



XACML MAP Authorization Profile

Version 1.0

OASIS Standard

19 January 2015

Specification URLs

This version:

- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/os/xacml-map-authz-v1.0-os.doc> (Authoritative)
- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/os/xacml-map-authz-v1.0-os.html>
- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/os/xacml-map-authz-v1.0-os.pdf>

Previous version:

- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v1.0-csprd01.doc> (Authoritative)
- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v1.0-csprd01.html>
- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v1.0-csprd01.pdf>

Latest version:

- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.doc> (Authoritative)
- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.html>
- <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.pdf>

Technical Committee:

OASIS eXtensible Access Control Markup Language (XACML) TC

Chairs:

Bill Parducci (bill@parducci.net), Individual
Hal Lockhart (hal.lockhart@oracle.com), Oracle

Editors:

Richard Hill (richard.c.hill@boeing.com), The Boeing Company
John Tolbert (john.tolbert@queraltinc.com), Queralt, Inc.
Steve Legg (steven.legg@viewds.com), ViewDS

Related work:

This specification is related to:

- *eXtensible Access Control Markup Language (XACML) Version 3.0.* Edited by Erik Rissanen. Latest version. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html>.
- TNC MAP Content Authorization
http://www.trustedcomputinggroup.org/resources/tnc_map_content_authorization.

Abstract:

This specification defines a profile for the use of XACML in expressing policies for TCG TNC Metadata Access Points (MAP). It defines standard attribute identifiers useful in such policies, in which a MAP utilizes an XACML PDP to make MAP content authorization decisions.

Status:

This document was last revised or approved by the membership of OASIS on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC by using the “Send A Comment” button on the Technical Committee’s web page at <https://www.oasis-open.org/committees/xacml/>.

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 section of the Technical Committee web page (<https://www.oasis-open.org/committees/xacml/ipr.php>).

Citation format:

When referencing this specification the following citation format should be used:

[xacml-map-authz-v1.0]

XACML MAP Authorization Profile Version 1.0. Edited by Richard Hill, John Tolbert, and Steve Legg. 19 January 2015. OASIS Standard. <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/os/xacml-map-authz-v1.0-os.html>. Latest version: <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.html>.

Notices

Copyright © OASIS Open 2015. All Rights Reserved.

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

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

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

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

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

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

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

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

Table of Contents

1	Introduction	5
1.1	Overview (non-normative)	5
1.2	Glossary.....	6
1.3	Terminology	8
1.4	Normative References	8
1.5	Non-Normative References	8
2	Profile	9
2.1	Subject Attributes.....	9
2.1.1	Role	9
2.1.2	Task.....	9
2.2	Resource Attributes	10
2.2.1	Overview.....	10
2.2.2	Metadata-Type	10
2.2.3	Identifier-Type.....	10
2.2.4	Is-Map-Client-Identifier	11
2.2.5	Is-Self-Identifier	12
2.2.6	On-Link	12
2.2.7	Metadata-Attribute	13
2.2.8	Identifier Attribute	14
2.3	Action Attributes.....	15
2.3.1	Action-Id	15
2.3.2	Request-Type	16
2.3.3	Purge-Own-Metadata	16
2.3.4	Publish-Request-Subtype.....	16
2.4	Environment Attributes	17
2.4.1	Dry-Run	17
2.5	Obligation Caching	18
2.5.1	Overview.....	18
2.5.2	Maximum-Policy-Lag.....	18
3	Profile Identifier.....	19
4	Conformance	20
4.1	Overview	20
4.2	Attribute Identifiers	20
4.3	Attribute Values	21
Appendix A.	Acknowledgements	22
Appendix B.	Revision History	25

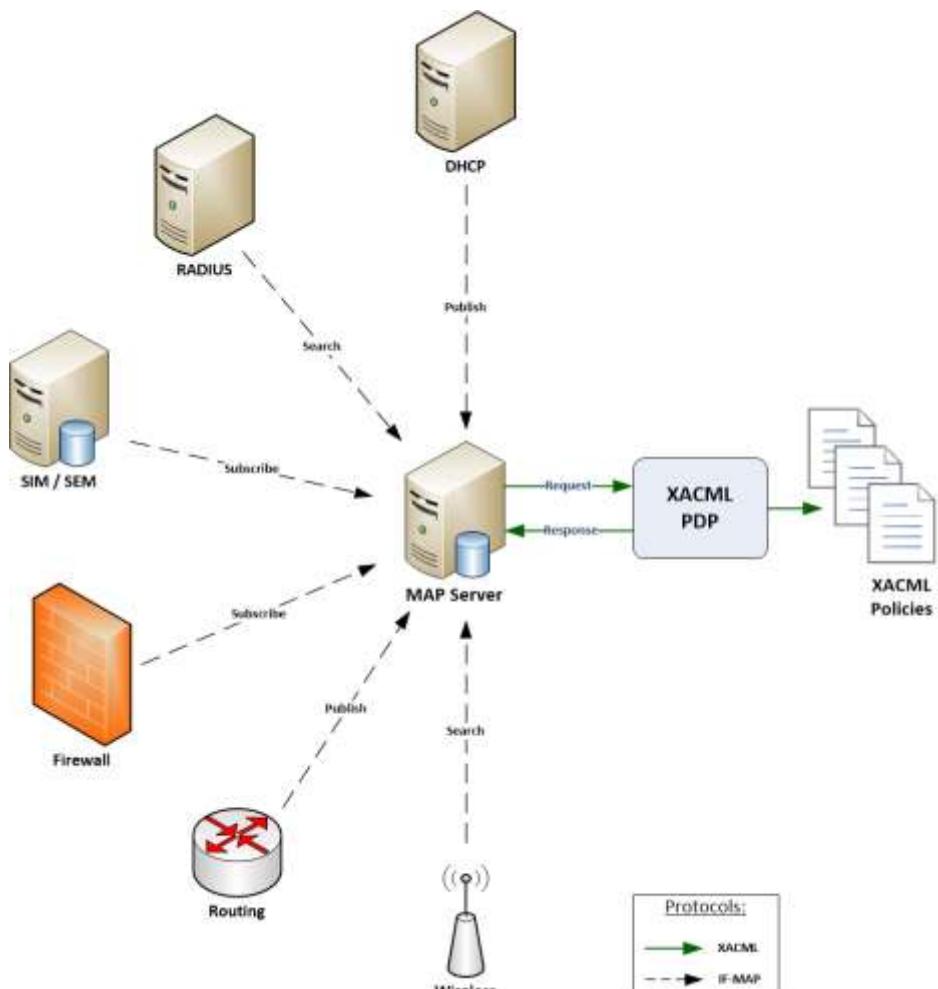
1 Introduction

2 1.1 Overview (non-normative)

3 {Non-normative}

4 The Trusted Computing Group (TCG) provides vendor-neutral standards through the Trusted Network
5 Connect (TNC) Working Group for Network Access Controls (NAC). TNC defines an open architecture
6 and interfaces for NAC, in which the IF-MAP interface is most relevant to the context of this profile. The
7 IF-MAP protocol allows devices to *publish*, *subscribe* and *search* data events through a Metadata Access
8 Point (MAP) server (see figure 1). The MAP server stores state information about devices, users, and
9 flows in a network (see figure 2) and automatically aggregates, correlates, and distributes data to and
10 from IF-MAP enabled devices on a network. TNC also provides an authorization model for the MAP that
11 provides access control to metadata and constrains which operations a MAP Client can perform [TNC-
12 **MAP-Authz**]. The TNC MAP authorization model defines the use of an XACML Policy Decision Point
13 (PDP) when making MAP access control decisions. This profile describes attributes for such decisions
14 between the MAP server and the XACML PDP and is based on, and aligned with [TNC-MAP-Authz]. All
15 examples in [xacml-map-authz-v1.0] are non-normative.

16



18

19 *Figure 1: Example MAP – XACML scenario*

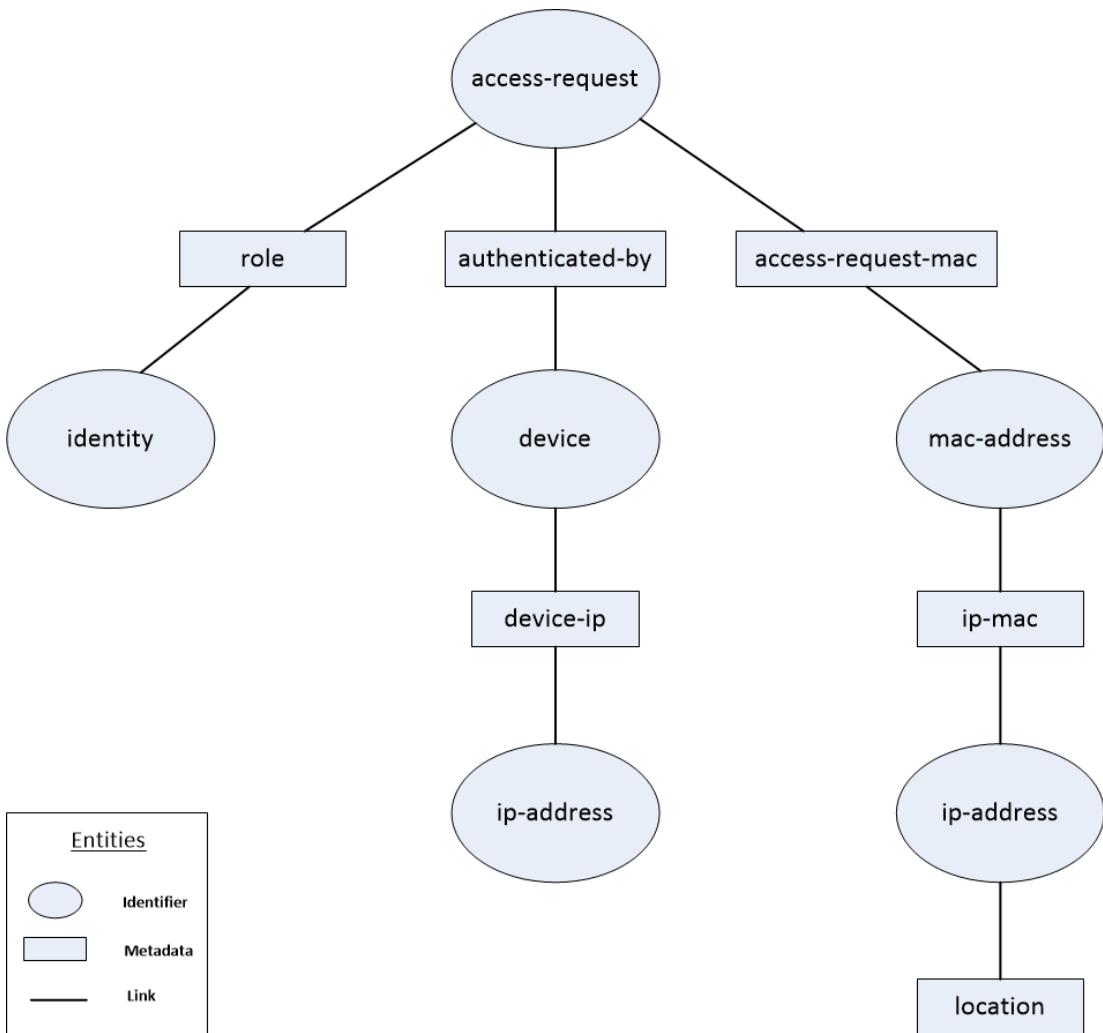


Figure 2: Example labeled graph representation of an IF-MAP data model

1.2 Glossary

Administrative-Domain

A string value defined by an organization as an optional qualifier to prevent name conflicts and can be used to group identifiers.

Content Selector

A MAP server resource attribute filter that controls which parts of a metadata item or identifier are used as XACML request attributes.

Extended Identifier

One of two classes of identifier that is defined in an external schema, which allow vendors and other standards to extend the identifier space for new applications and use cases for IF-MAP.

IF-MAP

The Interface for Metadata Access Points (IF-MAP) is an element of the TNC architecture that specifies a standard interface between a MAP and other elements of the TNC architecture.

- 36 **IF-MAP Request**
37 A message sent from a MAP client to a MAP server using the IF-MAP standard client/server
38 protocol. Also see [TNC-MAP-Authz, Section 2.2.3 IF-MAP Requests].
- 39 **Identifier**
40 An identifier is an XML element, in which the IF-MAP interface specification defines a set of
41 identifiers, or namespace that can be used to reference metadata items and represents a globally
42 unique label of a node within the undirected, labeled graph representation of the IF-MAP data
43 model.
- 44 **Link**
45 Within the undirected, labeled graph representation of the IF-MAP data model, links represent the
46 graph's edges and contains information about the relationship between two identifiers.
- 47 **MAP**
48 Metadata Access Point (MAP) is a server that provides device, user, and network flow state
49 information to MAP Clients.
- 50 **MAP Client**
51 A client to a MAP server [TNC-MAP-Authz, Section 2.2.2 MAP Client].
- 52 **Metadata Item**
53 A metadata item is an XML element which is the basic unit of content that can be attached to
54 identifiers or links within the undirected, labeled graph representation of the IF-MAP data model.
- 55 **NAC**
56 Network Access Control. A unified set of network technologies and protocols to provide policy
57 based network access controls.
- 58 **Original Identifier**
59 One of two classes of identifier for network-oriented elements. The 5 original identifier types are:
60 access-request, device, identity, ip-address, and mac-address.
- 61 **PEP**
62 Policy enforcement point as defined in [XACML3].
- 63 **PIP**
64 Policy information point as defined in [XACML3].
- 65 **purgePublisher**
66 A purgePublisher request is sent by a MAP client and is typically used to remove its own
67 published data from the MAP server.
- 68 **publisher-id**
69 A publisher-id is an attribute of a metadata item that indicates which MAP Client published the
70 metadata to the MAP server.
- 71 **Publish Request Subtype**
72 Each publish request is a sequence of operations. Each operation has a publish subtype *update*,
73 *notify* or *delete*.
- 74 **Self-Identifier**
75 A MAP client's identity identifier with the administrative-domain "ifmap:client".
- 76 **TCG**
77 Trusted Computing Group is a standards organization that defines and promotes open, vendor-
78 neutral standards for trusted computing platforms.

79 **TNC**
80 Trusted Network Connect is a working group of TCG that defines open architecture protocol
81 specifications for network endpoint integrity and security.

82 **Top-level attribute**
83 An XML attribute of the root element of an XML document. Metadata items and extended
84 identifiers are expressed in XML documents.

85 **1.3 Terminology**

86 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
87 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described
88 in [RFC2119].

89 **1.4 Normative References**

- 90 **[RFC2119]** Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP
91 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 92
- 93 **[TNC-IF-MAP]** TNC IF-MAP Binding for SOAP, version 2.1
94 http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_s
95 pecification
- 96
- 97 **[TNC-MAP-Authz]** MAP Content Authorization, version 1.0
98 http://www.trustedcomputinggroup.org/resources/tnc_map_content_authorization
- 99
- 100 **[XACML3]** OASIS Standard, "eXtensible Access Control Markup Language (XACML)
101 Version 3.0", January 2013. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.doc>
- 102
- 103 **[XACML2]** OASIS Standard, "eXtensible Access Control Markup Language (XACML)
104 Version 2.0", February 2005. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
- 105
- 106 **[XACML1]** OASIS Standard, "eXtensible Access Control Markup Language (XACML)
107 Version 1.0", February 2003. <http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf>
- 108
- 109 **[XMLSCHEMA11-2]** D. Peterson, S. , A. Malhotra, M. , H. S. Thompson, P. V. Biron, Editors, W3C
110 Recommendation, 5 April 2012, <http://www.w3.org/TR/2012/REC-xmlschema11-2-20120405/>. Latest version available at <http://www.w3.org/TR/xmlschema11-2/>
- 111

115 **1.5 Non-Normative References**

- 116 **[XACMLIntro]** OASIS XACML TC, *A Brief Introduction to XACML*, 14 March 2003,
117 http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html
- 118
- 119

120 **2 Profile**

121 **2.1 Subject Attributes**

122 **2.1.1 Role**

123 The MAP Client role values MUST be designated with the following attribute identifier:

```
124     urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role
```

125 The **DataType** of this attribute is <http://www.w3.org/2001/XMLSchema#string>
126 [XMLSCHEMA11-2].

127 This attribute MUST denote the role assigned to the MAP client's session and MUST be omitted if the
128 session has no roles. Role names beginning with "ifmap:" or "tcg:" are reserved and MUST only be used
129 in accordance with [TNC-MAP-Authz]. The [TNC-MAP-Authz] specification for a list of pre-defined roles,
130 as well as roles derived from metadata, LDAP groups or certificates. It is RECOMMENDED to use URNs
131 when defining roles to avoid role conflicts.

132

133 **Example 1**

134 The following is an example of a role attribute in which the MAP Client is a TNC Flow Controller,
135 such as a firewall, in a target match:

```
136 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
137   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
138     >tcg:flow-controller</AttributeValue>  
139   <AttributeDesignator  
140     MustBePresent="false"  
141     Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"  
142     AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role"  
143     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
144 </Match>
```

145

146 **2.1.2 Task**

147 The MAP Client task values MUST be designated with the following attribute identifier:

```
148     urn:oasis:names:tc:xacml:3.0:if-  
149     map:content:subject:task:RELATIONSHIP: IDENTIFIER-TYPE
```

150 The **DataType** of this attribute is <http://www.w3.org/2001/XMLSchema#string>
151 [XMLSCHEMA11-2].

152 This attribute MUST denote the task assigned to the MAP client. Both RELATIONSHIP and IDENTIFIER-
153 TYPE MUST be URL-encoded.

154

155 **Example 2**

156 The following is an example of an attribute identifier:

```
157     urn:oasis:names:tc:xacml:3.0:if-map:content:subject:task:member-  
158     of:http%3A//www.trustedcomputinggroup.org/2010/IFMAP-ICS-  
159     METADATA/1#overlay-network-group
```

160

161 2.2 Resource Attributes

162 2.2.1 Overview

163

164 For an IF-MAP publish request, each metadata item in the publish request is treated as a resource. Each
165 attribute defined in section 2.2 Resource Attributes refers to a metadata item or identifier found in the
166 MAP database.

167 When a MAP Server retrieves data for a MAP Client, in response to a search or subscribe request, each
168 metadata item in the MAP database is treated as a resource. In that context, each attribute defined in this
169 section refers to a metadata item or identifier within the MAP database. For an IF-MAP purgePublisher
170 request, the decision request MUST NOT include attributes defined in section 2.2 Resource Attributes.

171 2.2.2 Metadata-Type

172 The Metadata-Type value MUST be designated with the following attribute identifier:

173 urn:oasis:names:tc:xacml:3.0;if-map:content:resource:metadata-type

174 The DataType of this attribute is <http://www.w3.org/2001/XMLSchema#string>

175 [XMLSHEMA11-2]. This attribute denotes the type of the metadata item. The value of this attribute
176 MUST be of the form **NAMESPACE#TYPE**, in which *NAMESPACE* represents the URI of the meta
177 namespace and *TYPE* represents the top-level XML element name to the right of *the prefix*. This attribute
178 MUST be a singleton and MUST be present if the MAP Client request is not *purgePublisher*.

179

180 Example 3

181 The following is an example of a metadata-type attribute in a target match:

```
182 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
183   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
184     >http://www.trustedcomputinggroup.org/2010/IFMAP-METADATA/2#device-
185     ip</AttributeValue>
186   <AttributeDesignator
187     MustBePresent="false"
188     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
189     AttributeId="urn:oasis:names:tc:xacml:3.0;if-
190     map:content:resource:metadata-type"
191     DataType="http://www.w3.org/2001/XMLSchema#string"/>
192 </Match>
```

193

194 2.2.3 Identifier-Type

195 The Identifier-Type value MUST be designated with the following attribute identifier:

196 urn:oasis:names:tc:xacml:3.0;if-map:content:resource:identifier-type

197 The DataType of this attribute is <http://www.w3.org/2001/XMLSchema#string>

198 [XMLSHEMA11-2].

199

200 The following applies to these IF-MAP identifier types:

- 201 • **Extended identifier types** MUST be of the form **NAMESPACE#ELEMENT-NAME**, in which
202 *NAMESPACE* represents the URI of the extended identifier's XML schema and *ELEMENT-NAME*
203 represents the XML element name within the schema. This attribute MUST be present in a
204 decision request if the MAP Client request is not *purgePublisher*.

205

- 206 • **Original identifier types** MUST denote the type of identifier. Example values are *access-request*, *identity*, *device*, *ip-address*, and *mac-address*.

209 The following applies to decision requests associated with:

- 210 • An **identifier**. Then the *identifier-type* attribute MUST denote the type of identifier. Example
211 values are *access-request*, *identity*, *device*, *ip-address*, and *mac-address*.
- 212 • A **link**. Then the attribute *identifier-type* attribute MUST have two values denoting the types of the
213 two identifiers, with the exception of a link between two identifiers of the same identifier type, in
214 which case the *identifier-type* attribute MUST have one value.

217 **Example 4**

218 The following is an example of an identity-type attribute in a target match:

```
219 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
220   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
221     >ip-address</AttributeValue>  
222   <AttributeDesignator  
223     MustBePresent="false"  
224     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"  
225     AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
226       map:content:resource:identifier-type"  
227     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
228 </Match>
```

231 **2.2.4 Is-Map-Client-Identifier**

232 The Is-Map-Client-Identifier value MUST be designated with the following attribute identifier:

```
233   urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-map-client-  
234     identifier
```

235 The **DataType** of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>
236 [XMLSCHEMA11-2]. This attribute indicates a MAP client identifier if and only if one or both identifiers in
237 the request has the form of a MAP Client identifier in which case the value MUST be set to *true* if all of
238 the following are true, otherwise the value MUST be set to *false* or omit the attribute altogether:

- 239 • The identifier is not extended.
240 • Its identifier-type is “identity”.
241 • Its administrative-domain is ifmap:client.

243 This attribute MUST be present if the MAP Client request is not *purgePublisher*.

245 **Example 5**

246 The following is an example of an is-map-client-identifier attribute in a target match:

```
247 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">  
248   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"  
249     >true</AttributeValue>  
250   <AttributeDesignator  
251     MustBePresent="true"  
252     Category="urn:oasis:names:tc:xacml:3.0:attribute-  
253       category:resource"
```

```
254     AttributeId="urn:oasis:names:tc:xacml:3.0:if-
255 map:content:resource:is-map-client-identifier"
256     DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
257 </Match>
```

258

259 **2.2.5 Is-Self-Identifier**

260 The Is-Self-Identifier value MUST be designated with the following attribute identifier:

```
261     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-self-
262 identifier
```

263 The DataType of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>
264 [XMLSCHEMA11-2]. This attribute indicates whether the identifier of the resource is the self-identifier of
265 the subject MAP Client and it MUST be true if and only if one or both identifiers in the request are the
266 subject MAP Client., otherwise it MUST be set to false or omitted altogether. This attribute MUST be
267 present if the MAP Client request is not *purgePublisher*.

268

269 **Example 6**

270 The following is an example of the is-self-identifier attribute in a target match in which one identifier
271 MUST be the subjects MAP Clients self-identifier:

```
272 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
273     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">
274         >true</AttributeValue>
275     <AttributeDesignator
276         MustBePresent="false"
277         Category="urn:oasis:names:tc:xacml:3.0:attribute-
278 category:resource"
279         AttributeId="urn:oasis:names:tc:xacml:3.0:if-
280 map:content:resource:is-self-identifier"
281         DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
282 </Match>
```

283

284 **2.2.6 On-Link**

285 The On-Link value MUST be designated with the following attribute identifier:

```
286     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:on-link
```

287 The DataType of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>
288 [XMLSCHEMA11-2]. This attribute indicates that the metadata item is or will be attached to a *link*, if set to
289 *true*. If *false*, this attribute indicates that the metadata item is attached to an *identifier*. This attribute
290 MUST be present if the MAP Client request is not *purgePublisher*.

291

292 **Example 7**

293 The following is an example of the on-link attribute in a target match. The attribute value of *true*
294 indicates that the metadata item is or will be attached to a link:

```
295 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
296     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean">
297         >true</AttributeValue>
298     <AttributeDesignator
299         MustBePresent="false"
300         Category="urn:oasis:names:tc:xacml:3.0:attribute-
301 category:resource"
```

```
302     AttributeId="urn:oasis:names:tc:xacml:3.0:if-
303     map:content:resource:on-link"
304         DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
305     </Match>
306
307
```

308 **2.2.7 Metadata-Attribute**

309 The family of Metadata-Attribute values MUST be designated with the following attribute identifier:

```
310     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-
311     attribute
```

312 The **DataType** of this attribute is <http://www.w3.org/2001/XMLSchema#string> [XMLSCHEMA11-2]. This attribute denotes the name of a top-level attribute and MUST be extended to have the form:

```
315     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-
316     attribute:ATTR
```

317 In which **ATTR** is replaced by the name of a top-level attribute of the metadata item.

318

319 **Example 8**

320 Example URN values in the attribute family are:

```
321     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-
322     attribute:name
323     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-
324     attribute:administrative-domain
```

325

326 The following conditions apply:

- 327 • The value of the XACML attribute MUST be the value of the top-level attribute of the metadata item.
- 329 • If the IF-MAP metadata item does not have a top-level attribute named ATTR, then the XACML attribute corresponding to ATTR MUST NOT be present.
- 331 • The attribute MUST be included if Content Selector [TNC-MAP-Authz, Section 3.5.5 Content Selector] chooses it, otherwise it MAY be included.

333

334 **Example 9**

335 The following is an example of a VariableDefinition in which the metadata-attribute **name** attribute needs to match the name of an Overlay Network that the MAP Client is a member of:

```
337 <VariableDefinition VariableId="metadata-name-matches-subject-
338 backhaul-interface">
339     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-
340     in">
341         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
342     one-and-only">
343             <AttributeDesignator
344                 MustBePresent="true"
345                 Category="urn:oasis:names:tc:xacml:3.0:attribute-
346                 category:resource"
347                 AttributeId="urn:oasis:names:tc:xacml:3.0:if-
348                 map:content:resource:metadata-attribute:name"
349                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
350         </Apply>
```

```
351
352     <AttributeDesignator
353         MustBePresent="false"
354         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
355         subject"
356         AttributeId="urn:oasis:names:tc:xacml:3.0:if-
357         map:content:subject:member-
358         of:http%3A//www.trustedcomputinggroup.org/2010/IFMAP-ICS-
359         METADATA/1#overlay-network-group"
360         DataType="http://www.w3.org/2001/XMLSchema#string"/>
361     </Apply>
362 </VariableDefinition>>
363
```

364 2.2.8 Identifier Attribute

365 The family of *identifier-attribute* values MUST be prefixed with the following attribute identifier:

```
366     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-
367     attribute
```

368 This attribute denotes the top-level attribute of the IF-MAP identifier and MUST be extended to have the
369 form:

```
370     urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-
371     attribute:IDENTIFIER-TYPE:ATTR
```

372 In which **IDENTIFIER-TYPE** is the type string of an identifier in a decision request and **ATTR** is replaced
373 by the top-level attribute of the identifier. The value of the XACML attribute MUST be the value of the top-
374 level attribute of the metadata item. Both IDENTIFIER-TYPE and ATTR *MUST* be *URL encoded*.

375 The following conditions apply to a link between two identifiers of the same type in which both identifiers
376 have the attribute ATTR:

- 377 • The decision request attribute MUST have two values if the values for ATTR are not equal
378 [XACML1, Section A14.1 Equality predicates].
- 379 • The decision request attribute MUST have one value if the values for ATTR are equal [XACML1,
380 Section A14.1 Equality predicates].

381

382 The DataType of this attribute MUST be <http://www.w3.org/2001/XMLSchema#string>
383 [XMLSCHEMA11-2] except for the following cases:

384

- 385 1.) The DataType of this attribute is [urn:oasis:names:tc:xacml:2.0:data-
386 type:ipAddress](urn:oasis:names:tc:xacml:2.0:data-type:ipAddress) if both of the following are true:
 - 387 a. The identifier's type is *ip-address*.
 - 388 b. The ATTR extension is *value*.
- 389 2.) The DataType of this attribute is <urn:oasis:names:tc:xacml:1.0:data-type:x500Name>
390 if all of the following are true:
 - 392 a. The identifier's type is *identity*.
 - 393 b. The identity *subtype* is *x500Name*.
 - 394 c. The ATTR extension is *name*.
- 395 3.) The DataType of this attribute is <urn:oasis:names:tc:xacml:2.0:data-type:dnsName>
396 if all of the following is true:

398 a. The identifier's type is *identity*.
399 b. The identity *subtype* is dns-name
400 c. The ATTR extension is *name*.
401
402 This attribute MUST NOT be present in the decision request unless the identifier has a top-level attribute
403 named ATTR, or ATTR is administrative-domain. If ATTR is administrative-domain and the identifier has
404 no administrative-domain attribute, then the attribute value MUST be an empty string.

405

406 **Example 10**

407 The following is an example of a target match in which the *identity* (IDENTIFIER-TYPE) type (ATTR)
408 MUST match the identity type hip-hit, which is the Host Identity Protocol (HIP), Host Identity Tag
409 (HIT):

```
410 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
411   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
412     >hip-hit</AttributeValue>  
413   <AttributeDesignator  
414     MustBePresent="true"  
415     Category="urn:oasis:names:tc:xacml:3.0:attribute-  
416     category:resource"  
417     AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:  
418     identifier-attribute:identity:type"  
419     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
420 </Match>>
```

421

422 **2.3 Action Attributes**

423 **2.3.1 Action-Id**

424 The Action-Id value MUST be designated with the following attribute identifier:

```
425   urn:oasis:names:tc:xacml:1.0:action:action-id
```

426 The DataType of this attribute is <http://www.w3.org/2001/XMLSchema#string>
427 [XMLSCHEMA11-2]. This attribute indicates that the MAP Client is requesting to *read* or *write* metadata
428 in the MAP database and MUST be present in the decision request. If the MAP Client request type to the
429 MAP server is either *search* or *subscribe* then this attribute's value MUST be *read*, otherwise it MUST be
430 *write*.

431

432 **Example 11**

433 The following is an example of a target match in which the MAP Client is allowed to read metadata in
434 the MAP database:

```
435 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
436   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
437     >read</AttributeValue>  
438   <AttributeDesignator  
439     MustBePresent="false"  
440     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
441     AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"  
442     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
443 </Match>
```

444

445 **2.3.2 Request-Type**

446 The Request-Type value MUST be designated with the following attribute identifier:

447 urn:oasis:names:tc:xacml:3.0:if-map:content:action:request-type

448 The DataType of this attribute is <http://www.w3.org/2001/XMLSchema#string>

449 [XMLSCHEMA11-2]. This attribute denotes the IF-MAP request type that is sent to the MAP server and
450 MUST have one of the following values: *publish*, *subscribe*, *search*, or *purgePublisher*

451

452 **Example 12**

453 The following is an example of a target match in which the request type is *purgePublisher*:

```
454 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
455   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
456     >purgePublisher</AttributeValue>
457   <AttributeDesignator
458     MustBePresent="false"
459     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
460     AttributeId="urn:oasis:names:tc:xacml:3.0:if-
461       map:content:action:request-type"
462     DataType="http://www.w3.org/2001/XMLSchema#string"/>
463 </Match>
```

464

465

466 **2.3.3 Purge-Own-Metadata**

467 The Purge-Own-Metadata value MUST be designated with the following attribute identifier:

468 urn:oasis:names:tc:xacml:3.0:if-map:content:action:purge-own-metadata

469 The DataType of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>

470 [XMLSCHEMA11-2]. This attribute denotes whether the MAP Client is attempting to purge its own
471 metadata items or metadata items published by another MAP Client. This attribute value is true if purging
472 its own metadata; otherwise the value is *false*:

473

474 **Example 13**

475 The following is an example of a target match in which a MAP Client may purge its own metadata:

```
476 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
477   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
478     >true</AttributeValue>
479   <AttributeDesignator
480     MustBePresent="false"
481     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
482     AttributeId="urn:oasis:names:tc:xacml:3.0:if-
483       map:content:action:purge-own-metadata"
484     DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
485 </Match>
```

486

487 **2.3.4 Publish-Request-Subtype**

488 The Publish-Request-Subtype value MUST be designated with the following attribute identifier:

489 urn:oasis:names:tc:xacml:3.0:if-map:content:action:publish-request-
490 subtype

491 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#string>
492 [XMLSHEMA11-2]. This attribute denotes the type of an operation within an IF-MAP *publish* request and
493 MUST have one of the following values: *update*, *notify*, or *delete*. This attribute MUST be present in the
494 decision request if, and only if, the IF-MAP request type is *publish*.

495

496 Example 14

497 The following is an example of a target match in which the IF-MAP publish request operation is
498 *notify*:

```
499 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
500   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
501     >notify</AttributeValue>  
502   <AttributeDesignator  
503     MustBePresent="false"  
504     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
505     AttributeId=" urn:oasis:names:tc:xacml:3.0:if-  
506       map:content:action:publish-request-subtype"  
507       DataType="http://www.w3.org/2001/XMLSchema#string"/>  
508 </Match>
```

509

510 2.4 Environment Attributes

511 2.4.1 Dry-Run

512 The Dry-Run value MUST be designated with the following attribute identifier:

```
513   urn:oasis:names:tc:xacml:3.0:if-map:content:environment:dry-run
```

514 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>
515 [XMLSHEMA11-2]. This attribute MUST be a singleton (bag of one) and MUST be present. A dry-run
516 PolicySet allows MAP administrators to test new PolicySets before they are used in a production
517 environment. A second use of dry-run policies is to allow for monitoring of certain activities. The value of
518 *true* indicates the use of a dry-run PolicySet. The value of *false* indicates that a dry-run PolicySet will not
519 be used.

520

521 Example 15

522 The following is an example of a target match that checks for a dry run:

```
523 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">  
524   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"  
525     >true</AttributeValue>  
526   <AttributeDesignator  
527     MustBePresent="false"  
528     Category="urn:oasis:names:tc:xacml:3.0:attribute-  
529       category:environment"  
530     AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
531       map:content:environment:dry-run"  
532     DataType="http://www.w3.org/2001/XMLSchema#boolean"/>  
533 </Match>
```

534

535

536 **2.5 Obligation Caching**

537 **2.5.1 Overview**

538

539 The <Obligation> element will be used in the XACML response to notify the requestor that an additional
540 processing requirement is needed if the obligation's *FulfillOn* attribute is *Permit*. This profile defines an
541 obligation that indicates when a MAP server is required to cache an XACML decision for no more than a
542 specified period of time. Each *caching* obligation MUST contain exactly one *maximum-policy-lag*
543 attribute. In the case where the XACML response contains two or more caching obligations, then the
544 *caching* obligation with the shortest *maximum-policy-lag* attribute value MUST be used.

545 The Caching Obligation MUST be designated with the following identifier:

546 urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:caching

547 **2.5.2 Maximum-Policy-Lag**

548 The *maximum-policy-lag* value MUST be designated with the following identifier:

549 urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:maximum-policy-
550 lag

551 The *maximum-policy-lag* attribute indicates the maximum length of time, in seconds, that a MAP server
552 can cache an XACML decision before new XACML request will need to be made. The *DataType* of this
553 attribute is <http://www.w3.org/2001/XMLSchema#integer> [XMLSCHEMA11-2], in which its value MUST
554 be a nonnegative integer.

555

556 **Example 16**

557 The following is an example of a caching obligation:

```
558 <ObligationExpressions>
559   <ObligationExpression
560     ObligationId="urn:oasis:names:tc:xacml:3.0:if-
561     map:content:obligation:caching"
562     FulfillOn="Permit">
563       <AttributeAssignmentExpression
564         AttributeId="urn:oasis:names:tc:xacml:3.0:if-
565         map:content:obligation:maximum-policy-lag">
566           <AttributeValue
567             DataType="http://www.w3.org/2001/XMLSchema#integer"
568             >60</AttributeValue>
569           </AttributeAssignmentExpression>
570         </ObligationExpression>
571   </ObligationExpressions>
```

572 **3 Profile Identifier**

573 The following identifier MUST be used as the identifier for this profile when an identifier in the form of a
574 URI is required.

575 `urn:oasis:names:tc:xacml:3.0:if-map:content`

576

4 Conformance

577

4.1 Overview

578 Conformance to [xacml-map-authz-v1.0] is defined for **policies** and **requests** generated and transmitted
579 within and between XACML systems.

580

4.2 Attribute Identifiers

581 Conformant XACML **policies** and **requests** MUST use the attribute identifiers defined in Section 2 for
582 their specified purpose and MUST NOT use any other identifiers for the purposes defined by attributes in
583 this profile. The following table lists the attributes that MUST be supported.

584

urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role
urn:oasis:names:tc:xacml:3.0:if-map:content:subject:task: <i>RELATIONSHIP:IDENTIFIER-TYPE</i>
urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-type
urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-type
urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-map-client- identifier
urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-self-identifier
urn:oasis:names:tc:xacml:3.0:if-map:content:resource:on-link
urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata- attribute:ATTR
urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier- attribute:IDENTIFIER-TYPE:ATTR
urn:oasis:names:tc:xacml:3.0:if-map:content:action:request-type
urn:oasis:names:tc:xacml:3.0:if-map:content:action:purge-own-metadata
urn:oasis:names:tc:xacml:3.0:if-map:content:action:publish-request- subtype
urn:oasis:names:tc:xacml:3.0:if-map:content:environment:dry-run

urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:caching

urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:maximum-policy-lag

585 4.3 Attribute Values

586 XACML **policies** and **requests**, that conform to [xacml-map-authz-v1.0], MUST use attribute values in
587 the specified range or patterns as defined for each attribute in Section 2 of this document (when a range
588 or pattern is specified).

589 NOTE (non-normative): In order to correctly process XACML **policies** and **requests**, that
590 conform to [xacml-map-authz-v1.0], **PIP** and **PEP** modules may need to translate native data
591 values into the datatypes and formats specified in [xacml-map-authz-v1.0].

592 Appendix A. Acknowledgements

593 {Non-normative}

594 The following individuals have participated in the creation of this specification and are gratefully
595 acknowledged:

596 Participants:

597 Richard Hill, The Boeing Company
598 John Tolbert, The Boeing Company
599 Steve Venema, The Boeing Company
600 Stephen Hatch, The Boeing Company
601 Nancy Cam-Winget, Cisco Systems
602 Arne Welzel, FHH
603 Josef von Helden, FHH
604 James Tan, Infoblox
605 David Vigier, Infoblox
606 Stu Bailey, Infoblox
607 Navin Boddu, Infoblox
608 Steve Hanna, Juniper
609 Clifford Kahn, Juniper
610 Lisa Lorenzin, Juniper
611 Venkata Srikanth Damaraju, Juniper
612 Atul Shah, Microsoft
613 Trevor Freeman, Microsoft
614 Charles Schmidt, The Mitre Corporation
615 Steven Legg, ViewDS

616 617 Committee members during profile development:

Person	Organization	Role
David Brossard	Axiomatics	Member
Gerry Gebel	Axiomatics	Member
Srijith Nair	Axiomatics	Member
Erik Rissanen	Axiomatics	Member
Richard Skedd	BAE SYSTEMS plc	Member
Abbie Barbir	Bank of America	Member
Radu Marian	Bank of America	Member
Rakesh Radhakrishnan	Bank of America	Member
Ronald Jacobson	CA Technologies	Member
Masum Hasan	Cisco Systems	Member
Anil Tappetla	Cisco Systems	Member
Robert van Herk	Connectis	Member
Danny Thorpe	Dell	Voting Member
Gareth Richards	EMC	Member
Remon Sinnema	EMC	Voting Member
Matt Crooke	First Point Global Pty Ltd.	Member
Allan Foster	Forgerock Inc.	Member

Michiharu Kudo	IBM	Member
Sridhar Muppidi	IBM	Member
Vernon Murdoch	IBM	Member
Nataraj Nagaratnam	IBM	Member
Gregory Neven	IBM	Member
Franz-Stefan Preiss	IBM	Member
Ron Williams	IBM	Member
David Chadwick	Individual	Member
David Choy	Individual	Member
Bill Parducci*	Individual	Chair
Mike Schmidt	Individual	Member
David Laurance	JPMorgan Chase Bank, N.A.	Member
Eliot Solomon	JPMorgan Chase Bank, N.A.	Member
Thomas Hardjono	M.I.T.	Member
Anthony Nadalin	Microsoft	Member
Vishwesh Bavadekar	NextLabs, Inc.	Member
Andy Han	NextLabs, Inc.	Member
Naomaru Itoi	NextLabs, Inc.	Member
Arun Shah	OpenIAM, LLC	Member
Kamalendu Biswas	Oracle	Member
Willem de Pater	Oracle	Member
Rich Levinson	Oracle	Secretary
Hal Lockhart	Oracle	Chair
Prateek Mishra	Oracle	Member
Sid Mishra	Oracle	Member
Roger Wigenstam	Oracle	Member
YanJiong WANG	Primeton Technologies, Inc.	Member
Kenneth Peeples	Red Hat	Member
Anil Saldhana	Red Hat	Member
Darran Rolls	SailPoint Technologies	Member
Jan Herrmann	Siemens AG	Member
Crystal Hayes	The Boeing Company	Voting Member
Richard Hill	The Boeing Company	Voting Member
Greg Smith	The Boeing Company	Member
John Tolbert	The Boeing Company	Voting Member
Bernard Butler	TSSG	Member
Steven Davy	TSSG	Member
Martin Smith	US Department of Homeland Security	Member
John Davis	Veterans Health Administration	Member

Duane DeCouteau	Veterans Health Administration	Member
Mohammad Jafari	Veterans Health Administration	Voting Member
David Staggs	Veterans Health Administration	Member
Gil Kirkpatrick	ViewDS	Member
Steven Legg	ViewDS	Voting Member
Johann Nallathamby	WSO2	Member
Asela Pathberiya	WSO2	Member
Prabath Siriwardena	WSO2	Member

618

619 Appendix B. Revision History

620 {Non-normative}

621

Revision	Date	Editor	Changes Made
WD 1	5/2/2013	Richard Hill, John Tolbert,	Initial committee draft.
WD 2	7/15/2013	Richard Hill, John Tolbert	Updated to reflect changes in the TNC MAP Content Authorization v31 specification. Added figure 2 Added definitions to Glossary, Added Non-Normative Reference Added subject task attribute Added attribute examples Removed delete-metadata-by-other-client attribute Added purge-own-metadata attribute
WD 3	10/28/2013	Richard Hill, John Tolbert, Steven Legg	Addressed comments from WD 2 review. Updated to reflect changes in the TNC MAP Content Authorization v33 specification. Added Caching Obligation Updated Appendix A. Acknowledgements
WD 4	11/12/2013	Richard Hill, John Tolbert, Steven Legg	Addressed comments from WD 3 review.
WD 5	2/23/2014	Richard Hill	Addressed OASIS TAB comments from the CSPRD01 30 day review.

622