of an earlier `<saml2p:AuthnRequest>` message).

406 **3.5.2.2 Message Content**

407 Assuming a successful response, the `<saml2p:Response>` message issued by an Identity Provider
408 MUST contain exactly one assertion (either a `<saml2:Assertion>` or an
409 `<saml2:EncryptedAssertion>` element). The assertion MUST contain exactly one
410 `<saml2:AuthnStatement>` element and MAY contain zero or one `<saml2:AttributeStatement>`
411 elements.

412 The `<saml2:AuthnStatement>` element of the assertions issued by an Identity Provider MUST contain
413 a SessionIndex attribute.

414 The `<saml2:Subject>` element of the assertions issued by an Identity Provider SHOULD contain a
415 `<saml2:NameID>` element. It MUST NOT contain a `<saml2:EncryptedID>` or `<saml2:BaseID>`
416 element. In the absence of a `<saml2p:NameIDPolicy>` Format attribute in the Service Provider's
417 `<saml2p:AuthnRequest>` message, or a `<md:NameIDFormat>` element in the Service Provider's
418 metadata, the Format of the `<saml2:NameID>` SHOULD be set to
419 `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`.

420 **3.6 Single Logout**

421 **3.6.1 Logout Requests**

422 **3.6.1.1 Binding and Security Requirements**

423 The `<saml2p:LogoutRequest>` message issued by an Identity Provider or Service Provider MUST be
424 communicated using the HTTP-REDIRECT binding [SAML2Bind]. The message MUST be signed.

425 The endpoints at which an Identity Provider or Service Provider receives a `<saml2p:LogoutRequest>`
426 message SHOULD be protected by TLS/SSL.

427 TBD: Use of encryption?

428 **3.6.2 Logout Responses**

429 **3.6.2.1 Binding and Security Requirements**

430 The <saml2p:LogoutResponse> message issued by an Identity Provider or Service Provider MUST be
431 communicated using the HTTP-REDIRECT binding [SAML2Bind]. The message MUST be signed.

432 The endpoints at which an Identity Provider or Service Provider receives a <saml2p:LogoutResponse>
433 message SHOULD be protected by TLS/SSL.

434 Appendix A. Open Issues

- 435 • Need an alternative to IOP, or agreement to drop PKI outside of metadata exchange. Alternative
436 needs to specify PKI to some degree AND address the exact content and semantics of metadata
437 as relates to runtime certificate evaluation and/or identity of SAML peer.
- 438 • Should CDC discovery profile remain MTI?
- 439 • Should responses via artifact remain MTI?
- 440 • Dropped "unspecified" and "basic" formats for names and attribute naming.
- 441 • Need for non-trivial attribute value support?
- 442 • Need for more than exact AuthnContext matching?
- 443 • Noted specific AuthnRequest content to support, needs review.
- 444 • Need for specific MTI behavior on ACS checking?
- 445 • Added constraint on number of assertions and statements.
- 446 • Added requirement for SP support of SessionNotOnOrAfter.
- 447 • Added Encryption as MTI for logout.
- 448 • Need some clarification of some of the original single logout language around user consent.
- 449 • Is SSL a MUST for deployers? If so, why require encryption?
- 450 • Updated crypto algorithm conformance rules for implementers and deployers?
- 451 • Populate with conformance assertions/tests.