



---

## 2      **SAML Metadata Extension for a 3      Standalone Attribute Requester**

4      **Committee Draft 01, 11 April 2005**

5      **Document identifier:**

6                sstc-saml-metadata-ext-cd-01

7      **Location:**

8                [http://www.oasis-open.org/committees/documents.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)

9      **Editors:**

10               Tom Scavo ([trscavo@gmail.com](mailto:trscavo@gmail.com)), individual  
11               Scott Cantor ([cantor.2@osu.edu](mailto:cantor.2@osu.edu)), Internet2

12     **Contributors:**

13               Tom Wisniewski, Entrust

14     **Abstract:**

15               This specification defines an extension to the SAML V2.0 metadata specification [SAML2Meta].  
16               The extension defines a role descriptor that describes a standalone SAML V1.x or V2.0 attribute  
17               requester, that is, an attribute requester not bound to a SAML single sign-on profile. Readers are  
18               advised to familiarize themselves with that specification before reading this one.

19     **Status:**

20               This is a **Committee Draft** approved by the Security Services Technical Committee on 15 April  
21               2005.

22               Committee members should submit comments and potential errata to the [security-](mailto:security-services@lists.oasis-open.org)  
23               [services@lists.oasis-open.org](mailto:services@lists.oasis-open.org) list. Others should submit them by filling out the web form located  
24               at [http://www.oasis-open.org/committees/comments/form.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security). The  
25               committee will publish on its web page (<http://www.oasis-open.org/committees/security>) a catalog  
26               of any changes made to this document as a result of comments.

27               For information on whether any patents have been disclosed that may be essential to  
28               implementing this specification, and any offers of patent licensing terms, please refer to the  
29               Intellectual Property Rights web page for the Security Services TC (<http://www.oasis->  
30               [open.org/committees/security/ipr.php](http://www.oasis-open.org/committees/security/ipr.php)).

# 31 Table of Contents

32	1 Introduction.....	3
33	1.1 Notation.....	3
34	1.2 Motivating Use Cases.....	4
35	2 Metadata Extension for SAML V2.0.....	5
36	2.1 Namespaces.....	5
37	2.2 Element <md:RoleDescriptor>.....	5
38	2.3 Complex Type AttributeRequesterDescriptorType.....	5
39	2.4 Example.....	6
40	3 References.....	8
41	3.1 Normative References.....	8
42	3.2 Non-Normative References.....	8
43		

# 44 1 Introduction

45 This specification defines an extension to the SAML V2.0 metadata specification. The extension defines  
46 a role descriptor that describes a standalone SAML attribute requester, that is, an attribute requester not  
47 bound to a SAML single sign-on profile. The profile addresses both SAML V1.x and SAML V2.0.

48 Unless specifically noted, nothing in this document should be taken to conflict with the SAML V2.0  
49 metadata specification [SAML2Meta]. Readers are advised to familiarize themselves with that  
50 specification before reading this one.

## 51 1.1 Notation

52 This specification uses normative text to define an extension to the SAML V2.0 metadata specification.

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

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

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

61 Listings of XML schemas appear like this.

62 Example code listings appear like this.

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

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAML2Core].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace [SAML2Meta].
mdext:	urn:oasis:names:tc:SAML:metadata:extension	This is the SAML V2.0 metadata extension namespace, defined by this document and its accompanying schema [MDext-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].
ds:	http://www.w3.org/2000/09/xmldsig#	This is the W3C XML Signature specification [XMLSig].

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

69    **1.2 Motivating Use Cases**

70    A primary SAML use case is browser single sign-on, but several non-browser use cases are emerging  
71    that incorporate a standalone attribute requester ([SAMLX509], [GridShib], [LionShare]). Such a role is  
72    not supported by [SAML2Meta]. This specification defines a new role descriptor type designed to support  
73    a typical non-browser scenario.

74    A SAML metadata extension that supports this use case is described in Section 2. Relevant references  
75    are listed in Section 3.

## 76 2 Metadata Extension for SAML V2.0

77 This section defines a new role descriptor type that supports the non-browser use case described in  
78 Section 1.

### 79 2.1 Namespaces

80 The SAML V2.0 metadata specification [SAML2Meta] and its accompanying schema [SAML2Meta-xsd]  
81 define the following namespace:

82 `urn:oasis:names:tc:SAML:2.0:metadata`

83 By convention, the namespace prefix `md:` is used to refer to the above namespace.

84 This specification defines a new namespace:

85 `urn:oasis:names:tc:SAML:metadata:extension`

86 The prefix `mdext:` is used here and in the accompanying schema [MDext-XSD] to refer to this new  
87 namespace. In what follows, any unqualified type is assumed to belong to this new namespace.

### 88 2.2 Element <md:RoleDescriptor>

89 The `<md:RoleDescriptor>` element defined in [SAML2Meta] is an abstract extension point that  
90 contains descriptive information common across various entity roles. New roles can be defined by  
91 extending its abstract `md:RoleDescriptorType` complex type, which is the approach taken here.

### 92 2.3 Complex Type AttributeRequesterDescriptorType

93 Complex type `AttributeRequesterDescriptorType` extends complex type `md:RoleDescriptorType` with  
94 content specific to attribute requesters, that is, consumers of SAML attributes. The type  
95 `AttributeRequesterDescriptorType` contains the following additional attributes and elements:

96 `WantAssertionsSigned` [Optional]

97       Optional attribute that indicates a requirement for assertions received by this service provider to  
98       be signed. If omitted, the value is assumed to be `false`. This requirement is in addition to any  
99       requirement for signing derived from the use of a particular profile/binding combination.

100 `<md:NameIDFormat>` [Zero or More]

101       Zero or more elements of type `xsd:anyURI` that enumerate the name identifier formats  
102       supported by this service provider. See Section 8.3 of [SAML2Core] for some possible values of  
103       this element.

104 `<md:AttributeConsumingService>` [Zero or More]

105       Zero or more elements that describe an application or service provided by this service provider  
106       that requires or desires the use of SAML attributes. It is RECOMMENDED that deployers provide  
107       at least one such element to facilitate configuration of policy by attribute providers.

108 At most one `<md:AttributeConsumingService>` element can have the attribute `isDefault` set to  
109 `true`. When multiple elements are specified and none has the attribute `isDefault` set to `true`, then  
110 the first element whose `isDefault` attribute is not set to `false` is to be used as the default. If all  
111 elements have their `isDefault` attribute set to `false`, then the first element is considered the default.

112 Instances of **AttributeRequesterDescriptorType** are declared using the `<md:RoleDescriptor>`  
113 element with an `xsi:type` of **AttributeRequesterDescriptorType**. See the example in Section 2.4.  
114 See [SAML1xMeta] for specifics on the transformation and use of particular elements and attributes for  
115 use with SAML V1.x.

116 The following schema fragment defines the **AttributeRequesterDescriptorType** complex type:

```
117 <complexType name="AttributeRequesterDescriptorType">
118     <complexContent>
119         <extension base="md:RoleDescriptorType">
120             <sequence>
121                 <element ref="md:NameIDFormat" minOccurs="0" maxOccurs="unbounded"/>
122                 <element ref="md:AttributeConsumingService" minOccurs="0"
123 maxOccurs="unbounded"/>
124             </sequence>
125             <attribute name="WantAssertionsSigned" type="boolean" use="optional"/>
126         </extension>
127     </complexContent>
128 </complexType>
```

## 129 2.4 Example

130 Following is a metadata example for a SAML attribute requester that supports both SAML V1.1 and  
131 SAML V2.0.

```
132 <md:EntityDescriptor
133     xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
134     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
135     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
136     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
137     entityID="https://gs.org/gridshib">
138     <!-- insert ds:Signature element here -->
139     <md:RoleDescriptor
140         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
141         xmlns:mdext="urn:oasis:names:tc:SAML:metadata:extension"
142         xsi:type="mdext:AttributeRequesterDescriptorType"
143         protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:oasis:names:tc:SAML:2.0:protocol">
144         <md:KeyDescriptor use="signing">
145             <ds:KeyInfo>
146                 <ds:KeyName>Requester Key</ds:KeyName>
147             </ds:KeyInfo>
148         </md:KeyDescriptor>
149         <md:NameIDFormat>
150             urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
151         </md:NameIDFormat>
152         <md:AttributeConsumingService isDefault="true" index="0">
153             <md:ServiceName xml:lang="en">
154                 Shibalized Grid Service
155             </md:ServiceName>
156             <md:RequestedAttribute
157                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
158                 Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
159                 FriendlyName="eduPersonEntitlement">
160                 <saml:AttributeValue xsi:type="xsd:anyURI">
161                     https://gs.org/gridshib/entitlements/123456789
162                 </saml:AttributeValue>
163             </md:RequestedAttribute>
164             <md:RequestedAttribute
165                 NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"
166                 Name="urn:mace:dir:attribute-def:eduPersonEntitlement">
167                 <saml:AttributeValue xsi:type="xsd:anyURI">
168                     https://gs.org/gridshib/entitlements/123456789
169             </md:RequestedAttribute>

```

```
170      </saml:AttributeValue>
171      </md:RequestedAttribute>
172      </md:AttributeConsumingService>
173  </md:RoleDescriptor>
174  <md:Organization>
175      <md:OrganizationName xml:lang="en">
176          GridShib Service Provider
177      </md:OrganizationName>
178      <md:OrganizationDisplayName xml:lang="en">
179          GridShib Service Provider @ Some Location
180      </md:OrganizationDisplayName>
181      <md:OrganizationURL xml:lang="en">
182          http://www.gs.org/
183      </md:OrganizationURL>
184  </md:Organization>
185  <md>ContactPerson contactType="technical">
186      <md:SurName>GridShib Support</md:SurName>
187      <md:EmailAddress>gridshib-support@gs.org</md:EmailAddress>
188  </md>ContactPerson>
189 </md:EntityDescriptor>
```

## 190 3 References

191 The following works are cited in the body of this specification.

### 192 3.1 Normative References

- 193 [RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF  
194 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 195 [MDext-XSD] S. Cantor et al., SAML metadata extension schema. OASIS SSTC, April 2005.  
196 Document ID sstc-saml-metadata-ext-schema. See <http://www.oasis-open.org/committees/security/>.
- 197 [SAML2Core] S. Cantor et al., *Assertions and Protocols for the OASIS Security Assertion  
Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID  
200 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-core-<br/>2.0-os.pdf).
- 202 [SAML2Meta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language  
(SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-  
204 os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 205 [SAML2Meta-xsd] S. Cantor et al., SAML V2.0 metadata schema. OASIS Standard, March 2005.  
206 Document ID saml-schema-metadata-2.0. See [http://www.oasis-open.org/committees/  
download.php/11903/saml-2.0-os-xsd.zip](http://www.oasis-open.org/committees/<br/>207 download.php/11903/saml-2.0-os-xsd.zip).
- 208 [SAML1xMeta] G. Whitehead and S. Cantor, *Metadata Profile for the OASIS Security Assertion  
Markup Language (SAML) V1.x*. OASIS, March 2005. Document ID draft-  
210 saml1x-metadata-05. See <http://www.oasis-open.org/committees/security/>.
- 211 [SAMLX509] R. Randall, *SAML X.509 Authentication-based Attribute Sharing Profile*. OASIS  
212 SSTC, February 2005. Document ID sstc-saml-x509-authn-based-attribute-  
213 protocol-profile-2.0-draft-02. See [http://www.oasis-open.org/committees/security/](http://www.oasis-open.org/committees/<br/>214 security/).
- 215 [Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web  
216 Consortium Recommendation, May 2001. See  
217 <http://www.w3.org/TR/xmlschema-1/>.
- 218 [XMLSig] D. Eastlake et al., *XML-Signature Syntax and Processing*, World Wide Web  
219 Consortium, February 2002. <http://www.w3.org/TR/xmldsig-core/>.

### 220 3.2 Non-Normative References

- 221 [GridShib] *GridShib: A Policy Controlled Attribute Framework*. See  
222 <http://grid.ncsa.uiuc.edu/GridShib/>.
- 223 [LionShare] *LionShare Peer-to-Peer File Sharing*. See <http://lionshare.its.psu.edu/main/>.

## 224 A. Acknowledgments

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

- 227 • Conor Cahill, AOL
- 228 • John Hughes, (formerly) Atos Origin
- 229 • Hal Lockhart, BEA Systems
- 230 • Mike Beach, Boeing
- 231 • Rebekah Metz, Booz Allen Hamilton
- 232 • Rick Randall, Booz Allen Hamilton
- 233 • Ronald Jacobson, Computer Associates
- 234 • Gavneraj Sodhi, Computer Associates
- 235 • Thomas Wisniewski, Entrust
- 236 • Carolina Canales-Valenzuela, Ericsson
- 237 • Dana Kaufman, Forum Systems
- 238 • Irving Reid, Hewlett-Packard
- 239 • Guy Denton, IBM
- 240 • Heather Hinton, IBM
- 241 • Maryann Hondo, IBM
- 242 • Michael McIntosh, IBM
- 243 • Anthony Nadalin, IBM
- 244 • Nick Ragouzis, individual
- 245 • Scott Cantor, Internet2
- 246 • Bob Morgan, Internet2
- 247 • Peter Davis, Neustar
- 248 • Jeff Hodges, Neustar
- 249 • Frederick Hirsch, Nokia
- 250 • Senthil Sengodan, Nokia
- 251 • Abbie Barbir, Nortel Networks
- 252 • Scott Kiester, Novell
- 253 • Cameron Morris, Novell
- 254 • Paul Madsen, NTT
- 255 • Steve Anderson, OpenNetwork
- 256 • Ari Kermaier, Oracle
- 257 • Vamsi Motukuru, Oracle
- 258 • Brian Campbell, Ping Identity
- 259 • Darren Platt, Ping Identity
- 260 • Prateek Mishra, Principal Identity
- 261 • Jim Lien, RSA Security

- 262     • John Linn, RSA Security  
263     • Rob Philpott, RSA Security  
264     • Jahan Moreh, Sigaba  
265     • Eve Maler, Sun Microsystems  
266     • Ronald Monzillo, Sun Microsystems  
267     • Emily Xu, Sun Microsystems  
268     • Greg Whitehead, Trustgenix

269 **Appendix B. Notices**

270 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that  
271 might be claimed to pertain to the implementation or use of the technology described in this document or  
272 the extent to which any license under such rights might or might not be available; neither does it  
273 represent that it has made any effort to identify any such rights. Information on OASIS's procedures with  
274 respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights  
275 made available for publication and any assurances of licenses to be made available, or the result of an  
276 attempt made to obtain a general license or permission for the use of such proprietary rights by  
277 implementors or users of this specification, can be obtained from the OASIS Executive Director.

278 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications,  
279 or other proprietary rights which may cover technology that may be required to implement this  
280 specification. Please address the information to the OASIS Executive Director.

281 **Copyright © OASIS Open 2005. All Rights Reserved.**

282 This document and translations of it may be copied and furnished to others, and derivative works that  
283 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published  
284 and distributed, in whole or in part, without restriction of any kind, provided that the above copyright  
285 notice and this paragraph are included on all such copies and derivative works. However, this document  
286 itself may not be modified in any way, such as by removing the copyright notice or references to OASIS,  
287 except as needed for the purpose of developing OASIS specifications, in which case the procedures for  
288 copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required  
289 to translate it into languages other than English.

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

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