



XACML MAP Authorization Profile Version 1.0

Committee Specification Draft 01 / Public Review Draft 01

14 November 2013

Specification URIs

This 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>

Previous version:

N/A

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.w.tolbert@boeing.com), The Boeing Company

Steve Legg (steven.legg@viewds.com), ViewDS

Related work:

This specification is related to:

- *eXtensible Access Control Markup Language (XACML) Version 3.0*. 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 OASIS eXtensible Access Control Markup Language (XACML) TC 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.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://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 (<http://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. 14 November 2013. OASIS Committee Specification Draft 01 / Public Review Draft 01. <http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v1.0-csprd01.html>.

Notices

Copyright © OASIS Open 2013. 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 <http://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

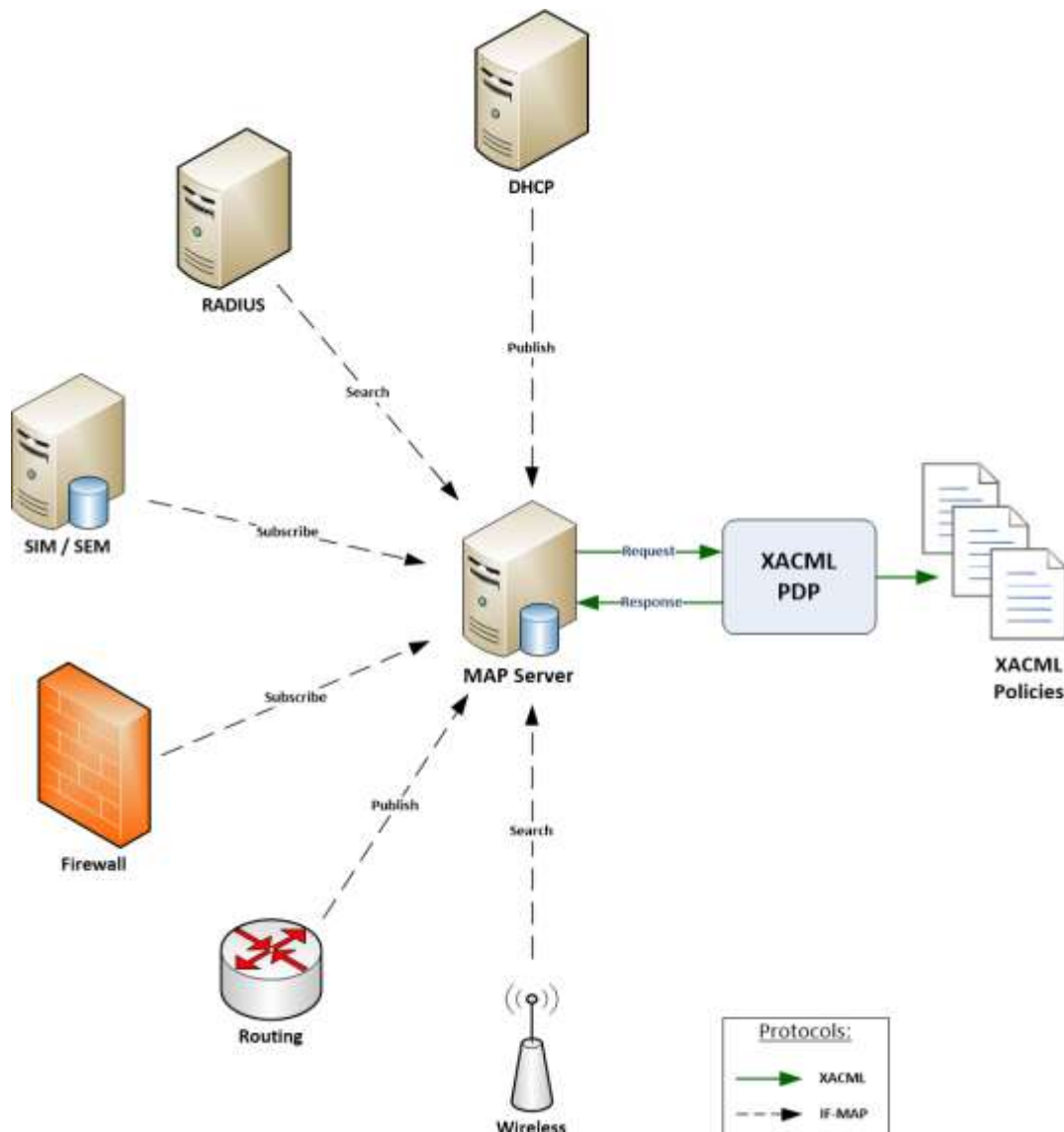
Table of Contents

1	Introduction.....	5
1.1	Glossary.....	6
1.2	Terminology.....	7
1.3	Normative References.....	8
1.4	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.....	9
2.2.1	Metadata-Type.....	10
2.2.2	Identifier-Type.....	10
2.2.3	Is-Map-Client-Identifier.....	11
2.2.4	Is-Self-Identifier.....	11
2.2.5	On-Link.....	12
2.2.6	Metadata-Attribute.....	12
2.2.7	Identifier Attribute.....	13
2.3	Action Attributes.....	15
2.3.1	Action-Id.....	15
2.3.2	Request-Type.....	15
2.3.3	Purge-Own-Metadata.....	15
2.3.4	Publish-Request-Subtype.....	16
2.4	Environment Attributes.....	16
2.4.1	Dry-Run.....	16
2.5	Obligation Caching.....	17
2.5.1	Maximum-Policy-Lag.....	17
3	Identifiers.....	18
3.1	Profile Identifier.....	18
4	Conformance.....	19
4.1	Attribute Identifiers.....	19
4.2	Attribute Values.....	20
Appendix A.	Acknowledgements.....	21
Appendix B.	Revision History.....	24

1 Introduction

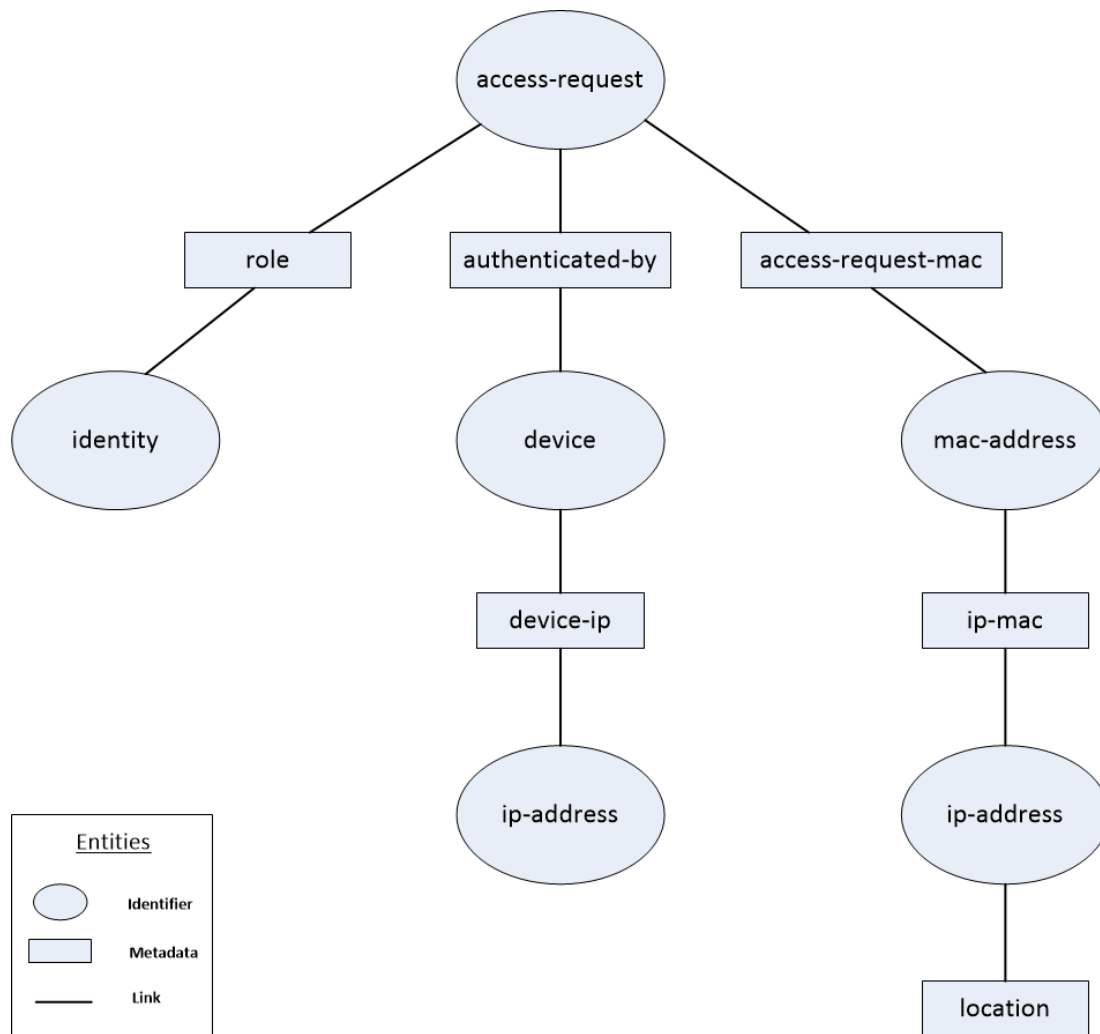
{Non-normative}

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



16

17 *Figure 1: Example MAP – XACML scenario*



18
19 *Figure 2: Example labeled graph representation of an IF-MAP data model*

20
21 **1.1 Glossary**

22 **Administrative-Domain**

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

25 **Content Selector**

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

28 **Extended Identifier**

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

31 **IF-MAP**

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

34 **Identifier**

35 An identifier is an XML element, in which the IF-MAP interface specification defines a set of
36 identifiers, or namespace that can be used to reference metadata items and represents a globally
37 unique label of a node within the undirected, labeled graph representation of the IF-MAP data
38 model.

39 **Link**

40 Within the undirected, labeled graph representation of the IF-MAP data model, links represent the
41 graph's edges and contains information about the relationship between two identifiers.

42 **MAP**

43 Metadata Access Point (MAP) is a server that provides device, user, and network flow state
44 information to IF-MAP clients.

45 **Metadata Item**

46 A metadata item is an XML element which is the basic unit of content that can be attached to
47 identifiers or links within the undirected, labeled graph representation of the IF-MAP data model.

48 **NAC**

49 Network Access Control. A unified set of network technologies and protocols to provide policy
50 based network access controls.

51 **Original Identifier**

52 One of two classes of identifier for network-oriented elements. The 5 original identifier types are:
53 access-request, device, identity, ip-address, and mac-address.

54 **purgePublisher**

55 A purgePublisher request is sent by a MAP client and is typically used to remove its own
56 published data from the MAP server.

57 **publisher-id**

58 A publisher-id is an attribute of a metadata item that indicates which IF-MAP client published the
59 metadata to the MAP server.

60 **Publish Request Subtype**

61 Each publish request is a sequence of operations. Each operation has a publish subtype *update*,
62 *notify* or *delete*.

63 **Self-Identifier**

64 A MAP client's identity identifier with the administrative-domain "ifmap:client".

65 **TCG**

66 Trusted Computing Group is a standards organization that defines and promotes open, vendor-
67 neutral standards for trusted computing platforms.

68 **TNC**

69 Trusted Network Connect is a working group of TCG that defines open architecture protocol
70 specifications for network endpoint integrity and security.

71 **Top-level attribute**

72 An XML attribute of the root element of an XML document. Metadata items and extended
73 identifiers are expressed in XML documents.

74

75 **1.2 Terminology**

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

79 **1.3 Normative References**

80 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
81 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
82

83 **[TNC-IF-MAP]** TNC IF-MAP Binding for SOAP, version 2.1
84 [http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_s](http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification)
85 [pecification](http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification)
86

87 **[TNC-MAP-Authz]** MAP Content Authorization, version 1.0
88 http://www.trustedcomputinggroup.org/resources/tnc_map_content_authorization
89

90 **[XACML3]** OASIS Standard, "eXtensible Access Control Markup Language (XACML)
91 Version 3.0", January 2013. [http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-](http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.doc)
92 [spec-en.doc](http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.doc)
93

94 **[XACML2]** OASIS Standard, "eXtensible Access Control Markup Language (XACML)
95 Version 2.0", February 2005. [http://docs.oasis-](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)
96 [open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)
97

98 **[XACML1]** OASIS Standard, "eXtensible Access Control Markup Language (XACML)
99 Version 1.0", February 2003. [http://www.oasis-](http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf)
100 [open.org/committees/download.php/2406/oasis-xacml-1.0.pdf](http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf)
101

102 **1.4 Non-Normative References**

103 **[XACMLIntro]** OASIS XACML TC, *A Brief Introduction to XACML*, 14 March 2003,
104 [http://www.oasis-](http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html)
105 [open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html](http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html)
106
107
108

109 2 Profile

110 2.1 Subject Attributes

111 2.1.1 Role

112 The IF-MAP client role values shall be designated with the following attribute identifier:

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

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

115 This attribute shall denote the role assigned to the MAP client's session and MUST be omitted if the
116 session has no roles. Role names beginning with "ifmap:" or "tcg:" are reserved and MUST only be used
117 in accordance to the TCG specifications. Please see the TCG MAP Content Authorization specification
118 for a list of pre-defined roles, as well as roles derived from metadata, LDAP groups or certificates. It is
119 RECOMMENDED to use URNs when defining roles to avoid role conflicts.

120

121 The following is an example of a role attribute in which the IF-MAP client is a TNC Flow Controller, such
122 as a firewall, in a target match:

```
123 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
124   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
125     >tcg:flow-controller</AttributeValue>  
126   <AttributeDesignator  
127     MustBePresent="false"  
128     Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"  
129     AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role"  
130     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
131 </Match>
```

132

133 2.1.2 Task

134 The IF-MAP client task values shall be designated with the following attribute identifier:

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

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

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

140

141 The following is an example of an attribute identifier:

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

145

146 2.2 Resource Attributes

147 For an IF-MAP publish request, each metadata item in the publish request is treated as a resource. Each
148 attribute defined in this section refers to a metadata item or identifier found in the MAP database.

149 When a MAP Server retrieves data for a MAP Client, in response to a search or subscribe request, each
150 metadata item in the MAP database is treated as a resource. In that context, each attribute defined in this

151 section refers to a metadata item or identifier within the MAP database. For an IF-MAP purgePublisher
152 request, the decision request MUST NOT include attributes defined in this section.

153 2.2.1 Metadata-Type

154 The Metadata-Type value shall be designated with the following attribute identifier:

155 `urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-type`

156 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#string>. This attribute
157 denotes the type of the metadata item. The value of this attribute must be of the form
158 **NAMESPACE#TYPE**, in which *NAMESPACE* represents the URI of the meta namespace and *TYPE*
159 represents the top-level XML element name to the right of *the prefix*. This attribute MUST be a singleton
160 and MUST be present if the IF-MAP client request is not *purgePublisher*.

161

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

```
163 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
164   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
165     >http://www.trustedcomputinggroup.org/2010/IFMAP-METADATA/2#device-  
166   ip</AttributeValue>  
167   <AttributeDesignator  
168     MustBePresent="false"  
169     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"  
170     AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
171     map:content:resource:metadata-type"  
172     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
173 </Match>
```

174

175 2.2.2 Identifier-Type

176 The Identifier-Type value shall be designated with the following attribute identifier:

177 `urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-type`

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

179

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

- 181 • **Extended identifier types** MUST be of the form **NAMESPACE#ELEMENT-NAME**, in which
182 *NAMESPACE* represents the URI of the extended identifier's XML schema and *ELEMENT-NAME*
183 represents the XML element name within the schema. This attribute MUST be present in a
184 decision request if the IF-MAP client request is not *purgePublisher*.
185
- 186 • **Original identifier types** MUST denote the type of identifier. Example values are *access-*
187 *request*, *identity*, *device*, *ip-address*, and *mac-address*.

188

189 The following applies to decision requests associated with:

- 190 • An **identifier**. Then the *identifier-type* attribute SHALL denote the type of identifier. Example
191 values are *access-request*, *identity*, *device*, *ip-address*, and *mac-address*.
192
- 193 • A **link**. Then the attribute *identifier-type* attribute SHALL have two values denoting the types of
194 the two identifiers, with the exception of a link between two identifiers of the same identifier type,
195 in which case the *identifier-type* attribute SHALL have one value.

196

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

```
198 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
199   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
```

```
200     >ip-address</AttributeValue>
201     <AttributeDesignator
202       MustBePresent="false"
203       Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
204       AttributeId="urn:oasis:names:tc:xacml:3.0:if-
205 map:content:resource:identifier-type"
206       DataType="http://www.w3.org/2001/XMLSchema#string"/>
207 </Match>
```

208
209

210 2.2.3 Is-Map-Client-Identifier

211 The Is-Map-Client-Identifier value shall be designated with the following attribute identifier:

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

214 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>. This attribute
215 indicates a MAP client identifier if and only if one or both identifiers in the request has the form of a MAP
216 Client identifier in which case the value must be set to *true* if all of the following are true, otherwise the
217 value must be set to *false* or omit the attribute altogether:

- 218 • The identifier is not extended.
- 219 • Its identifier-type is "identity".
- 220 • Its administrative-domain is ifmap:client.

221

222 This attribute **MUST** be present if the IF-MAP client request is not *purgePublisher*.

223

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

```
225 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
226   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
227     >true</AttributeValue>
228   <AttributeDesignator
229     MustBePresent="true"
230     Category="urn:oasis:names:tc:xacml:3.0:attribute-
231 category:resource"
232     AttributeId="urn:oasis:names:tc:xacml:3.0:if-
233 map:content:resource:is-map-client-identifier"
234     DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
235 </Match>
```

236

237 2.2.4 Is-Self-Identifier

238 The Is-Self-Identifier value shall be designated with the following attribute identifier:

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

241 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>. This attribute
242 indicates whether the identifier of the resource is the self-identifier of the subject MAP Client and it **MUST**
243 be true if and only if one or both identifiers in the request are the subject MAP Client., otherwise it **MUST**
244 be set to false or omitted altogether. This attribute **MUST** be present if the IF-MAP client request is not
245 *purgePublisher*.

246

247 The following is an example of the is-self-identifier attribute in a target match in which one identifier must
248 be the subjects MAP Clients self-identifier:

```
249 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">  
250   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"  
251     >true</AttributeValue>  
252   <AttributeDesignator  
253     MustBePresent="false"  
254     Category="urn:oasis:names:tc:xacml:3.0:attribute-  
255     category:resource"  
256     AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
257     map:content:resource:is-self-identifier"  
258     DataType="http://www.w3.org/2001/XMLSchema#boolean"/>  
259 </Match>
```

260

261 2.2.5 On-Link

262 The On-Link value shall be designated with the following attribute identifier:

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

264 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>. This attribute
265 indicates that the metadata item is or will be attached to a *link*, if set to *true*. If *false*, this attribute indicates
266 that the metadata item is attached to an *identifier*. This attribute MUST be present if the IF-MAP client
267 request is not *purgePublisher*.

268

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

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

282

283

284 2.2.6 Metadata-Attribute

285 The family of Metadata-Attribute values shall be designated with the following attribute identifier:

```
286 urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-  
287 attribute
```

288 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#string>. This attribute
289 denotes the name of a top-level attribute and MUST be extended to have the form:

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

292 In which **ATTR** is replaced by the name of a top-level attribute of the metadata item. Example URN
293 values in the attribute family are:

```
294 urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-  
295 attribute:name
```

296 urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-
297 attribute:**administrative-domain**

298

299 The following conditions apply:

- 300 • The value of the XACML attribute **MUST** be the value of the top-level attribute of the metadata
301 item.
- 302 • If the IF-MAP metadata item does not have a top-level attribute named **ATTR**, then the XACML
303 attribute corresponding to **ATTR** **MUST NOT** be present.
- 304 • The attribute **MUST** be included if the MAP Content Selector chooses it, otherwise it **MAY** be
305 included.

306

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

```
309 <VariableDefinition VariableId="metadata-name-matches-subject-  
310 backhaul-interface">  
311   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-  
312   in">  
313     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-  
314     one-and-only">  
315       <AttributeDesignator  
316         MustBePresent="true"  
317         Category="urn:oasis:names:tc:xacml:3.0:attribute-  
318         category:resource"  
319         AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
320         map:content:resource:metadata-attribute:name"  
321         DataType="http://www.w3.org/2001/XMLSchema#string"/>  
322       </Apply>  
323     </Apply>  
324     <AttributeDesignator  
325       MustBePresent="false"  
326       Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-  
327       subject"  
328       AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
329       map:content:subject:member-  
330       of:http%3A//www.trustedcomputinggroup.org/2010/IFMAP-ICS-  
331       METADATA/1#overlay-network-group"  
332       DataType="http://www.w3.org/2001/XMLSchema#string"/>  
333     </Apply>  
334   </VariableDefinition>>
```

335

336 2.2.7 Identifier Attribute

337 The family of *identifier-attribute* values shall be prefixed with the following attribute identifier:

338 urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-
339 attribute

340 This attribute denotes the top-level attribute of the IF-MAP identifier and **MUST** be extended to have the
341 form:

342 urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-
343 attribute:IDENTIFIER-TYPE:ATTR

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

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

- 349 • The decision request attribute SHALL have two values if the values for *ATTR* are not equal.
- 350 • The decision request attribute SHALL have one value if the values for *ATTR* are equal.

351

352 The `DataType` of this attribute MUST be <http://www.w3.org/2001/XMLSchema#string> except
353 for the following cases:

354

355 1.) The `DataType` of this attribute is [urn:oasis:names:tc:xacml:2.0:data-](urn:oasis:names:tc:xacml:2.0:data-type:ipAddress)
356 [type:ipAddress](urn:oasis:names:tc:xacml:2.0:data-type:ipAddress) if both of the following are true:

- 357 a. The identifier's type is *ip-address*.
- 358 b. The *ATTR* extension is *value*.

359

360 2.) The `DataType` of this attribute is <urn:oasis:names:tc:xacml:1.0:data-type:x500Name>
361 if all of the following are true:

- 362 a. The identifier's type is *identity*.
- 363 b. The identity *subtype* is *x500Name*.
- 364 c. The *ATTR* extension is *name*.

365

366 3.) The `DataType` of this attribute is <urn:oasis:names:tc:xacml:2.0:data-type:dnsName>
367 if all of the following are true:

- 368 a. The identifier's type is *identity*.
- 369 b. The identity *subtype* is *dns-name*
- 370 c. The *ATTR* extension is *name*.

371

372 This attribute MUST NOT be present in the decision request unless the identifier has a top-level attribute
373 named *ATTR*, or *ATTR* is *administrative-domain*. If *ATTR* is *administrative-domain* and the identifier has
374 no *administrative-domain* attribute, then the attribute value MUST be an empty string.

375

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

```
378 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
379   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
380     >hip-hit</AttributeValue>  
381   <AttributeDesignator  
382     MustBePresent="true"  
383     Category="urn:oasis:names:tc:xacml:3.0:attribute-  
384     category:resource"  
385     AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:  
386     identifier-attribute:identity:type"  
387     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
388 </Match>>
```

389

390 2.3 Action Attributes

391 2.3.1 Action-Id

392 The Action-Id value shall be designated with the following attribute identifier:

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

394 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#string>. This attribute
395 indicates that the IF-MAP client is requesting to *read* or *write* metadata in the MAP database and **MUST**
396 be present in the decision request. If the IF-MAP client request type to the MAP server is either *search* or
397 *subscribe* then this attribute's value **MUST** be *read*, otherwise it **MUST** be *write*.

398

399 The following is an example of a target match in which the IF-MAP Client is allowed to read metadata in
400 the MAP database:

```
401 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
402   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
403     >read</AttributeValue>  
404   <AttributeDesignator  
405     MustBePresent="false"  
406     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
407     AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"  
408     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
409 </Match>
```

410

411 2.3.2 Request-Type

412 The Request-Type value shall be designated with the following attribute identifier:

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

414 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#string>. This attribute
415 denotes the IF-MAP request type that is sent to the MAP server and **MUST** have one of the following
416 values: *publish*, *subscribe*, *search*, or *purgePublisher*

417

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

```
419 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
420   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
421     >purgePublisher</AttributeValue>  
422   <AttributeDesignator  
423     MustBePresent="false"  
424     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
425     AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
426     map:content:action:request-type"  
427     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
428 </Match>
```

429

430

431 2.3.3 Purge-Own-Metadata

432 The Purge-Own-Metadatatype shall be designated with the following attribute identifier:

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

434 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#boolean>. This attribute
435 denotes whether the IF-MAP client is attempting to purge its own metadata items or metadata items

436 published by another IF-MAP client. This attribute value is true if purging its own metadata; otherwise the
437 value is *false*:

438

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

```
440 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">  
441   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"  
442     >true</AttributeValue>  
443   <AttributeDesignator  
444     MustBePresent="false"  
445     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
446     AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
447 map:content:action:purge-own-metadata"  
448     DataType="http://www.w3.org/2001/XMLSchema#boolean"/>  
449 </Match>
```

450

451 2.3.4 Publish-Request-Subtype

452 The Publish-Request-Subtype value shall be designated with the following attribute identifier:

```
453 urn:oasis:names:tc:xacml:3.0:if-map:content:action:publish-request-  
454 subtype
```

455 The `DataType` of this attribute is <http://www.w3.org/2001/XMLSchema#string>. This attribute
456 denotes the type of an operation within an IF-MAP *publish* request and **MUST** have one of the following
457 values: *update*, *notify*, or *delete*. This attribute must be present in the decision request if, and only if, the
458 IF-MAP request type is *publish*.

459

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

```
461 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
462   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"  
463     >notify</AttributeValue>  
464   <AttributeDesignator  
465     MustBePresent="false"  
466     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
467     AttributeId="urn:oasis:names:tc:xacml:3.0:if-  
468 map:content:action:publish-request-subtype"  
469     DataType="http://www.w3.org/2001/XMLSchema#string"/>  
470 </Match>
```

471

472 2.4 Environment Attributes

473 2.4.1 Dry-Run

474 The Dry-Run value shall be designated with the following attribute identifier:

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

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

481

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


```
483 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
484   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
485     >true</AttributeValue>
486   <AttributeDesignator
487     MustBePresent="false"
488     Category="urn:oasis:names:tc:xacml:3.0:attribute-
489 category:environment"
490     AttributeId="urn:oasis:names:tc:xacml:3.0:if-
491 map:content:environment:dry-run"
492     DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
493 </Match>
```

494
495

496 2.5 Obligation Caching

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

503 The Caching Obligation shall be designated with the following identifier:

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

505 2.5.1 Maximum-Policy-Lag

506 The *maximum-policy-lag* value shall be designated with the following identifier:

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

509 The *maximum-policy-lag* attribute indicates the maximum length of time, in seconds, that a MAP server
510 can cache an XACML decision before new XACML request will need to be made. The *DataType* of this
511 attribute is <http://www.w3.org/2001/XMLSchema#integer>, in which its value must be a nonnegative
512 integer.

513

514 The following is an example of a caching obligation:

```
515 <ObligationExpressions>
516   <ObligationExpression
517     ObligationId="urn:oasis:names:tc:xacml:3.0:if-
518 map:content:obligation:caching"
519     FulfillOn="Permit">
520     <AttributeAssignmentExpression
521       AttributeId="urn:oasis:names:tc:xacml:3.0:if-
522 map:content:obligation:maximum-policy-lag">
523       <AttributeValue
524         DataType="http://www.w3.org/2001/XMLSchema#integer"
525         >60</AttributeValue>
526       </AttributeAssignmentExpression>
527     </ObligationExpression>
528 </ObligationExpressions>
```

529 **3 Identifiers**

530 This profile defines the following URN identifiers.

531 **3.1 Profile Identifier**

532 The following identifier SHALL be used as the identifier for this profile when an identifier in the form of a
533 URI is required.

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

535

4 Conformance

536
537

Conformance to this profile is defined for **policies** and **requests** generated and transmitted within and between XACML systems.

538

4.1 Attribute Identifiers

539
540
541

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

542

Note: “M” is mandatory “O” is optional.

543

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

urn:oasis:names:tc:xacml:3.0:if-map:content:environment:dry-run	M
urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:caching	M
urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:maximum-policy-lag	M

544 **4.2 Attribute Values**

545 Conformant XACML *policies* and *requests* SHALL use attribute values in the specified range or patterns
546 as defined for each attribute in Section 2 (when a range or pattern is specified).

547 NOTE: In order to process conformant XACML *policies* and *requests* correctly, *PIP* and
548 *PEP* modules may have to translate native data values into the datatypes and formats
549 specified in this profile.

550 Appendix A. Acknowledgements

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

553 **Participants:**

554 Richard Hill, The Boeing Company
555 John Tolbert, The Boeing Company
556 Steve Venema, The Boeing Company
557 Stephen Hatch, The Boeing Company
558 Nancy Cam-Winget, Cisco Systems
559 Arne Welzel, FHH
560 Josef von Helden, FHH
561 James Tan, Infoblox
562 David Vigier, Infoblox
563 Stu Bailey, Infoblox
564 Navin Boddu, Infoblox
565 Steve Hanna, Juniper
566 Clifford Kahn, Juniper
567 Lisa Lorenzin, Juniper
568 Venkata Srikar Damaraju, Juniper
569 Atul Shah, Microsoft
570 Trevor Freeman, Microsoft
571 Charles Schmidt, The Mitre Corporation
572 Steven Legg, ViewDS

573 **Committee members during profile development:**

574

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 Croke	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

575

576

Appendix B. Revision History

577

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.

578

579