XACML MAP Authorization Profile Version 1.0

Committee Specification 01

07 April 2014

Specification URIs

This version:

http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/cs01/xacml-map-authz-v1.0-cs01.doc (Authoritative)
http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/cs01/xacml-map-authz-v1.0-cs01.html
http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/cs01/xacml-map-authz-v1.0-cs01.pdf

Previous version:

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

Latest version:

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

Technical Committee:

OASIS eXtensible Access Control Markup Language (XACML) TC

Chairs:

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

Editors:

Richard Hill (richard.c.hill@boeing.com), The Boeing Company
John Tolbert (john.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*. Edited by Erik Rissanen. Latest version. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html.
- TNC MAP Content Authorization http://www.trustedcomputinggroup.org/resources/tnc_map_content_authorization

Abstract:

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

Status:

This document was last revised or approved by the 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. Edited by Richard Hill, John Tolbert, and Steve Legg. 07 April 2014. OASIS Committee Specification 01. http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/cs01/xacml-map-authz-v1.0-cs01.html. Latest version: http://docs.oasis-open.org/xacml/xacml-map-authz/v1.0/xacml-map-authz-v1.0.html.

Notices

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

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

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

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

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

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

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

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

Table of Contents

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

1 Introduction

1.1 Overview (non-normative)

{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 a 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]**. All examples in [xacml-map-authz-v1.0] are non-normative.

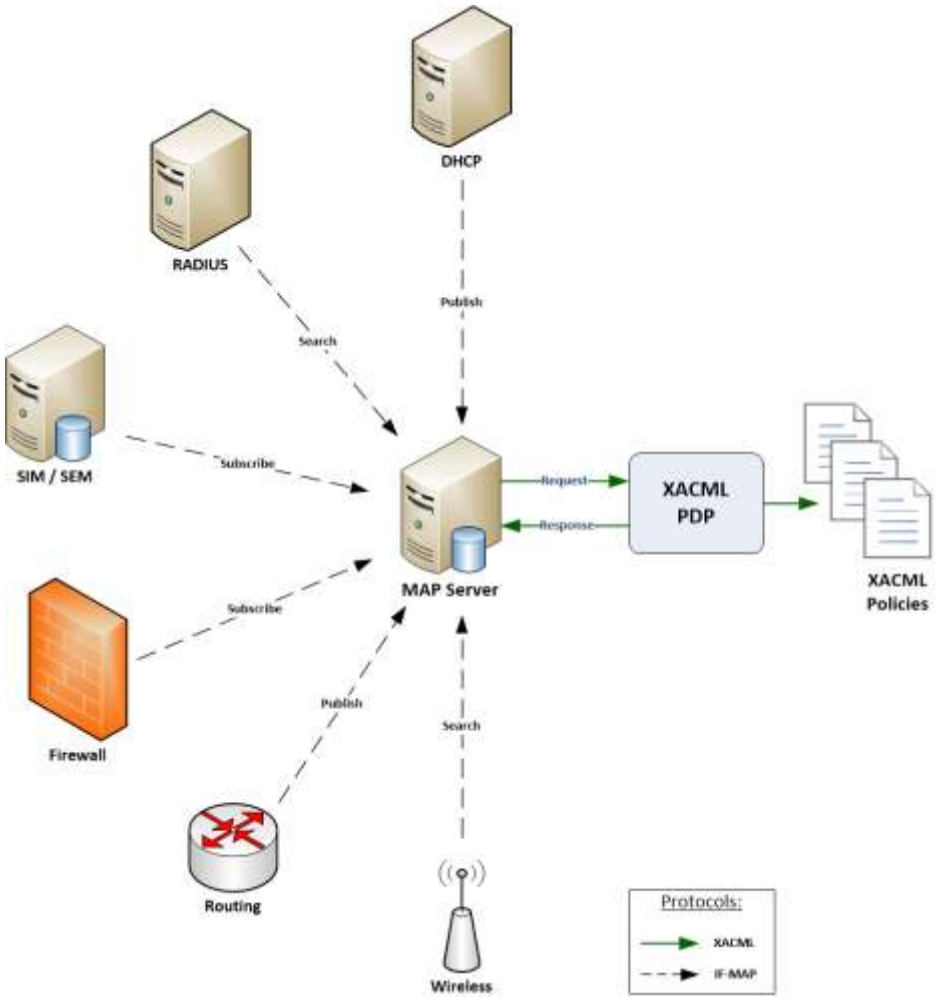

Figure 1: Example MAP – XACML scenario

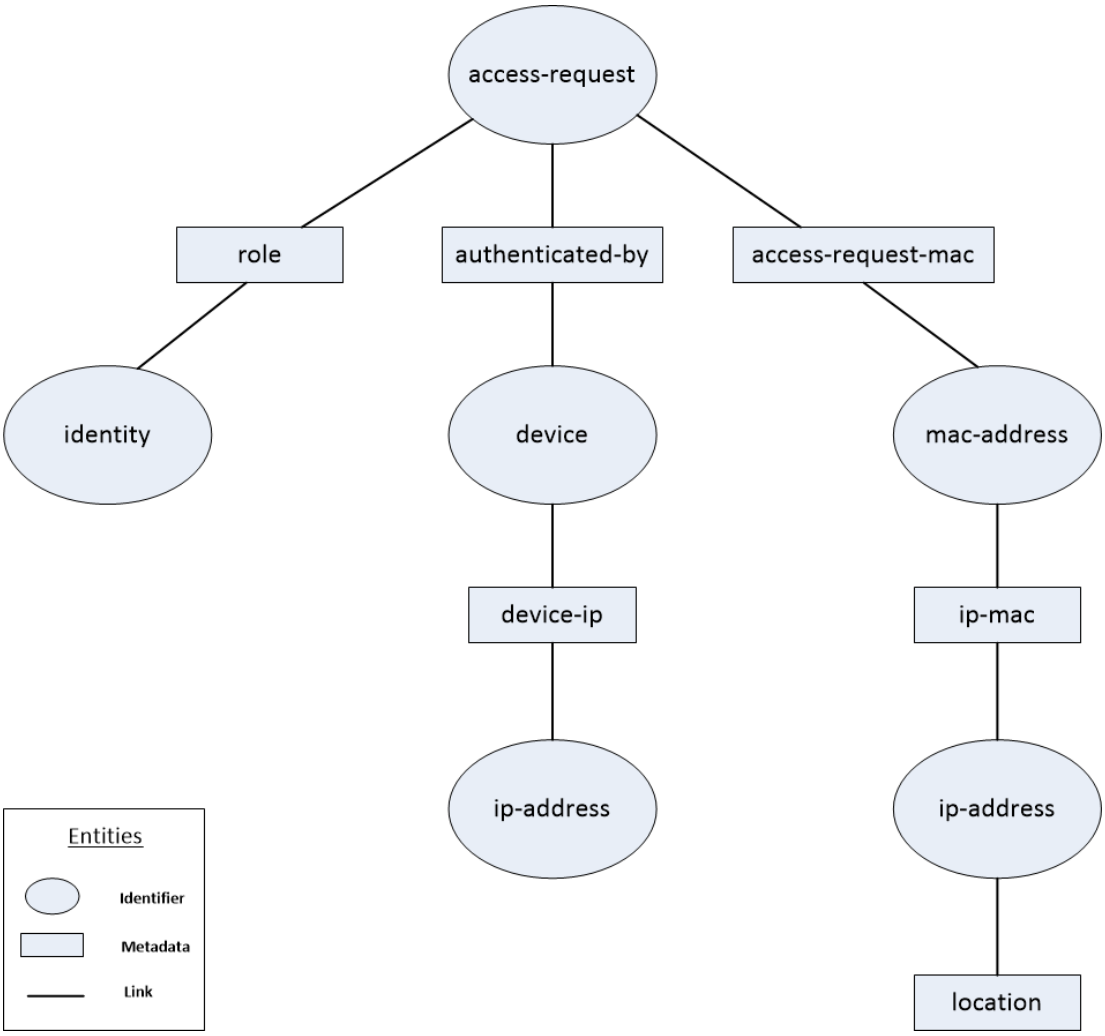

Figure 2: Example labeled graph representation of an IF-MAP data model

1.2 Glossary

Administrative-Domain

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

Content Selector

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

Extended Identifier

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

IF-MAP

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

IF-MAP Request

A message sent from a MAP client to a MAP server using the IF-MAP standard client/server protocol. Also see [TNC-MAP-Authz, Section 2.2.3 IF-MAP Requests].

Identifier

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 represents a globally unique label of a node within the undirected, labeled graph representation of the IF-MAP data model.

Link

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

MAP

Metadata Access Point (MAP) is a server that provides device, user, and network flow state information to MAP Clients.

MAP Client

A client to a MAP server [TNC-MAP-Authz, Section 2.2.2 MAP Client].

Metadata Item

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-MAP data model.

NAC

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

Original Identifier

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.

PEP

Policy enforcement point as defined in [XACML3].

PIP

Policy information point as defined in [XACML3].

purgePublisher

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

publisher-id

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

Publish Request Subtype

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

Self-Identifier

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

TCG

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

TNC

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

Top-level attribute

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

1.3 Terminology

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 described in **[RFC2119]**.

1.4 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[TNC-IF-MAP] TNC IF-MAP Binding for SOAP, version 2.1 http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification

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

[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

[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-core-spec-os.pdf

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

[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/

1.5 Non-Normative References

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

2 Profile

2.1 Subject Attributes

2.1.1 Role

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

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

The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#string` [XMLSCHEMA11-2].

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

Example 1

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

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

2.1.2 Task

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

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

The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#string` [XMLSCHEMA11-2].

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

Example 2

The following is an example of an attribute identifier:

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

2.2 Resource Attributes

2.2.1 Overview

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

When a MAP Server retrieves data for a MAP Client, in response to a search or subscribe request, 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 the MAP database. For an IF-MAP purgePublisher request, the decision request MUST NOT include attributes defined in section 2.2 Resource Attributes.

2.2.2 Metadata-Type

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

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

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

[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 the 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 request is not *purgePublisher*.

Example 3

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

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

2.2.3 Identifier-Type

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

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

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

[XMLSCHEMA11-2].

The following applies to these IF-MAP identifier types:

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

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

The following applies to decision requests associated with:

- An **identifier**. Then the *identifier-type* attribute MUST denote the type of identifier. Example values are *access-request*, *identity*, *device*, *ip-address*, and *mac-address*.

- A **link**. Then the attribute *identifier-type* attribute MUST have two values denoting the types 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 MUST have one value.

Example 4

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

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

2.2.4 Is-Map-Client-Identifier

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

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

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 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 attribute altogether:

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

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

Example 5

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

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



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

2.2.5 Is-Self-Identifier

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

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

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

Example 6

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:

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

2.2.6 On-Link

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

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

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 *purgePublisher*.

Example 7

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

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

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

2.2.7 Metadata-Attribute

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

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

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:

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

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

Example 8

Example URN values in the attribute family are:

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

The following conditions apply:

- The value of the XACML attribute MUST be the value of the top-level attribute of the metadata item.
- 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.
- The attribute MUST be included if Content Selector [TNC-MAP-Authz, Section 3.5.5 Content Selector] chooses it, otherwise it MAY be included.

Example 9

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

```
<VariableDefinition VariableId="metadata-name-matches-subject-
backhaul-interface">
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-
in">
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-
one-and-only">
      <AttributeDesignator
        MustBePresent="true"
        Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource"
        AttributeId="urn:oasis:names:tc:xacml:3.0:if-
map:content:resource:metadata-attribute:name"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Apply>
```

```
    <AttributeDesignator
      MustBePresent="false"
      Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"
      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"
      DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </Apply>
</VariableDefinition>>
```

2.2.8 Identifier Attribute

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

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

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

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

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

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

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

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

1.) The `DataType` of this attribute is `urn:oasis:names:tc:xacml:2.0:data-type:ipAddress` if both of the following are true:
   a. The identifier's type is *ip-address*.
   b. The *ATTR* extension is *value.*

2.) The `DataType` of this attribute is `urn:oasis:names:tc:xacml:1.0:data-type:x500Name` if all of the following are true:
   a. The identifier's type is *identity*.
   b. The identity *subtype* is x500Name.
   c. The *ATTR* extension is *name*.

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

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

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 value MUST be an empty string.

Example 10

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):

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

2.3 Action Attributes

2.3.1 Action-Id

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

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

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 in the MAP database and MUST be present in the decision request. If the MAP Client request type to the MAP server is either *search* or *subscribe* then this attribute's value MUST be *read*, otherwise it MUST be *write*.

Example 11

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

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

2.3.2 Request-Type

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

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

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*

Example 12

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

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

2.3.3 Purge-Own-Metadata

The Purge-Own-Metadatavalue MUST be designated with the following attribute identifier:

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

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*:

Example 13

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

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

2.3.4 Publish-Request-Subtype

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

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

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 MUST have one of the following values: *update*, *notify*, or *delete*. This attribute MUST be present in the decision request if, and only if, the IF-MAP request type is *publish*.

Example 14

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

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

2.4 Environment Attributes

2.4.1 Dry-Run

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

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

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 PolicySet 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 activities. 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.

Example 15

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

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

2.5 Obligation Caching

2.5.1 Overview

The <Obligation> element will be used in the XACML response to notify the requestor that an 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 required 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 with the shortest *maximum-policy-lag* attribute value MUST be used.

The Caching Obligation MUST be designated with the following identifier:

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

2.5.2 Maximum-Policy-Lag

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

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

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. The `DataType` of this attribute is http://www.w3.org/2001/XMLSchema#integer [XMLSCHEMA11-2], in which its value MUST be a nonnegative integer.

Example 16

The following is an example of a caching obligation:

```
<ObligationExpressions>
  <ObligationExpression
      ObligationId="urn:oasis:names:tc:xacml:3.0:if-
map:content:obligation:caching"
      FulfillOn="Permit">
    <AttributeAssignmentExpression
        AttributeId="urn:oasis:names:tc:xacml:3.0:if-
map:content:obligation:maximum-policy-lag">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#integer"
        >60</AttributeValue>
    </AttributeAssignmentExpression>
  </ObligationExpression>
</ObligationExpressions>
```

3 Profile Identifier

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

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

4 Conformance

4.1 Overview

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

4.2 Attribute Identifiers

Conformant XACML ***policies*** and ***requests*** MUST use the attribute identifiers defined in Section 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 MUST be supported.

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

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

4.3 Attribute Values

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

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

Appendix A. Acknowledgements

{Non-normative}

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

Participants:

Richard Hill, The Boeing Company
John Tolbert, The Boeing Company
Steve Venema, The Boeing Company
Stephen Hatch, The Boeing Company
Nancy Cam-Winget, Cisco Systems
Arne Welzel, FHH
Josef von Helden, FHH
James Tan, Infoblox
David Vigier, Infoblox
Stu Bailey, Infoblox
Navin Boddu, Infoblox
Steve Hanna, Juniper
Clifford Kahn, Juniper
Lisa Lorenzin, Juniper
Venkata Srikar Damaraju, Juniper
Atul Shah, Microsoft
Trevor Freeman, Microsoft
Charles Schmidt, The Mitre Corporation
Steven Legg, ViewDS

Committee members during profile development:

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

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

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

620

Appendix B. Revision History

{Non-normative}

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