



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

Committee Draft 02, 1 September 2006

Document identifier:

sstc-saml-metadata-ext-query-cd-02

Location:

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

Editors:

Tom Scavo, NCSA
Scott Cantor, Internet2

Contributors:

Tom Wisniewski, Entrust

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.

Status:

This is a **Committee Draft** approved by the Security Services Technical Committee on 28 August 2006.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them by filling out the web form located at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security.

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

29 **Table of Contents**

30 1 Introduction..... 3
31 1.1 Notation..... 3
32 2 Metadata Extension for SAML V2.0 and V1.x Query Requesters..... 5
33 2.1 Required Information..... 5
34 2.2 Namespaces..... 5
35 2.3 Element <md:RoleDescriptor>..... 5
36 2.4 Abstract Complex Type QueryDescriptorType..... 5
37 2.5 Complex Type AuthnQueryDescriptorType..... 6
38 2.6 Complex Type AttributeQueryDescriptorType..... 6
39 2.7 Complex Type AuthzDecisionQueryDescriptorType..... 7
40 2.8 Example..... 7
41 3 References..... 9
42 3.1 Normative References..... 9
43 Appendix A. Acknowledgments..... 10
44 Appendix B. Notices..... 11
45

46 1 Introduction

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

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

53 1.1 Notation

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

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

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

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

63 Listings of XML schemas appear like this.

64 Example code listings appear like this.

66 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
67 their respective namespaces as follows, whether or not a namespace declaration is present in the
68 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].

69

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

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.

103 <md:NameIDFormat> [Zero or More]
104 Zero or more elements of type **xsd:anyURI** that enumerate the name identifier formats
105 supported by this requester. See Section 8.3 of [SAML2Core] for some possible values of this
106 element.

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

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

```
110 <complexType name="QueryDescriptorType" abstract="true">  
111   <complexContent>  
112     <extension base="md:RoleDescriptorType">  
113       <sequence>  
114         <element ref="md:NameIDFormat" minOccurs="0" maxOccurs="unbounded"/>  
115       </sequence>  
116       <attribute name="WantAssertionsSigned" type="boolean" use="optional"/>  
117     </extension>  
118   </complexContent>  
119 </complexType>
```

120 2.5 Complex Type AuthnQueryDescriptorType

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

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

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

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

```
129 <complexType name="AuthnQueryDescriptorType">  
130   <complexContent>  
131     <extension base="md:QueryDescriptorType"/>  
132   </complexContent>  
133 </complexType>
```

134 2.6 Complex Type AttributeQueryDescriptorType

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

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

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

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

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

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

```
151 <complexType name="AttributeQueryDescriptorType">  
152   <complexContent>  
153     <extension base="md:QueryDescriptorType">  
154       <sequence>  
155         <element ref="md:AttributeConsumingService" minOccurs="0"  
156 maxOccurs="unbounded"/>  
157       </sequence>  
158     </extension>  
159   </complexContent>  
160 </complexType>
```

161 2.7 Complex Type AuthzDecisionQueryDescriptorType

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

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

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

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

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

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

```
173 <complexType name="AuthzDecisionQueryDescriptorType">  
174   <complexContent>  
175     <extension base="md:QueryDescriptorType">  
176       <sequence>  
177         <element ref="query:ActionNamespace" minOccurs="0"  
178 maxOccurs="unbounded"/>  
179       </sequence>  
180     </extension>  
181   </complexContent>  
182 </complexType>
```

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

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

185 2.8 Example

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

```
188 <md:EntityDescriptor  
189   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"  
190   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  
191   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
```

```

192   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
193   entityID="https://gs.org/gridshib">
194   <!-- insert ds:Signature element here -->
195   <md:RoleDescriptor
196     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
197     xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
198     xsi:type="query:AttributeQueryDescriptorType"
199     protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
200 urn:oasis:names:tc:SAML:2.0:protocol">
201     <md:KeyDescriptor use="signing">
202       <ds:KeyInfo>
203         <ds:KeyName>Requester Key</ds:KeyName>
204       </ds:KeyInfo>
205     </md:KeyDescriptor>
206     <md:NameIDFormat>
207       urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
208     </md:NameIDFormat>
209     <md:AttributeConsumingService isDefault="true" index="0">
210       <md:ServiceName xml:lang="en">
211         Shibbolized Grid Service
212       </md:ServiceName>
213       <md:RequestedAttribute
214         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
215         Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
216         FriendlyName="eduPersonScopedAffiliation">
217       </md:RequestedAttribute>
218       <md:RequestedAttribute
219         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
220         Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
221         FriendlyName="eduPersonEntitlement">
222         <saml:AttributeValue xsi:type="xsd:anyURI">
223           https://gs.org/gridshib/entitlements/123456789
224         </saml:AttributeValue>
225       </md:RequestedAttribute>
226     </md:AttributeConsumingService>
227   </md:RoleDescriptor>
228   <md:Organization>
229     <md:OrganizationName xml:lang="en">
230       GridShib Service Provider
231     </md:OrganizationName>
232     <md:OrganizationDisplayName xml:lang="en">
233       GridShib Service Provider @ Some Location
234     </md:OrganizationDisplayName>
235     <md:OrganizationURL xml:lang="en">
236       http://www.gs.org/
237     </md:OrganizationURL>
238   </md:Organization>
239   <md:ContactPerson contactType="technical">
240     <md:SurName>GridShib Support</md:SurName>
241     <md:EmailAddress>gridshib-support@gs.org</md:EmailAddress>
242   </md:ContactPerson>
243 </md:EntityDescriptor>

```

244 3 References

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

246 3.1 Normative References

- 247 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
248 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 249 **[MDext-XSD]** T. Scavo et al. *Metadata Extension Schema for SAML V2.0 and V1.x Query*
250 *Requesters*. OASIS SSTC, July 2006. Document ID sstc-saml-metadata-ext-
251 query.xsd. See <http://www.oasis-open.org/committees/security/>.
- 252 **[SAML1xMeta]** G. Whitehead and S. Cantor. *Metadata Profile for the OASIS Security Assertion*
253 *Markup Language (SAML) V1.x*. OASIS, July 2006. Document ID draft-sstc-
254 saml1x-metadata-07. See <http://www.oasis-open.org/committees/security/>.
- 255 **[SAML2Core]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion*
256 *Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID
257 saml-core-2.0-os. See [http://docs.oasis-open.org/security/saml/v2.0/saml-core-
258 2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf).
- 259 **[SAML2Meta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language*
260 *(SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-
261 os. See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 262 **[SAML2Meta-xsd]** S. Cantor et al. *SAML V2.0 metadata schema*. OASIS Standard, March 2005.
263 Document ID saml-schema-metadata-2.0. See [http://docs.oasis-
264 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).
- 265 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
266 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
267 xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/).
- 268 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*, World Wide Web
269 Consortium, February 2002. See <http://www.w3.org/TR/xmlsig-core/>.

270 **Appendix A. Acknowledgments**

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

- 273 • Hal Lockhart, BEA Systems, Inc.
- 274 • Steve Anderson, BMC Software
- 275 • Thomas Wisniewski, Entrust
- 276 • Ashish Patel, France Telecom
- 277 • Greg Whitehead, Hewlett-Packard
- 278 • Heather Hinton, IBM
- 279 • Anthony Nadalin, IBM
- 280 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 281 • Scott Cantor, Internet2
- 282 • Bob Morgan, Internet2
- 283 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 284 • Peter Davis, Neustar, Inc.
- 285 • Jeff Hodges, Neustar, Inc.
- 286 • Frederick Hirsch, Nokia Corporation
- 287 • Abbie Barbir, Nortel Networks Limited
- 288 • Paul Madsen, NTT Corporation
- 289 • Ari Kermaier, Oracle Corporation
- 290 • Prateek Mishra, Oracle Corporation
- 291 • John Hughes, PA Consulting
- 292 • Brian Campbell, Ping Identity Corporation
- 293 • Rob Philpott, RSA Security
- 294 • Jahan Moreh, Sigaba Corp.
- 295 • Bhavna Bhatnagar, Sun Microsystems
- 296 • Eve Maler, Sun Microsystems
- 297 • Emily Xu, Sun Microsystems
- 298 • David Staggs, Veterans Health Administration

299 **Appendix B. Notices**

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

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

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

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

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

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