



SAML V2.0 Metadata Profile for Algorithm Support Version 1.0

Committee Draft 01 29 June 2010

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-cd-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-cd-01.odt>
(Authoritative)

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-cd-01.pdf>

Previous Version:

None

Latest Version:

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

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport.odt>
(Authoritative)

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

Latest Approved Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-cd-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-cd-01.odt>
(Authoritative)

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-cd-01.pdf>

Technical Committee:

OASIS Security Services TC

Chair:

Thomas Hardjono, M.I.T.
Nate Kingenstein, Internet2

Editor:

Scott Cantor, Internet2

Related Work:

This specification defines an extension for use with SAML V2.0 Metadata [SAML2Meta].

Declared XML Namespace(s):

urn:oasis:names:tc:SAML:metadata:algsupport

35 **Abstract:**

36 The SAML V2.0 Metadata specification [SAML2Meta] includes an element allowing entities to
37 describe the XML Encryption [XMLEnc] algorithms they support. This specification defines
38 metadata extension elements to enable entities to describe the XML Signature [XMLSig]
39 algorithms they support, and a profile for using both elements to enable better algorithm agility for
40 profiles that rely on metadata.

41 **Status**

42 This document was last revised or approved by the SSTC on the above date. The level of
43 approval is also listed above. Check the current location noted above for possible later revisions
44 of this document. This document is updated periodically on no particular schedule.

45 TC members should send comments on this specification to the TC's email list. Others
46 should send comments to the TC by using the "Send A Comment" button on the TC's
47 web page at <http://www.oasis-open.org/committees/security>.

48 For information on whether any patents have been disclosed that may be essential to
49 implementing this specification, and any offers of patent licensing terms, please refer to the IPR
50 section of the TC web page (<http://www.oasis-open.org/committees/security/ipr.php>).

51 The non-normative errata page for this specification is located at [http://www.oasis-](http://www.oasis-open.org/committees/security)
52 [open.org/committees/security](http://www.oasis-open.org/committees/security).

53 Notices

54 Copyright © OASIS Open 2010. All Rights Reserved.

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

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

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

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

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

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

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

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

97 **Table of Contents**

98 1 Introduction..... 5
99 1.1 Notation..... 5
100 1.2 Normative References..... 6
101 1.3 Non-Normative References..... 6
102 2 SAML V2.0 Metadata Profile for Algorithm Support..... 7
103 2.1 Required Information..... 7
104 2.2 Profile Description..... 7
105 2.3 Expression of Encryption Capabilities..... 7
106 2.4 Expression of Signature Capabilities..... 8
107 2.4.1 Element <alg:DigestMethod>..... 8
108 2.4.2 Element <alg:SigningMethod>..... 8
109 2.5 Metadata Consumers..... 9
110 2.6 Security Considerations..... 9
111 2.7 Example..... 10
112 3 Conformance..... 11
113 3.1 SAML V2.0 Metadata Profile for Algorithm Support Version 1.0..... 11
114 Appendix A. Acknowledgements..... 12
115 Appendix B. Revision History..... 13
116

1 Introduction

The SAML V2.0 Metadata specification [SAML2Meta] includes an `<md:EncryptionMethod>` element intended to communicate the XML Encryption [XMLEnc] algorithms supported for use with the key described by a containing `<md:KeyDescriptor>` element. The use of this element is not completely defined by the original specification, and there is no comparable support for communicating the XML Signature [XMLSig] algorithms supported by an entity. This profile addresses both considerations to improve algorithm agility and interoperability for deployments that make use of metadata.

There are more general standards for the description of security requirements of communicating endpoints, such as [WS-SecPol]. This specification is not intended as a replacement for such mechanisms, but is directed at systems with fewer requirements that are already designed around SAML V2.0 Metadata.

1.1 Notation

This specification uses normative text.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC2119]:

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

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

Listings of XML schemas appear like this.

Example code listings appear like this.

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

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAML2Core].
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace [SAML2Core].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace [SAML2Meta].
alg:	urn:oasis:names:tc:SAML:metadata:algsupport	This is the SAML V2.0 metadata extension namespace defined by this document and its accompanying schema [AlgSup-XSD].
xenc:	http://www.w3.org/2001/04/xmlenc#	This is the XML Encryption namespace [XMLEnc].
xsd:	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.

144 This specification uses the following typographical conventions in text: <SAML*E*lement>,
145 <ns:ForeignElement>, Attribute, **Datatype**, OtherCode.

146 1.2 Normative References

- 147 **[AlgSup-XSD]** OASIS Working Draft, *Metadata Extension Schema for SAML V2.0 Metadata*
148 *Profile for Algorithm Support Version 1.0*, June 2010. <http://docs.oasis->
149 [open.org/security/saml/Post2.0/sstc-saml-metadata-alsupport.xsd](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-alsupport.xsd)
- 150 **[RFC2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
151 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>
- 152 **[SAML2Core]** OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion*
153 *Markup Language (SAML) V2.0*, March 2005. <http://docs.oasis->
154 [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)
- 155 **[SAML2Errata]** OASIS Approved Errata, *SAML V2.0 Errata*, October 2009. <http://docs.oasis->
156 [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)
- 157 **[SAML2Meta]** OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language*
158 *(SAML) V2.0*, March 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml->
159 [metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
- 160 **[XMLEnc]** D. Eastlake et al. *XML Encryption Syntax and Processing*. World Wide Web
161 Consortium Recommendation. <http://www.w3.org/TR/2002/REC-xmlenc-core->
162 [20021210/](http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/)
- 163 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
164 Consortium Recommendation, May 2001. <http://www.w3.org/TR/2001/REC->
165 [xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/)
- 166 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide Web
167 Consortium Recommendation, May 2001. <http://www.w3.org/TR/2001/REC->
168 [xmlschema-2-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/)
- 169 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing, Second Edition*. World
170 Wide Web Consortium Recommendation, June 2008.
171 <http://www.w3.org/TR/xmlsig-core/>

172 1.3 Non-Normative References

- 173 **[RFC4051]** IETF RFC 4051, *Additional XML Security Uniform Resource Identifiers*, April
174 2005. <http://www.ietf.org/rfc/rfc4051.txt>
- 175 **[WS-SecPol]** OASIS Standard, *WS-SecurityPolicy 1.3*, February 2009. <http://docs.oasis->
176 [open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.pdf](http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.pdf)
- 177

2 SAML V2.0 Metadata Profile for Algorithm Support

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:metadata:algsupport

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

Description: Given below.

Updates: None.

2.2 Profile Description

One of the interoperability challenges in large-scale, and long-term, SAML deployments is the selection of XML Signature [XMLSig] and XML Encryption [XMLEnc] algorithms at runtime when communicating with peer entities. In particular, accounting for software limitations that prevent support of newer algorithms, while supporting those algorithms where possible to gradually strengthen systems, is difficult to manage without knowledge of a peer's capabilities. This profile makes use of SAML metadata to enable deployments to document their algorithm capabilities and preferences. It also allows for future expansion to address the interoperability requirements of more complex algorithms.

This profile provides guidance on the use of the `<md:EncryptionMethod>` element defined in the SAML V2.0 Metadata specification [SAML2Meta], and defines extension elements, `<alg:SigningMethod>` and `<alg:DigestMethod>`, to address comparable requirements related to XML Signature usage.

2.3 Expression of Encryption Capabilities

The SAML V2.0 Metadata specification [SAML2Meta] permits zero or more `<md:EncryptionMethod>` elements to appear inside a `<md:KeyDescriptor>` element. This profile provides guidance for the use of this element only in enclosing elements whose `use` attribute is omitted or set to "encryption".

In the common case that a `<md:KeyDescriptor>` element contains an asymmetric encryption key, an `<md:EncryptionMethod>` element SHOULD be present for each of a Block or Stream Encryption, and a Key Transport or Key Agreement algorithm. The Key Transport or Key Agreement algorithm(s) listed MUST be compatible with the associated encryption key.

If the `<md:KeyDescriptor>` element contains or identifies by reference a symmetric key (e.g., a name referring to a shared master secret or password), then an `<md:EncryptionMethod>` element SHOULD be present for a Block or Stream Encryption algorithm, and MAY be present for other algorithm types such as Symmetric Key Wrap or Key Derivation.

Per [XMLEnc], the `<md:EncryptionMethod>` element MUST contain an `Algorithm` attribute containing the identifier for the algorithm defined for use with the specification. If the algorithm permits varying key sizes, the element MAY contain an `<xenc:KeySize>` element defining a key size for the algorithm that the entity will accept. If the algorithm definition includes the specification of additional public content that the party performing encryption needs, that content MAY also be present.

If multiple `<md:EncryptionMethod>` elements identifying algorithms of the same general type are present, they MUST be listed in order of preference by the entity.

215 2.4 Expression of Signature Capabilities

216 This profile defines a pair of extension elements for the expression of an entity's capability to verify digests
217 and signatures with particular algorithms. While not strictly meant as an expression of policy, it is a natural
218 assumption that a peer stating support for particular algorithms requires their use.

219 An entity SHOULD include one or more `<alg:DigestMethod>` and `<alg:SigningMethod>` elements
220 in its metadata by means of the `<md:Extensions>` element in its `<md:EntityDescriptor>` element,
221 and/or in its roles (elements whose type is based on `md:RoleDescriptorType`).

222 If a signature algorithm permits varying key sizes, the `<alg:SigningMethod>` element MAY contain
223 `MinKeySize` and/or `MaxKeySize` attributes bounding the key size for the algorithm that the entity
224 supports. If the algorithm definition includes the specification of additional public content that the party
225 creating a signature or digest needs, that content MAY also be present.

226 If multiple elements of the same type are present, they MUST be listed in order of preference by the entity.

227 2.4.1 Element `<alg:DigestMethod>`

228 The `<alg:DigestMethod>` element describes a Message Digest algorithm. It contains the following
229 attribute:

230 `Algorithm` [Required]

231 Identifies the algorithm by means of the URL defined for its use with the XML Signature specification
232 [XMLSig].

233 This element also permits the use of arbitrary elements defined in any namespace.

234 The schema for the `<alg:DigestMethod>` element, and its corresponding `alg:DigestMethodType`
235 complex type, is as follows:

```
236 <element name="DigestMethod" type="alg:DigestMethodType"/>  
237 <complexType name="DigestMethodType">  
238   <sequence>  
239     <any namespace="##any" minOccurs="0" maxOccurs="unbounded"/>  
240   </sequence>  
241   <attribute name="Algorithm" type="anyURI" use="required"/>  
242 </complexType>
```

243 2.4.2 Element `<alg:SigningMethod>`

244 The `<alg:SigningMethod>` element describes a Signature or Message Authentication Code algorithm.
245 It contains the following attributes:

246 `Algorithm` [Required]

247 Identifies the algorithm by means of the URL defined for its use with the XML Signature specification
248 [XMLSig].

249 `MinKeySize` [Optional]

250 The smallest key size, in bits, that the entity supports in conjunction with the algorithm. If omitted, no
251 minimum is implied.

252 `MaxKeySize` [Optional]

253 The largest key size, in bits, that the entity supports in conjunction with the algorithm. If omitted, no
254 maximum is implied.

255 This element also permits the use of arbitrary elements defined in any namespace.

256 The schema for the `<alg:SigningMethod>` element, and its corresponding `alg:SigningMethodType`
257 complex type, is as follows:

```
258 <element name="SigningMethod" type="alg:SigningMethodType"/>
259 <complexType name="SigningMethodType">
260   <sequence>
261     <any namespace="##any" minOccurs="0" maxOccurs="unbounded"/>
262   </sequence>
263   <attribute name="Algorithm" type="anyURI" use="required"/>
264   <attribute name="MinKeySize" type="positiveInteger"/>
265   <attribute name="MaxKeySize" type="positiveInteger"/>
266 </complexType>
```

267 2.5 Metadata Consumers

268 A consumer of metadata that wishes to perform XML Signature or XML Encryption operations with
269 knowledge of the peer entity (this is not always true of signatures) **MUST** consult the peer's metadata to
270 determine the intersection of the algorithms, key sizes, and other parameters as defined by particular
271 algorithms that it supports and that the peer entity supports.

272 The elements describing this support in metadata **SHOULD** be consulted in order, and the metadata
273 consumer **SHOULD** select the first algorithm encountered that it supports for use with a particular entity
274 (subject to local policy).

275 With respect to use of XML Signature, the presence of any `<alg:DigestMethod>` and
276 `<alg:SigningMethod>` elements at the level of a role element **MUST** take precedence over any such
277 elements at the level of an `<md:EntityDescriptor>` element, and the two sets are not combined if
278 both are present.

279 In the absence of an element describing support for a particular algorithm type (e.g., no
280 `<alg:DigestMethod>` elements), the metadata consumer is free to select any algorithm that it
281 supports. The absence of metadata therefore implies no information, rather than lack of support.

282 2.6 Security Considerations

283 The use of metadata as a means of "negotiating" the algorithms to use exposes both parties to attacks
284 traditionally associated with such mechanisms, such as step-down attacks in which the metadata is
285 compromised to influence the selection of a weaker algorithm than the parties might otherwise support.

286 The exchange and verification of metadata should always be subject to appropriate security controls to
287 mitigate this threat, and entities should always be prepared to reject the use of algorithms that they deem
288 insufficiently secure.

289 **2.7 Example**

290 The example presented shows a partial metadata instance for a service provider that supports (as a
291 relying party) a number of newer/stronger signature and digest algorithms defined in [RFC4051]. It also
292 specifies support for encryption via two AES variants using an RSA key as a transport.

```
293 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"  
294   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"  
295   xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"  
296   entityID="https://serviceprovider.example.com/SAML">  
297   <Extensions>  
298     <alg:DigestMethod  
299       Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>  
300     <alg:DigestMethod  
301       Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>  
302     <alg:SignatureMethod MinKeySize="256" MaxKeySize="511"  
303       Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>  
304     <alg:SignatureMethod MinKeySize="2048" MaxKeySize="4096"  
305       Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>  
306   </Extensions>  
307   <SPSSODescriptor  
308     protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">  
309     <KeyDescriptor>  
310       <ds:KeyInfo>...RSA key elided...</ds:KeyInfo>  
311       <EncryptionMethod  
312         Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>  
313       <EncryptionMethod  
314         Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>  
315       <EncryptionMethod  
316         Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>  
317     </KeyDescriptor>  
318     ...  
319   </SPSSODescriptor>  
320   ...  
321 </EntityDescriptor>
```

322 **3 Conformance**

323 **3.1 SAML V2.0 Metadata Profile for Algorithm Support Version 1.0**

324 A metadata producer conforms to this profile if it has the ability to produce metadata in accordance with
325 sections 2.3 and 2.4.

326 A metadata consumer conforms to this profile if it can consume extended metadata produced in
327 accordance with sections 2.3 and 2.4 and conforms to the normative statements in section 2.5.

328 **Appendix A. Acknowledgements**

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

- 331 • Rob Philpott, EMC Corporation
- 332 • John Bradley, Individual
- 333 • Scott Cantor, Internet2
- 334 • Nate Klingenstein, Internet2
- 335 • Thomas Hardjono, M.I.T.
- 336 • Anthony Nadalin, Microsoft Corporation
- 337 • Thinh Nguyenphu, Nokia Siemens Networks Gmb
- 338 • Phil Hunt, Oracle Corporation
- 339 • Ari Kermaier, Oracle Corporation
- 340 • Hal Lockhart, Oracle Corporation
- 341 • Emily Xu, Oracle Corporation
- 342 • Anil Saldhana, Red Hat
- 343 • David Staggs, Veterans Health Administration

344 **Appendix B. Revision History**

- 345 ● Draft 01, first working draft.
- 346 ● Committee Draft 01, CD edits.