XACML Data Loss Prevention / Network Access Control (DLP/NAC) Profile Version 1.0

Working Draft 02

6 September 2013

Specification URIs

This version:

http://docs.oasis-open.org/xacml/3.0/dlp-nac/v1.0/wd-02/xacml-3.0-dlp-nac-v1.0-wd-01-en.doc (Authoritative)

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/xacml/3.0/dlp-nac/v1.0/wd-02/xacml-3.0-dlp-nac-v1.0-wd-01-en.doc (Authoritative)

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:

John Tolbert (john.w.tolbert@boeing.com), The Boeing Company
Richard Hill (richard.c.hill@boeing.com), The Boeing Company
Crystal Hayes (crystal.l.hayes@boeing.com), The Boeing Company

Related work:

This specification is related to:

- *eXtensible Access Control Markup Language (XACML) Version 3.0*. Latest version. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html.

Abstract:

This specification defines a profile for the use of XACML in expressing policies for data loss prevention and network access control tools and technologies. It defines standard attribute identifiers useful in such policies, and recommends attribute value ranges for certain attributes.

Status:

This document was last revised or approved by the 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-dlp-nac-v1.0]

XACML Data Loss Prevention / Network Access Control Profile Version 1.0. 18 September 2013. http://docs.oasis-open.org/xacml/3.0/dlp-nac/v1.0/wd-01/xacml-3.0-dlp-nac-v1.0-wd-01-en.doc.

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 http://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

{Non-normative}

This specification defines a profile for the use of the OASIS eXtensible Access Control Markup Language (XACML) **[XACML3]** to write and enforce policies to govern data loss prevention (DLP) tools and to provide access control for network resources. Use of this profile requires no changes or extensions to the **[XACML3]** standard.

This specification begins with a non-normative discussion of the topics and terms of interest in this profile. The normative section of the specification describes the attributes defined by this profile and provides recommended usage patterns for attribute values.

This specification assumes the reader is somewhat familiar with XACML. A brief overview sufficient to understand these examples is available in **[XACMLIntro]**.

Enterprises have legal, regulatory, and business reasons to protect their information, as exemplified by privacy, contracts, financial regulations, and export regulations. Organizations interpret those legal agreements, regulations, and business rules to form security and information protection policies, expressed in natural languages. Business policies and regulations are then instantiated as machine-enforceable access control policies. Most organizations employ a variety of security software tools to enforce access control policies and monitor compliance. In many cases, each tool must be configured independently of the others, leading to duplicative efforts and increased risk of inconsistent implementations.

XACML-conformant access control systems provide scalable and consistent access control policy management, enforcement, and compliance for web services, web applications, and data objects in a variety of repositories. The XACML policy format and reference architecture can be extended to promote policy consistency and efficient administration in the following areas.

DLP tools monitor “data-in-use” at endpoints (e.g., desktops, laptops, and mobile devices), “data-in-motion” on networks, and “data-at-rest” in storage systems. DLP tools enforce access control policies at these locations to prevent unauthorized access to and unintended disclosure of sensitive data. If DLP systems standardized on the XACML policy format, enterprise policy authorities could use the same language to define access control policies for endpoints, networks, servers, applications, web services, and file repositories. The cost savings and improvements to security posture canbe substantial.

Network Access Control (NAC) technologies enforce access control policies to restrict and regulate network traffic between routers, switches, firewalls, Virtual Private Network (VPN) devices, servers, and endpoint devices. Resources are commonly identified by Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, and Domain Name Service (DNS) names. Traffic flows between devices according to defined ports and protocols, which can be described, grouped, and used as attributes in access control policies.

XACML policy format is suitable for and should be used to create, enforce, and exchange policies between different DLP and NAC systems. Subject information, including a rich set of metadata about subjects, will be expressed as subject attributes. Data objects and network resources will be expressed as resource attributes. Subject requests and traffic operations will be expressed as action attributes.

This profile serves as a framework of common data loss prevention and network resource attributes upon which access control policies can be written, and to promote federated authorization for access to data objects and network resources. This profile will also provide XACML software developers and access control policy authors guidance on supporting DLP and NAC use cases.

1.1 Glossary

Data Loss Prevention (DLP)

DLP tools monitor “data-in-use” at endpoints (e.g., desktops, laptops, and mobile devices), “data-in-motion” on networks, and “data-at-rest” in storage systems. DLP tools enforce access control

policies at these locations to prevent unauthorized access to and unintended disclosure of sensitive data.

Discretionary Access Control (DAC)

DAC is an access control methodology wherein subjects are granted access to resources based primarily upon attributes of the subjects. Administrators can assign access permissions, sometimes called entitlements, to groups, roles, and other attributes, which are then associated with specific subjects.

Mandatory Access Control (MAC)

MAC is an access control methodology wherein subjects obtain access to resources based on the evaluation of subject, resource, action, and environment attributes. Access requests typically include resource attributes such as visible labels and metadata tags, which convey information about the sensitivity of the associated resource.

1.2 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]**.

1.3 Normative References

[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.

[XACML3] OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version 3.0", April 2010. 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

1.4 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

[ISO3166] ISO 3166 Maintenance agency (ISO 3166/MA), http://www.iso.org/iso/country_codes.htm

[DublinCore] Dublin Core Metadata Element Set, version 1.1. http://dublincore.org/documents/dces/

1.5 Scope

DLP and NAC tools are policy-driven enforcement systems. This profile defines standard XACML attributes for these DLP and NAC use cases, and recommends the adoption of standardized attribute values.

1.6 Use cases

1.6.1 Data Loss Prevention

1.6.1.1 Prevent sensitive data from being read/modified by unauthorized users

This generic use case encompasses many permutations of these attributes. Consider the nearly ubiquitous case where an administrator needs to limit the actions of users to certain groups for each action type. For example, Group 1 should be able to create data objects in the target location; group 2 should be able to edit data objects in the same location; groups 1, 2, and 3 should be able to read the contents without being able to edit them; and groups 1 and 4 should be able to delete the data objects. These policies must be enforced on a plethora of computing and network devices with diverse operating systems.

Comment [q1]: You mention what group 1 & 2 should be able to do, but you don't mention what group 3 should be able to do, unless its read only?

Comment [j2]: Yes, read only

1.6.1.2 Prevent sensitive data from being emailed to unauthorized users

Email systems are often the vector through which sensitive data escapes, both intentionally and unintentionally, without authorization. To prevent data loss, security administrators must be able to define and enforce policies that limit which subjects may email certain types of resources to specific recipient subjects. These policies may be enforced on the email client and/or the email gateway servers.

1.6.1.3 Prevent sensitive data from being transferred via web-mail

Security administrators need to be able to prohibit subjects from transferring sensitive data resources via web-mail systems. These policies may be enforced on endpoint devices such as desktops, laptops, and mobile devices, and on web proxy computers and appliances.

1.6.1.4 Prevent sensitive data from being copied from one computer to another

Security administrators need to be able to ensure data containment, i.e., certain data objects must not be copied or transferred outside of special or high-security computing and network environments. These policies may be enforced on endpoint devices (such as desktops, laptops, and mobile devices), servers, network devices, and firewalls.

1.6.1.5 Prevent sensitive data from being transferred to removable media

Removable media is another common vector for data loss. Security administrators must be able to enforce policies to prohibit subjects from transferring specific resources to removable media devices. These policies will be enforced on endpoint devices and servers.

1.6.1.6 Prevent sensitive data from being transferred to disallowed URLs

Data exfiltration may occur via standard web protocols such as HTTP and HTTPS. Security administrators need to be able to prohibit subjects from transferring specific resources via HTTP(S) outside the local domain or to certain disallowed URLs. These policies may be enforced at endpoint devices as well as firewalls, network devices, web proxies, and web portals.

1.6.2 Network Access Control

1.6.2.1 Prevent traffic flow between network resources, based on protocol

Network devices that control the flow of network traffic (e.g. firewall) may need to restrict network traffic based on policy regarding the type of protocols allowed. For example, a policy may disallow transfer of resources using unsecured protocols such as ftp, but will allow the more secure sftp protocol.

1.6.2.2 Restrict users to certain network resources, based on subject attributes

Network devices that control access to network resources (e.g. VPN) may restrict an authenticated user's access to subnets, such as secure access zones or enclaves, based on policy regarding the type of subject attributes.

1.7 Disclaimer

2 Profile

2.1 Resource Attributes

The following Resource Attributes defined in section 10.2.6 of **[XACML3]** facilitate the description of DLP and NAC objects for the purpose of creating access control policies.

2.1.1 Resource-id

The Resource-id value shall be designated with the following attribute identifier:

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

The `DataType` of this attribute is `http://www.w3.org/2001/XMLSchema#anyURI`. This attribute denotes the uniform resource identifier of the requested resource.

2.1.2 Resource-location

The Resource-location value shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:1.0:resource:resource-location
```

Allowable `DataTypes` for this attribute are: `http://www.w3.org/2001/XMLSchema#anyURI`, `urn:oasis:names:tc:xacml:2.0:data-type:ipAddress`, `urn:oasis:names:tc:xacml:2.0:data-type:dnsName`, and `urn:ogc:def:dataType:geoxacml:1.0:geometry`. This attribute denotes the logical and/or physical location of the requested resource.

2.2 Subject Attributes

2.2.1 Subject-ID

This is the identifier for the subject issuing the request, which may include user identifiers, machine identifiers, and/or application identifiers.

Subject-ID classification values shall be designated with the following attribute identifier:

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

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

2.2.2 Subject-ID-Qualifier

This identifier indicates the security domain of the subject. It identifies the administrator and ***policy*** that manages the name-space in which the ***subject*** id is administered.

Subject-ID-Qualifier classification values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier
```

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

2.2.3 Recipient-Subject-ID

This identifier indicates the entity that will receive the results of the request, which may include user identifiers, machine identifiers, and/or application identifiers.

Subject-ID classification values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:1.0:subject:recipient-subject-id
```

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

2.2.4 Recipient-Subject-ID-Qualifier

This identifier indicates the security domain of the recipient subject. It identifies the administrator and ***policy*** that manages the name-space in which the ***recipient-subject*** id is administered.

Subject-ID-Qualifier classification values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:1.0:subject:recipient-subject-id-qualifier
```

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

2.2.5 Requesting-Machine

This identifier indicates the address of the machine from which the access request originated. Requesting-machine classification values shall be designated with the following attribute identifier.

```
urn:oasis:names:tc:xacml:1.0:subject:requesting-machine
```

The following DataTypes can be used with this attribute: urn:oasis:names:tc:xacml:2.0:data-type:ipAddress, urn:oasis:names:tc:xacml:2.0:data-type:dnsName

Comment [q3]: Yes, macAddress is needed.
1.) I propose adding `urn:oasis:names:tc:xacml:3.0:data-type:macAddress.`
2.) There may be cases where you would want both the requesting machine's IP and MAC. Do we allow 2 of this attribute with different data types?

Comment [j4]: MAC address?

2.2.6 Recipient-Machine

This identifier indicates the address of the machine(s) to which the access will be granted. Recipient-machine classification values shall be designated with the following attribute identifier.

```
urn:oasis:names:tc:xacml:1.0:subject:recipient-machine
```

The following DataTypes can be used with this attribute: urn:oasis:names:tc:xacml:2.0:data-type:ipAddress, urn:oasis:names:tc:xacml:2.0:data-type:dnsName. The attribute value may include full paths including volume names, where applicable. The attribute may take multiple values.

Comment [q5]: Yes, macAddress is needed.
1.) I propose adding `urn:oasis:names:tc:xacml:3.0:data-type:macAddress.`
2.)There may be cases where you would want both the recipient machine's IP and MAC. Do we allow 2 of this attribute with different data types?

Comment [j6]: MAC address?

2.2.7 Recipient-removable-media

This identifier indicates whether or not the destination of the action is a removable media device. Recipient-removable-media classification values shall be designated with the following attribute identifier.

```
urn:oasis:names:tc:xacml:1.0:subject:recipient-removable-media
```

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

Comment [q7]: Is this an extension of the 1.0 subject or do we want to make it a new 3.0 attribute?

Comment [j8]: Need feedback from the TC

2.2.8 Authentication-Time

This identifier indicates the time at which the ***subject*** was authenticated. Authentication-Time classification values shall be designated with the following attribute identifier.

```
urn:oasis:names:tc:xacml:1.0:subject:authentication-time
```

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

2.2.9 Authentication-Method

This identifier indicates the method used to authenticate the ***subject***. Authentication-Method classification values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:1.0:subject:authentication-method
```

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

2.2.10 Request-Time

This identifier indicates the time at which the ***subject*** initiated the ***access*** request, according to the ***PEP***. Request-Time classification values shall be designated with the following attribute identifier:

```
urn:oasis:names:tc:xacml:1.0:subject:request-time
```

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

2.2.11 IP Address

This identifier indicates the location where authentication credentials were activated, expressed as an IP Address:

```
urn:oasis:names:tc:xacml:3.0:subject:authn-locality:ip-address
```

The DataType of this attribute is urn:oasis:names:tc:xacml:2.0:data-type:ipAddress.

2.2.12 DNS Name

This identifier indicates that the subject location is expressed as a DNS name.
`urn:oasis:names:tc:xacml:3.0:subject:authn-locality:dns-name`

The DataType of this attribute is urn:oasis:names:tc:xacml:2.0:data-type:dnsName.

2.3 Action Attributes

The following action attribute values correspond to the action-id identifier:
`urn:oasis:names:tc:xacml:1.0:action:action-id.`

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

Additional action-IDs can be defined as needed.

Data Loss Prevention	*Network Access Control*
Create	SMTP
Read	FTP
Update	SFTP
Delete	IMAP
Copy	POP
Email-send	RPC
HTTP GET	HTTP
HTTP PUT	HTTPS
HTTP POST	LDAP
HTTP HEAD	TCP (ports can be specified)
HTTP DELETE	UDP (ports can be specified)
HTTP OPTIONS	

2.4 Obligations

The <Obligation> element will be used in the XACML response to notify requestor that additional processing requirements are needed. This profile focuses on the use of obligations to encryption and visual marking. The XACML response may contains one or more obligations. Processing of an obligation is application specific. An <Obligation> may contain the object (resource) action pairing information. If multiple vocabularies are used for resource definitions the origin of the vocabulary MUST be identified.

The obligation should conform to following structure:

Comment [q9]: Should there also be a 3.0 authn-locality:macAddress?

Comment [j10]: Need feedback from TC on whether or not to create urn:oasis:names:tc:xacml:3.0:subject:authn-locality:macAddress.

```
urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation
```

2.4.1 Encrypt

The Encrypt obligation shall be designated with the following identifier:

```
urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt
```

The encrypt obligation can be used to command PEPs (Policy Enforcement Points) to encrypt the resource. This profile does not specify the type of encryption or other parameters to be used; rather, the details of implementation are left to the discretion of policy authors and software developers as to how to best meet their individual requirements.

The following is an example of the Encrypt obligation:

```
<ObligationExpressions>
  <ObligationExpression
   ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"
   FulfillOn="Permit"/>
  </ObligationExpression>
</ObligationExpressions>
```

2.4.2 Marking

Marking classification values shall be designated with the following identifier:

```
urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking
```

The marking obligation can be used to command PEPs (Policy Enforcement Points) to embed visual marks, sometimes called watermarks, on data viewed both on-screen and in printed form. Policy authors may use this obligation to meet legal or contractual requirements by forcing PEPs to display text or graphics in accordance with <Permit> decisions. This profile does not specify the text or graphics which can be rendered; rather, the details of implementation are left to the discretion of policy authors as to how to best meet their individual requirements.

The following is an example of the marking obligation:

```
<ObligationExpressions>
  <ObligationExpression
      ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"
      FulfillOn="Permit">
    <AttributeAssignmentExpression
        AttributeId="urn:oasis:names:tc:xacml:3.0:example:attribute:text">
      <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string"
        >Copyright 2011 Acme</AttributeValue>
    </AttributeAssignmentExpression>
  </ObligationExpression>
</ObligationExpressions>
```

Comment [q11]: Should we reuse ipc encrypt?

Comment [j12]: I would assume having profile-specific obligations might be preferred?

Comment [q13]: Should we reuse ipc marking?

Comment [j14]: I would assume having profile-specific obligations might be preferred?

3 Identifiers

This profile defines the following URN identifiers.

3.1 Profile Identifier

The following identifier SHALL 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:dlp-nac
```

4 Examples (non-normative)

This section contains examples of how the profile attributes can be used.

4.1 DLP use cases

4.1.1 Prevent sensitive data from being read/modified by unauthorized users

This example illustrates the above use case with the following scenario:

Acme security policy restricts the ability to read and modify certain documents on a "need-to-know" basis, according to the mandatory access control model. Subjects with appropriate attributes, which may include roles, group memberships, etc., will succeed in accessing these documents, while those without the requisite attribute values will fail.

Resource Attributes	Values
Resource-ID	http://confidential.acme.com/eyes-only.xml
Resource-location	webserver1.acme.com

Subject Attributes	Values
Subject-ID	Alice
Subject-ID-qualifier	acme.com
Requesting-machine	alice-laptop.acme.com

Action Attributes	Values
Action-ID	Read, Update

This sample policy can be summarized as follows:

Target: This policy is only applicable to Resource-location = "webserver1.acme.com"

Rule: This rule is only applicable if Resource-ID contains "confidential\.acme\.com"

Then if

Subject-ID-qualifier = "acme.com"

Requesting-machine contains "\.acme\.com" AND

Action-ID = "Read" OR "Update" THEN

PERMIT

Obligation:

On PERMIT mark AND encrypt the resource

4.1.2 Prevent sensitive data from being emailed to unauthorized users

Acme security policy prohibits sending confidential information to users outside the acme.com domain. Alice attempts to send a document to Bob at Wileycorp.com. The request fails. Sample attributes and values are listed below.

Resource Attributes	Values
Resource-ID	http://confidential.acme.com/eyes-only.xml
Resource-location	webserver1.acme.com

Subject Attributes	Values
Subject-ID	Alice
Subject-ID-qualifier	acme.com
Recipient-subject-ID	Bob@Wileycorp.com
Recipient-subject-ID-qualifier	Wileycorp.com
Requesting-machine	alice-repository.acme.com

Action Attributes	Values
Action-ID	Email-send

This sample policy can be summarized as follows:

Target: This policy is only applicable to Resource-location = "webserver1.acme.com"
AND Resource-ID contains "confidential\.acme\.com"

Rule: This rule is only applicable if Action-ID = "Email-send"
Then if
Subject-ID-qualifier = "acme.com" AND
Recipient-subject-ID contains "@[Aa][Cc][Mm][Ee]\.[Cc][Oo][Mm]" AND
Recipient-subject-ID-qualifier = "acme.com" AND
Requesting-machine contains "\.acme\.com" THEN
PERMIT

Obligation:
On PERMIT mark AND encrypt the resource

4.1.3 Prevent sensitive data from being transferred via web-mail

Acme security policy prohibits sending proprietary information to personal web-mail accounts. Alice attempts to send a document to her account at big-email-service.com so that she can work on it after-hours. The request fails. Sample attributes and values are listed below.

Comment [q15]: There may be cases where there may be a company web email like OWA, which is allowed, but 'personal" email accounts are not.

Resource Attributes	Values
Resource-ID	http://confidential.acme.com/eyes-only.xml
Resource-location	webserver1.acme.com

Subject Attributes	Values
Subject-ID	Alice
Subject-ID-qualifier	acme.com
Recipient-subject-ID	Alice@big-email-service.com
Recipient-subject-ID-qualifier	big-email.service.com
Requesting-machine	alice-repository.acme.com

Action Attributes	Values
Action-ID	HTTP(S)

This sample policy can be summarized as follows:

Target: This policy is only applicable to Resource-location = "webserver1.acme.com"
AND Resource-ID contains "confidential\.acme\.com"

Rule: This rule is only applicable if Action-ID contains "HTTP"
Then if
Subject-ID-qualifier = "acme.com" AND
Recipient-subject-ID contains @[Aa][Cc][Mm][Ee]\.[Cc][Oo][Mm]" AND
Recipient-subject-ID-qualifier = "acme.com" AND
Requesting-machine contains "\.acme\.com" THEN
PERMIT

Obligation:
On PERMIT mark AND encrypt the resource.

4.1.4 Prevent sensitive data from being copied from one computer to another

Acme security policy disallows copying highly sensitive data from a hardened computer to other computers. Any attempt to copy must fail. Sample attributes and values are listed below.

Comment [q16]: I'm making the assumption that copies can only be made on the hardened computer, in which the original resides.

Resource Attributes	Values
Resource-ID	http://confidential.acme.com/eyes-only.xml
Resource-location	fortress.acme.com

Subject Attributes	Values

Subject-ID	Alice
Subject-ID-qualifier	acme.com
Requesting-machine	alice-desktop.acme.com
Recipient-machine	public-facing.acme.com

Action Attributes	**Values**
Action-ID	Copy

This sample policy can be summarized as follows:

Target: This policy is only applicable to Resource-location = "fortress.acme.com"
AND Resource-ID contains "confidential\.acme\.com"

Rule: This rule is only applicable if Action-ID = "Copy"
Then if
Requesting-machine = Recipient-machine
PERMIT

Obligation:
On PERMIT mark AND encrypt the resource.

Comment [q17]: This may not be needed if the original is already encrypted and marked, then the copy would be too.

4.1.5 Prevent sensitive data from being transferred to removable media

Acme security policy prohibits the transfer of sensitive data to removable media, such as CDs, DVDs, and USB drives. Any attempt to copy data to removable media must fail. Sample attributes and values are provided below:

Resource Attributes	**Values**
Resource-ID	http://confidential.acme.com/eyes-only.xml
Resource-location	webserver1.acme.com

Subject Attributes	**Values**
Subject-ID	Alice
Subject-ID-qualifier	acme.com
Requesting-machine	alice-laptop.acme.com
Recipient-removable-media	TRUE

Action Attributes	**Values**
Action-ID	Copy

This sample policy can be summarized as follows:

Target: This policy is only applicable to Resource-location = “webserver1.acme.com”
AND Resource-ID contains “confidential\.acme\.com”

Rule: This rule is only applicable if Action-ID = Copy
Then if
Subject-ID-qualifier = “acme.com” AND
Requesting-machine contains “\.acme\.com” AND
Recipient-removable-media = “TRUE” THEN
DENY

4.1.6 Prevent sensitive data from being transferred to disallowed URLs

Acme security policy prohibits sensitive data from being transferred outside the organization to specific sites. Alice attempts to upload a sensitive document, but the attempt fails. Sample attributes and values follow:

Resource Attributes	Values
Resource-ID	http://confidential.acme.com/eyes-only.xml
Resource-location	webserver1.acme.com

Subject Attributes	Values
Subject-ID	Alice
Subject-ID-qualifier	acme.com
Requesting-machine	alice-laptop.acme.com
Recipient-machine	cloudstoragesite.com

Action Attributes	Values
Action-ID	HTTP,

This sample policy can be summarized as follows:

Target: This policy is only applicable to Resource-location = “webserver1.acme.com”

Rule: This rule is only applicable if Resource-ID contains “confidential\.acme\.com”
Then if
Action-ID contains “HTTP” OR
Action-ID contains “FTP” THEN
DENY

Obligation:
On DENY log transfer attempt.

4.2 NAC use case examples

4.2.1 Prevent traffic flow between network resources, based on protocol

Acme security policy prohibits sensitive data from being transferred using unsecure protocols. Alice attempts to retrieve a document resource on a server using the ftp protocol, in which case the attempt fails.

Resource Attributes	Values
Resource-location	192.168.0.1

Subject Attributes	Values
Subject-ID	CN=Alice, OU=Contractor, O=Acme, C=US

Action Attributes	Values
Action-ID	FTP

This sample policy can be summarized as follows:

Target: This policy is only applicable if Subject-ID contains "O=Acme"

Rule:

If Action-ID = "FTP"

DENY

4.2.2 Restrict users to certain network resources, based on subject attributes

Acme security policy restricts access to certain secure access zones based on an authenticated subject DN of an user when using certificate-based authentication and the destination IP address. Alice, a contractor at Acme, attempts access a server containing sensitive data within a secure access zone, but is denied based on her subject DN OU status.

Resource Attributes	Values
Resource-location	10.0.0.1

Subject Attributes	Values
Subject-ID	CN=Alice, OU=Contractor, O=Acme, C=US

Action Attributes	Values
Action-ID	HTTP

This sample policy can be summarized as follows:

Target: This policy is only applicable to resource type *Resource-location* = 10\.\d*\.\d*\.\d*

Rule: This rule is only applicable if Subject-ID contains “O=Acme”
Then if
Subject-ID also contains “OU=Employee” AND
Action-ID = HTTP
THEN
PERMIT

5 Conformance

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

5.1 Attribute Identifiers

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

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

Identifiers	
urn:oasis:names:tc:xacml:1.0:resource:resource-id	M
urn:oasis:names:tc:xacml:1.0:resource:resource-location	M
urn:oasis:names:tc:xacml:1.0:subject:subject-id	M
urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier	M
urn:oasis:names:tc:xacml:1.0:subject:recipient-subject-id	M
urn:oasis:names:tc:xacml:1.0:subject:recipient-subject-id-qualifier	M
urn:oasis:names:tc:xacml:1.0:subject:requesting-machine	M
urn:oasis:names:tc:xacml:1.0:subject:recipient-machine	M
urn:oasis:names:tc:xacml:1.0:subject:recipient-removable-media	M
urn:oasis:names:tc:xacml:1.0:subject:authentication-time	M
urn:oasis:names:tc:xacml:1.0:subject:authentication-method	M
urn:oasis:names:tc:xacml:1.0:subject:request-time	M
urn:oasis:names:tc:xacml:3.0:subject:authn-locality:ip-address	M
urn:oasis:names:tc:xacml:3.0:subject:authn-locality:dns-name	M
urn:oasis:names:tc:xacml:1.0:action:action-id	M

urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt	M
urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking	M

5.2 Attribute Values

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

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

Appendix A. Acknowledgements

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

Participants:

John Tolbert, The Boeing Company
Richard Hill, The Boeing Company
Crystal Hayes, The Boeing Company

Committee members during profile development:

Person	Organization	Role

464

Appendix B. Revision History

Revision	Date	Editor	Changes Made
WD 1	8/21/2013	John Tolbert	Initial committee draft.
WD 2	9/6/2013	John Tolbert, Richard Hill, Crystal Hayes	Added glossary terms, text for use cases and examples, attributes for recipient machine and recipient-removable-media, and data-types for macAddress.