



Metadata Extension for SAML V2.0 and V1.x Query Requesters

OASIS Standard
1 November 2007

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query-os.html>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query-os.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query-os.pdf>

Previous Version:

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query-cs-01.html>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query-cs-01.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query-cs-01.pdf>

Latest Version:

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query.html>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query.odt>

<http://docs.oasis-open.org/security/saml/Post2.0/ssstc-saml-metadata-ext-query.pdf>

Technical Committee:

OASIS Security Services TC

Chairs:

Hal Lockhart, BEA Systems, Inc.

Brian Campbell, Ping Identity

Editors:

Tom Scavo, NCSA

Scott Cantor, Internet2

Related Work:

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

Abstract:

This specification defines an extension to the SAML V2.0 metadata specification [SAML2Meta]. The extension defines role descriptor types that describe a standalone SAML V1.x or V2.0 query requester for each of the three predefined query types. Readers are advised to familiarize themselves with that specification before reading this one.

34 **Status:**

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

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

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

Notices

45

46 Copyright © OASIS Open 2007. All Rights *Reserved*.

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

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

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

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

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

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

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

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

89

90 **Table of Contents**

91 1 Introduction..... 5
92 1.1 Notation..... 5
93 1.2 Normative References..... 6
94 2 Metadata Extension for SAML V2.0 and V1.x Query Requesters..... 7
95 2.1 Required Information..... 7
96 2.2 Namespaces..... 7
97 2.3 Element <md:RoleDescriptor>..... 7
98 2.4 Abstract Complex Type QueryDescriptorType..... 7
99 2.5 Complex Type AuthnQueryDescriptorType..... 8
100 2.6 Complex Type AttributeQueryDescriptorType..... 8
101 2.7 Complex Type AuthzDecisionQueryDescriptorType..... 9
102 2.8 Example..... 9
103 Appendix A. Acknowledgments..... 11
104

105 1 Introduction

106 This specification defines an extension to the SAML V2.0 metadata specification. The extension defines
107 a set of role descriptor types that describe a standalone SAML query requester for each of the three
108 predefined query types. The profile addresses both SAML V1.x and SAML V2.0 query requesters.

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

112 1.1 Notation

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

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

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

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

122 Listings of XML schemas appear like this.

123 Example code listings appear like this.

125 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
126 their respective namespaces as follows, whether or not a namespace declaration is present in the
127 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].
query:	urn:oasis:names:tc:SAML:metadata:ext:query	This is the SAML V2.0 metadata query requester 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 XML Signature namespace [XMLSig] .

128

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. <http://www.ietf.org/rfc/rfc2119.txt>.
- 134 **[MDext-XSD]** T. Scavo et al. *Metadata Extension Schema for SAML V2.0 and V1.x Query*
135 *Requesters*. OASIS Committee Specification, May 2007. Document ID sstc-
136 saml-metadata-ext-query.xsd. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
137 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 138 **[SAML1xMeta]** G. Whitehead and S. Cantor. *Metadata Profile for the OASIS Security Assertion*
139 *Markup Language (SAML) V1.x*. OASIS Committee Specification, May 2007.
140 Document ID sstc-saml1x-metadata-cs-01. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
141 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 142 **[SAML2Core]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*
143 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
144 saml-core-2.0-os. See [http://docs.oasis-open.org/security/saml/v2.0/saml-core-](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
145 [2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).
- 146 **[SAML2Meta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language*
147 *(SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-
148 os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 149 **[SAML2Meta-xsd]** S. Cantor et al. *SAML V2.0 metadata schema*. OASIS Standard, March 2005.
150 Document ID saml-schema-metadata-2.0. See [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd)
151 [open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd).
- 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-](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/)
154 [xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/).
- 155 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*, World Wide Web
156 Consortium, February 2002. See <http://www.w3.org/TR/xmlsig-core/>.

2 Metadata Extension for SAML V2.0 and V1.x Query Requesters

This extension defines new role descriptor types that support the requester role of the three predefined SAML query types: authentication, attribute, and authorization decision.

2.1 Required Information

Identification: `urn:oasis:names:tc:SAML:metadata:ext:query`

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

Description: Given below.

Updates: Extends the SAML V2.0 metadata specification [SAML2Meta].

2.2 Namespaces

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

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

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

This specification defines a new namespace:

```
urn:oasis:names:tc:SAML:metadata:ext:query
```

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

2.3 Element `<md:RoleDescriptor>`

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

2.4 Abstract Complex Type `QueryDescriptorType`

Abstract complex type `QueryDescriptorType` extends complex type `md:RoleDescriptorType` with content generally applicable to query requesters. The type `QueryDescriptorType` contains the following additional attributes and elements:

`WantAssertionsSigned` [Optional]

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

188 <md:NameIDFormat> [Zero or More]
189 Zero or more elements of type **xsd:anyURI** that enumerate the name identifier formats
190 supported by this requester. See section 8.3 of [SAML2Core] for some possible values of this
191 element.

192 As an abstract type, this type serves as a basis for the additional types defined in the following sections
193 and is not used in metadata instances directly.

194 The following schema fragment defines the **QueryDescriptorType** complex type:

```
195 <complexType name="QueryDescriptorType" abstract="true">  
196 <complexContent>  
197 <extension base="md:RoleDescriptorType">  
198 <sequence>  
199 <element ref="md:NameIDFormat" minOccurs="0" maxOccurs="unbounded"/>  
200 </sequence>  
201 <attribute name="WantAssertionsSigned" type="boolean" use="optional"/>  
202 </extension>  
203 </complexContent>  
204 </complexType>
```

205 2.5 Complex Type AuthnQueryDescriptorType

206 Complex type **AuthnQueryDescriptorType** extends complex type **QueryDescriptorType** into a
207 concrete type usable to represent authentication query requesters. It contains no additional elements or
208 attributes.

209 Instances of **AuthnQueryDescriptorType** are declared using the <md:RoleDescriptor> element with
210 an xsi:type of **AuthnQueryDescriptorType**.

211 See the SAML V1.x Metadata Profile [SAML1xMeta] for specifics on the transformation and use of
212 particular elements and attributes for use with SAML V1.x.

213 The following schema fragment defines the **AuthnQueryDescriptorType** complex type:

```
214 <complexType name="AuthnQueryDescriptorType">  
215 <complexContent>  
216 <extension base="query:QueryDescriptorType"/>  
217 </complexContent>  
218 </complexType>
```

219 2.6 Complex Type AttributeQueryDescriptorType

220 Complex type **AttributeQueryDescriptorType** extends complex type **QueryDescriptorType** with
221 content specific to attribute query requesters, that is, consumers of SAML attributes. The type
222 **AttributeQueryDescriptorType** contains the following additional elements:

223 <md:AttributeConsumingService> [Zero or More]
224 Zero or more elements that describe an application or service provided by this requester that
225 requires or desires the use of SAML attributes. It is RECOMMENDED that deployers provide at
226 least one such element to facilitate configuration of policy by attribute providers.

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

231 Instances of **AttributeQueryDescriptorType** are declared using the `<md:RoleDescriptor>` element
232 with an `xsi:type` of **AttributeQueryDescriptorType**. See the example in section 2.8.

233 See the SAML V1.x Metadata Profile [SAML1xMeta] for specifics on the transformation and use of
234 particular elements and attributes for use with SAML V1.x.

235 The following schema fragment defines the **AttributeQueryDescriptorType** complex type:

```
236 <complexType name="AttributeQueryDescriptorType">  
237 <complexContent>  
238 <extension base="query:QueryDescriptorType">  
239 <sequence>  
240 <element ref="md:AttributeConsumingService" minOccurs="0"  
241 maxOccurs="unbounded"/>  
242 </sequence>  
243 </extension>  
244 </complexContent>  
245 </complexType>
```

246 2.7 Complex Type AuthzDecisionQueryDescriptorType

247 Complex type **AuthzDecisionQueryDescriptorType** extends complex type **QueryDescriptorType** with
248 content specific to authorization decision query requesters, that is, policy enforcement points. The type
249 **AuthzDecisionQueryDescriptorType** contains the following additional elements:

250 `<query:ActionNamespace>` [Zero or More]

251 Zero or more elements of type `xsd:anyURI` that enumerate the action namespaces supported by
252 this requester. See section 8.1 of [SAML2Core] for some possible values of this element.

253 Instances of **AuthzDecisionQueryDescriptorType** are declared using the `<md:RoleDescriptor>`
254 element with an `xsi:type` of **AuthzDecisionQueryDescriptorType**.

255 See the SAML V1.x Metadata Profile [SAML1xMeta] for specifics on the transformation and use of
256 particular elements and attributes for use with SAML V1.x.

257 The following schema fragment defines the **AuthzDecisionQueryDescriptorType** complex type:

```
258 <complexType name="AuthzDecisionQueryDescriptorType">  
259 <complexContent>  
260 <extension base="query:QueryDescriptorType">  
261 <sequence>  
262 <element ref="query:ActionNamespace" minOccurs="0"  
263 maxOccurs="unbounded"/>  
264 </sequence>  
265 </extension>  
266 </complexContent>  
267 </complexType>
```

268 The following schema fragment defines the `<query:ActionNamespace>` element:

```
269 <element name="ActionNamespace" type="anyURI"/>
```

270 2.8 Example

271 Following is a metadata example for a SAML attribute query requester that supports both SAML V1.1
272 and SAML V2.0.

```
273 <md:EntityDescriptor  
274 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"  
275 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  
276 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
```

```

277   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
278   entityID="https://gs.org/gridshib">
279   <!-- insert ds:Signature element here -->
280   <md:RoleDescriptor
281     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
282     xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
283     xsi:type="query:AttributeQueryDescriptorType"
284     protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
285 urn:oasis:names:tc:SAML:2.0:protocol">
286     <md:KeyDescriptor use="signing">
287       <ds:KeyInfo>
288         <ds:KeyName>Requester Key</ds:KeyName>
289       </ds:KeyInfo>
290     </md:KeyDescriptor>
291     <md:NameIDFormat>
292       urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
293     </md:NameIDFormat>
294     <md:AttributeConsumingService isDefault="true" index="0">
295       <md:ServiceName xml:lang="en">
296         Shibbolized Grid Service
297       </md:ServiceName>
298       <md:RequestedAttribute
299         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
300         Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
301         FriendlyName="eduPersonScopedAffiliation">
302       </md:RequestedAttribute>
303       <md:RequestedAttribute
304         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
305         Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
306         FriendlyName="eduPersonEntitlement">
307         <saml:AttributeValue xsi:type="xsd:anyURI">
308           https://gs.org/gridshib/entitlements/123456789
309         </saml:AttributeValue>
310       </md:RequestedAttribute>
311     </md:AttributeConsumingService>
312   </md:RoleDescriptor>
313   <md:Organization>
314     <md:OrganizationName xml:lang="en">
315       GridShib Service Provider
316     </md:OrganizationName>
317     <md:OrganizationDisplayName xml:lang="en">
318       GridShib Service Provider @ Some Location
319     </md:OrganizationDisplayName>
320     <md:OrganizationURL xml:lang="en">
321       http://www.gs.org/
322     </md:OrganizationURL>
323   </md:Organization>
324   <md:ContactPerson contactType="technical">
325     <md:SurName>GridShib Support</md:SurName>
326     <md:EmailAddress>mailto:gridshib-support@gs.org</md:EmailAddress>
327   </md:ContactPerson>
328 </md:EntityDescriptor>

```

329 **Appendix A. Acknowledgments**

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

- 332 ● Hal Lockhart, BEA Systems, Inc.
- 333 ● Steve Anderson, BMC Software
- 334 ● Rob Philpott, EMC Corporation
- 335 ● Carolina Canales-Valenzuela, Ericsson
- 336 ● Dana Kaufman, Forum Systems
- 337 ● Ashish Patel, France Telecom
- 338 ● Greg Whitehead, Hewlett-Packard Company
- 339 ● Heather Hinton, IBM
- 340 ● Anthony Nadalin, IBM
- 341 ● Conor P. Cahill, Intel
- 342 ● Scott Cantor, Internet2
- 343 ● Bob Morgan, Internet2
- 344 ● Tom Scavo, National Center for Supercomputing Applications
- 345 ● Peter Davis, NeuStar
- 346 ● Jeff Hodges, NeuStar
- 347 ● Frederick Hirsch, Nokia
- 348 ● Abbie Barbir, Nortel
- 349 ● Paul Madsen, NTT Corporation
- 350 ● Ari Kermaier, Oracle
- 351 ● Prateek Mishra, Oracle
- 352 ● Brian Campbell, Ping Identity
- 353 ● Bhavna Bhatnagar, Sun Microsystems
- 354 ● Eve Maler, Sun Microsystems
- 355 ● Emily Xu, Sun Microsystems
- 356 ● David Staggs, Veteran's Health Administration

357 The editors would also like to acknowledge the special contributions of the following individual:

- 358 ● Tom Wisniewski, Entrust