Mode: All
Left file: C:\OASIS\XACML\v3.0\IF-MAP\IF-MAP XACML Profile v5\Diff\xacml-map-authz-v1.0-csprd01.doc
Right file: C:\OASIS\XACML\v3.0\IF-MAP\IF-MAP XACML Profile v5\Diff\xacml-3.0-map-authz-v1.0-wd05.doc

1	1	
2	2	
3	3	XACML MAP Authorization Profile Version 1.0
4		Committee Specification Draft 01 /
5		Public Review Draft 01
6		14 November 2013
	4	Working Draft 05
	5	23 February 2014
7	6	Specification URIs
8	7	This version:
9		HYPERLINK "http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v » 1.0-csprd01.doc"□http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map » -authz-v1.0-csprd01.doc (Authoritative)
10		HYPERLINK "http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v » 1.0-csprd01.html"□http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-ma » p-authz-v1.0-csprd01.html
11		HYPERLINK "http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v » 1.0-csprd01.pdf"□http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/csprd01/xacml-map » -authz-v1.0-csprd01.pdf
	8	http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-3.0-map-authz-v1.0-wd05.doc (A » uthoritative)
	9	http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-3.0-map-authz-v1.0-wd05.html
	10	http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-3.0-map-authz-v1.0-wd05.pdf
12	11	Previous version:
13	12	N/A
14	13	Latest version:
15	14	http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.doc (Authoritat » ive)
16	15	http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.html
17	16	http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.pdf
18	17	Technical Committee:
19	18	OASIS eXtensible Access Control Markup Language (XACML) TC
20	19	Chairs:
21	20	Bill Parducci (bill@parducci.net), Individual
22	21	Hal Lockhart (hal.lockhart@oracle.com), Oracle
23	22	Editors:
24	23	Richard Hill (richard.c.hill@boeing.com), The Boeing Company
25	24	John Tolbert (john.w.tolbert@boeing.com), The Boeing Company
26	25	Steve Legg (steven.legg@viewds.com), ViewDS
27	26	Related work:
28	27	This specification is related to:
29	28	eXtensible Access Control Markup Language (XACML) Version 3.0. Latest version.
30	29	http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html.
31	30	TNC MAP Content Authorization http://www.trustedcomputinggroup.org/resources/tnc_map_cont » ent_authorization
32	31	Abstract:
33	32	This specification defines a profile for the use of XACML in expressing policies for TCG T » NC Metadata Access Points (MAP). It defines standard attribute identifiers useful in suc » h policies, in which a MAP utilizes an XACML PDP to make MAP content authorization decis » ions.
34	33	Status:
35	34	This document was last revised or approved by the OASIS eXtensible Access Control Markup L » anguage (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.
36	35	Technical Committee members should send comments on this specification to the Technical Co

		» mmittee’s email list. Others should send comments to the Technical Committee by using th
		» e “Send A Comment” button on the Technical Committee’s web page at http://www.oasis-open
		» .org/committees/xacml/.
37	36	For information on whether any patents have been disclosed that may be essential to implem
		» enting 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.oa
		» sis-open.org/committees/xacml/ipr.php).
38	37	Citation format:
39	38	When referencing this specification the following citation format should be used:
40	39	[xacml-map-authz-v1.0]
41		XACML MAP Authorization Profile Version 1.0. 14 November 2013. OASIS Committee Specificati
		» on Draft 01 / Public Review Draft 01. HYPERLINK "http://docs.oasis-open.org/xacml/xacml-
		» map-authz/v1.0/csprd01/xacml-map-authz-v1.0-csprd01.html"□http://docs.oasis-open.org/xac
		» ml/xacml-map-authz/v1.0/csprd01/xacml-map-authz-v1.0-csprd01.html.
	40	XACML MAP Authorization Profile Version 1.0. 23 February 2014. Working Draft 05. http://do
		» cs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-3.0-map-authz-v1.0-wd05.html.
42	41	
43	42	Notices
44		Copyright © OASIS Open 2013. All Rights Reserved.
	43	Copyright © OASIS Open 2014. All Rights Reserved.
45	44	All capitalized terms in the following text have the meanings assigned to them in the OASI
		» S Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be f
		» ound at the OASIS website.
46	45	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 pr
		» epared, 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 a
		» ny way, including by removing the copyright notice or references to OASIS, except as nee
		» ded for the purpose of developing any document or deliverable produced by an OASIS Techn
		» ical Committee (in which case the rules applicable to copyrights, as set forth in the OA
		» SIS IPR Policy, must be followed) or as required to translate it into languages other th
		» an English.
47	46	The limited permissions granted above are perpetual and will not be revoked by OASIS or it
		» s successors or assigns.
48	47	This document and the information contained herein is provided on an "AS IS" basis and OAS
		» IS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRAN
		» TY 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.
49	48	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 Specifica
		» tion or OASIS Standard, to notify OASIS TC Administrator and provide an indication of it
		» s 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.
50	49	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 o
		» f 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 dis
		» claims any obligation to do so.
51	50	OASIS takes no position regarding the validity or scope of any intellectual property or ot
		» her rights that might be claimed to pertain to the implementation or use of the technolo
		» gy 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 ide
		» ntify any such rights. Information on OASIS' procedures with respect to rights in any do

		» cument 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 o
		» f licenses to be made available, or the result of an attempt made to obtain a general li
		» cense or permission for the use of such proprietary rights by implementers or users of t
		» his OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC A
		» dministrator. 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 f
		» act, Essential Claims.
52	51	The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, a
		» nd should be used only to refer to the organization and its official outputs. OASIS welc
		» omes reference to, and implementation and use of, specifications, while reserving the ri
		» ght to enforce its marks against misleading uses. Please see http://www.oasis-open.org/p
		» olicies-guidelines/trademark for above guidance.
53	52	
54	53	Table of Contents
55	54	1 Introduction 5
56		1.1 Glossary 6
57		1.2 Terminology 7
58		1.3 Normative References 8
59		1.4 Non-Normative References 8
	55	1.1 Overview (non-normative) 5
	56	1.2 Glossary 6
	57	1.3 Terminology 8
	58	1.4 Normative References 8
	59	1.5 Non-Normative References 8
60	60	2 Profile 9
61	61	2.1 Subject Attributes 9
62	62	2.1.1 Role 9
63	63	2.1.2 Task 9
64		2.2 Resource Attributes 9
65		2.2.1 Metadata-Type 10
66		2.2.2 Identifier-Type 10
67		2.2.3 Is-Map-Client-Identifier 11
68		2.2.4 Is-Self-Identifier 11
69		2.2.5 On-Link 12
70		2.2.6 Metadata-Attribute 12
71		2.2.7 Identifier Attribute 13
	64	2.2 Resource Attributes 10
	65	2.2.1 Overview 10
	66	2.2.2 Metadata-Type 10
	67	2.2.3 Identifier-Type 10
	68	2.2.4 Is-Map-Client-Identifier 11
	69	2.2.5 Is-Self-Identifier 12
	70	2.2.6 On-Link 12
	71	2.2.7 Metadata-Attribute 13
	72	2.2.8 Identifier Attribute 14
72	73	2.3 Action Attributes 15
73	74	2.3.1 Action-Id 15
74		2.3.2 Request-Type 15
75		2.3.3 Purge-Own-Metadata 15
	75	2.3.2 Request-Type 16
	76	2.3.3 Purge-Own-Metadata 16
76	77	2.3.4 Publish-Request-Subtype 16
77		2.4 Environment Attributes 16
78		2.4.1 Dry-Run 16

79		2.5 Obligation Caching 17
80		2.5.1 Maximum-Policy-Lag 17
81		3 Identifiers 18
82		3.1 Profile Identifier 18
83		4 Conformance 19
84		4.1 Attribute Identifiers 19
85		4.2 Attribute Values 20
86		Appendix A. Acknowledgements 21
87		Appendix B. Revision History 24
	78	2.4 Environment Attributes 17
	79	2.4.1 Dry-Run 17
	80	2.5 Obligation Caching 18
	81	2.5.1 Overview 18
	82	2.5.2 Maximum-Policy-Lag 18
	83	3 Profile Identifier 19
	84	4 Conformance 20
	85	4.1 Overview 20
	86	4.2 Attribute Identifiers 20
	87	4.3 Attribute Values 21
	88	Appendix A. Acknowledgements 22
	89	Appendix B. Revision History 25

88	90	
89	91	
90	92	Introduction
	93	Overview (non-normative)
	94	
91	95	{Non-normative}
92		The Trusted Computing Group (TCG) provides vendor-neutral standards through the Trusted Ne » twork 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 an » d search data events through a Metadata Access Point (MAP) server (see figure 1). The M » AP server stores state information about devices, users, and flows in a network (see fig » ure 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 ca » n perform [TNC-MAP-Authz]. The TNC MAP authorization model defines the use of an XACML P » olicy Decision Point (PDP) when making MAP access control decisions. This profile descri » bes attributes for such decisions between the MAP server and the XACML PDP and is based » on, and aligned with [TNC-MAP-Authz].
	96	The Trusted Computing Group (TCG) provides vendor-neutral standards through the Trusted Ne » twork 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 an » d search data events through a Metadata Access Point (MAP) server (see figure 1). The M » AP server stores state information about devices, users, and flows in a network (see fig » ure 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 a MAP Client can pe » rform [TNC-MAP-Authz]. The TNC MAP authorization model defines the use of an XACML Polic » y 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]. All examples in [xacml-map-authz-v1.0] are non-normati » ve.
93	97	

94	98	
95	99	Figure 1: Example MAP – XACML scenario
96	100	
97	101	Figure 2: Example labeled graph representation of an IF-MAP data model
98	102	
99	103	Glossary
100	104	Administrative-Domain
101	105	A string value defined by an organization as an optional qualifier to prevent name conflic » ts and can be used to group identifiers.
102	106	Content Selector
103	107	A MAP server resource attribute filter that controls which parts of a metadata item or ide » ntifier are used as XACML request attributes.
104	108	Extended Identifier
105	109	One of two classes of identifier that is defined in an external schema, which allow vendor » s and other standards to extend the identifier space for new applications and use cases » for IF-MAP.
106	110	IF-MAP
107	111	The Interface for Metadata Access Points (IF-MAP) is an element of the TNC architecture th » at specifies a standard interface between a MAP and other elements of the TNC architectu » re.
	112	IF-MAP Request
	113	A message sent from a MAP client to a MAP server using the IF-MAP standard client/server p » rotocol. Also see [TNC-MAP-Authz, Section 2.2.3 IF-MAP Requests].
	114	
108	115	Identifier
109	116	An identifier is an XML element, in which the IF-MAP interface specification defines a set » of identifiers, or namespace that can be used to reference metadata items and represent » s a globally unique label of a node within the undirected, labeled graph representation » of the IF-MAP data model.
110	117	Link
111	118	Within the undirected, labeled graph representation of the IF-MAP data model, links repres » ent the graph’s edges and contains information about the relationship between two identi » fiers.
112	119	MAP
113		Metadata Access Point (MAP) is a server that provides device, user, and network flow state » information to IF-MAP clients.
	120	Metadata Access Point (MAP) is a server that provides device, user, and network flow state » information to MAP Clients.
	121	MAP Client
	122	A client to a MAP server [TNC-MAP-Authz, Section 2.2.2 MAP Client].
114	123	Metadata Item
115		A metadata item is an XML element which is the basic unit of content that can be attached » to identifiers or links within the undirected, labeled graph representation of the IF-M » AP data model.
	124	A metadata item is an XML element which is the basic unit of content that can be attached » to identifiers or links within the undirected, labeled graph representation of the IF-MA » P data model.
116	125	NAC
117	126	Network Access Control. A unified set of network technologies and protocols to provide pol » icy based network access controls.
118	127	Original Identifier
119	128	One of two classes of identifier for network-oriented elements. The 5 original identifier » types are: access-request, device, identity, ip-address, and mac-address.
	129	PEP
	130	Policy enforcement point as defined in [XACML3].

	131	PIP
	132	Policy information point as defined in [XACML3].
120	133	purgePublisher
121	134	A purgePublisher request is sent by a MAP client and is typically used to remove its own p » ublished data from the MAP server.
122	135	publisher-id
123		A publisher-id is an attribute of a metadata item that indicates which IF-MAP client publi » shed the metadata to the MAP server.
	136	A publisher-id is an attribute of a metadata item that indicates which MAP Client publishe » d the metadata to the MAP server.
124	137	Publish Request Subtype
125	138	Each publish request is a sequence of operations. Each operation has a publish subtype upd » ate, notify or delete.
126	139	Self-Identifier
127	140	A MAP client’s identity identifier with the administrative-domain “ifmap:client”.
128	141	TCG
129	142	Trusted Computing Group is a standards organization that defines and promotes open, vendor » -neutral standards for trusted computing platforms.
130	143	TNC
131	144	Trusted Network Connect is a working group of TCG that defines open architecture protocol » specifications for network endpoint integrity and security.
132	145	Top-level attribute
133	146	An XML attribute of the root element of an XML document. Metadata items and extended ident » ifiers are expressed in XML documents.
134	147	
135	148	Terminology
136	149	The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT” » , “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as describ » ed in [RFC2119].
137	150	Normative References
138		[RFC2119] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, http » ://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.
	151	[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", B » CP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.
139	152	
140	153	[TNC-IF-MAP] TNC IF-MAP Binding for SOAP, version 2.1
141	154	http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specific » ation
142	155	
143	156	[TNC-MAP-Authz] MAP Content Authorization, version 1.0
144	157	http://www.trustedcomputinggroup.org/resources/tnc_map_c » ontent_authorization
145	158	
146	159	[XACML3] OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version » 3.0", January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.doc
147	160	
148	161	[XACML2] OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version » 2.0", February 2005. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-cor » e-spec-os.pdf
149	162	
150	163	[XACML1] OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version » 1.0", February 2003. http://www.oasis-open.org/committees/download.php/2406/oasis-xac » ml-1.0.pdf
151	164	
	165	[XMLSCHEMA11-2] D. Peterson, S. , A. Malhotra, M. , H. S. Thompson, P. V. Biron, Editors,

		» W3C 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/
152	166	Non-Normative References
153	167	[XACMLIntro] OASIS XACML TC, A Brief Introduction to XACML, 14 March 2003, http://www.o
		» asis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html
154	168	
155	169	
156	170	
157	171	Profile
158	172	Subject Attributes
159	173	Role
160		The IF-MAP client role values shall be designated with the following attribute identifier:
	174	The MAP Client role values MUST be designated with the following attribute identifier:
161	175	urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role
162		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string.
163		This attribute shall denote the role assigned to the MAP client’s session and MUST be omit
		» ted if the session has no roles. Role names beginning with “ifmap:” or “tcg:” are reserv
		» ed and MUST only be used in accordance to the TCG specifications. Please see the TCG MAP
		» Content Authorization specification for a list of pre-defined roles, as well as roles d
		» erived from metadata, LDAP groups or certificates. It is RECOMMENDED to use URNs when de
		» fining roles to avoid role conflicts.
	176	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string [XMLSCHEMA11-2]
		» .
	177	This attribute MUST denote the role assigned to the MAP client’s session and MUST be omitt
		» ed if the session has no roles. Role names beginning with “ifmap:” or “tcg:” are reserve
		» d and MUST only be used in accordance with [TNC-MAP-Authz]. The [TNC-MAP-Authz] specific
		» ation for a list of pre-defined roles, as well as roles derived from metadata, LDAP grou
		» ps or certificates. It is RECOMMENDED to use URNs when defining roles to avoid role conf
		» licts.
164	178	
165		The following is an example of a role attribute in which the IF-MAP client is a TNC Flow C
		» ontroller, such as a firewall, in a target match:
	179	Example 1
	180	The following is an example of a role attribute in which the MAP Client is a TNC Flow Cont
		» roller, such as a firewall, in a target match:
166	181	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
167	182	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
168	183	>tcg:flow-controller</AttributeValue>
169	184	<AttributeDesignator
170	185	MustBePresent="false"
171	186	Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
172	187	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role"
173	188	DataType="http://www.w3.org/2001/XMLSchema#string"/>
174	189	</Match>
175	190	
176	191	Task
177		The IF-MAP client task values shall be designated with the following attribute identifier:
	192	The MAP Client task values MUST be designated with the following attribute identifier:
178	193	urn:oasis:names:tc:xacml:3.0:if-map:content:subject:task:RELATIONSHIP:IDENTIFIER-TYPE
179		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string.
180		This attribute shall denote the task assigned to the MAP client. Both RELATIONSHIP and IDE
		» NTIFIER-TYPE MUST be URL-encoded.
	194	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string [XMLSCHEMA11-2]
		» .
	195	This attribute MUST denote the task assigned to the MAP client. Both RELATIONSHIP and IDEN

		» TIFIER-TYPE MUST be URL-encoded.
181	196	
	197	Example 2
182	198	The following is an example of an attribute identifier:
183	199	urn:oasis:names:tc:xacml:3.0:if-map:content:subject:task:member-of:http%3A//www.trustedcom » putinggroup.org/2010/IFMAP-ICS-METADATA/1#overlay-network-group
184	200	
185	201	Resource Attributes
186		For an IF-MAP publish request, each metadata item in the publish request is treated as a r » esource. Each attribute defined in this section refers to a metadata item or identifier » found in the MAP database.
187		When a MAP Server retrieves data for a MAP Client, in response to a search or subscribe re » quest, each metadata item in the MAP database is treated as a resource. In that context, » each attribute defined in this section refers to a metadata item or identifier within t » he MAP database. For an IF-MAP purgePublisher request, the decision request MUST NOT inc » lude attributes defined in this section.
	202	Overview
	203	
	204	For an IF-MAP publish request, each metadata item in the publish request is treated as a r » esource. Each attribute defined in section 2.2 Resource Attributes refers to a metadata » item or identifier found in the MAP database.
	205	When a MAP Server retrieves data for a MAP Client, in response to a search or subscribe re » quest, each metadata item in the MAP database is treated as a resource. In that context, » each attribute defined in this section refers to a metadata item or identifier within t » he MAP database. For an IF-MAP purgePublisher request, the decision request MUST NOT inc » lude attributes defined in section 2.2 Resource Attributes.
188	206	Metadata-Type
189		The Metadata-Type value shall be designated with the following attribute identifier:
	207	The Metadata-Type value MUST be designated with the following attribute identifier:
190	208	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-type
191		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. This attribute » denotes the type of the metadata item. The value of this attribute must be of the form » NAMESPACE#TYPE, in which NAMESPACE represents the URI of the meta namespace and TYPE rep » resents the top-level XML element name to the right of the prefix. This attribute MUST b » e a singleton and MUST be present if the IF-MAP client request is not purgePublisher.
	209	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string
	210	[XMLSCHEMA11-2]. This attribute denotes the type of the metadata item. The value of this » attribute MUST be of the form NAMESPACE#TYPE, in which NAMESPACE represents the URI of t » he meta namespace and TYPE represents the top-level XML element name to the right of the » prefix. This attribute MUST be a singleton and MUST be present if the MAP Client reques » t is not purgePublisher.
192	211	
	212	Example 3
193	213	The following is an example of a metadata-type attribute in a target match:
194	214	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
195	215	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
196	216	>http://www.trustedcomputinggroup.org/2010/IFMAP-METADATA/2#device-ip</AttributeValue>
197	217	<AttributeDesignator
198	218	MustBePresent="false"
199	219	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
200	220	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-type"
201	221	DataType="http://www.w3.org/2001/XMLSchema#string"/>
202	222	</Match>
203	223	
204	224	Identifier-Type

205		The Identifier-Type value shall be designated with the following attribute identifier:
	225	The Identifier-Type value MUST be designated with the following attribute identifier:
206	226	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-type
207		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string.
	227	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string
	228	[XMLSCHEMA11-2].
208	229	
209	230	The following applies to these IF-MAP identifier types:
210		Extended identifier types MUST be of the form NAMESPACE#ELEMENT-NAME, in which NAMESPACE r » epresents the URI of the extended identifier's XML schema and ELEMENT-NAME represents th » e XML element name within the schema. This attribute MUST be present in a decision reque » st if the IF-MAP client request is not purgePublisher.
	231	Extended identifier types MUST be of the form NAMESPACE#ELEMENT-NAME, in which NAMESPACE r » epresents the URI of the extended identifier's XML schema and ELEMENT-NAME represents th » e XML element name within the schema. This attribute MUST be present in a decision reque » st if the MAP Client request is not purgePublisher.
211	232	
212	233	Original identifier types MUST denote the type of identifier. Example values are access-r » equest, identity, device, ip-address, and mac-address.
213	234	
214	235	The following applies to decision requests associated with:
215		An identifier. Then the identifier-type attribute SHALL denote the type of identifier. Exa » mple values are access-request, identity, device, ip-address, and mac-address.
	236	An identifier. Then the identifier-type attribute MUST denote the type of identifier. Exam » ple values are access-request, identity, device, ip-address, and mac-address.
216	237	
217		A link. Then the attribute identifier-type attribute SHALL have two values denoting the ty » pes of the two identifiers, with the exception of a link between two identifiers of the » same identifier type, in which case the identifier-type attribute SHALL have one value.
	238	A link. Then the attribute identifier-type attribute MUST have two values denoting the typ » es of the two identifiers, with the exception of a link between two identifiers of the s » ame identifier type, in which case the identifier-type attribute MUST have one value.
218	239	
	240	Example 4
219	241	The following is an example of an identity-type attribute in a target match:
220	242	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
221	243	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
222	244	>ip-address</AttributeValue>
223	245	<AttributeDesignator
224	246	MustBePresent="false"
225	247	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
226	248	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-type"
227	249	DataType="http://www.w3.org/2001/XMLSchema#string"/>
228	250	</Match>
229	251	
230	252	
231	253	Is-Map-Client-Identifier
232		The Is-Map-Client-Identifier value shall be designated with the following attribute identi » fier:
	254	The Is-Map-Client-Identifier value MUST be designated with the following attribute identif » ier:
233	255	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-map-client-identifier
234		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean. This attribute » indicates a MAP client identifier if and only if one or both identifiers in the request » has the form of a MAP Client identifier in which case the value must be set to true if

		» all of the following are true, otherwise the value must be set to false or omit the attr » ibute altogether:
	256	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean [XMLSCHEMA11-2] » . This attribute indicates a MAP client identifier if and only if one or both identifier » s in the request has the form of a MAP Client identifier in which case the value MUST be » set to true if all of the following are true, otherwise the value MUST be set to false » or omit the attribute altogether:
235	257	The identifier is not extended.
236	258	Its identifier-type is “identity”.
237	259	Its administrative-domain is ifmap:client.
238	260	
239		This attribute MUST be present if the IF-MAP client request is not purgePublisher.
	261	This attribute MUST be present if the MAP Client request is not purgePublisher.
240	262	
	263	Example 5
241	264	The following is an example of an is-map-client-identifier attribute in a target match:
242	265	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
243	266	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
244	267	>true</AttributeValue>
245	268	<AttributeDesignator
246	269	MustBePresent="true"
247	270	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
248	271	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-map-client-identi » fier"
249	272	DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
250	273	</Match>
251	274	
252	275	Is-Self-Identifier
253		The Is-Self-Identifier value shall be designated with the following attribute identifier:
	276	The Is-Self-Identifier value MUST be designated with the following attribute identifier:
254	277	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-self-identifier
255		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean. This attribute » indicates whether the identifier of the resource is the self-identifier of the subject » MAP Client and it MUST be true if and only if one or both identifiers in the request are » the subject MAP Client., otherwise it MUST be set to false or omitted altogether. This » attribute MUST be present if the IF-MAP client request is not purgePublisher.
	278	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean [XMLSCHEMA11-2] » . This attribute indicates whether the identifier of the resource is the self-identifier » of the subject MAP Client and it MUST be true if and only if one or both identifiers in » the request are the subject MAP Client., otherwise it MUST be set to false or omitted a » ltogether. This attribute MUST be present if the MAP Client request is not purgePublishe » r.
256	279	
257		The following is an example of the is-self-identifier attribute in a target match in which » one identifier must be the subjects MAP Clients self-identifier:
	280	Example 6
	281	The following is an example of the is-self-identifier attribute in a target match in which » one identifier MUST be the subjects MAP Clients self-identifier:
258	282	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
259	283	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
260	284	>true</AttributeValue>
261	285	<AttributeDesignator
262	286	MustBePresent="false"
263	287	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
264	288	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-self-identifier"

265	289	DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
266	290	</Match>
267	291	
268	292	On-Link
269		The On-Link value shall be designated with the following attribute identifier:
	293	The On-Link value MUST be designated with the following attribute identifier:
270	294	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:on-link
271		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean. This attribut » e indicates that the metadata item is or will be attached to a link, if set to true. If » false, this attribute indicates that the metadata item is attached to an identifier. Thi » s attribute MUST be present if the IF-MAP client request is not purgePublisher.
	295	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean [XMLSCHEMA11-2] » . This attribute indicates that the metadata item is or will be attached to a link, if » set to true. If false, this attribute indicates that the metadata item is attached to an » identifier. This attribute MUST be present if the MAP Client request is not purgePublis » her.
272	296	
	297	Example 7
273	298	The following is an example of the on-link attribute in a target match. The attribute valu » e of true indicates that the metadata item is or will be attached to a link:
274	299	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
275	300	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
276	301	>true</AttributeValue>
277	302	<AttributeDesignator
278	303	MustBePresent="false"
279	304	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
280	305	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:on-link"
281	306	DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
282	307	</Match>
283	308	
284	309	
285	310	Metadata-Attribute
286		The family of Metadata-Attribute values shall be designated with the following attribute i » dentifier:
	311	The family of Metadata-Attribute values MUST be designated with the following attribute id » entifier:
287	312	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-attribute
288		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. This attribute » denotes the name of a top-level attribute and MUST be extended to have the form:
	313	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:
289	314	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-attribute:ATTR
290		In which ATTR is replaced by the name of a top-level attribute of the metadata item. Examp » le URN values in the attribute family are:
	315	In which ATTR is replaced by the name of a top-level attribute of the metadata item.
	316	
	317	Example 8
	318	Example URN values in the attribute family are:
291	319	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-attribute:name
292	320	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-attribute:administrative-dom » ain
293	321	
294	322	The following conditions apply:
295	323	The value of the XACML attribute MUST be the value of the top-level attribute of the metad

		» ata item.
296	324	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.
297		The attribute MUST be included if the MAP Content Selector chooses it, otherwise it MAY b » e included.
	325	The attribute MUST be included if Content Selector [TNC-MAP-Authz, Section 3.5.5 Content » Selector] chooses it, otherwise it MAY be included.
298	326	
299		The following is an example of a VariableDefinition in which the metadata-attribute name a » ttribute needs to match the name of an Overlay Network that the IF-MAP Client is a membe » r of:
	327	Example 9
	328	The following is an example of a VariableDefinition in which the metadata-attribute name a » ttribute needs to match the name of an Overlay Network that the MAP Client is a member o » f:
300	329	<VariableDefinition VariableId="metadata-name-matches-subject- backhaul-interface">
301	330	<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-in">
302	331	<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
303	332	<AttributeDesignator
304	333	MustBePresent="true"
305	334	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
306	335	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-attribu » te:name"
307	336	DataType="http://www.w3.org/2001/XMLSchema#string"/>
308	337	</Apply>
309	338	
310	339	<AttributeDesignator
311	340	MustBePresent="false"
312	341	Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
313	342	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:subject:member-of:http%3A// » www.trustedcomputinggroup.org/2010/IFMAP-ICS-METADATA/1#overlay-network-group"
314	343	DataType="http://www.w3.org/2001/XMLSchema#string"/>
315	344	</Apply>
316	345	</VariableDefinition>>
317	346	
318	347	Identifier Attribute
319		The family of identifier-attribute values shall be prefixed with the following attribute i » dentifier:
	348	The family of identifier-attribute values MUST be prefixed with the following attribute id » entifier:
320	349	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-attribute
321	350	This attribute denotes the top-level attribute of the IF-MAP identifier and MUST be extend » ed to have the form:
322	351	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-attribute:IDENTIFIER-TYPE: » ATTR
323	352	In which IDENTIFIER-TYPE is the type string of an identifier in a decision request and ATT » R is replaced by the top-level attribute of the identifier. The value of the XACML attri » bute MUST be the value of the top-level attribute of the metadata item. Both IDENTIFIER- » TYPE and ATTR MUST be URL encoded.
324	353	The following conditions apply to a link between two identifiers of the same type in which » both identifiers have the attribute ATTR:
325		The decision request attribute SHALL have two values if the values for ATTR are not equal.
326		The decision request attribute SHALL have one value if the values for ATTR are equal.
	354	The decision request attribute MUST have two values if the values for ATTR are not equal [» XACML1, Section A14.1 Equality predicates].

	355	The decision request attribute MUST have one value if the values for ATTR are equal [XACML » 1, Section A14.1 Equality predicates].
327	356	
328		The DataType of this attribute MUST be http://www.w3.org/2001/XMLSchema#string except for » the following cases:
	357	The DataType of this attribute MUST be http://www.w3.org/2001/XMLSchema#string [XMLSCHEMA1 » 1-2] except for the following cases:
329	358	
330	359	The DataType of this attribute is urn:oasis:names:tc:xacml:2.0:data-type:ipAddress if both » of the following are true:
331	360	The identifier's type is ip-address.
332	361	The ATTR extension is value.
333	362	
334	363	The DataType of this attribute is urn:oasis:names:tc:xacml:1.0:data-type:x500Name if all o » f the following are true:
335	364	The identifier's type is identity.
336	365	The identity subtype is x500Name.
337	366	The ATTR extension is name.
338	367	
339	368	The DataType of this attribute is urn:oasis:names:tc:xacml:2.0:data-type:dnsName if all of » the following is true:
340	369	The identifier's type is identity.
341	370	The identity subtype is dns-name
342	371	The ATTR extension is name.
343	372	
344	373	This attribute MUST NOT be present in the decision request unless the identifier has a top » -level attribute named ATTR, or ATTR is administrative-domain. If ATTR is administrative » -domain and the identifier has no administrative-domain attribute, then the attribute va » lue MUST be an empty string.
345	374	
346		The following is an example of a target match in which the identity (IDENTIFIER-TYPE) type » (ATTR) must match the identity type hip-hit, which is the Host Identity Protocol (HIP), » Host Identity Tag (HIT) :
	375	Example 10
	376	The following is an example of a target match in which the identity (IDENTIFIER-TYPE) type » (ATTR) MUST match the identity type hip-hit, which is the Host Identity Protocol (HIP), » Host Identity Tag (HIT):
347	377	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
348	378	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
349	379	>hip-hit</AttributeValue>
350	380	<AttributeDesignator
351	381	MustBePresent="true"
352	382	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
353	383	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:resource: identifier-attribut » e:identity:type"
354	384	DataType="http://www.w3.org/2001/XMLSchema#string"/>
355	385	</Match>>
356	386	
357	387	Action Attributes
358	388	Action-Id
359		The Action-Id value shall be designated with the following attribute identifier:
	389	The Action-Id value MUST be designated with the following attribute identifier:
360	390	urn:oasis:names:tc:xacml:1.0:action:action-id
361		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. This attribute » indicates that the IF-MAP client is requesting to read or write metadata in the MAP dat

		» abase and MUST be present in the decision request. If the IF-MAP client request type to
		» the MAP server is either search or subscribe then this attribute's value MUST be read, o
		» therwise it MUST be write.
	391	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string [XMLSCHEMA11-2].
		» This attribute indicates that the MAP Client is requesting to read or write metadata i
		» n the MAP database and MUST be present in the decision request. If the MAP Client reques
		» t type to the MAP server is either search or subscribe then this attribute's value MUST
		» be read, otherwise it MUST be write.
362	392	
363		The following is an example of a target match in which the IF-MAP Client is allowed to rea
		» d metadata in the MAP database:
	393	Example 11
	394	The following is an example of a target match in which the MAP Client is allowed to read m
		» etadata in the MAP database:
364	395	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
365	396	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
366	397	>read</AttributeValue>
367	398	<AttributeDesignator
368	399	MustBePresent="false"
369	400	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
370	401	AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
371	402	DataType="http://www.w3.org/2001/XMLSchema#string"/>
372	403	</Match>
373	404	
374	405	Request-Type
375		The Request-Type value shall be designated with the following attribute identifier:
	406	The Request-Type value MUST be designated with the following attribute identifier:
376	407	urn:oasis:names:tc:xacml:3.0:if-map:content:action:request-type
377		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. This attribute
		» denotes the IF-MAP request type that is sent to the MAP server and MUST have one of the
		» following values: publish, subscribe, search, or purgePublisher
	408	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string [XMLSCHEMA11-2].
		» This attribute denotes the IF-MAP request type that is sent to the MAP server and MUST
		» have one of the following values: publish, subscribe, search, or purgePublisher
378	409	
	410	Example 12
379	411	The following is an example of a target match in which the request type is purgePublisher:
380	412	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
381	413	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
382	414	>purgePublisher</AttributeValue>
383	415	<AttributeDesignator
384	416	MustBePresent="false"
385	417	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
386	418	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:action:request-type"
387	419	DataType="http://www.w3.org/2001/XMLSchema#string"/>
388	420	</Match>
389	421	
390	422	
391	423	Purge-Own-Metadata
392		The Purge-Own-Metadatavalue shall be designated with the following attribute identifier:
	424	The Purge-Own-Metadatavalue MUST be designated with the following attribute identifier:
393	425	urn:oasis:names:tc:xacml:3.0:if-map:content:action:purge-own-metadata
394		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean. This attribute
		» denotes whether the IF-MAP client is attempting to purge its own metadata items or meta
		» data items published by another IF-MAP client. This attribute value is true if purging i

		» ts own metadata; otherwise the value is false:
	426	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean [XMLSCHEMA11-2] » . This attribute denotes whether the MAP Client is attempting to purge its own metadata » items or metadata items published by another MAP Client. This attribute value is true if » purging its own metadata; otherwise the value is false:
395	427	
	428	Example 13
396	429	The following is an example of a target match in which a MAP Client may purge its own meta » data:
397	430	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
398	431	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
399	432	>true</AttributeValue>
400	433	<AttributeDesignator
401	434	MustBePresent="false"
402	435	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
403	436	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:action:purge-own-metadata"
404	437	DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
405	438	</Match>
406	439	
407	440	Publish-Request-Subtype
408		The Publish-Request-Subtype value shall be designated with the following attribute identif » ier:
	441	The Publish-Request-Subtype value MUST be designated with the following attribute identifi » er:
409	442	urn:oasis:names:tc:xacml:3.0:if-map:content:action:publish-request-subtype
410		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string. This attribute » denotes the type of an operation within an IF-MAP publish request and MUST have one of t » he following values: update, notify, or delete. This attribute must be present in the de » cision request if, and only if, the IF-MAP request type is publish.
	443	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#string [XMLSCHEMA11-2]. » This attribute denotes the type of an operation within an IF-MAP publish request and MU » ST have one of the following values: update, notify, or delete. This attribute MUST be p » resent in the decision request if, and only if, the IF-MAP request type is publish.
411	444	
	445	Example 14
412	446	The following is an example of a target match in which the IF-MAP publish request operatio » n is notify:
413	447	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
414	448	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
415	449	>notify</AttributeValue>
416	450	<AttributeDesignator
417	451	MustBePresent="false"
418	452	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
419	453	AttributeId=" urn:oasis:names:tc:xacml:3.0:if-map:content:action:publish-request-subty » pe"
420	454	DataType="http://www.w3.org/2001/XMLSchema#string"/>
421	455	</Match>
422	456	
423	457	Environment Attributes
424	458	Dry-Run
425		The Dry-Run value shall be designated with the following attribute identifier:
	459	The Dry-Run value MUST be designated with the following attribute identifier:
426	460	urn:oasis:names:tc:xacml:3.0:if-map:content:environment:dry-run
427		The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean. This attribute » MUST be a singleton (bag of one) and MUST be present. A dry-run PolicySet allows MAP ad

		» ministrators to test new PolicySets before they are used in a production environment. A » second use of dry-run policies is to allow for monitoring of certain activities. The val » ue of true indicates the use of a dry-run PolicySet. The value of false indicates that a » dry-run PolicySet will not be used.
	461	The DataType of this attribute is http://www.w3.org/2001/XMLSchema#boolean [XMLSCHEMA11-2] » . This attribute MUST be a singleton (bag of one) and MUST be present. A dry-run PolicyS » et allows MAP administrators to test new PolicySets before they are used in a production » environment. A second use of dry-run policies is to allow for monitoring of certain act » ivities. The value of true indicates the use of a dry-run PolicySet. The value of false » indicates that a dry-run PolicySet will not be used.
428	462	
	463	Example 15
429	464	The following is an example of a target match that checks for a dry run:
430	465	<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
431	466	<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#boolean"
432	467	>true</AttributeValue>
433	468	<AttributeDesignator
434	469	MustBePresent="false"
435	470	Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
436	471	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:environment:dry-run"
437	472	DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
438	473	</Match>
439	474	
440	475	
441	476	Obligation Caching
442		The <Obligation> element will be used in the XACML response to notify the requestor that a » n additional processing requirement is needed if the obligation's FulfillOn attribute is » Permit. This profile defines an obligation that indicates when a MAP server is require » d to cache an XACML decision for no more than a specified period of time. Each caching » obligation must contain exactly one maximum-policy-lag attribute. In the case where the » XACML response contains two or more caching obligations, then the caching obligation wit » h the shortest maximum-policy-lag attribute value must be used.
443		The Caching Obligation shall be designated with the following identifier:
	477	Overview
	478	
	479	The <Obligation> element will be used in the XACML response to notify the requestor that a » n additional processing requirement is needed if the obligation's FulfillOn attribute is » Permit. This profile defines an obligation that indicates when a MAP server is require » d to cache an XACML decision for no more than a specified period of time. Each caching » obligation MUST contain exactly one maximum-policy-lag attribute. In the case where the » XACML response contains two or more caching obligations, then the caching obligation wit » h the shortest maximum-policy-lag attribute value MUST be used.
	480	The Caching Obligation MUST be designated with the following identifier:
444	481	urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:caching
445	482	Maximum-Policy-Lag
446		The maximum-policy-lag value shall be designated with the following identifier:
	483	The maximum-policy-lag value MUST be designated with the following identifier:
447	484	urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:maximum-policy-lag
448		The maximum-policy-lag attribute indicates the maximum length of time, in seconds, that a » MAP server can cache an XACML decision before new XACML request will need to be made. Th » e DataType of this attribute is http://www.w3.org/2001/XMLSchema#integer, in which its v » alue must be a nonnegative integer.
	485	The maximum-policy-lag attribute indicates the maximum length of time, in seconds, that a » MAP server can cache an XACML decision before new XACML request will need to be made. Th » e DataType of this attribute is http://www.w3.org/2001/XMLSchema#integer [XMLSCHEMA11-2

		»], in which its value MUST be a nonnegative integer.
449	486	
	487	Example 16
450	488	The following is an example of a caching obligation:
451	489	<ObligationExpressions>
452	490	<ObligationExpression
453	491	ObligationId="urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:caching"
454	492	FulfillOn="Permit">
455	493	<AttributeAssignmentExpression
456	494	AttributeId="urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:maximum-policy » -lag">
457	495	<AttributeValue
458	496	DataType="http://www.w3.org/2001/XMLSchema#integer"
459	497	>60</AttributeValue>
460	498	</AttributeAssignmentExpression>
461	499	</ObligationExpression>
462	500	</ObligationExpressions>
463		Identifiers
464		This profile defines the following URN identifiers.
465	501	Profile Identifier
466		The following identifier SHALL be used as the identifier for this profile when an identifi » er in the form of a URI is required.
	502	The following identifier MUST be used as the identifier for this profile when an identifie » r in the form of a URI is required.
467	503	urn:oasis:names:tc:xacml:3.0:if-map:content
468	504	Conformance
469		Conformance to this profile is defined for policies and requests generated and transmitted » within and between XACML systems.
	505	Overview
	506	Conformance to [xacml-map-authz-v1.0] is defined for policies and requests generated and t » ransmitted within and between XACML systems.
470	507	Attribute Identifiers
471		Conformant XACML policies and requests SHALL use the attribute identifiers defined in Sect » ion 2 for their specified purpose and SHALL NOT use any other identifiers for the purpos » es defined by attributes in this profile. The following table lists the attributes that » must be supported.
472		Note: “M” is mandatory “O” is optional.
473		
474		Identifiers
475		urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role M
476		urn:oasis:names:tc:xacml:3.0:if-map:content:subject:task: RELATIONSHIP:IDENTIFIER-TYPE M
477		urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-type M
478		urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-type M
479		urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-map-client-identifier M
480		urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-self-identifier M
481		urn:oasis:names:tc:xacml:3.0:if-map:content:resource:on-link M
482		urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-attribute:ATTR M
483		urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-attribute:IDENTIFIER-TYPE: » ATTR M
484		urn:oasis:names:tc:xacml:3.0:if-map:content:action:request-type M
485		urn:oasis:names:tc:xacml:3.0:if-map:content:action:purge-own-metadata M
486		urn:oasis:names:tc:xacml:3.0:if-map:content:action:publish-request-subtype M
487		urn:oasis:names:tc:xacml:3.0:if-map:content:environment:dry-run M
488		urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:caching M
489		urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:maximum-policy-lag M

	508	Conformant XACML policies and requests MUST use the attribute identifiers defined in Secti » on 2 for their specified purpose and MUST NOT use any other identifiers for the purposes » defined by attributes in this profile. The following table lists the attributes that M » UST be supported.
	509	
	510	urn:oasis:names:tc:xacml:3.0:if-map:content:subject:role
	511	urn:oasis:names:tc:xacml:3.0:if-map:content:subject:task: RELATIONSHIP:IDENTIFIER-TYPE
	512	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-type
	513	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-type
	514	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-map-client-identifier
	515	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:is-self-identifier
	516	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:on-link
	517	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:metadata-attribute:ATTR
	518	urn:oasis:names:tc:xacml:3.0:if-map:content:resource:identifier-attribute:IDENTIFIER-TYPE: » ATTR
	519	urn:oasis:names:tc:xacml:3.0:if-map:content:action:request-type
	520	urn:oasis:names:tc:xacml:3.0:if-map:content:action:purge-own-metadata
	521	urn:oasis:names:tc:xacml:3.0:if-map:content:action:publish-request-subtype
	522	urn:oasis:names:tc:xacml:3.0:if-map:content:environment:dry-run
	523	urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:caching
	524	urn:oasis:names:tc:xacml:3.0:if-map:content:obligation:maximum-policy-lag
490	525	Attribute Values
491		Conformant XACML policies and requests SHALL use attribute values in the specified range o » r patterns as defined for each attribute in Section 2 (when a range or pattern is specif » ied).
492		NOTE: In order to process conformant XACML policies and requests correctly, PIP and PEP mo » dules may have to translate native data values into the datatypes and formats specified » in this profile.
	526	XACML policies and requests, that conform to [xacml-map-authz-v1.0], MUST use attribute va » lues in the specified range or patterns as defined for each attribute in Section 2 of th » is document (when a range or pattern is specified).
	527	NOTE (non-normative): In order to correctly process XACML policies and requests, that conf » orm to [xacml-map-authz-v1.0], PIP and PEP modules may need to translate native data val » ues into the datatypes and formats specified in [xacml-map-authz-v1.0].
493	528	Acknowledgements
	529	{Non-normative}
494	530	The following individuals have participated in the creation of this specification and are » gratefully acknowledged:
495	531	Participants:
496	532	Richard Hill, The Boeing Company
497	533	John Tolbert, The Boeing Company
498	534	Steve Venema, The Boeing Company
499	535	Stephen Hatch, The Boeing Company
500	536	Nancy Cam-Winget, Cisco Systems
501	537	Arne Welzel, FHH
502	538	Josef von Helden, FHH
503	539	James Tan, Infoblox
504	540	David Vigier, Infoblox
505	541	Stu Bailey, Infoblox
506	542	Navin Boddu, Infoblox
507	543	Steve Hanna, Juniper
508	544	Clifford Kahn, Juniper
509	545	Lisa Lorenzin, Juniper
510	546	Venkata Srikar Damaraju, Juniper
511	547	Atul Shah, Microsoft

512	548 Trevor Freeman, Microsoft
513	549 Charles Schmidt, The Mitre Corporation
514	550 Steven Legg, ViewDS
515	551
516	552 Committee members during profile development:
517	553 Person
518	554 Organization
519	555 Role
520	556
521	557 David Brossard
522	558 Axiomatics
523	559 Member
524	560
525	561 Gerry Gebel
526	562 Axiomatics
527	563 Member
528	564
529	565 Srijith Nair
530	566 Axiomatics
531	567 Member
532	568
533	569 Erik Rissanen
534	570 Axiomatics
535	571 Member
536	572
537	573 Richard Skedd
538	574 BAE SYSTEMS plc
539	575 Member
540	576
541	577 Abbie Barbir
542	578 Bank of America
543	579 Member
544	580
545	581 Radu Marian
546	582 Bank of America
547	583 Member
548	584
549	585 Rakesh Radhakrishnan
550	586 Bank of America
551	587 Member
552	588
553	589 Ronald Jacobson
554	590 CA Technologies
555	591 Member
556	592
557	593 Masum Hasan
558	594 Cisco Systems
559	595 Member
560	596
561	597 Anil Tappetla
562	598 Cisco Systems
563	599 Member
564	600
565	601 Robert van Herk
566	602 Connectis

567	603 Member
568	604
569	605 Danny Thorpe
570	606 Dell
571	607 Voting Member
572	608
573	609 Gareth Richards
574	610 EMC
575	611 Member
576	612
577	613 Remon Sinnema
578	614 EMC
579	615 Voting Member
580	616
581	617 Matt Crooke
582	618 First Point Global Pty Ltd.
583	619 Member
584	620
585	621 Allan Foster
586	622 Forgerock Inc.
587	623 Member
588	624
589	625 Michiharu Kudo
590	626 IBM
591	627 Member
592	628
593	629 Sridhar Muppidi
594	630 IBM
595	631 Member
596	632
597	633 Vernon Murdoch
598	634 IBM
599	635 Member
600	636
601	637 Nataraj Nagaratnam
602	638 IBM
603	639 Member
604	640
605	641 Gregory Neven
606	642 IBM
607	643 Member
608	644
609	645 Franz-Stefan Preiss
610	646 IBM
611	647 Member
612	648
613	649 Ron Williams
614	650 IBM
615	651 Member
616	652
617	653 David Chadwick
618	654 Individual
619	655 Member
620	656
621	657 David Choy

622	658	Individual
623	659	Member
624	660	
625	661	Bill Parducci*
626	662	Individual
627	663	Chair
628	664	
629	665	Mike Schmidt
630	666	Individual
631	667	Member
632	668	
633	669	David Laurance
634	670	JPMorgan Chase Bank, N.A.
635	671	Member
636	672	
637	673	Eliot Solomon
638	674	JPMorgan Chase Bank, N.A.
639	675	Member
640	676	
641	677	Thomas Hardjono
642	678	M.I.T.
643	679	Member
644	680	
645	681	Anthony Nadalin
646	682	Microsoft
647	683	Member
648	684	
649	685	Vishwesh Bavadekar
650	686	NextLabs, Inc.
651	687	Member
652	688	
653	689	Andy Han
654	690	NextLabs, Inc.
655	691	Member
656	692	
657	693	Naomaru Itoi
658	694	NextLabs, Inc.
659	695	Member
660	696	
661	697	Arun Shah
662	698	OpenIAM, LLC
663	699	Member
664	700	
665	701	Kamalendu Biswas
666	702	Oracle
667	703	Member
668	704	
669	705	Willem de Pater
670	706	Oracle
671	707	Member
672	708	
673	709	Rich Levinson
674	710	Oracle
675	711	Secretary
676	712	

677	713	Hal Lockhart
678	714	Oracle
679	715	Chair
680	716	
681	717	Prateek Mishra
682	718	Oracle
683	719	Member
684	720	
685	721	Sid Mishra
686	722	Oracle
687	723	Member
688	724	
689	725	Roger Wigenstam
690	726	Oracle
691	727	Member
692	728	
693	729	YanJiong WANG
694	730	Primeton Technologies, Inc.
695	731	Member
696	732	
697	733	Kenneth Peeples
698	734	Red Hat
699	735	Member
700	736	
701	737	Anil Saldhana
702	738	Red Hat
703	739	Member
704	740	
705	741	Darran Rolls
706	742	SailPoint Technologies
707	743	Member
708	744	
709	745	Jan Herrmann
710	746	Siemens AG
711	747	Member
712	748	
713	749	Crystal Hayes
714	750	The Boeing Company
715	751	Voting Member
716	752	
717	753	Richard Hill
718	754	The Boeing Company
719	755	Voting Member
720	756	
721	757	Greg Smith
722	758	The Boeing Company
723	759	Member
724	760	
725	761	John Tolbert
726	762	The Boeing Company
727	763	Voting Member
728	764	
729	765	Bernard Butler
730	766	TSSG
731	767	Member

732	768	
733	769	Steven Davy
734	770	TSSG
735	771	Member
736	772	
737	773	Martin Smith
738	774	US Department of Homeland Security
739	775	Member
740	776	
741	777	John Davis
742	778	Veterans Health Administration
743	779	Member
744	780	
745	781	Duane DeCouteau
746	782	Veterans Health Administration
747	783	Member
748	784	
749	785	Mohammad Jafari
750	786	Veterans Health Administration
751	787	Voting Member
752	788	
753	789	David Staggs
754	790	Veterans Health Administration
755	791	Member
756	792	
757	793	Gil Kirkpatrick
758	794	ViewDS
759	795	Member
760	796	
761	797	Steven Legg
762	798	ViewDS
763	799	Voting Member
764	800	
765	801	Johann Nallathamby
766	802	WSO2
767	803	Member
768	804	
769	805	Asela Pathberiya
770	806	WSO2
771	807	Member
772	808	
773	809	Prabath Siriwardena
774	810	WSO2
775	811	Member
776	812	
777	813	
778	814	
779	815	
780	816	Revision History
	817	{Non-normative}
781	818	
782	819	Revision Date Editor Changes Made
783	820	WD 1 5/2/2013 Richard Hill, John Tolbert, Initial committee draft.
784	821	WD 2 7/15/2013 Richard Hill, John Tolbert Updated to reflect changes in the TNC MAP Conten » t Authorization v31 specification.

785	822	Added figure 2
786	823	Added definitions to Glossary,
787	824	Added Non-Normative Reference
788	825	Added subject task attribute
789	826	Added attribute examples
790	827	Removed delete-metadata-by-other-client attribute
791	828	Added purge-own-metadata attribute
792	829	WD 3 10/28/2013 Richard Hill, John Tolbert, Steven Legg Addressed comments from WD 2 revie » w.
793	830	Updated to reflect changes in the TNC MAP Content Authorization v33 specification.
794	831	Added Caching Obligation
795	832	Updated Appendix A. Acknowledgements
796	833	
797	834	WD 4 11/12/2013 Richard Hill, John Tolbert, Steven Legg Addressed comments from WD 3 revie » w.
798		
	835	WD 5 2/23/2014 Richard Hill Addressed OASIS TAB comments from the CSPRD01 30 day review.
799	836	
800	837	
801	838	
802	839	
803	840	
804	841	
805	842	
806	843	
807	844	
808	845	□
809	846	
810	847	
811	848	
812	849	
813	850	
814	851	
815	852	
816	853	
817	854	
818	855	
819	856	
820	857	
821	858	
822	859	
823	860	
824	861	□
825	862	
826	863	
827	864	
828	865	
829	866	
830	867	
831	868	
832	869	
833	870	
834	871	
835		xacml-map-authz-v1.0-csprd01 14 November 2013
836		Standards Track Work Product Copyright © OASIS Open 2013. All Rights Reserved. Pa

		» ge 1 of 24
	872	xacml-3.0-map-authz-v1.0-wd05 23 November 2014
	873	Standards Track Work Product Copyright © OASIS Open 2014. All Rights Reserved. Pa
		» ge 25 of 25
837	874	
838	875	
839	876	Copyright © OASIS Open 2004.All Rights Reserved. Page 5 of 5
840	877	
841	878	
842	879	
843	880	
844	881	
845	882	
846	883	