

---

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

## 3 Version 2.0

4 **Working Draft 023**  
5 **March 109, 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	<b>[RFC2119]</b>	IETF RFC 2119, <i>Key words for use in RFCs to Indicate Requirement Levels</i> , 138 March 1997. <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
139	<b>[RFC2616]</b>	IETF RFC 2616, <i>Hypertext Transfer Protocol – HTTP/1.1</i> , June 1999. 140 <a href="http://www.ietf.org/rfc/rfc2616.txt">http://www.ietf.org/rfc/rfc2616.txt</a>
141	<b>[RFC2818]</b>	IETF RFC 2818, <i>HTTP Over TLS</i> , May 2000. <a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a>
142	<b>[HoKSSO]</b>	<a href="#">OASIS Committee Specification, SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0, August 2009</a> . <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf</a> <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso-cs-01.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso-cs-01.pdf</a>
146	<b>[IdPDisco]</b>	OASIS Committee Specification, <i>Identity Provider Discovery Service Protocol and Profile</i> , March 2008. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf</a>
149	<b>[MetaAttr]</b>	OASIS Committee Specification, <i>SAML V2.0 Metadata Extension for Entity Attributes Version 1.0</i> , August 2009. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf</a>
152	<b>[MetaIOP]</b>	OASIS Committee Specification, <i>SAML V2.0 Metadata Interoperability Profile Version 1.0</i> , August 2009. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf</a>
155	<b>[SAML2Core]</b>	OASIS Standard, <i>Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf</a>
158	<b>[SAML2Meta]</b>	OASIS Standard, <i>Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf</a>
161	<b>[SAML2Bind]</b>	OASIS Standard, <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf</a>
164	<b>[SAML2Prof]</b>	OASIS Standard, <i>Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0</i> , March 2005. <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf</a>
167	<b>[SAML2Err]</b>	OASIS Approved Errata, <i>SAML V2.0 Errata</i> . <a href="http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf">http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf</a>
169	<b>[SAML-X500]</b>	OASIS Committee Specification, <i>SAML V2.0 X.500/LDAP Attribute Profile</i> , March 2008. <a href="http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf">http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-x500.pdf</a>

## 172 Non-Normative References

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

---

## 174 2 SAML V2.0 Implementation Profile

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

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

### 186 2.1 Required Information

187 **Identification:** TBD

188 **Contact information:** TBD

189 **Description:** Given below

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

### 191 2.2 Metadata and Trust Management

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

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

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

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

202 | Implementations MUST support the following mechanisms for the importation of metadata:

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

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

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

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

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

## 226     **2.2.1 Conformance Criteria**

227     TBD

## 228     **2.3 Name Identifiers**

229     In conjunction with their support of the SAML V2.0 profiles referenced by subsequent sections, Identity  
230     Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier  
231     formats, in accordance with the normative obligations associated with them by [SAML2Core]:

- 232       • urn:oasis:names:tc:SAML:2.0:nameid-format:persistent  
233       • urn:oasis:names:tc:SAML:2.0:nameid-format:transient
- 234     Support for other formats is OPTIONAL.

## 235     **2.3.1 Conformance Criteria**

236     TBD

## 237     **2.4 Attributes**

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

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

## 245     **2.4.1 Conformance Criteria**

246     TBD

## 247     **2.5 Browser Single Sign-On**

248     This section defines an implementation profile of the SAML V2.0 Web Browser SSO [pProfile](#)  
249     [SAML2Prof].

- 250 **2.5.1 Identity Provider Discovery**
- 251 Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery  
252 Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].
- 253 **2.5.1.1 Conformance Criteria**
- 254 TBD
- 255 **2.5.2 Authentication Requests**
- 256 **2.5.2.1 Binding and Security Requirements**
- 257 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect  
258 binding [SAML2Bind] for the transmission of <saml2p:AuthnRequest> messages, including the  
259 generation or verification of signatures in conjunction with this binding.
- 260 Support for other bindings is OPTIONAL.
- 261 **2.5.2.1.1 Conformance Criteria**
- 262 TBD
- 263 **2.5.2.2 Message Content**
- 264 In addition to standard core- and profile-driven requirements, Service Provider implementations MUST  
265 support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes  
266 (when appropriate):
- 267
  - AssertionConsumerServiceURL
  - ProtocolBinding
  - ForceAuthn
  - IsPassive
  - AttributeConsumingServiceIndex
  - <saml2p:RequestedAuthnContext>
  - <saml2p:NameIDPolicy>
- 268 Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and  
269 attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate  
270 errors when confronted by particular request options. However, implementations MUST fully support the  
271 options enumerated above.
- 272 Implementations MAY limit their support of the <saml2p:RequestedAuthnContext> element to the  
273 value "exact" for the Comparison attribute.
- 274 **2.5.2.2.1 Conformance Criteria**
- 275 TBD

282 **2.5.3 Responses**

283 **2.5.3.1 Binding and Security Requirements**

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

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

288 | Identity Providers and Service Providers [implementations](#) MUST support the generation and consumption  
289 | of unsolicited <saml2p:Response> messages (i.e., responses that are not the result of a  
290 | <saml2p:AuthnRequest> message).

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

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

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

301 **2.5.3.1.1 Conformance Criteria**

302 TBD

303 **2.5.3.2 Message Content**

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

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

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

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

315 **2.5.3.2.1 Conformance Criteria**

316 TBD

317 **2.5.4 Artifact Resolution**

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

321 **2.5.4.1 Artifact Resolution Requests**

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

325 ~~Implementations MUST support the use of SAML message signatures to authenticate requests; support~~  
326 ~~for TLS or other transport-based authentication in conjunction with the SAML SOAP binding is~~  
327 ~~OPTIONAL. Implementations MUST support the use of SAML message signatures and TLS server~~  
328 ~~authentication to authenticate requests; support for TLS client authentication, or other forms of~~  
329 ~~authentication in conjunction with the SAML SOAP binding, is OPTIONAL.~~

330 **2.5.4.1.1 Conformance Criteria**

331 TBD

332 **2.5.4.2 Artifact Resolution Responses**

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

336 ~~Implementations MUST support the use of SAML message signatures to authenticate requests; support~~  
337 ~~for TLS or other transport-based authentication in conjunction with the SAML SOAP binding is~~  
338 ~~OPTIONAL. Implementations MUST support the use of SAML message signatures and TLS server~~  
339 ~~authentication to authenticate responses; support for TLS client authentication, or other forms of~~  
340 ~~authentication in conjunction with the SAML SOAP binding, is OPTIONAL.~~

341 **2.5.4.2.1 Conformance Criteria**

342 TBD

343 **2.6 Browser Holder of Key Single Sign-On**

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

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

348 **2.6.1 Conformance Criteria**

349 TBD

350 **2.7 Single Logout**

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

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

355 | **2.7.1 Logout Requests**

356 | **2.7.1.1 Binding and Security Requirements**

357 | Identity Provider and Service Provider implementations MUST support the HTTP Redirect and use of the  
358 | SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the transmission issuance of  
359 | <saml2p:LogoutRequest> messages, including the generation or verification of message signatures in  
360 | conjunction with both bindings, and MUST support the SAML SOAP (using HTTP as a transport) and  
361 | HTTP-Redirect bindings [SAML2Bind] for the reception of <saml2p:LogoutRequest> messages.

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

364 | Support for other bindings is OPTIONAL.

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

368 | Support for other bindings is OPTIONAL.

369 | Support for TLS or other transport-based authentication in conjunction with the SAML SOAP binding is  
370 | OPTIONAL.

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

373 | **2.7.1.1.1 Conformance Criteria**

374 | TBD

375 | **2.7.1.2 User Interface Behavior**

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

378 | **2.7.1.2.1 Conformance Criteria**

379 | TBD

380 | **2.7.2 Logout Responses**

381 | **2.7.2.1 Binding and Security Requirements**

382 | Identity Provider implementations MUST support the SAML SOAP (using HTTP as a transport) and  
383 | HTTP-Redirect bindings [SAML2Bind] for the issuance of <saml2p:LogoutResponse> messages, and  
384 | MUST support the SAML SOAP (using HTTP as a transport) binding [SAML2Bind] for the reception of  
385 | <saml2p:LogoutResponse> messages.

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

388 | Support for other bindings is OPTIONAL.

389 | Implementations MUST support the use of SAML message signatures and TLS server authentication to  
authenticate responses; support for TLS client authentication, or other forms of authentication in  
conjunction with the SAML SOAP binding, is OPTIONAL. Identity Provider and Service Provider  
390 | implementations MUST support the use of the HTTP-Redirect and SAML SOAP (using HTTP as a  
391 | transport) bindings [SAML2Bind] for the transmission of <saml2p:LogoutResponse> messages;  
392 | including the generation or verification of message signatures in conjunction with both bindings. Support  
393 | for TLS or other transport-based authentication in conjunction with the SAML SOAP binding is  
394 | OPTIONAL.

397 | Support for other bindings is OPTIONAL.

### 398 | **2.7.2.1.1 Conformance Criteria**

399 | TBD

---

400 | **3 Conformance Classes**

401 | **3.1 Standard**

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

404 | **3.2 Standard with Logout**

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

407 | **3.3 Full**

408 | Conforming Identity Provider and/or Service Provider implementations MUST support all normative  
409 | requirements in section 2.

---

## 410 Appendix A. Open Issues

- 411     • Need an alternative to IOP, or agreement to drop PKI outside of metadata exchange. Alternative  
412       needs to specify PKI to some degree AND address the exact content and semantics of metadata  
413       as relates to runtime certificate evaluation and/or identity of SAML peer.
- 414     • ~~Security features required in support of SOAP binding? Client signing, server signing + TLS~~
- 415     • Do implementations need to be able to prevent non-use of TLS on front-channel?
- 416     • Need for more than exact AuthnContext matching?
- 417     • Need for specific MTI behavior on ACS checking?
- 418     • Need some clarification of some of the original single logout language around user consent.
- 419     • Updated crypto algorithm conformance rules for implementers and deployers?
- 420     • Populate with conformance criteria.
- 421     • Is feature discussion of AuthnContext and metadata tagging enough to cover LOA issues?
- 422     • ~~Add metadata publication requirement...~~
- 423     • IdP proxying
- 424     • ~~Mandating Responses from IdP during SSO? Need to bump HoK reference to new profile version once it reaches CS.~~
- 425

---

## 426 Appendix B. Change Log

- 427 |     • Draft 01: first working draft based on similar document created by InCommon fEderation
- 428 |     • Draft 02: first round of feedback incorporated, deployment section dropped, new section on
- 429 |       Artifact Resolution added, artifact added for SSO responses, SOAP added for logout, discovery
- 430 |       moved under SSO, language on non-string attributes added, changed SHOULD to MUST for IdP
- 431 |       support of selected AuthnRequest features
- 432 |     • Draft 03: moved Artifact Resolution into a SSO profile subsection, new language on SOAP
- 433 |       security and SLO bindings, added metadata publication via WKL, added language on IdP error
- 434 |       handling, added Holder of Key SSO profile, added Conformance Classes