



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

Committee Specification Draft 01

02 October 2014

Specification URIs

This version:

<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/csd01/xacml-3.0-dlp-nac-v1.0-csd01.doc>
(Authoritative)
<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/csd01/xacml-3.0-dlp-nac-v1.0-csd01.html>
<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/csd01/xacml-3.0-dlp-nac-v1.0-csd01.pdf>

Previous version:

N/A

Latest version:

<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/xacml-3.0-dlp-nac-v1.0.doc>
(Authoritative)
<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/xacml-3.0-dlp-nac-v1.0.html>
<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/xacml-3.0-dlp-nac-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:

John Tolbert (john.tolbert@queraltinc.com), Queralt, Inc.
Richard Hill (richard.c.hill@boeing.com), The Boeing Company
Crystal Hayes (crystal.l.hayes@boeing.com), The Boeing Company
David Brossard (david.brossard@axiomatics.com), Axiomatics AB
Hal Lockhart (hal.lockhart@oracle.com), Oracle
Steven 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. 22 January 2013. OASIS Standard. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-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. It

also defines several new functions for comparing IP addresses and DNS names, not provided in the XACML 3.0 core specification.

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. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC’s public comment list, after subscribing to it by following the instructions at the “[Send A Comment](#)” button on the TC’s web page at <https://www.oasis-open.org/committees/xacml/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<https://www.oasis-open.org/committees/xacml/ipr.php>).

Citation format:

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

[xacml-dlp-nac-v1.0]

XACML Data Loss Prevention / Network Access Control (DLP/NAC) Profile Version 1.0. Edited by John Tolbert, Richard Hill, Crystal Hayes, David Brossard, Hal Lockhart, and Steven Legg. 02 October 2014. OASIS Committee Specification Draft 01. <http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0-csd01/xacml-3.0-dlp-nac-v1.0-csd01.html>. Latest version: <http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/xacml-3.0-dlp-nac-v1.0.html>.

Notices

Copyright © OASIS Open 2014. All Rights Reserved.

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

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

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

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

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

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

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

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

Table of Contents

1	Introduction	6
1.1	Glossary	6
1.2	Terminology	7
1.3	Normative References	7
1.4	Non-Normative References	8
1.5	Scope	8
1.6	Use cases	8
1.6.1	Data Loss Prevention	8
1.6.2	Network Access Control	9
1.7	Disclaimer	9
2	Profile	10
2.1	Network Datatypes	10
2.1.1	Portranges	10
2.1.2	IP Address Datatypes	10
2.1.3	IP Address Functions	11
2.1.4	DNS Name Datatypes	12
2.1.5	DNS Name Functions	12
2.2	Resource Attributes	13
2.2.1	Resource-id	13
2.2.2	Resource-location	13
2.3	Access Subject Attributes	14
2.3.1	Subject-ID	14
2.3.2	Subject-Security-Domain	14
2.3.3	Authentication-Time	14
2.3.4	Authentication-Method	14
2.3.5	Request-Time	14
2.3.6	IP Address	14
2.3.7	DNS Name	14
2.4	Recipient Subject Attributes	15
2.4.1	Subject-ID	15
2.4.2	Subject-Security-Domain	15
2.5	Requesting Machine Attributes	15
2.5.1	Subject-ID	15
2.6	Recipient Machine Attributes	15
2.6.1	Subject-ID	15
2.6.2	Removable-Media	16
2.7	Codebase Attributes	16
2.7.1	Authorized-Application	16
2.8	Action Attributes	16
2.8.1	Action-ID	16
2.8.2	Action-Protocol	16
2.8.3	Action-Method	17
2.9	Obligations	17

2.9.1 Encrypt	17
2.9.2 Log.....	18
2.9.3 Marking.....	18
3 Identifiers	19
3.1 Profile Identifier.....	19
4 Examples (non-normative)	20
4.1 DLP use cases.....	20
4.1.1 Prevent sensitive data from being read/modified by unauthorized users	20
4.1.2 Prevent sensitive data from being emailed to unauthorized users	22
4.1.3 Prevent sensitive data from being transferred via web-mail	25
4.1.4 Prevent sensitive data from being copied/printed from one computer to another	28
4.1.5 Prevent sensitive data from being transferred to removable media.....	31
4.1.6 Prevent sensitive data from being transferred to disallowed URLs	33
4.1.7 Prevent sensitive data from being copied from one resource to another	35
4.1.8 Prevent sensitive data from being read/modified by unauthorized applications	37
4.2 NAC use case examples	40
4.2.1 Prevent traffic flow between network resources, based on protocol.....	40
4.2.2 Restrict users to certain network resources, based on subject-id.....	41
5 Conformance	43
5.1 IP Address and DNS Name Datatypes and Functions	43
5.2 Category Identifiers.....	43
5.3 Attribute Identifiers.....	44
5.4 Attribute Values	45
Appendix A. Acknowledgments	46
Appendix B. Revision History	47

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, contracts, privacy, financial, 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 will be 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. Requests made by subjects 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

Attribute Based Access Control (ABAC)

ABAC is an access control methodology wherein subjects are granted access to resources based primarily upon attributes of the subjects, resources, actions, and environments identified in a

particular request context. Attributes are characteristics of the elements above, which may be assigned by administrators and stored in Policy Information Points [XACML 3], or may be ascertained by Policy Decision Points [XACML 3] at runtime.

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.

Network Access Control (NAC)

NAC is an access control methodology wherein subjects obtain access to network-layer resources (routers, switches, and endpoints) based on the evaluation of subject, resource, action, and environment attributes. Subjects may include users and devices. Actions may include commonly defined services and protocols as well as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports.

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, <i>Key words for use in RFCs to Indicate Requirement Levels</i> , http://www.ietf.org/rfc/rfc2119.txt , IETF RFC 2119, March 1997. |
| [RFC 3986] | T. Berners-Lee, <i>Uniform Resource Identifier (URI): Generic Syntax</i> , http://www.rfc-editor.org/rfc/rfc3986.txt , IETF RFC 3986, January 2005 |
| [XACML-IPC] | OASIS Standard, eXtensible Access Control Markup Language (XACML) Intellectual Property Controls (IPC) profile, Version 1.0, March 2013. http://docs.oasis-open.org/xacml/3.0/ipc/v1.0/cs02/xacml-3.0-ipc-v1.0-cs02-en.pdf |
| [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 |
| [JSON] | <i>JSON Profile of XACML 3.0 Version 1.0</i> . Edited by David Brossard. 15 May 2014. OASIS Committee Specification Draft 03 / Public Review Draft 03. http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/csprd03/xacml-json-http- |

v1.0-csprd03.html. Latest version: <http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/xacml-json-http-v1.0.html>.

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 target 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 enforceable on a plethora of computing and network devices with diverse operating systems.

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. For example, a policy may prohibit sending proprietary information to recipients who are not licensed to have it [XACML-IPC]. 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/printed 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

139 policies may be enforced on endpoint devices (such as desktops, laptops, and mobile devices), servers,
140 printers, network devices, and firewalls.

141 **1.6.1.5 Prevent sensitive data from being transferred to removable media**

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

145 **1.6.1.6 Prevent sensitive data from being transferred to disallowed URLs**

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

150 **1.6.1.7 Prevent sensitive data from being copied from one resource to another**

151 Sensitive data may not be copied from a specific resource or location to another. This prevents malicious
152 actors from copying data into new files or databases to evade security controls.

153 **1.6.1.8 Prevent sensitive data from being read/modified by unauthorized** 154 **applications**

155 Policies may stipulate which applications can read or modify resources to prevent insecure applications or
156 malware-compromised applications from contaminating or exfiltrating sensitive data. This use case
157 assumes that the Policy Decision Point (PDP) can call an external configuration management database to
158 determine if the application is on the approved list.

159 **1.6.2 Network Access Control**

160 **1.6.2.1 Prevent traffic flow between network resources, based on protocol**

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

164 **1.6.2.2 Restrict users to certain network resources, based on subject attributes**

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

168 **1.7 Disclaimer**

2 Profile

2.1 Network Datatypes

This section defines several datatypes and functions related to determining network location using either IP Address or DNS name. Network locations are used as both Resource and Subject Attributes as described in the sections below.

2.1.1 Portranges

Both IP Address types and DNS Name types MAY include a port range list. An IP port is a 16 bit number expressed in decimal. Port 0 is not used. Thus valid values for a portnumber range from 1 to 65536. The syntax SHALL be:

portrange = portnumber | "-"portnumber | portnumber "-"[portnumber]

portrangelist = portrange ["," portrange]

where "portnumber" is a decimal port number. When two port numbers are given in a range, the first must be lower than the second. The port range includes the given ports. If the port range is of the form "-x", where "x" is a port number, then the range is all ports numbered "x" and below. If the port range is of the form "x-", then the range is all ports numbered "x" and above.

Port range is the same as defined in A.2 of [XACML3]. Port range list allows multiple non contiguous ranges to be specified. The port ranges in a given port range list MAY appear in any order and MAY overlap. The port range list indicates all the ports in any of the ranges.

2.1.2 IP Address Datatypes

The "urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-value" primitive type represents an IPv4 or IPv6 network address value, with optional port. The syntax SHALL be:

ipAddress-value = ipAddress [":" port]

For an IPv4 address or IPv6 address, the address is formatted in accordance with the syntax for a "host" in [RFC 3986], section 3.2.2. (Note that an IPv6 address, in this syntax, is enclosed in literal "[" "]" brackets.) The subnet mask SHALL be omitted.

The "urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-pattern" primitive type represents an IPv4 or IPv6 network address pattern, with optional portrange list.

The syntax SHALL be:

ipAddressrange = ipAddress | "-" ipAddress | ipAddress "-"[ipAddress]

ipAddressrangelist = ipAddressrange ["," ipAddressrange]

ipAddress-pattern = ipAddressrangelist [":" portrangelist]

The subnet mask SHALL be omitted. When two IP addresses are given in a range, the first must be lower than the second. The IP address range includes the given IP addresses. If the IP address range is of the form "-x", where "x" is an IP address, then the range is all IP addresses numbered "x" and below. If the IP address range is of the form "x-", then the range is all IP addresses numbered "x" and above. IP address range list allows multiple non contiguous ranges to be specified. The IP address ranges in a given IP address range list MAY appear in any order and MAY overlap. The IP address range list indicates all the IP addresses in any of the ranges.

Note that any string which is a valid IP Address value is by definition a valid IP Address pattern.

Examples

Valid ipAddress-values

192.168.1.2
101.86.23.0:443
[602:ea8:85a3:8d3:223:8a2e:370:ff04]
[602:ea8:85a3::370:ff04]
[2001:db8:85a3:8d3:1319:8a2e:370:7348]:80

Invalid ipAddress-values

192.168.1.556 // value too large
101.12.2.1-101.12.2.127 // ip address range not allowed
192.168.54.3/16 // mask not allowed
101.86.23.0:443-1024 // port range not allowed
[602:ea8:85a3:8d3:223:8a2e:cex:ff04] // value not hexadecimal
[602:ea8::85a3::370:ff04] // multiple ::
[2001:db8:85a3:8d3:1319:8a2e:370:7348]:80-200 // port range not allowed

Valid ipAddress-patterns

192.168.1.2-192.168.1.125
101.86.23.0-101.86.100.255, 101.20.1.1-101.86.50.255:443
[602:ea8:85a3:8d3:223:8a2e:370:ff04]:1-1023
[602:ea8:85a3::370:1]-[602:ea8:85a3::370:ff04]:80

Invalid ipAddress-patterns

192.168.5.2-192.168.1.125 // range not low to high
[602:ea8:85a3:8d3:223:8a2e:370:ff04]:1-90000 // port out of range

2.1.3 IP Address Functions

The following functions are matching functions for the IP Address datatypes.

- urn:oasis:names:tc:xacml:3.0:function:ipAddress-match

This function SHALL take one argument of data-type “urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-pattern” and a second argument of type “urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-value” and SHALL return an “http://www.w3.org/2001/XMLSchema#boolean”. The function SHALL return “True” if and only if the following conditions are met.

- The first and second arguments SHALL both be of the same IP version (4 or 6).
- The value of the second argument SHALL be identical to one of the values in the IP address range list of the first argument.
- Any port or port range values in either argument SHALL be ignored.

Otherwise, it SHALL return “False”.

252

253 • urn:oasis:names:tc:xacml:3.0:function:ipAddress-endpoint-match

254 • This function SHALL take one argument of data-type “urn:oasis:names:tc:xacml:3.0:data-
 255 type:ipAddress-pattern” and a second argument of type “urn:oasis:names:tc:xacml:3.0:data-
 256 type:ipAddress-value” and SHALL return an “http://www.w3.org/2001/XMLSchema#boolean”. The
 257 function SHALL return “True” if and only if the following conditions are met.

258 • The first and second arguments SHALL both be of the same IP version (4 or 6).

259 • The value of the second argument SHALL be identical to one of the values in the IP address
 260 range list of the first argument.

261 • The first argument SHALL contain a port range list and the second SHALL contain a port
 262 value which is included in the port range list of the first.

263 Otherwise, it SHALL return “False”.

264

265 • urn:oasis:names:tc:xacml:3.0:function:ipAddress-value-equal

266 This function SHALL take two arguments of data-type “urn:oasis:names:tc:xacml:3.0:data-
 267 type:ipAddress-value” and SHALL return an “http://www.w3.org/2001/XMLSchema#boolean”. The
 268 function SHALL return “True” if and only if the following conditions are met.

269 • The first and second arguments SHALL both be of the same IP version (4 or 6).

270 • The value of the first argument SHALL have a value identical to the second argument.

271 • Any port value in either argument SHALL be ignored.

272 Otherwise, it SHALL return “False”.

273 2.1.4 DNS Name Datatypes

274 The “urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value” primitive type represents a Domain Name
 275 Service (DNS) host name, with optional port. The syntax SHALL be:

276 dnsName-value = hostname [":" port]

277 The hostname is formatted in accordance with [RFC 3986], section 3.2.2.

278

279 The “urn:oasis:names:tc:xacml:3.0:data-type:dnsName-pattern” primitive type represents a Domain Name
 280 Service (DNS) host name, with optional portrange list. The syntax SHALL be:

281 dnsName-pattern = hostname [":" portrangelist]

282 The hostname is formatted in accordance with [RFC 3986], section 3.2.2, except that a wildcard “*” may
 283 be used in the left-most component of the hostname to indicate “any subdomain” under the domain
 284 specified to its right.

285 2.1.5 DNS Name Functions

286 The following functions are matching functions for the DNS Name datatypes.

287 • urn:oasis:names:tc:xacml:3.0:function:dnsName-match

288 This function SHALL take one argument of data-type “urn:oasis:names:tc:xacml:3.0:data-
 289 type:dnsName-pattern” and a second argument of type “urn:oasis:names:tc:xacml:3.0:data-
 290 type:dnsName-value” and SHALL return an “http://www.w3.org/2001/XMLSchema#boolean”. The
 291 function SHALL return “True” if and only if the following conditions are met.

292 • The number of name components in the second argument SHALL be the same as the
 293 number in the first argument and each component in the second argument SHALL be
 294 identical to the corresponding component in the first argument, except that if the leftmost

component in the first argument has the value “*” it SHALL be deemed to match any value in the corresponding component of the second argument. (Any port or port range values in either argument SHALL be ignored.)

Otherwise, it SHALL return “False”.

- urn:oasis:names:tc:xacml:3.0:function:dnsName-endpoint-match
- This function SHALL take one argument of data-type “urn:oasis:names:tc:xacml:3.0:data-type:dnsName-pattern” and a second argument of type “urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value” and SHALL return an “http://www.w3.org/2001/XMLSchema#boolean”. The function SHALL return “True” if and only if the following conditions are met.
 - The number of name components in the second argument SHALL be the same as the number in the first argument and each component in the second argument SHALL be identical to the corresponding component in the first argument, except that if the leftmost component in the first argument has the value “*” it SHALL be deemed to match any value in the corresponding component of the second argument.
 - The first argument SHALL contain a port range list and the second SHALL contain a port value which is included in the port range list of the first.

Otherwise, it SHALL return “False”.

- urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal
- This function SHALL take two arguments of data-type “urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value” and SHALL return an “http://www.w3.org/2001/XMLSchema#boolean”. The function SHALL return “True” if and only if the following conditions are met.
 - The number of name components in the second argument SHALL be the same as the number in the first argument and each component in the second argument SHALL be identical to the corresponding component in the first argument. (Any port values in either argument SHALL be ignored.)

Otherwise, it SHALL return “False”.

2.2 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.

2.2.1 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.

2.2.2 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:3.0:data-type:ipAddress-value`, `urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value`, and `urn:ogc:def:dataType:geoxacml:1.0:geometry`. This attribute denotes the logical and/or physical location of the requested resource.

2.3 Access Subject Attributes

The attributes in this section appear in conjunction with the access subject category [XACML3].

```
urn:oasis:names:tc:xacml:1.0:subject-category:access-subject
```

2.3.1 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>.

2.3.2 Subject-Security-Domain

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

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

```
urn:oasis:names:tc:xacml:3.0:subject:subject-security-domain
```

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

2.3.3 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>.

2.3.4 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>.

2.3.5 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>.

2.3.6 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:3.0:data-type:ipAddress-value`.

2.3.7 DNS Name

This identifier indicates that the subject location is expressed as a DNS name.

377 urn:oasis:names:tc:xacml:3.0:subject:authn-locality:dns-name
378 The `DataType` of this attribute is urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value.

379 2.4 Recipient Subject Attributes

380 The attributes in this section appear in conjunction with the recipient subject category [XACML3]:

381 urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject

382 2.4.1 Subject-ID

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

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

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

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

388 2.4.2 Subject-Security-Domain

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

391 Subject-Security-Domain classification values shall be designated with the following attribute identifier:

392 urn:oasis:names:tc:xacml:3.0:subject:subject-security-domain

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

394 2.5 Requesting Machine Attributes

395 The attributes in this section appear in conjunction with the requesting machine category [XACML3].

396 urn:oasis:names:tc:xacml:1.0:subject-category:requesting-machine

397 2.5.1 Subject-ID

398 This identifier indicates the address of the machine from which the access request originated.

399 Requesting-machine classification values shall be designated with the following attribute identifier.

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

401 The following `DataTypes` can be used with this attribute: urn:oasis:names:tc:xacml:3.0:data-
402 type:ipAddress-value and urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value. For Media Access
403 Control (MAC) addresses, use <http://www.w3.org/2001/XMLSchema#string>.

404 2.6 Recipient Machine Attributes

405 The following identifier is defined to indicate the machine to which access is intended to be granted.

406 urn:oasis:names:tc:xacml:3.0:subject-category:recipient-machine

407 The shorthand notation for this category in the JSON representation [XACML3] is RecipientMachine.

408 2.6.1 Subject-ID

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

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

412 The following `DataTypes` can be used with this attribute: urn:oasis:names:tc:xacml:3.0:data-
413 type:ipAddress-value and urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value. The attribute value
414 may include full paths including volume names, where applicable. For Media Access Control (MAC)

addresses, use <http://www.w3.org/2001/XMLSchema#string>. The attribute may take multiple values.

2.6.2 Removable-Media

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

`urn:oasis:names:tc:xacml:3.0:subject:removable-media`

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

2.7 Codebase Attributes

2.7.1 Authorized-Application

This identifier indicates whether or not the requesting application is approved for the actions requested.

`urn:oasis:names:tc:xacml:3.0:codebase:authorized-application`

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

2.8 Action Attributes

In order to create fine-grained access control rules and policies, specific action attributes must be defined. Action attributes will be grouped according to type of action.

2.8.1 Action-ID

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#boolean>.

The following action-id attributes are defined.

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

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

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

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

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

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

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

Additional action-IDs can be defined as needed.

2.8.2 Action-Protocol

For both DLP and NAC purposes, standard protocols must be available for policy authors to use.

The following action attribute values correspond to the action-protocol identifier:

`urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-protocol`

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

The list below contains a number of common protocols which can be used to construct DLP and NAC policies. The list is not comprehensive, and may be extended as need by implementers.

SMTP
FTP

SFTP
IMAP
POP
RPC
HTTP
HTTPS
LDAP
TCP (ports can be specified as TCP:81, TCP:100-120, etc.)
UDP (ports can be specified as UDP:54, UDP:100-120)

2.8.3 Action-Method

The following action attribute values correspond to the action-protocol identifier:

`urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-method`

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

The list below contains a number of action-methods which can be used to construct DLP and NAC policies. The list is based on HTTP as an example, and is not comprehensive. Additional methods may be created as needed by implementers.

GET
PUT
POST
HEAD
DELETE
OPTIONS

2.9 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:

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

2.9.1 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>
```

2.9.2 Log

The Log obligation shall be designated with the following identifier:

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

The log obligation can be used to command PEPs to make an electronic record of the access request and result. Examples of log types are syslog, application logs, operating system logs, etc. Policy authors can use this obligation to meet legal, contractual, or organizational policy requirements by forcing PEPs to record the request and response. Policy authors may find that logging both <Permit> and <Deny> decisions may be advantageous depending on the business or legal requirements. This profile does not specify the content that should be written to the log.

The following is an example of the Log obligation:

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

2.9.3 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 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>
```

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

Access Subject Attributes	Values
Subject-ID	Alice
Subject-Security-Domain	acme.com

Requesting Machine Attributes	Values
Subject-ID	alice-laptop.acme.com

Action Attributes	Values
Action-ID	Read, Update

4.1.1.1 Description

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

Access-Subject.Subject-Security-Domain = “acme.com”

Requesting-machine.Subject-ID matches “*.acme.com” AND

Action-ID = “Read” OR “Update” THEN

PERMIT

Obligation:

554 On PERMIT mark AND encrypt the resource

555 4.1.1.2 Sample Implementation in XACML 3.0

```
556 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
557   PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase411"
558   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
559   applicable"
560   Version="1.0">
561     <Description>4.1.1 Prevent sensitive data from being read/modified by unauthorized
562     users</Description>
563     <Target>
564       <AnyOf>
565         <AllOf>
566           <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
567             <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
568             >webserver1.acme.com</AttributeValue>
569             <AttributeDesignator
570               AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
571               DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
572               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
573               MustBePresent="false"/>
574             </Match>
575           </AllOf>
576         </AnyOf>
577       </Target>
578       <Rule
579         Effect="Permit"
580         RuleId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase411.confidentialAcme">
581         <Target>
582           <AnyOf>
583             <AllOf>
584               <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
585                 <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
586                 >confidential.acme.com</AttributeValue>
587                 <AttributeDesignator
588                   AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
589                   DataType="http://www.w3.org/2001/XMLSchema#anyURI"
590                   Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
591                   MustBePresent="false"/>
592                 </Match>
593             </AllOf>
594           </AnyOf>
595           <AnyOf>
596             <AllOf>
597               <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
598                 <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
599                 >acme.com</AttributeValue>
600                 <AttributeDesignator
601                   AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-
602                   domain"
603                   DataType="http://www.w3.org/2001/XMLSchema#string"
604                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
605                   MustBePresent="false"/>
606                 </Match>
607               <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-match">
608                 <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:dnsName-pattern"
609                 >*.acme.com</AttributeValue>
610                 <AttributeDesignator
611                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
612                   DataType="urn:oasis:names:tc:xacml:2.0:data-type:dnsName-value"
613                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-
614                   machine"
615                   MustBePresent="false"/>
616                 </Match>
617             </AllOf>
618           </AnyOf>
619         </AnyOf>
620       </AllOf>
621       <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
622         <AttributeValue
623           DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
```

```

624         <AttributeDesignator
625             AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
626             DataType="http://www.w3.org/2001/XMLSchema#string"
627             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
628             MustBePresent="false"/>
629     </Match>
630 </AllOf>
631 <AllOf>
632     <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
633         <AttributeValue
634             DataType="http://www.w3.org/2001/XMLSchema#string">update</AttributeValue>
635         <AttributeDesignator
636             AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
637             DataType="http://www.w3.org/2001/XMLSchema#string"
638             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
639             MustBePresent="false"/>
640     </Match>
641 </AllOf>
642 </AnyOf>
643 </Target>
644 <ObligationExpressions>
645     <ObligationExpression
646         ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"
647         FulfillOn="Permit">
648         <AttributeAssignmentExpression
649             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
650             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
651             <AttributeDesignator
652                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
653                 DataType="http://www.w3.org/2001/XMLSchema#anyURI"
654                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
655                 MustBePresent="false"/>
656             </AttributeAssignmentExpression>
657         </ObligationExpression>
658     <ObligationExpression
659         ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"
660         FulfillOn="Permit">
661         <AttributeAssignmentExpression
662             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
663             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
664             <AttributeDesignator
665                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
666                 DataType="http://www.w3.org/2001/XMLSchema#anyURI"
667                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
668                 MustBePresent="false"/>
669             </AttributeAssignmentExpression>
670         </ObligationExpression>
671     </ObligationExpressions>
672 </Rule>
673 </Policy>

```

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

Access Subject Attributes	Values
Subject-ID	Alice

Subject-Security-Domain	acme.com
-------------------------	----------

Recipient Subject Attributes	Values
Subject-ID	Bob@Wileycorp.com
Subject-Security-Domain	Wileycorp.com

Requesting Machine Attributes	Values
Subject-ID	alice-repository.acme.com

Action Attributes	Values
Action-ID	Email-send

4.1.2.1 Description

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

Access-Subject.Subject-Security-Domain = “acme.com” AND

Recipient-Subject.Subject-ID contains “[Aa][Cc][Mm][Ee]\.[Cc][Oo][Mm]” AND

Recipient-Subject.Subject-Security-Domain = “acme.com” AND

Requesting-machine.Subject-ID matches “*.acme.com” THEN

PERMIT

Obligation:

On PERMIT mark AND encrypt the resource

4.1.2.2 Sample Implementation in XACML 3.0

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicyId="urn:oasis:names:tc:xacml:dlp nac:policies.useCase412"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable"
  Version="1.0">
  <Description>4.1.2 Prevent sensitive data from being emailed to unauthorized
users</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
          <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            >webserver1.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
            DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule RuleId="4.1.2 Prevent sensitive data from being emailed to unauthorized
users"
    Condition="true"
    Outcome="permit"/>
</Policy>
```

```

719     </Match>
720   </AllOf>
721 </AnyOf>
722 <AnyOf>
723   <AllOf>
724     <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
725       <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
726         >confidential.acme.com</AttributeValue>
727       <AttributeDesignator
728         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
729         DataType="http://www.w3.org/2001/XMLSchema#anyURI"
730         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
731         MustBePresent="false"/>
732     </Match>
733   </AllOf>
734 </AnyOf>
735 </Target>
736 <Rule
737   Effect="Permit"
738   RuleId="urn:oasis:names:tc:xacml:dlp nac.policies.useCase412.sendEmail">
739   <Description>This rule is only applicable if Action-ID = "Email-send"</Description>
740   <Target>
741     <AnyOf>
742       <AllOf>
743         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
744           <AttributeValue
745             DataType="http://www.w3.org/2001/XMLSchema#string">Email-
746 send</AttributeValue>
747           <AttributeDesignator
748             AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
749             DataType="http://www.w3.org/2001/XMLSchema#string"
750             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
751             MustBePresent="false"
752           />
753         </Match>
754         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
755           <AttributeValue
756             DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
757           <AttributeDesignator
758             AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-
759 domain"
760             DataType="http://www.w3.org/2001/XMLSchema#string"
761             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
762             MustBePresent="false"
763           />
764         </Match>
765         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
766           <AttributeValue
767             DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
768           <AttributeDesignator
769             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
770             DataType="urn:oasis:names:tc:xacml:1.0:rfc822Name"
771             Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-
772 subject"
773             MustBePresent="false"
774           />
775         </Match>
776         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
777           <AttributeValue
778             DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
779           <AttributeDesignator
780             AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-
781 domain"
782             DataType="http://www.w3.org/2001/XMLSchema#string"
783             Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-
784 subject"
785             MustBePresent="false"
786           />
787         </Match>
788         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-match">
789           <AttributeValue
790             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-pattern"
791             >*.acme.com</AttributeValue>

```

```

      <AttributeDesignator
        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        DataType="urn:oasis:names:tc:xacml:2.0:data-type:dnsName-value"
        Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-
machine"
        MustBePresent="false"
      />
    </Match>
  </Allof>
</AnyOf>
</Target>
<ObligationExpressions>
  <ObligationExpression
    ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"
    FulfillOn="Permit">
    <AttributeAssignmentExpression
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
      <AttributeDesignator
        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI"
        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
        MustBePresent="false"
      />
    </AttributeAssignmentExpression>
  </ObligationExpression>
  <ObligationExpression
    ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"
    FulfillOn="Permit">
    <AttributeAssignmentExpression
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
      <AttributeDesignator
        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI"
        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
        MustBePresent="false"
      />
    </AttributeAssignmentExpression>
  </ObligationExpression>
</ObligationExpressions>
</Rule>
</Policy>

```

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.

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

Access Subject Attributes	Values
Subject-ID	Alice
Subject-Security-Domain	acme.com

Recipient Subject Attributes	Values
------------------------------	--------

Subject-ID	Alice@big-email-service.com
Subject-Security-Domain	big-email.service.com

Requesting Machine Attributes	Values
Subject-ID	alice-repository.acme.com

Action Attributes	Values
Action-Protocol	HTTP(S)

4.1.3.1 Description

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-Protocol contains “HTTP”
Then if

Access-Subject.Subject-Security-Domain = “acme.com” AND
Recipient-Subject.Subject-ID contains @[Aa][Cc][Mm][Ee]\.[Cc][Oo][Mm]” AND
Recipient-Subject.Subject-Security-Domain = “acme.com” AND
Requesting-Machine.Subject-ID matches “*.acme.com” THEN
PERMIT

Obligation:

On PERMIT mark AND encrypt the resource.

4.1.3.2 Sample Implementation in XACML 3.0

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicyId="urn:oasis:names:tc:xacml:dlp nac.policies.useCase413"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable"
  Version="1.0">
  <Description>4.1.3 Prevent sensitive data from being transferred via web-
mail</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
          <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            >webserver1.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
            DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"/>
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
          <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
            >confidential.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
```

```

888         DataType="http://www.w3.org/2001/XMLSchema#anyURI"
889         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
890         MustBePresent="false"
891     />
892 </Match>
893 </AllOf>
894 </AnyOf>
895 </Target>
896 <Rule
897     Effect="Permit"
898     RuleId="urn:oasis:names:tc:xacml:dlp_nac:policies.useCase413.allowHTTP">
899     <Description>This rule is only applicable if Action-Protocol contains
900     "HTTP"</Description>
901     <Target>
902         <AnyOf>
903             <AllOf>
904                 <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-contains">
905                     <AttributeValue
906                         DataType="http://www.w3.org/2001/XMLSchema#string">HTTP</AttributeValue>
907                     <AttributeDesignator
908                         AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-
909 protocol"
910                         DataType="http://www.w3.org/2001/XMLSchema#string"
911                         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
912                         MustBePresent="false"
913                     />
914                 </Match>
915                 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
916                     <AttributeValue
917                         DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
918                     <AttributeDesignator
919                         AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-
920 domain"
921                         DataType="http://www.w3.org/2001/XMLSchema#string"
922                         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
923 subject"
924                         MustBePresent="false"
925                     />
926                 </Match>
927                 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
928                     <AttributeValue
929                         DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
930                     <AttributeDesignator
931                         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
932                         DataType="urn:oasis:names:tc:xacml:1.0:rfc822Name"
933                         Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-
934 subject"
935                         MustBePresent="false"
936                     />
937                 </Match>
938                 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
939                     <AttributeValue
940                         DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
941                     <AttributeDesignator
942                         AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-
943 domain"
944                         DataType="http://www.w3.org/2001/XMLSchema#string"
945                         Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-
946 subject"
947                         MustBePresent="false"
948                     />
949                 </Match>
950                 <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-match">
951                     <AttributeValue
952                         DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-pattern"
953                         >*.acme.com</AttributeValue>
954                     <AttributeDesignator
955                         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
956                         DataType="urn:oasis:names:tc:xacml:2.0:data-type:dnsName-value"
957                         Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-
958 machine"
959                         MustBePresent="false"
960                     />

```

```

961         </Match>
962     </AllOf>
963 </AnyOf>
964 </Target>
965 <ObligationExpressions>
966     <ObligationExpression
967         ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"
968         FulfillOn="Permit">
969         <AttributeAssignmentExpression
970             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
971             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
972             <AttributeDesignator
973                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
974                 DataType="http://www.w3.org/2001/XMLSchema#anyURI"
975                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
976                 MustBePresent="false"
977             />
978         </AttributeAssignmentExpression>
979     </ObligationExpression>
980     <ObligationExpression
981         ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"
982         FulfillOn="Permit">
983         <AttributeAssignmentExpression
984             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
985             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
986             <AttributeDesignator
987                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
988                 DataType="http://www.w3.org/2001/XMLSchema#anyURI"
989                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
990                 MustBePresent="false"
991             />
992         </AttributeAssignmentExpression>
993     </ObligationExpression>
994 </ObligationExpressions>
995 </Rule>
996 </Policy>

```

4.1.4 Prevent sensitive data from being copied/printed 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.

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

Access Subject Attributes	Values
Subject-ID	Alice
Subject-Security-Domain	acme.com

Requesting Machine Attributes	Values
Subject-ID	alice-desktop.acme.com

Recipient Machine Attributes	Values
Subject-ID	public-facing.acme.com

1006

Action Attributes	Values
Action-ID	Copy or Print

1007 **4.1.4.1 Description**

1008 This sample policy can be summarized as follows:

1009

1010 **Target:** This policy is only applicable to Resource-location = "fortress.acme.com"

1011 AND Resource-ID contains "confidential.acme.com"

1012

1013 **Rule:** This rule is only applicable if Action-ID = "Copy" or "Print"

1014 Then if

1015 Requesting-Machine.Subject-ID = Recipient-Machine.Subject-ID

1016 PERMIT

1017

1018 **Obligation:**

1019 On PERMIT mark AND encrypt the resource.

1020 **4.1.4.2 Sample Implementation in XACML 3.0**

```
1021 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
1022   PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase414"
1023   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
1024   applicable"
1025   Version="1.0">
1026     <Description>4.1.4 Prevent sensitive data from being copied/printed from one computer
1027     to another</Description>
1028     <Target>
1029       <AnyOf>
1030         <AllOf>
1031           <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
1032             <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1033             >fortress.acme.com</AttributeValue>
1034             <AttributeDesignator
1035               AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
1036               DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1037               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1038               MustBePresent="false"/>
1039           </Match>
1040           <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
1041             <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
1042             >confidential.acme.com</AttributeValue>
1043             <AttributeDesignator
1044               AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1045               DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1046               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1047               MustBePresent="false"
1048             />
1049           </Match>
1050         </AllOf>
1051       </AnyOf>
1052     </Target>
1053     <Rule
1054       Effect="Permit"
1055       RuleId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase414.copyOrPrint">
1056       <Description>This rule is only applicable if Action-ID = "Copy" or
1057       "Print"</Description>
1058       <Target>
1059         <AnyOf>
```



```

1060      <Allof>
1061        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1062          <AttributeValue
1063            DataType="http://www.w3.org/2001/XMLSchema#string">Copy</AttributeValue>
1064          <AttributeDesignator
1065            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1066            DataType="http://www.w3.org/2001/XMLSchema#string"
1067            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1068            MustBePresent="false"
1069          />
1070        </Match>
1071      </Allof>
1072      <Allof>
1073        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1074          <AttributeValue
1075            DataType="http://www.w3.org/2001/XMLSchema#string">Print</AttributeValue>
1076          <AttributeDesignator
1077            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1078            DataType="http://www.w3.org/2001/XMLSchema#string"
1079            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1080            MustBePresent="false"
1081          />
1082        </Match>
1083      </Allof>
1084    </AnyOf>
1085  </Target>
1086  <Condition>
1087    <Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:ipAddress-value-equal">
1088      <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-one-and-
1089only" >
1090        <AttributeDesignator
1091          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
1092          DataType="urn:oasis:names:tc:xacml:2.0:data-type:ipAddress-value"
1093          Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-
1094machine"
1095          MustBePresent="false"
1096        />
1097      </Apply>
1098      <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-one-and-
1099only" >
1100        <AttributeDesignator
1101          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
1102          DataType="urn:oasis:names:tc:xacml:2.0:data-type:ipAddress-value"
1103          Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-machine"
1104          MustBePresent="false"
1105        />
1106      </Apply>
1107    </Apply>
1108  </Condition>
1109  <ObligationExpressions>
1110    <ObligationExpression
1111      ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"
1112      FulfillOn="Permit">
1113      <AttributeAssignmentExpression
1114        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1115        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1116      <AttributeDesignator
1117        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1118        DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1119        Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1120        MustBePresent="false"
1121      />
1122    </AttributeAssignmentExpression>
1123  </ObligationExpression>
1124  <ObligationExpression
1125    ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"
1126    FulfillOn="Permit">
1127    <AttributeAssignmentExpression
1128      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1129      Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1130    <AttributeDesignator
1131      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1132      DataType="http://www.w3.org/2001/XMLSchema#anyURI"

```

```

1133         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1134         MustBePresent="false"
1135     />
1136 </AttributeAssignmentExpression>
1137 </ObligationExpression>
1138 </ObligationExpressions>
1139 </Rule>
1140 </Policy>

```

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

Access Subject Attributes	Values
Subject-ID	Alice
Subject-Security-Domain	acme.com

Requesting Machine Attributes	Values
Subject-ID	alice-laptop.acme.com

Recipient Machine Attributes	Values
Removable-media	true

Action Attributes	Values
Action-ID	Copy or Print

4.1.5.1 Description

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

Access-Subject.Subject-Security-Domain = "acme.com" AND

Requesting-Machine.Subject-ID matches "*.acme.com" AND

Recipient-Machine.Removable-Media = "TRUE" THEN

DENY

4.1.5.2 Sample Implementation in XACML 3.0

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicyId="urn:oasis.names.tc.xacml.dlp_nac.policies.useCase415"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable"
  Version="1.0">
  <Description>4.1.5 Prevent sensitive data from being transferred to removable
media</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
          <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            >webserver1.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
            DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"/>
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
          <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
            >confidential.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType="http://www.w3.org/2001/XMLSchema#anyURI"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"
            />
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule
    Effect="Deny"
    RuleId="urn:oasis.names.tc.xacml.dlp_nac.policies.useCase415.copy">
    <Description>Rule: This rule is only applicable if Action-ID = Copy</Description>
    <Target>
      <AnyOf>
        <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">Copy</AttributeValue>
            <AttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
              MustBePresent="false"
              />
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
            <AttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-
domain"
              DataType="http://www.w3.org/2001/XMLSchema#string"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject"
              MustBePresent="false"
              />
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-match">
            <AttributeValue
              DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-pattern"
              >*.acme.com</AttributeValue>
            <AttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
              DataType="urn:oasis:names:tc:xacml:2.0:data-type:dnsName-value"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-
machine"
```

```

1234         MustBePresent="false"
1235     />
1236 </Match>
1237 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
1238     <AttributeValue
1239         DataType="http://www.w3.org/2001/XMLSchema#boolean">true</AttributeValue>
1240     <AttributeDesignator
1241         AttributeId="urn:oasis:names:tc:xacml:3.0:subject:removable-media"
1242         DataType="http://www.w3.org/2001/XMLSchema#boolean"
1243         Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-
1244 machine"
1245         MustBePresent="false"
1246     />
1247 </Match>
1248 </AllOf>
1249 </AnyOf>
1250 </Target>
1251 </Rule>
1252 </Policy>

```

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

Access Subject Attributes	Values
Subject-ID	Alice
Subject-Security-Domain	acme.com

Requesting Machine Attributes	Values
Subject-ID	alice-laptop.acme.com

Recipient Machine Attributes	Values
Subject-ID	cloudstoragesite.com

Action Attributes	Values
Action-Protocol	HTTP

4.1.6.1 Description

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-Protocol contains "HTTP" OR
Action-Protocol contains "FTP" THEN
DENY

Obligation:

On DENY log transfer attempt.

4.1.6.2 Sample Implementation in XACML 3.0

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase416"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable"
  Version="1.0">
  <Description>4.1.6 Prevent sensitive data from being transferred to disallowed
URLs</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
          <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            >webserver1.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
            DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule
    Effect="Deny"
    RuleId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase416.confidentialDomain">
    <Description>This rule is only applicable if Resource-ID contains
"confidential.acme.com"</Description>
    <Target>
      <AnyOf>
        <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
              >confidential.acme.com</AttributeValue>
            <AttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
              DataType="http://www.w3.org/2001/XMLSchema#anyURI"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
              MustBePresent="false"
            />
          </Match>
        </AllOf>
      </AnyOf>
    </AnyOf>
    <AllOf>
      <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">HTTP</AttributeValue>
        <AttributeDesignator
          AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-protocol"
          DataType="http://www.w3.org/2001/XMLSchema#string"
          Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
          MustBePresent="false"
        />
      </Match>
    </AllOf>
  </Rule>
  <AllOf>
    <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```

1334         <AttributeValue
1335             DataType="http://www.w3.org/2001/XMLSchema#string">FTP</AttributeValue>
1336         <AttributeDesignator
1337             AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-
1338 protocol"
1339             DataType="http://www.w3.org/2001/XMLSchema#string"
1340             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1341             MustBePresent="false"
1342         />
1343     </Match>
1344 </AllOf>
1345 </AnyOf>
1346 </Target>
1347 <ObligationExpressions>
1348     <ObligationExpression
1349         ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:log-transfer-
1350 attempt"
1351         FulfillOn="Deny">
1352         <AttributeAssignmentExpression
1353             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1354             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1355             <AttributeDesignator
1356                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1357                 DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1358                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1359                 MustBePresent="false"
1360             />
1361             </AttributeAssignmentExpression>
1362             <AttributeAssignmentExpression
1363                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1364                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
1365                 <AttributeValue
1366                     DataType="http://www.w3.org/2001/XMLSchema#string">Transfer</AttributeValue>
1367                 </AttributeAssignmentExpression>
1368             </ObligationExpression>
1369         </ObligationExpressions>
1370     </Rule>
1371 </Policy>

```

4.1.7 Prevent sensitive data from being copied from one resource to another

Acme security policy prohibits copying proprietary information from one resource to another. Alice attempts to copy sensitive data from one resource to a new one she just created. 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

Access Subject Attributes	Values
Subject-ID	Alice
Subject-Security-Domain	acme.com

Action Attributes	Values
Action-ID	Copy

4.1.7.1 Description

This sample policy can be summarized as follows:

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

Rule: This rule is only applicable if Action-ID = "Copy"

Then if

Access-Subject.Subject-Security-Domain = "acme.com"

DENY

Obligation:

On DENY log copy attempt.

4.1.7.2 Sample Implementation in XACML 3.0

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase417"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
  applicable"
  Version="1.0">
  <Description>4.1.7 Prevent sensitive data from being copied from one resource to
  another</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
          <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            >webserver1.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
            DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"/>
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
            >confidential.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType="http://www.w3.org/2001/XMLSchema#anyURI"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"
            />
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule
    Effect="Deny"
    RuleId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase417.copy">
    <Description>This rule is only applicable if Action-ID contains "Copy"</Description>
    <Target>
      <AnyOf>
        <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">Copy</AttributeValue>
            <AttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
```

```

1440         DataType="http://www.w3.org/2001/XMLSchema#string"
1441         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1442         MustBePresent="false"
1443     />
1444 </Match>
1445 </AllOf>
1446 </AnyOf>
1447 <AnyOf>
1448     <AllOf>
1449         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1450             <AttributeValue
1451                 DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
1452             <AttributeDesignator
1453                 AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-domain"
1454                 DataType="http://www.w3.org/2001/XMLSchema#string"
1455                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
1456                 MustBePresent="false"
1457             />
1458         </Match>
1459     </AllOf>
1460 </AnyOf>
1461 </Target>
1462 <ObligationExpressions>
1463     <ObligationExpression
1464         ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:log-transfer-
1465 attempt"
1466         FulfillOn="Deny">
1467         <AttributeAssignmentExpression
1468             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1469             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1470             <AttributeDesignator
1471                 AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1472                 DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1473                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1474                 MustBePresent="false"
1475             />
1476             </AttributeAssignmentExpression>
1477             <AttributeAssignmentExpression
1478                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1479                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
1480                 <AttributeDesignator
1481                     AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1482                     DataType="http://www.w3.org/2001/XMLSchema#string"
1483                     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1484                     MustBePresent="false"
1485                 />
1486                 </AttributeAssignmentExpression>
1487             </ObligationExpression>
1488         </ObligationExpressions>
1489     </Rule>
1490 </Policy>

```

4.1.8 Prevent sensitive data from being read/modified by unauthorized applications

Acme security policy prohibits unapproved applications from reading and modifying sensitive data. Alice attempts to open a sensitive document with an unauthorized application. 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

Access Subject Attributes	Values
Subject-ID	Alice
Subject-Security-Domain	acme.com

Codebase Attribute	Values
Authorized-application	false

Action Attributes	Values
Action-Protocol	HTTP

4.1.8.1 Description

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-Protocol contains “HTTP”
Then if

Access-Subject.Subject-Security-Domain = “acme.com” AND Authorized-application = false
DENY

Obligation:

On DENY log attempt to use an authorized application

4.1.8.2 Sample Implementation in XACML 3.0

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase418"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable"
  Version="1.0">
  <Description>4.1.8 Prevent sensitive data from being read/modified by unauthorized
applications</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
          <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            >webserver1.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
            DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"/>
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
            >confidential.acme.com</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType="http://www.w3.org/2001/XMLSchema#anyURI"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            MustBePresent="false"
          />
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
```

```

1543         </Match>
1544     </AllOf>
1545 </AnyOf>
1546 </Target>
1547 <Rule
1548     Effect="Deny"
1549     RuleId="urn:oasis:names:tc:xacml:dlp_nac:policies.useCase418.httpProtocol">
1550     <Description>This rule is only applicable if Action-Protocol contains
1551 HTTP</Description>
1552     <Target>
1553         <AnyOf>
1554             <AllOf>
1555                 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1556                     <AttributeValue
1557                         DataType="http://www.w3.org/2001/XMLSchema#string">HTTP</AttributeValue>
1558                     <AttributeDesignator
1559                         AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-
1560 protocol"
1561                         DataType="http://www.w3.org/2001/XMLSchema#string"
1562                         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1563                         MustBePresent="false"
1564                     />
1565                 </Match>
1566                 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1567                     <AttributeValue
1568                         DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
1569                     <AttributeDesignator
1570                         AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-
1571 domain"
1572                         DataType="http://www.w3.org/2001/XMLSchema#string"
1573                         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
1574                         MustBePresent="false"
1575                     />
1576                 </Match>
1577                 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
1578                     <AttributeValue
1579                         DataType="http://www.w3.org/2001/XMLSchema#boolean">false</AttributeValue>
1580                     <AttributeDesignator
1581                         AttributeId="urn:oasis:names:tc:xacml:3.0:codebase:authorized-
1582 application"
1583                         DataType="http://www.w3.org/2001/XMLSchema#boolean"
1584                         Category="urn:oasis:names:tc:xacml:1.0:subject-category:codebase"
1585                         MustBePresent="false"
1586                     />
1587                 </Match>
1588             </AllOf>
1589         </AnyOf>
1590     </Target>
1591     <ObligationExpressions>
1592         <ObligationExpression
1593             ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:log-transfer-
1594 attempt"
1595             FulfillOn="Deny">
1596                 <AttributeAssignmentExpression
1597                     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1598                     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1599                     <AttributeDesignator
1600                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1601                         DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1602                         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1603                         MustBePresent="false"
1604                     />
1605                     </AttributeAssignmentExpression>
1606                     <AttributeAssignmentExpression
1607                         AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1608                         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
1609                         <AttributeValue
1610                             DataType="http://www.w3.org/2001/XMLSchema#string">access</AttributeValue>
1611                         </AttributeAssignmentExpression>
1612                     </ObligationExpression>
1613                 </ObligationExpressions>
1614             </Rule>
1615 </Policy>

```

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

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

Action Attributes	Values
Action-Protocol	FTP

4.2.1.1 Description

This sample policy can be summarized as follows:

Target: This policy is only applicable if Subject-ID ends with “O=Acme,C=US”

Rule:

If Action-Protocol = “FTP”

DENY

4.2.1.2 Sample Implementation in XACML 3.0

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase421"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable"
  Version="1.0">
  <Description>4.2.1 Prevent traffic flow between network resources, based on
protocol</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-match">
          <AttributeValue DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
            >O=Acme,C=US</AttributeValue>
          <AttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
            DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
            Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
            MustBePresent="false"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule
    Effect="Deny"
    RuleId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase421.ftpProtocol">
    <Description>This rule is only applicable if Action-Protocol equals
FTP</Description>
```

```

1660     <Target>
1661       <AnyOf>
1662         <AllOf>
1663           <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1664             <AttributeValue
1665               DataType="http://www.w3.org/2001/XMLSchema#string">FTP</AttributeValue>
1666             <AttributeDesignator
1667               AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-
1668 protocol"
1669               DataType="http://www.w3.org/2001/XMLSchema#string"
1670               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1671               MustBePresent="false"
1672             />
1673           </Match>
1674         </AllOf>
1675       </AnyOf>
1676     </Target>
1677   </Rule>
1678 </Policy>

```

4.2.2 Restrict users to certain network resources, based on subject-id

Acme security policy restricts access to certain secure access zones based on an authenticated subject DN of a 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-id OU value.

Resource Attributes	Values
Resource-location	10.0.0.1

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

Action Attributes	Values
Action-Protocol	HTTP
Action-Method	GET

4.2.2.1 Description

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 ends with "O=Employee,O=Acme,C=US"

Then if

Action-Protocol = "HTTP" AND

Action-Method = "GET"

THEN

PERMIT

4.2.2.2 Sample Implementation in XACML 3.0

```

1700 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"

```

```

1701     PolicyId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase422"
1702     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
1703     applicable"
1704     Version="1.0">
1705     <Description>4.2.2 Restrict users to certain network resources, based on subject-
1706     id</Description>
1707     <Target>
1708         <AnyOf>
1709             <AllOf>
1710                 <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:ipAddress-match">
1711                     <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-
1712     pattern"
1713                         >10.0.0.0-10.255.255.255</AttributeValue>
1714                     <AttributeDesignator
1715                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
1716                         DataType="urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-value"
1717                         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1718                         MustBePresent="false"/>
1719                     </Match>
1720                 </AllOf>
1721             </AnyOf>
1722         </Target>
1723     <Rule
1724         Effect="Permit"
1725         RuleId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase422.employee">
1726         <Description>This rule is only applicable if subject-id ends with
1727     O=Employee,O=Acme,C=US</Description>
1728         <Target>
1729             <AnyOf>
1730                 <AllOf>
1731                     <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-match">
1732                         <AttributeValue DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
1733                             >O=Employee,O=Acme,C=US</AttributeValue>
1734                         <AttributeDesignator
1735                             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
1736                             DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
1737                             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
1738                             MustBePresent="false"/>
1739                         </Match>
1740                     <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1741                         <AttributeValue
1742                             DataType="http://www.w3.org/2001/XMLSchema#string">HTTP</AttributeValue>
1743                         <AttributeDesignator
1744                             AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-protocol"
1745                             DataType="http://www.w3.org/2001/XMLSchema#string"
1746                             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1747                             MustBePresent="false"/>
1748                     <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1749                         <AttributeValue
1750                             DataType="http://www.w3.org/2001/XMLSchema#string">GET</AttributeValue>
1751                         <AttributeDesignator
1752                             AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-method"
1753                             DataType="http://www.w3.org/2001/XMLSchema#string"
1754                             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1755                             MustBePresent="false"/>
1756                     </Match>
1757                 </AllOf>
1758             </AnyOf>
1759         </Target>
1760     </Rule>
1761 </Policy>

```

5 Conformance

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

5.1 IP Address and DNS Name Datatypes and Functions

Conformant XACML **policies** and **requests** SHALL use the IP Address and DNS Name datatypes and functions defined in Section 2 for their specified purpose and SHALL NOT use any other identifiers for the purposes defined by attributes in this profile. Conformant XACML PDPs SHALL implement these datatypes and functions. The following table lists the datatypes and functions that must be supported.

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

Identifiers	
urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-value	M
urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-pattern	M
urn:oasis:names:tc:xacml:3.0:function:ipAddress-match	M
urn:oasis:names:tc:xacml:3.0:function:ipAddress-endpoint-match	M
urn:oasis:names:tc:xacml:3.0:function:ipAddress-value-equal	M
urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value	M
urn:oasis:names:tc:xacml:3.0:data-type:dnsName-pattern	M
urn:oasis:names:tc:xacml:3.0:function:dnsName-match	M
urn:oasis:names:tc:xacml:3.0:function:dnsName-endpoint-match	M
urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal	M

5.2 Category Identifiers

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

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

Identifiers

urn:oasis:names:tc:xacml:1.0:subject-category:access-subject	M
urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject	M
urn:oasis:names:tc:xacml:1.0:subject-category:requesting-machine	M
urn:oasis:names:tc:xacml:3.0:subject-category:recipient-machine	M
urn:oasis:names:tc:xacml:1.0:subject-category:codebase	M
urn:oasis:names:tc:xacml:3.0:attribute-category:action	M

1780

1781 5.3 Attribute Identifiers

1782 Conformant XACML *policies* and *requests* SHALL use the attribute identifiers defined in Section 2 for
 1783 their specified purpose and SHALL NOT use any other identifiers for the purposes defined by attributes in
 1784 this profile. The following table lists the attributes that must be supported.

1785 Note: “M” is mandatory “O” is optional.

1786

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:3.0:subject:subject-security-domain	M
urn:oasis:names:tc:xacml:3.0:subject: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:3.0:codebase:authorized-application	M

urn:oasis:names:tc:xacml:1.0:action:action-id	M
urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-protocol	M
urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-method	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

5.4 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. Acknowledgments

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
David Brossard, Axiomatics AB
Hal Lockhart, Oracle
Steven Legg, ViewDS

Committee members during profile development:

Person	Organization	Role
--------	--------------	------

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.
WD 3	10/18/2013	John Tolbert, David Brossard	Added glossary terms, edited text, added sample policy for use case example 1.
WD 4	11/18/2013	Hal Lockhart	Added IP Address and DNS Name datatypes and functions. Adjusted attribute definitions and example to use new datatypes. Added them to conformance section.
WD 5	3/18/2014	John Tolbert	Separated action-id, action-protocol, and action-method. Moved authorized-application from subject to codebase category.
WD 6	6/10/2014	John Tolbert, Richard Hill, Hal Lockhart	Added Log obligation, inserted policy examples, fixed typos and some word changes. Removed Mask from IP address datatypes. Removed network match function. Replaced IP address wildcards with IP address range list.
WD 7	6/26/2014	Hal Lockhart	Fixed typo in ipAddress-pattern definition. Corrected typos, conformance to profile and datatype mismatches in examples
WD 8	7/30/2014	Steven Legg	<p>Defined a recipient-machine subject category to hold attributes of the machine to which access is intended to be granted.</p> <p>Defined a JSON short name for recipient-machine and added a reference to the JSON Profile.</p> <p>Replaced recipient-subject-id, requesting-machine and recipient-machine attributes with the subject-id attribute in the recipient-subject, requesting-machine and recipient-machine subject categories respectively.</p> <p>Replaced subject-id-qualifier attribute with a new subject-security-domain attribute that is a better fit for the purpose.</p> <p>Moved and renamed recipient-subject-id-qualifier to subject-security-domain in the recipient-subject category.</p> <p>Replaced the recipient-removable-media attribute with the removable-media attribute in</p>

			<p>the recipient-machine category.</p> <p>Updated the examples in section 4 to reflect the preceding changes.</p> <p>Rewrote the XACML policy in example 4.1.2.2 to be consistent with its high level description.</p> <p>Added a missing term for (Action-ID = "Copy") into the XACML policy in section 4.1.5.2.</p> <p>Tweaked the matching of DNs in the examples in section 4.2 and added sample XACML policies.</p> <p>Added category identifiers to the Conformance section and revised the attribute identifiers.</p>
WD09	7/30/2014	Steven Legg	Accepted the changes to WD08.

1807