



# SAML V2.0 Metadata Extension for Entity Attributes Version 1.0

## Committee Specification 01

4 August 2009

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-metadata-attr-cs-01.html>  
<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-metadata-attr-cs-01.odt> (Authoritative)  
<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-metadata-attr-cs-01.pdf>

#### Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-metadata-attr-cd-01.html>  
<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-metadata-attr-cd-01.odt> (Authoritative)  
<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-metadata-attr-cd-01.pdf>

#### Latest Version:

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

### Technical Committee:

OASIS Security Services TC

### Chair(s):

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

### Editors:

Scott Cantor, Internet2

### Declared XML Namespaces(s):

urn:oasis:names:tc:SAML:metadata:attribute

### Abstract:

This profile defines an extension element for use in attaching SAML attributes to an `<md:EntityDescriptor>` or `<md:EntitiesDescriptor>` element, to communicate an arbitrary set of additional information about an entity in its metadata.

32 **Status**

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

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

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

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

## 44 Notices

45 Copyright © OASIS Open 2009. All Rights Reserved.

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

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

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

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

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

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

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

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

88 **Table of Contents**

89 1 Introduction..... 5  
90 1.1 Notation..... 5  
91 1.2 Normative References..... 6  
92 2 SAML V2.0 Metadata Extension for Entity Attributes..... 7  
93 2.1 Required Information..... 7  
94 2.2 Profile Overview..... 7  
95 2.3 Element <mdattr:EntityAttributes>..... 7  
96 2.4 Assertion Profile..... 8  
97 3 Conformance..... 9  
98 3.0.1 SAML V2.0 Metadata Extension for Entity Attributes..... 9  
99 Appendix A. Acknowledgements..... 10  
100 Appendix B. Revision History..... 11  
101

# 1 Introduction

The SAML V2.0 metadata specification [SAML2Meta] includes the `<md:Extensions>` element in various places, including the `<md:EntityDescriptor>` and `<md:EntitiesDescriptor>` elements, for use in extending the specification by carrying externally defined content. This profile defines such an extension element, `<mdattr:EntityAttributes>`, as a container for one or more `<saml:Attribute>` or `<saml:Assertion>` elements. It allows an arbitrary set of attribute information to be carried within an entity's (or a group of entities') metadata to communicate additional information about that entity (or group) to a metadata consumer.

## 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 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].
mdattr:	urn:oasis:names:tc:SAML:metadata:attribute	This is the namespace defined by this document and its accompanying schema [MetaAttr-xsd].
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.
xsi:	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

This specification uses the following typographical conventions in text: `<SAMLelement>`, `<ns:ForeignElement>`, Attribute, **Datatype**, OtherCode.

## 128 1.2 Normative References

- 129 **[MetaAttr-xsd]** S. Cantor. SAML V2.0 Metadata Extension for Entity Attributes Schema. OASIS  
130 SSTC, November 2008. Document ID sstc-metadata-attr.xsd. See  
131 <http://www.oasis-open.org/committees/security/>.
- 132 **[RFC2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
133 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 134 **[SAML2Core]** OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion  
135 Markup Language (SAML) V2.0*. March 2005. [http://docs.oasis-open.org/security/  
136 saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).
- 137 **[SAML2Meta]** OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language  
138 (SAML) V2.0*. March 2005. [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-<br/>139 metadata-2.0-os.pdf).
- 140 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web  
141 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-  
143 xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-<br/>142 xmlschema-1-20010502/). Note that this specification normatively references  
[Schema2], listed below.
- 144 **[Schema2]** Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide Web  
145 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-  
xmlschema-2-20010502/](http://www.w3.org/TR/2001/REC-<br/>146 xmlschema-2-20010502/).

## 147 2 SAML V2.0 Metadata Extension for Entity Attributes

### 148 2.1 Required Information

149 **Identification:** urn:oasis:names:tc:SAML:metadata:attribute

150 **Contact information:** [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org)

151 **Description:** Given below.

152 **Updates:** None.

### 153 2.2 Profile Overview

154 SAML deployments and SAML-enabled applications often make extensive use of the  
155 `<saml:Attribute>` element as a vehicle for carrying and consuming arbitrary structured information  
156 about assertion subjects. This profile defines a metadata extension element as a container for one or  
157 more such elements, or more generically for communicating a SAML attribute assertion. It allows attribute  
158 information to be carried within an entity's (or a group of entities') metadata to communicate additional  
159 information about that entity (or group) to a metadata consumer, much as an assertion can carry  
160 attributes about a subject.

161 In some SAML deployments, metadata is often maintained and signed by a third party federation  
162 operator, and this mechanism allows that operator to include extensible information (possibly signed by  
163 still another party) about the federation's member sites, such as their adherence to optional federation  
164 policies. Metadata consumers can then choose to process or ignore such information as they deem  
165 necessary.

166 This profiles defines no specific attributes to be communicated, but additional profiles might leverage it to  
167 do so.

### 168 2.3 Element `<mdattr:EntityAttributes>`

169 The `<mdattr:EntityAttributes>` element is a wrapper for one or more `<saml:Attribute>` or  
170 `<saml:Assertion>` elements. Assertions that appear MUST conform to the profile in section 2.4, and  
171 will contain only attribute statements. Relying parties MUST process assertions in accordance with the  
172 standard processing rules in [SAML2Core].

173 If this element is used within the `<md:Extensions>` element of an `<md:EntityDescriptor>` element,  
174 then it binds the enclosed SAML attributes (or the attributes within the enclosed assertions) to the  
175 enclosing entity.

176 If this element is used within the `<md:Extensions>` element of an `<md:EntitiesDescriptor>`  
177 element, then only `<saml:Attribute>` elements are to be used; `<saml:Assertion>` elements MUST  
178 NOT be included. The enclosed attributes are bound to each `<md:EntityDescriptor>` within the  
179 enclosing `<md:EntitiesDescriptor>` element.

180 The meaning of this element is undefined by this profile if it appears anywhere else within a metadata  
181 instance, or within any other XML document.

182 Finally, this element MUST NOT appear more than once within a given `<md:Extensions>` element.

183 The following schema fragment defines the `<mdattr:EntityAttributes>` element:

```
184 <element name="EntityAttributes" type="mdattr:EntityAttributesType"/>  
185 <complexType name="EntityAttributesType">  
186 <choice maxOccurs="unbounded">
```

```
187     <element ref="saml:Attribute"/>
188     <element ref="saml:Assertion"/>
189   </sequence>
190 </complexType>
```

## 191 2.4 Assertion Profile

192 All SAML assertions that appear in an `<mdattr:EntityAttributes>` element MUST conform to the  
193 following restrictions:

- 194 ● The assertion's `<saml:Subject>` element MUST contain a `<saml:NameID>` element with a  
195 Format of `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`. The value of the  
196 `<saml:NameID>` MUST correspond to the `entityID` of the enclosing  
197 `<md:EntityDescriptor>` element.
- 198 ● The assertion's subject element MUST NOT include any `<saml:SubjectConfirmation>`  
199 elements.
- 200 ● One (and only one) `<saml:AttributeStatement>` element MUST be included. Other  
201 statement types MUST NOT be included.
- 202 ● The assertion MUST be independently signed (rather than inheriting a signature from the  
203 metadata itself).

204 Apart from the above constraints, any other legal assertion content MAY be included, including the  
205 `<saml:Conditions>` element and any conditions within it.



206 **3 Conformance**

207 **3.0.1 SAML V2.0 Metadata Extension for Entity Attributes**

208 A metadata producer conforms to this profile if it has the ability to produce extended metadata in  
209 accordance with section 2.

210 A metadata consumer conforms to this profile if it can consume extended metadata in accordance with  
211 section 2.

## 212 **Appendix A. Acknowledgements**

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

- 215 • Rob Philpott, EMC Corporation
- 216 • John Bradley, Individual
- 217 • Jeff Hodges, Individual
- 218 • Scott Cantor, Internet2
- 219 • Nate Klingenstein, Internet2
- 220 • Bob Morgan, Internet2
- 221 • Eric Tiffany, Liberty Alliance Project
- 222 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 223 • Peter Davis, NeuStar, Inc.
- 224 • Frederick Hirsch, Nokia Corporation
- 225 • Srinath Godavarthi, Nortel Networks Limited
- 226 • Paul Madsen, NTT Corporation
- 227 • Ari Kermaier, Oracle Corporation
- 228 • Hal Lockhart, Oracle Corporation
- 229 • Brian Campbell, Ping Identity Corporation
- 230 • Anil Saldhana, Red Hat
- 231 • Kent Spaulding, Skyworth TTG Holdings Limited
- 232 • Eve Maler, Sun Microsystems
- 233 • Emily Xu, Sun Microsystems
- 234 • Duane DeCouteau, Veterans Health Administration
- 235 • David Staggs, Veterans Health Administration

## 236 **Appendix B. Revision History**

- 237 ● Draft 01.
- 238 ● Draft 02, add option for assertions, fix the schema and conformance sections.
- 239 ● Committee Draft 01, CD edits.