



2 SAML Metadata Extension for Query 3 Requesters

4 Committee Draft 01, 14 March 2006

5 Document identifier:

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

7 Location:

8 http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

9 Editors:

10 Tom Scavo (trscavo@gmail.com), Individual
11 Scott Cantor (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 role descriptor types that describe a standalone SAML V1.x or V2.0 query
17 requester for each of the three predefined query types. Readers are advised to familiarize
18 themselves with that specification before reading this one.

19 Status:

20 This is a **Committee Draft** approved by the Security Services Technical Committee on 14 March
21 2006.

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 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.

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

29 **Table of Contents**

30 1 Introduction..... 3
31 1.1 Notation..... 3
32 2 Query Metadata Extensions for SAML V2.0..... 4
33 2.1 Namespaces..... 4
34 2.2 Element <md:RoleDescriptor>..... 4
35 2.3 Abstract Complex Type QueryDescriptorType..... 4
36 2.4 Complex Type AuthnQueryDescriptorType..... 5
37 2.5 Complex Type AttributeQueryDescriptorType..... 5
38 2.6 Complex Type AuthzDecisionQueryDescriptorType..... 6
39 2.7 Example..... 6
40 3 References..... 8
41 3.1 Normative References..... 8
42

43 1 Introduction

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

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

50 1.1 Notation

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

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

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

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

60 Listings of XML schemas appear like this.

61 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].
query:	urn:oasis:names:tc:SAML:metadata:ext:query	This is the SAML V2.0 metadata query 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].

66

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

2 Query Metadata Extensions for SAML V2.0

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

2.1 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 type is assumed to belong to this new namespace.

2.2 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.

2.3 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.

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

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

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

The following schema fragment defines the `QueryDescriptorType` complex type:

```
<complexType name="QueryDescriptorType" abstract="true">
  <complexContent>
    <extension base="md:RoleDescriptorType">
      <sequence>
        <element ref="md:NameIDFormat" minOccurs="0" maxOccurs="unbounded"/>
      </sequence>
      <attribute name="WantAssertionsSigned" type="boolean" use="optional"/>
    </extension>
  </complexContent>
</complexType>
```

```
108     </complexContent>
109 </complexType>
```

110 2.4 Complex Type AuthnQueryDescriptorType

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

114 Instances of **AuthnQueryDescriptorType** are declared using the `<md:RoleDescriptor>` element with
115 an `xsi:type` of **AuthnQueryDescriptorType**.

116 See for specifics on the transformation and use of particular elements and attributes for use with SAML
117 V1.x.

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

```
119 <complexType name="AuthnQueryDescriptorType">
120   <complexContent>
121     <extension base="md:QueryDescriptorType"/>
122   </complexContent>
123 </complexType>
```

124 2.5 Complex Type AttributeQueryDescriptorType

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

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

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

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

136 Instances of **AttributeQueryDescriptorType** are declared using the `<md:RoleDescriptor>` element
137 with an `xsi:type` of **AttributeQueryDescriptorType**. See the example in Section 2.7.

138 See for specifics on the transformation and use of particular elements and attributes for use with SAML
139 V1.x.

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

```
141 <complexType name="AttributeQueryDescriptorType">
142   <complexContent>
143     <extension base="md:QueryDescriptorType">
144       <sequence>
145         <element ref="md:AttributeConsumingService" minOccurs="0"
146 maxOccurs="unbounded"/>
147       </sequence>
148     </extension>
149   </complexContent>
150 </complexType>
```

151 2.6 Complex Type AuthzDecisionQueryDescriptorType

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

155 <ActionNamespace> [Zero or More]

156 Zero or more elements of type **xsd:anyURI** that enumerate the action namespaces supported by
157 this requester. See Section 8.1 of [SAML2Core] for some possible values of this element.

158 Instances of **AuthzDecisionQueryDescriptorType** are declared using the <md:RoleDescriptor>
159 element with an **xsi:type** of **AuthzDecisionQueryDescriptorType**.

160 See for specifics on the transformation and use of particular elements and attributes for use with SAML
161 V1.x.

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

```
163 <element name="ActionNamespace" type="anyURI"/>
164 <complexType name="AuthzDecisionQueryDescriptorType">
165   <complexContent>
166     <extension base="md:QueryDescriptorType">
167       <sequence>
168         <element ref="query:ActionNamespace" minOccurs="0"
169 maxOccurs="unbounded"/>
170       </sequence>
171     </extension>
172   </complexContent>
173 </complexType>
```

174 The following schema fragment defines the <ActionNamespace> element:

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

176 2.7 Example

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

```
179 <md:EntityDescriptor
180   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
181   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
182   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
183   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
184   entityID="https://gs.org/gridshib">
185   <!-- insert ds:Signature element here -->
186   <md:RoleDescriptor
187     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
188     xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
189     xsi:type="query:AttributeQueryDescriptorType"
190     protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
191 urn:oasis:names:tc:SAML:2.0:protocol">
192     <md:KeyDescriptor use="signing">
193       <ds:KeyInfo>
194         <ds:KeyName>Requester Key</ds:KeyName>
195       </ds:KeyInfo>
196     </md:KeyDescriptor>
197     <md:NameIDFormat>
198       urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
199     </md:NameIDFormat>
200     <md:AttributeConsumingService isDefault="true" index="0">
201       <md:ServiceName xml:lang="en">
```

```

202     Shibbolized Grid Service
203     </md:ServiceName>
204     <md:RequestedAttribute
205         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
206         Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
207         FriendlyName="eduPersonEntitlement">
208         <saml:AttributeValue xsi:type="xsd:anyURI">
209             https://gs.org/gridshib/entitlements/123456789
210         </saml:AttributeValue>
211     </md:RequestedAttribute>
212     <md:RequestedAttribute
213         NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri"
214         Name="urn:mace:dir:attribute-def:eduPersonEntitlement">
215         <saml:AttributeValue xsi:type="xsd:anyURI">
216             https://gs.org/gridshib/entitlements/123456789
217         </saml:AttributeValue>
218     </md:RequestedAttribute>
219 </md:AttributeConsumingService>
220 </md:RoleDescriptor>
221 <md:Organization>
222     <md:OrganizationName xml:lang="en">
223         GridShib Service Provider
224     </md:OrganizationName>
225     <md:OrganizationDisplayName xml:lang="en">
226         GridShib Service Provider @ Some Location
227     </md:OrganizationDisplayName>
228     <md:OrganizationURL xml:lang="en">
229         http://www.gs.org/
230     </md:OrganizationURL>
231 </md:Organization>
232 <md:ContactPerson contactType="technical">
233     <md:SurName>GridShib Support</md:SurName>
234     <md:EmailAddress>gridshib-support@gs.org</md:EmailAddress>
235 </md:ContactPerson>
236 </md:EntityDescriptor>

```

237 3 References

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

239 3.1 Normative References

- 240 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
241 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 242 **[MDext-XSD]** S. Cantor et al. SAML metadata extension schema. OASIS SSTC, February
243 2006. Document ID sstc-saml-metadata-ext-query.xsd. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
244 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).
- 245 **[SAML1xMeta]** G. Whitehead and S. Cantor. *Metadata Profile for the OASIS Security Assertion*
246 *Markup Language (SAML) V1.x*. OASIS, March 2005. Document ID sstc-saml1x-
247 metadata-cd-01. See <http://www.oasis-open.org/committees/security/>.
- 248 **[SAML2Core]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*
249 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
250 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)
251 [2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).
- 252 **[SAML2Meta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language*
253 *(SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-
254 os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 255 **[SAML2Meta-xsd]** S. Cantor et al. SAML V2.0 metadata schema. OASIS Standard, March 2005.
256 Document ID saml-schema-metadata-2.0. See [http://www.oasis-](http://www.oasis-open.org/committees/download.php/11903/saml-2.0-os-xsd.zip)
257 [open.org/committees/download.php/11903/saml-2.0-os-xsd.zip](http://www.oasis-open.org/committees/download.php/11903/saml-2.0-os-xsd.zip).
- 258 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
259 Consortium Recommendation, May 2001. See
260 <http://www.w3.org/TR/xmlschema-1/>.
- 261 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*, World Wide Web
262 Consortium, February 2002. See <http://www.w3.org/TR/xmlsig-core/>.

263 **A. Acknowledgments**

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

- 266 • Hal Lockhart, BEA Systems, Inc.
- 267 • Steve Anderson, BMC Software
- 268 • Rick Randall, Booz Allen Hamilton
- 269 • Nick Ragouzis, Enosis Group
- 270 • Thomas Wisniewski, Entrust
- 271 • Sharon Boeyen, Entrust
- 272 • Carolina Canales-Valenzuela, Ericsson
- 273 • Dana Kaufman, Forum Systems
- 274 • Ashish Patel, France Telecom
- 275 • Irving Reid, Hewlett-Packard Company
- 276 • Greg Whitehead, Hewlett-Packard Company
- 277 • Guy Denton, IBM
- 278 • Heather Hinton, IBM
- 279 • Anthony Nadalin, IBM
- 280 • Eric Tiffany, IEEE Industry Standards
- 281 • Prasanta Behera, Individual
- 282 • Scott Cantor, Internet2
- 283 • Bob Morgan, Internet2
- 284 • Jeff Hodges, NeuStar
- 285 • Frederick Hirsch, Nokia
- 286 • Paul Madsen, NTT Corporation
- 287 • Ari Kermaier, Oracle
- 288 • Prateek Mishra, Oracle
- 289 • Vamsi Motukuru, Oracle
- 290 • Brian Campbell, Ping Identity
- 291 • John Hughes, PA Consulting
- 292 • Rob Philpott, RSA Security
- 293 • Jahan Moreh, Sigaba
- 294 • Bhavna Bhatnagar, Sun Microsystems
- 295 • Eve Maler, Sun Microsystems
- 296 • David Staggs, Veteran's Health Admin

297 **Appendix B. Notices**

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

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

309 **Copyright © OASIS Open 2006. All Rights Reserved.**

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

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

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