
1 Kantara Initiative eGovernment 2 Implementation Profile of SAML V2.0

3 Version 2.0

4 **Working Draft 03**
5 **March 19, 2010**

6 **Document identifier:**
7 draft-kantara-egov-saml2-profile-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 an implementation profile for eGovernment use of SAML V2.0, suitable
17 for the purposes of testing conformance of implementations of SAML V2.0. It is not a deployment
18 profile, and does not provide for or reflect specific behavior expected of implementations when
19 used within a particular deployment context.

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

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

36
37 Copyright: The content of this document is copyright of Kantara Initiative. © 2010 Kantara
38 Initiative.
39

40 Table of Contents

41	1 Introduction.....	3
42	1.1 Notation.....	3
43	1.2 Normative References.....	4
44	2 SAML V2.0 Implementation Profile.....	5
45	2.1 Required Information.....	5
46	2.2 Metadata and Trust Management.....	5
47	2.2.1 Conformance Criteria.....	6
48	2.3 Name Identifiers.....	6
49	2.3.1 Conformance Criteria.....	6
50	2.4 Attributes.....	6
51	2.4.1 Conformance Criteria.....	6
52	2.5 Browser Single Sign-On.....	6
53	2.5.1 Identity Provider Discovery.....	7
54	2.5.1.1 Conformance Criteria.....	7
55	2.5.2 Authentication Requests.....	7
56	2.5.2.1 Binding and Security Requirements.....	7
57	2.5.2.1.1 Conformance Criteria.....	7
58	2.5.2.2 Message Content.....	7
59	2.5.2.2.1 Conformance Criteria.....	7
60	2.5.3 Responses.....	8
61	2.5.3.1 Binding and Security Requirements.....	8
62	2.5.3.1.1 Conformance Criteria.....	8
63	2.5.3.2 Message Content.....	8
64	2.5.3.2.1 Conformance Criteria.....	8
65	2.5.4 Artifact Resolution.....	9
66	2.5.4.1 Artifact Resolution Requests.....	9
67	2.5.4.1.1 Conformance Criteria.....	9
68	2.5.4.2 Artifact Resolution Responses.....	9
69	2.5.4.2.1 Conformance Criteria.....	9
70	2.6 Browser Holder of Key Single Sign-On.....	9
71	2.6.1 Conformance Criteria.....	9
72	2.7 Single Logout.....	9
73	2.7.1 Logout Requests.....	10
74	2.7.1.1 Binding and Security Requirements.....	10
75	2.7.1.1.1 Conformance Criteria.....	10
76	2.7.1.2 User Interface Behavior.....	10
77	2.7.1.2.1 Conformance Criteria.....	10
78	2.7.2 Logout Responses.....	10
79	2.7.2.1 Binding and Security Requirements.....	10
80	2.7.2.1.1 Conformance Criteria.....	10
81	3 Conformance Classes.....	11
82	3.1 Standard.....	11
83	3.2 Standard with Logout.....	11
84	3.3 Full.....	11
85	Appendix A. Open Issues.....	12
86	Appendix B. Change Log.....	13
87		

88 1 Introduction

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

93 The Kantara Initiative eGovernment Implementation Profile provides a SAML V2.0 conformance
94 specification for Identity Provider and Service Provider implementations operating in eGovernment
95 federations and deployments. The profile is based on the SAML V2.0 specifications created by the
96 Security Services Technical Committee (SSTC) of OASIS, and related specifications approved by that
97 body. It constrains and supplements the base SAML V2.0 features, elements, and attributes required for
98 eGovernment federations and deployments.

99 Implementation profiles define the features that software implementations must support such that
100 deployers can be assured of the ability to meet their own (possibly varied) deployment requirements.
101 Deployment profiles define specific options and constraints to which deployments are required to conform;
102 they guide product configuration and federation operations, and provide criteria against which actual
103 deployments may be tested. This document does not include a deployment profile, but reflects the
104 features deemed necessary or desirable from software implementations in support of a variety of
105 deployment profiles planned and in use. This includes requirements deemed useful to further the eventual
106 goal of interfederation between deployments.

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 [RFC2119]:

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	[RFC2119]	IETF RFC 2119, <i>Key words for use in RFCs to Indicate Requirement Levels</i> , 138 March 1997. http://www.ietf.org/rfc/rfc2119.txt
139	[RFC2616]	IETF RFC 2616, <i>Hypertext Transfer Protocol – HTTP/1.1</i> , June 1999. 140 http://www.ietf.org/rfc/rfc2616.txt
141	[RFC2818]	IETF RFC 2818, <i>HTTP Over TLS</i> , May 2000. http://www.ietf.org/rfc/rfc2818.txt
142	[HoKSSO]	OASIS Committee Specification, <i>SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0</i> , July 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso-cs-01.pdf
145	[IdPDisco]	OASIS Committee Specification, <i>Identity Provider Discovery Service Protocol and Profile</i> , March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf
148	[MetaAttr]	OASIS Committee Specification, <i>SAML V2.0 Metadata Extension for Entity Attributes Version 1.0</i> , August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf
151	[MetaIOP]	OASIS Committee Specification, <i>SAML V2.0 Metadata Interoperability Profile Version 1.0</i> , August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf
154	[SAML2Core]	OASIS Standard, <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
157	[SAML2Meta]	OASIS Standard, <i>Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
160	[SAML2Bind]	OASIS Standard, <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
163	[SAML2Prof]	OASIS Standard, <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
166	[SAML2Err]	OASIS Approved Errata, <i>SAML V2.0 Errata</i> . http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf
168	[SAML-X500]	OASIS Committee Specification, <i>SAML V2.0 X.500/LDAP Attribute Profile</i> , March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf

171 Non-Normative References

172	[eGov15]	Kyle Meadors, <i>Liberty Alliance eGov Profile for SAML 2.0 Version 1.5</i> .
-----	----------	---

173 2 SAML V2.0 Implementation Profile

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

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

185 2.1 Required Information

186 **Identification:** TBD

187 **Contact information:** TBD

188 **Description:** Given below

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

190 2.2 Metadata and Trust Management

191 Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of
192 SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 profiles referenced
193 by subsequent sections. Additional expectations around the use of particular metadata elements related to
194 profile behavior may be encountered in those sections.

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

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

197 It is OPTIONAL for implementations to support the generation or exportation of metadata, but
198 implementations MUST support the publication of metadata using the Well-Known-Location method
199 defined in section 4.1 of [SAML2Meta] (under the assumption that entityID values used are suitable for
200 such support).

201 Implementations MUST support the following mechanisms for the importation of metadata:

- 202 • local file
203 • remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL
204 [RFC2818]

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

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

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

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

225 **2.2.1 Conformance Criteria**

226 TBD

227 **2.3 Name Identifiers**

228 In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity
229 Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier
230 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 **2.3.1 Conformance Criteria**

235 TBD

236 **2.4 Attributes**

237 In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity
238 Provider and Service Provider implementations MUST support the generation and consumption of
239 <saml2:Attribute> elements that conform to the SAML V2.0 X.500/LDAP Attribute Profile [SAML-
240 X500].

241 The ability to support <saml2:AttributeValue> elements whose values are not simple strings (e.g.,
242 <saml2:NameID>, or other XML values) is OPTIONAL. Such content could be base64-encoded as an
243 alternative.

244 **2.4.1 Conformance Criteria**

245 TBD

246 **2.5 Browser Single Sign-On**

247 This section defines an implementation profile of the SAML V2.0 Web Browser SSO Profile [SAML2Prof].

248 **2.5.1 Identity Provider Discovery**

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

251 **2.5.1.1 Conformance Criteria**

252 TBD

253 **2.5.2 Authentication Requests**

254 **2.5.2.1 Binding and Security Requirements**

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

258 Support for other bindings is OPTIONAL.

259 **2.5.2.1.1 Conformance Criteria**

260 TBD

261 **2.5.2.2 Message Content**

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

- 265 • AssertionConsumerServiceURL
- 266 • ProtocolBinding
- 267 • ForceAuthn
- 268 • IsPassive
- 269 • AttributeConsumingServiceIndex
- 270 • <saml2p:RequestedAuthnContext>
- 271 • <saml2p:NameIDPolicy>

272 Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and
273 attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate
274 errors when confronted by particular request options. However, implementations MUST fully support the
275 options enumerated above.

276 Implementations MAY limit their support of the <saml2p:RequestedAuthnContext> element to the
277 value "exact" for the Comparison attribute.

278 **2.5.2.2.1 Conformance Criteria**

279 TBD

280 **2.5.3 Responses**

281 **2.5.3.1 Binding and Security Requirements**

282 Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST and
283 HTTP-Artifact bindings [SAML2Bind] for the transmission of <saml2p:Response> messages.

284 Support for other bindings, and for artifact types other than
285 urn:oasis:names:tc:SAML:2.0:artifact-04, is OPTIONAL.

286 Identity Provider and Service Provider implementations MUST support the generation and consumption of
287 unsolicited <saml2p:Response> messages (i.e., responses that are not the result of a
288 <saml2p:AuthnRequest> message).

289 Identity Provider implementations MUST support the issuance of <saml2p:Response> messages (with
290 appropriate status codes) in the course of encountering error conditions, provided that the user agent
291 remains available and the location to deliver the response is knowable. Note that this is a stronger
292 requirement than the comparable language in [SAML2Prof].

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

296 Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the
297 <saml2:EncryptedAssertion> element when using the HTTP-POST binding; support for the
298 <saml2:EncryptedID> and <saml2:EncryptedAttribute> elements is OPTIONAL.

299 **2.5.3.1.1 Conformance Criteria**

300 TBD

301 **2.5.3.2 Message Content**

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

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

308 Identity Provider implementations MUST support the inclusion of a `Consent` attribute in
309 <saml2p:Response> messages, and a `SessionIndex` attribute in <saml2:AuthnStatement>
310 elements.

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

313 **2.5.3.2.1 Conformance Criteria**

314 TBD

315 **2.5.4 Artifact Resolution**

316 Pursuant to the requirement in section 2.5.3.1 for support of the HTTP-Artifact binding [SAML2Bind] for
317 the transmission of <saml2p:Response> messages, implementations MUST support the SAML V2.0
318 Artifact Resolution profile [SAML2Prof] as constrained by the following subsections.

319 **2.5.4.1 Artifact Resolution Requests**

320 Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using
321 HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResolve>
322 messages.

323 Implementations MUST support the use of SAML message signatures and TLS server authentication to
324 authenticate requests; support for TLS client authentication, or other forms of authentication in conjunction
325 with the SAML SOAP binding, is OPTIONAL.

326 **2.5.4.1.1 Conformance Criteria**

327 TBD

328 **2.5.4.2 Artifact Resolution Responses**

329 Identity Provider and Service Provider implementations MUST support the use of the SAML SOAP (using
330 HTTP as a transport) binding [SAML2Bind] for the transmission of <saml2p:ArtifactResponse>
331 messages.

332 Implementations MUST support the use of SAML message signatures and TLS server authentication to
333 authenticate responses; support for TLS client authentication, or other forms of authentication in
334 conjunction with the SAML SOAP binding, is OPTIONAL.

335 **2.5.4.2.1 Conformance Criteria**

336 TBD

337 **2.6 Browser Holder of Key Single Sign-On**

338 This section defines an implementation profile of the SAML V2.0 Holder-of-Key Web Browser SSO Profile
339 Version 1.0 [HoKSSO].

340 The implementation requirements defined in section 2.5 for the non-holder-of-key profile apply to
341 implementations of this profile.

342 **2.6.1 Conformance Criteria**

343 TBD

344 **2.7 Single Logout**

345 This section defines an implementation profile of the SAML V2.0 Single Logout Profile [SAML2Prof].

346 For clarification, the technical requirements for each message type below reflect the intent to normatively
347 require initiation of logout by a Service Provider using either the front- or back-channel, and
348 initiation/propagation of logout by an Identity Provider using the back-channel.

349 **2.7.1 Logout Requests**

350 **2.7.1.1 Binding and Security Requirements**

351 Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding
352 [SAML2Bind] for the issuance of <saml2p:LogoutRequest> messages, and MUST support the SAML
353 SOAP (using HTTP as a transport) and HTTP-Redirect bindings [SAML2Bind] for the reception of
354 <saml2p:LogoutRequest> messages.

355 Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding
356 [SAML2Bind] for both issuance and reception of <saml2p:LogoutRequest> messages.

357 Support for other bindings is OPTIONAL.

358 Implementations MUST support the use of SAML message signatures and TLS server authentication to
359 authenticate requests; support for TLS client authentication, or other forms of authentication in conjunction
360 with the SAML SOAP binding, is OPTIONAL.

361 Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the
362 <saml2:EncryptedID> element when using the HTTP-Redirect binding.

363 **2.7.1.1.1 Conformance Criteria**

364 TBD

365 **2.7.1.2 User Interface Behavior**

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

368 **2.7.1.2.1 Conformance Criteria**

369 TBD

370 **2.7.2 Logout Responses**

371 **2.7.2.1 Binding and Security Requirements**

372 Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) and
373 HTTP-Redirect bindings [SAML2Bind] for the issuance of <saml2p:LogoutResponse> messages, and
374 MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the reception of
375 <saml2p:LogoutResponse> messages.

376 Service Provider implementations MUST support the SAML SOAP (using HTTP as a transport) binding
377 [SAML2Bind] for both issuance and reception of <saml2p:LogoutResponse> messages.

378 Support for other bindings is OPTIONAL.

379 Implementations MUST support the use of SAML message signatures and TLS server authentication to
380 authenticate responses; support for TLS client authentication, or other forms of authentication in
381 conjunction with the SAML SOAP binding, is OPTIONAL.

382 **2.7.2.1.1 Conformance Criteria**

383 TBD

384 **3 Conformance Classes**

385 **3.1 Standard**

386 Conforming Identity Provider and/or Service Provider implementations MUST support the normative
387 requirements in sections 2.2, 2.3, 2.4, and 2.5.

388 **3.2 Standard with Logout**

389 Conforming Identity Provider and/or Service Provider implementations MUST support the normative
390 requirements in sections 2.2, 2.3, 2.4, 2.5, and 2.7.

391 **3.3 Full**

392 Conforming Identity Provider and/or Service Provider implementations MUST support all normative
393 requirements in section 2.

394 Appendix A. Open Issues

- 395 • Need an alternative to IOP, or agreement to drop PKI outside of metadata exchange. Alternative
396 needs to specify PKI to some degree AND address the exact content and semantics of metadata
397 as relates to runtime certificate evaluation and/or identity of SAML peer.
- 398 • Do implementations need to be able to prevent non-use of TLS on front-channel?
- 399 • Need for more than exact AuthnContext matching?
- 400 • Need for specific MTI behavior on ACS checking?
- 401 • Need some clarification of some of the original single logout language around user consent.
- 402 • Updated crypto algorithm conformance rules for implementers and deployers?
- 403 • Populate with conformance criteria.
- 404 • Is feature discussion of AuthnContext and metadata tagging enough to cover LOA issues?
- 405 • IdP proxying
- 406 • Need to bump HoK reference to new profile version once it reaches CS.

407

Appendix B. Change Log

- 408 • Draft 01: first working draft based on similar document created by InCommon Federation
- 409 • Draft 02: first round of feedback incorporated, deployment section dropped, new section on
410 Artifact Resolution added, artifact added for SSO responses, SOAP added for logout, discovery
411 moved under SSO, language on non-string attributes added, changed SHOULD to MUST for IdP
412 support of selected AuthnRequest features
- 413 • Draft 03: moved Artifact Resolution into a SSO profile subsection, new language on SOAP
414 security and SLO bindings, added metadata publication via WKL, added language on IdP error
415 handling, added Holder of Key SSO profile, added Conformance Classes