



Metadata Profile for the OASIS Security Assertion Markup Language (SAML) V1.x

OASIS Standard
1 November 2007

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-os.html>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-os.odt>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-os.pdf>

Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-cs-01.html>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-cs-01.odt>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata-cs-01.pdf>

Latest Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata.html>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata.odt>
<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1x-metadata.pdf>

Technical Committee:

OASIS Security Services TC

Chairs:

Hal Lockhart, BEA Systems, Inc.
Brian Campbell, Ping Identity

Editors:

Greg Whitehead, Hewlett-Packard Company
Scott Cantor, Internet2

Related Work:

This specification supplements the SAML V2.0 metadata specification [SAML2Meta].

Declared XML Namespaces(s):

urn:oasis:names:tc:SAML:profiles:v1metadata

Abstract:

This specification defines a profile of the OASIS SAML V2.0 metadata specification for use in describing SAML V1.0 and V1.1 entities. Readers should be familiar with the SAML V2.0 metadata specification [SAML2Meta] before reading this document.

36 **Status:**

37 This document was last revised or approved by the SSTC on the above date. The level of
38 approval is also listed above.

39 Technical Committee members should send comments on this specification to the Technical
40 Committee's email list. Others should send comments to the Technical Committee by using the
41 "Send A Comment" button on the Technical Committee's web page at [http://www.oasis-
open.org/committees/security](http://www.oasis-
42 open.org/committees/security).

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

Notices

48 Copyright © OASIS Open 2007. All Rights Reserved.

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

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

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

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

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

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

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

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

91 **Table of Contents**

92 1 Introduction.....5
93 1.1 Notation.....5
94 1.2 Normative References.....6
95 1.3 Non-Normative References.....6
96 2 SAML V1.x Metadata Profile.....7
97 2.1 Required Information.....7
98 2.2 Profile Overview.....7
99 2.3 Element <md:EntitiesDescriptor>.....7
100 2.4 Element <md:EntityDescriptor>.....7
101 2.5 Element <md:IDPSSODescriptor>.....8
102 2.6 Element <md:SPSSODescriptor>.....9
103 2.7 Element <md:AttributeAuthorityDescriptor>.....10
104 2.8 Element <md:AuthnAuthorityDescriptor>.....10
105 2.9 Element <md:PDPDescriptor>.....10
106 2.10 Element <md:KeyDescriptor>.....11
107 Appendix A. Acknowledgements.....12

1 Introduction

108

109 This specification defines a profile of the SAML V2.0 metadata specification [SAML2Meta] for use in
110 describing SAML V1.0 and V1.1 entities and profiles.

111 Unless specifically noted, nothing in this document should be taken to conflict with the SAML V2.0
112 metadata specification. Readers are advised to familiarize themselves with that specification first.

1.1 Notation

113

114 This specification uses normative text to describe the use of SAML V2.0 metadata with SAML V1.0 and
115 V1.1 profiles.

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

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

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

124 Listings of XML schemas appear like this.

125 Example code listings appear like this.

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

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:1.0:assertion	This is the SAML V1.0 and V1.1 assertion namespace [SAML1Core].
samlp:	urn:oasis:names:tc:SAML:1.0:protocol	This is the SAML V1.0 and V1.1 protocol namespace [SAML1Core].
saml2:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].
saml1md:	urn:oasis:names:tc:SAML:profiles:v1metadata	This is the namespace defined by this document and its accompanying schema [SAML1MD-xsd].
xs:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.

129 This specification uses the following typographical conventions in text: <SAMLElement>,
130 <ns:ForeignElement>, Attribute, **Datatype**, OtherKeyword.

131 1.2 Normative References

- 132 [RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
133 RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- 134 [SAML11Bind] E. Maler et al. *Bindings and Profiles for the OASIS Security Assertion Markup
135 Language (SAML) V1.1*. OASIS, September 2003. Document ID oasis-sstc-saml-
136 bindings-1.1. See [http://www.oasis-
open.org/committees/download.php/3405/oasis-sstc-saml-bindings-1.1.pdf](http://www.oasis-
137 open.org/committees/download.php/3405/oasis-sstc-saml-bindings-1.1.pdf).
- 138 [SAML11Core] E. Maler et al. *Assertions and Protocols for the OASIS Security Assertion Markup
139 Language (SAML) V1.1*. OASIS, September 2003. Document ID oasis-sstc-saml-
140 core-1.1. See [http://www.oasis-open.org/committees/download.php/3406/oasis-
sstc-saml-core-1.1.pdf](http://www.oasis-open.org/committees/download.php/3406/oasis-
141 sstc-saml-core-1.1.pdf).
- 142 [SAML1MD-xsd] S. Cantor et al. SAML V1.x metadata schema. OASIS SSTC, July 2006.
143 Document ID sstc-saml1x-metadata. See [http://www.oasis-
open.org/committees/security/](http://www.oasis-
144 open.org/committees/security/).
- 145 [SAML2Core] S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
146 Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
147 saml-core-2.0-os. See [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-
148 core-2.0-os.pdf).
- 149 [SAML2Meta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
150 (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-
151 os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 152 [Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
153 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-
154 xmlschema-1-20010502/).

155 1.3 Non-Normative References

- 156 [SAML2Gloss] J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language
157 (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-glossary-2.0-os.
158 See <http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf>.

2 SAML V1.x Metadata Profile

159

160 SAML profiles require agreements between system entities regarding identifiers, binding/profile support
161 and endpoints, certificates and keys, and so forth. A metadata specification is useful for describing this
162 information in a standardized way.

163 Although SAML V1.0 and V1.1 did not include such a specification, SAML V2.0 includes one in
164 [SAML2Meta]. This specification profiles the SAML V2.0 metadata specification for use with the
165 SAML V1.0 and V1.1-based profiles and exchanges expected between system entities.

2.1 Required Information

166

167 **Identification:** `urn:oasis:names:tc:SAML:profiles:vlmetadata`

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

169 **Description:** Given below.

170 **Updates:** None

2.2 Profile Overview

171

172 SAML V2.0 metadata describes a system entity by means of the `<md:EntityDescriptor>` element
173 and a set of "roles" supported by the entity. Role elements profiled for use with SAML V1.0 and V1.1
174 include `<md:IDPSSODescriptor>`, `<md:SPSSODescriptor>`,
175 `<md:AttributeAuthorityDescriptor>`, `<md:AuthnAuthorityDescriptor>`, and
176 `<md:PDPDescriptor>`. Specific use of these elements MUST adhere to the profile outlined in the
177 following sections.

178 The SAML V2.0 roles of identity provider (IdP) and service provider (SP) correspond to the roles
179 described in the SAML V1.0 and V1.1 specifications as "source site" and "destination site". This
180 specification adopts the SAML V2.0 terminology [SAML2Gloss].

181 SAML V2.0 metadata uses a `protocolSupportEnumeration` attribute on each role element, the value
182 of which is a list of protocol URIs, to indicate which protocols are supported by an entity in a role.

183 SAML V2.0 metadata specifies the use of the SAML V2.0 protocol namespace URI to indicate support for
184 SAML V2.0. Since SAML V1.0 and V1.1 both use the same XML protocol namespace URI,
185 `urn:oasis:names:tc:SAML:1.0:protocol`, this convention is not adequate to distinguish between
186 support for SAML V1.0 and V1.1.

187 For this reason, we define distinct values for use in identifying SAML V1.0 or V1.1 protocol support: the
188 original value of `urn:oasis:names:tc:SAML:1.0:protocol` and a new value of
189 `urn:oasis:names:tc:SAML:1.1:protocol` respectively.

2.3 Element `<md:EntitiesDescriptor>`

190

191 This element is used as described in [SAML2Meta]. Multiple entities can be collected into groups using
192 this element.

2.4 Element `<md:EntityDescriptor>`

193

194 A SAML V1.x identity or service provider SHOULD be represented by exactly one
195 `<md:EntityDescriptor>`. Its unique identifier MUST be placed in the `entityID` XML attribute. It is

196 RECOMMENDED that this identifier follow the rules for SAML V2.0 "entity" identifiers, as described in
197 section 8.3.6 of [SAML2Core].

198 In the case of an identity provider, the `entityID` MUST match the `Issuer` attribute that the identity
199 provider includes in the assertions that it generates. In the case of a service provider, the `entityID`
200 MUST be the `<saml:Audience>` value that the service provider associates with itself (such as would be
201 used in assertions that contain a `<saml:AudienceRestrictionCondition>`).

202 The schema definition for the `entityID` XML attribute requires that the value be a URI of no more than
203 1024 characters in length. Therefore, only SAML V1.x entities able to identify themselves in this fashion
204 are able to use this profile.

205 For the purposes of SAML V1.x, only use of the `<md:IDPSSODescriptor>`, `<md:SPSSODescriptor>`,
206 `<md:AttributeAuthorityDescriptor>`, `<md:AuthnAuthorityDescriptor>`, and
207 `<md:PDPDescriptor>` elements is defined by this profile.

208 Use of the `<md:RoleDescriptor>` abstract element with an `xsi:type` derived from
209 **md:RoleDescriptorType** is undefined by this profile, but MAY be defined elsewhere as appropriate;
210 usage of the `protocolSupportEnumeration` attribute SHOULD be consistent with this profile when
211 used with SAML V1.x entities.

212 The use of the `<md:AffiliationDescriptor>` element is also undefined by this profile, as the
213 affiliation concept was introduced with SAML V2.0.

214 In other respects, this element is used as described in [SAML2Meta].

215 2.5 Element `<md:IDPSSODescriptor>`

216 A SAML V1.x identity provider MUST include this element in its metadata. The
217 `protocolSupportEnumeration` XML attribute MUST include at least one of the following values:

```
218 urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:  
219 1.1:protocol
```

220 For identity providers that support the SAML V1.x Browser/Artifact profile and the mandatory type 0x0001
221 artifact format [SAML11Bind], it is RECOMMENDED that the SHA-1 hash of their `entityID` be used as
222 their `SourceID` when constructing artifacts.

223 SAML V1.x identity providers that do not use the SHA-1 hash of their `entityID` as their `SourceID`
224 MUST include a `<saml1md:SourceID>` element containing the hex-encoded value of their 20-byte
225 `SourceID` in the `<Extensions>` element of their `<md:IDPSSODescriptor>`.

226 The schema [SAML1MD-xsd] for the `<saml1md:SourceID>` element is as follows:

```
227 <schema  
228   targetNamespace="urn:oasis:names:tc:SAML:profiles:vlmetadata"  
229   xmlns:saml1md="urn:oasis:names:tc:SAML:profiles:vlmetadata"  
230   xmlns="http://www.w3.org/2001/XMLSchema"  
231   elementFormDefault="unqualified"  
232   attributeFormDefault="unqualified"  
233   blockDefault="substitution"  
234   version="1.0">  
235   <annotation>  
236     <documentation>  
237       Document identifier: sstc-saml1x-metadata  
238       Location: http://www.oasis-open.org/committees/documents.php?  
239 wg_abbrev=security  
240       Revision history:  
241       V1.0 (March 2005):  
242         Initial version.  
243     </documentation>  
244   </annotation>  
245   <element name="SourceID">
```


246
247
248
249
250
251
252

```
<simpleType>  
  <restriction base="string">  
    <pattern value="[a-f0-9]{40}"/>  
  </restriction>  
</simpleType>  
</element>  
</schema>
```

253 Neither SAML V1.0 nor SAML V1.1 defines a protocol for initiating single sign-on at a service provider.
254 Accordingly, this specification does not define any `Binding` URIs for use with the
255 `<md:SingleSignOnService>` element. SAML V1.x identity providers MAY include a
256 `<md:SingleSignOnService>` element with a `Binding` attribute that refers to a single sign-on request
257 profile defined elsewhere. The `WantAuthnRequestsSigned` XML attribute MAY be used if it is
258 applicable to the request profile in question.

259 Likewise, neither SAML V1.0 nor 1.1 defines a protocol for single logout. Accordingly, this specification
260 does not define any `Binding` URIs for use with the `<md:SingleLogoutService>` element.
261 SAML V1.x identity providers MAY include a `<md:SingleLogoutService>` element with a `Binding`
262 attribute that refers to a single logout profile defined elsewhere.

263 The `<md:ArtifactResolutionService>` endpoint element is defined for use specifically in support of
264 the SAML V1.x Browser/Artifact profile [SAML11Bind]. This is analogous but not identical to its purpose in
265 [SAML2Meta]. In particular, SAML V2.0 artifacts are NOT the same as or interchangeable with SAML V1.x
266 artifacts and CANNOT be used in the SAML V1.x Browser/Artifact profile.

267 Related to this, the `index` XML attribute on these elements, while required by the schema, cannot be
268 used within the SAML V1.x Browser/Artifact profile and its use is undefined. That is, artifacts in SAML V1.x
269 are not indexed by endpoint. All endpoints are assumed to be equivalent and MUST share state so as to
270 have the ability to resolve any artifact issued by the identity provider.

271 The SAML V2.0 `<saml2:Attribute>` element (which can appear in this element) MAY be used to
272 document support for particular SAML V1.x attributes and values. By convention, the `NameFormat` and
273 `Name` XML attributes MUST be used to represent the SAML V1.x `AttributeNameSpace` and
274 `AttributeName` XML attributes, respectively. Any other XML attributes, such as `FriendlyName`, MAY
275 be present but are ignored for the purposes of identifying the corresponding SAML V1.x attribute.

276 Use of the `<md:ManageNameIDService>` and `<md:NameIDMappingService>` endpoint elements is
277 undefined.

278 In other respects, this element is used as described in [SAML2Meta].

279 **2.6 Element `<md:SPSSODescriptor>`**

280 A SAML V1.x service provider MUST include this element in its metadata. The
281 `protocolSupportEnumeration` XML attribute MUST include at least one of the following values:

```
282 urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:  
283 1.1:protocol
```

284 The `<md:AssertionConsumerService>` element's `Binding` XML attribute MUST contain the value
285 `urn:oasis:names:tc:SAML:1.0:profiles:browser-post` to indicate support for the SAML V1.x
286 Browser/POST profile, or `urn:oasis:names:tc:SAML:1.0:profiles:artifact-01` to indicate
287 support for the SAML V1.x Browser/Artifact profile [SAML11Bind].

288 Related to this, the use of the `index` XML attribute on these elements, while required by the schema,
289 cannot be referenced within the SAML V1.x Browser/Artifact or Browser/POST profiles and its use is
290 undefined.

291 The `AuthnRequestsSigned` XML attribute MAY be used if it is applicable to a request profile outside the
292 scope of the SAML V1.x specifications but supported by the service provider.

293 The `<md:RequestedAttribute>` element (which can appear within the optional

294 <md:AttributeConsumingService> child element) MAY be used to document requirements for
295 particular SAML V1.x attributes and values. By convention, the NameFormat and Name XML attributes
296 MUST be used to represent the SAML V1.x AttributeNamespace and AttributeName XML
297 attributes, respectively. Any other XML attributes, such as FriendlyName, MAY be present but are
298 ignored for the purposes of identifying the corresponding SAML V1.x attribute.

299 As with the <md:AssertionConsumerService> element, the use of the index XML attribute on the
300 <md:AttributeConsumingService> element is required by the schema, but it cannot be referenced
301 within the SAML V1.x Browser profiles and its use is undefined. As a consequence, the use of multiple
302 <md:AttributeConsumingService> elements within a single parent element is also undefined.

303 Neither SAML V1.0 nor V1.1 defines a protocol for single logout. Accordingly, this specification does not
304 define any Binding URIs for use with the <md:SingleLogoutService> element. SAML V1.x service
305 providers MAY include a <md:SingleLogoutService> element with a Binding attribute that refers to
306 a single logout profile defined elsewhere.

307 Use of the <md:ManageNameIDService> and <md:ArtifactResolutionService> endpoint
308 elements are undefined.

309 In other respects, this element is used as described in [SAML2Meta].

310 **2.7 Element <md:AttributeAuthorityDescriptor>**

311 A SAML V1.x attribute authority MUST include this element in its metadata. The
312 protocolSupportEnumeration XML attribute MUST include at least one of the following values:

```
313 urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:  
314 1.1:protocol
```

315 The SAML V2.0 <saml2:Attribute> element (which can appear in this element) MAY be used to
316 document support for particular SAML V1.x attributes and values. By convention, the NameFormat and
317 Name XML attributes MUST be used to represent the SAML V1.x AttributeNamespace and
318 AttributeName XML attributes, respectively.

319 In other respects, this element is used as described in [SAML2Meta].

320 Note that in most cases, the Binding attribute of the endpoints published within this element will have the
321 value urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding.

322 **2.8 Element <md:AuthnAuthorityDescriptor>**

323 A SAML V1.x authentication authority MUST include this element in its metadata. The
324 protocolSupportEnumeration XML attribute MUST include at least one of the following values:

```
325 urn:oasis:names:tc:SAML:1.0:protocol  
326 urn:oasis:names:tc:SAML:1.1:protocol
```

327 In other respects, this element is used as described in [SAML2Meta].

328 Note that in most cases, the Binding attribute of the endpoints published within this element will have the
329 value urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding.

330 **2.9 Element <md:PDPDescriptor>**

331 A SAML V1.x policy decision point MUST include this element in its metadata. The
332 protocolSupportEnumeration XML attribute MUST include at least one of the following values:

```
333 urn:oasis:names:tc:SAML:1.0:protocol urn:oasis:names:tc:SAML:
```

334 1.1:protocol

335 In other respects, this element is used as described in [SAML2Meta].

336 Note that in most cases, the `Binding` attribute of the endpoints published within this element will have the
337 value `urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding`.

338 **2.10 Element <md:KeyDescriptor>**

339 The `<md:KeyDescriptor>` element is supported by this profile for the purpose of documenting the
340 public key(s) used by an entity to secure SAML V1.x profiles and bindings. Because the use of encryption
341 is not defined by SAML V1.x, use of the `<md:EncryptionMethod>` element and the `use XML` attribute
342 value of `encryption` are also undefined.

343 In other respects, this element is used as described in [SAML2Meta].

344 Appendix A. Acknowledgements

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

- 347 ● Hal Lockhart, BEA Systems, Inc.
- 348 ● Steve Anderson, BMC Software
- 349 ● Rob Philpott, EMC Corporation
- 350 ● Carolina Canales-Valenzuela, Ericsson
- 351 ● Dana Kaufman, Forum Systems
- 352 ● Ashish Patel, France Telecom
- 353 ● Greg Whitehead, Hewlett-Packard Company
- 354 ● Heather Hinton, IBM
- 355 ● Anthony Nadalin, IBM
- 356 ● Conor P. Cahill, Intel
- 357 ● Scott Cantor, Internet2
- 358 ● Bob Morgan, Internet2
- 359 ● Tom Scavo, National Center for Supercomputing Applications
- 360 ● Peter Davis, NeuStar
- 361 ● Jeff Hodges, NeuStar
- 362 ● Frederick Hirsch, Nokia
- 363 ● Abbie Barbir, Nortel
- 364 ● Paul Madsen, NTT Corporation
- 365 ● Ari Kermaier, Oracle
- 366 ● Prateek Mishra, Oracle
- 367 ● Brian Campbell, Ping Identity
- 368 ● Bhavna Bhatnagar, Sun Microsystems
- 369 ● Eve Maler, Sun Microsystems
- 370 ● Emily Xu, Sun Microsystems
- 371 ● David Staggs, Veteran's Health Administration