



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

## Committee Specification 01

16 February 2015

### Specification URIs

#### This version:

<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/cs01/xacml-3.0-dlp-nac-v1.0-cs01.doc>  
(Authoritative)

<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/cs01/xacml-3.0-dlp-nac-v1.0-cs01.html>

<http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/cs01/xacml-3.0-dlp-nac-v1.0-cs01.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](mailto:bill@parducci.net)), Individual

Hal Lockhart ([hal.lockhart@oracle.com](mailto:hal.lockhart@oracle.com)), Oracle

#### Editors:

John Tolbert ([john.tolbert@queraltinc.com](mailto:john.tolbert@queraltinc.com)), Queralt, Inc.

Richard Hill ([richard.c.hill@boeing.com](mailto:richard.c.hill@boeing.com)), The Boeing Company

Crystal Hayes ([crystal.l.hayes@boeing.com](mailto:crystal.l.hayes@boeing.com)), The Boeing Company

David Brossard ([david.brossard@axiomatics.com](mailto:david.brossard@axiomatics.com)), Axiomatics AB

Hal Lockhart ([hal.lockhart@oracle.com](mailto:hal.lockhart@oracle.com)), Oracle

Steven Legg ([steven.legg@viewds.com](mailto: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](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. 16 February 2015. OASIS Committee Specification 01. <http://docs.oasis-open.org/xacml/xacml-3.0-dlp-nac/v1.0/cs01/xacml-3.0-dlp-nac-v1.0-cs01.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 2015. 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

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

### 52 **Data Loss Prevention (DLP)**

53 DLP tools monitor “data-in-use” at endpoints (e.g., desktops, laptops, and mobile devices), “data-  
54 in-motion” on networks, and “data-at-rest” in storage systems. DLP tools enforce access control  
55 policies at these locations to prevent unauthorized access to and unintended disclosure of sensitive  
56 data.

### 57 **Discretionary Access Control (DAC)**

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

### 62 **Mandatory Access Control (MAC)**

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

### 67 **Network Access Control (NAC)**

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

## 73 **1.2 Terminology**

74 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD  
75 NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described  
76 in [RFC2119].

## 77 **1.3 Normative References**

- 78 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,  
79 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 80 **[RFC 3986]** T. Berners-Lee, *Uniform Resource Identifier (URI): Generic Syntax*,  
81 <http://www.rfc-editor.org/rfc/rfc3986.txt>, IETF RFC 3986, January 2005
- 82 **[XACML-IPC]** OASIS Standard, *eXtensible Access Control Markup Language (XACML)  
83 Intellectual Property Controls (IPC) profile, Version 1.0*, March 2013.  
84 [http://docs.oasis-open.org/xacml/3.0/ipc/v1.0/cs02/xacml-3.0-ipc-v1.0-cs02-  
85 en.pdf](http://docs.oasis-open.org/xacml/3.0/ipc/v1.0/cs02/xacml-3.0-ipc-v1.0-cs02-<br/>85 en.pdf)
- 86 **[XACML3]** OASIS Standard, *eXtensible Access Control Markup Language (XACML)  
87 Version 3.0*, April 2010. [http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-  
88 spec-en.doc](http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-<br/>88 spec-en.doc)
- 89 **[XACML2]** OASIS Standard, *"eXtensible Access Control Markup Language (XACML)  
90 Version 2.0"*, February 2005. [http://docs.oasis-  
91 open.org/xacml/2.0/access\\_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-<br/>91 open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)
- 92 **[XACML1]** OASIS Standard, *"eXtensible Access Control Markup Language (XACML)  
93 Version 1.0"*, February 2003. [http://www.oasis-  
94 open.org/committees/download.php/2406/oasis-xacml-1.0.pdf](http://www.oasis-<br/>94 open.org/committees/download.php/2406/oasis-xacml-1.0.pdf)
- 95 **[JSON]** *JSON Profile of XACML 3.0 Version 1.0*. Edited by David Brossard. 15 May  
96 2014. OASIS Committee Specification Draft 03 / Public Review Draft 03.  
97 <http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/csprd03/xacml-json-http->



98 v1.0-csprd03.html. Latest version: [http://docs.oasis-open.org/xacml/xacml-json-](http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/xacml-json-http-v1.0.html)  
99 [http/v1.0/xacml-json-http-v1.0.html](http://v1.0/xacml-json-http-v1.0.html).

## 100 1.4 Non-Normative References

- 101 **[XACMLIntro]** OASIS XACML TC, *A Brief Introduction to XACML*, 14 March 2003,  
102 [http://www.oasis-](http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html)  
103 [open.org/committees/download.php/2713/Brief\\_Introduction\\_to\\_XACML.html](http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html)  
104 **[ISO3166]** ISO 3166 Maintenance agency (ISO 3166/MA),  
105 [http://www.iso.org/iso/country\\_codes.htm](http://www.iso.org/iso/country_codes.htm)  
106 **[DublinCore]** Dublin Core Metadata Element Set, version 1.1.  
107 <http://dublincore.org/documents/dces/>

## 108 1.5 Scope

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

## 112 1.6 Use cases

### 113 1.6.1 Data Loss Prevention

#### 114 1.6.1.1 Prevent sensitive data from being read/modified by unauthorized users

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

#### 122 1.6.1.2 Prevent sensitive data from being emailed to unauthorized users

123 Email systems are often the vector through which sensitive data escapes, both intentionally and  
124 unintentionally, without authorization. To prevent data loss, security administrators must be able to define  
125 and enforce policies that limit which subjects may email certain types of resources to specific recipient  
126 subjects. For example, a policy may prohibit sending proprietary information to recipients who are not  
127 licensed to have it **[XACML-IPC]**. These policies may be enforced on the email client and/or the email  
128 gateway servers.

#### 129 1.6.1.3 Prevent sensitive data from being transferred via web-mail

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

#### 133 1.6.1.4 Prevent sensitive data from being copied/printed from one computer to 134 another

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



139 **1.6.1.5 Prevent sensitive data from being transferred to removable media**  
140 Removable media is another common vector for data loss. Security administrators must be able to  
141 enforce policies to prohibit subjects from transferring specific resources to removable media devices.  
142 These policies will be enforced on endpoint devices and servers.

143 **1.6.1.6 Prevent sensitive data from being transferred to disallowed URLs**  
144 Data exfiltration may occur via standard web protocols such as HTTP and HTTPS. Security  
145 administrators need to be able to prohibit subjects from transferring specific resources via HTTP(S)  
146 outside the local domain or to certain disallowed URLs. These policies may be enforced at endpoint  
147 devices as well as firewalls, network devices, web proxies, and web portals.

148 **1.6.1.7 Prevent sensitive data from being copied from one resource to another**  
149 Sensitive data may not be copied from a specific resource or location to another. This prevents malicious  
150 actors from copying data into new files or databases to evade security controls.

151 **1.6.1.8 Prevent sensitive data from being read/modified by unauthorized**  
152 **applications**  
153 Policies may stipulate which applications can read or modify resources to prevent insecure applications or  
154 malware-compromised applications from contaminating or exfiltrating sensitive data. This use case  
155 assumes that the Policy Decision Point (PDP) can call an external configuration management database to  
156 determine if the application is on the approved list.

## 157 **1.6.2 Network Access Control**

158 **1.6.2.1 Prevent traffic flow between network resources, based on protocol**  
159 Network devices that control the flow of network traffic (e.g. firewall) may need to restrict network traffic  
160 based on policy regarding the type of protocols allowed. For example, a policy may disallow transfer of  
161 resources using unsecured protocols such as ftp, but will allow the more secure SFTP protocol.

162 **1.6.2.2 Restrict users to certain network resources, based on subject attributes**  
163 Network devices that control access to network resources (e.g. VPN) may restrict an authenticated user's  
164 access to certain subnets, such as secure access zones or enclaves, based on policy regarding the type  
165 of subject attributes.

## 166 **1.7 Disclaimer**

---

## 167 2 Profile

### 168 2.1 Network Datatypes

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

#### 172 2.1.1 Portranges

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

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

177 portrangelist = portrange ["," portrange]

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

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

#### 185 2.1.2 IP Address Datatypes

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

188 ipAddress-value = ipAddress [ ":" port ]

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

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

194 The syntax SHALL be:

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

196 ipAddressrangelist = ipAddressrange ["," ipAddressrange ]

197 ipAddress-pattern = ipAddressrangelist [ ":" portrangelist ]

198

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

206

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

208

209 **Examples**

210 Valid ipAddress-values

211 192.168.1.2

212 101.86.23.0:443

213 [602:ea8:85a3:8d3:223:8a2e:370:ff04]

214 [602:ea8:85a3::370:ff04]

215 [2001:db8:85a3:8d3:1319:8a2e:370:7348]:80

216

217 Invalid ipAddress-values

218 192.168.1.556

// value too large

219 101.12.2.1-101.12.2.127

// ip address range not allowed

220 192.168.54.3/16

// mask not allowed

221 101.86.23.0:443-1024

// port range not allowed

222 [602:ea8:85a3:8d3:223:8a2e:cex:ff04]

// value not hexadecimal

223 [602:ea8::85a3::370:ff04]

// multiple ::

224 [2001:db8:85a3:8d3:1319:8a2e:370:7348]:80-200

// port range not allowed

225

226

227 Valid ipAddress-patterns

228 192.168.1.2-192.168.1.125

229 101.86.23.0-101.86.100.255, 101.20.1.1-101.86.50.255:443

230 [602:ea8:85a3:8d3:223:8a2e:370:ff04]:1-1023

231 [602:ea8:85a3::370:1]-[602:ea8:85a3::370:ff04]:80

232

233 Invalid ipAddress-patterns

234 192.168.5.2-192.168.1.125

// range not low to high

235 [602:ea8:85a3:8d3:223:8a2e:370:ff04]:1-90000

// port out of range

236

237

238 **2.1.3 IP Address Functions**

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

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

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

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

249 Otherwise, it SHALL return “False”.

250

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

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

- 256 • The first and second arguments SHALL both be of the same IP version (4 or 6).
- 257 • The value of the second argument SHALL be identical to one of the values in the IP address  
258 range list of the first argument.
- 259 • The first argument SHALL contain a port range list and the second SHALL contain a port  
260 value which is included in the port range list of the first.

261 Otherwise, it SHALL return “False”.

262

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

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

- 267 • The first and second arguments SHALL both be of the same IP version (4 or 6).
- 268 • The value of the first argument SHALL have a value identical to the second argument.
- 269 • Any port value in either argument SHALL be ignored.

270 Otherwise, it SHALL return “False”.

## 271 2.1.4 DNS Name Datatypes

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

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

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

276

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

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

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

## 283 2.1.5 DNS Name Functions

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

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

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

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

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

296 Otherwise, it SHALL return "False".

297

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

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

303 • The number of name components in the second argument SHALL be the same as the  
304 number in the first argument and each component in the second argument SHALL be  
305 identical to the corresponding component in the first argument, except that if the leftmost  
306 component in the first argument has the value "\*" it SHALL be deemed to match any value in  
307 the corresponding component of the second argument.

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

310 Otherwise, it SHALL return "False".

311

312 • urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal

313 This function SHALL take two arguments of data-type "urn:oasis:names:tc:xacml:3.0:data-  
314 type:dnsName-value" and SHALL return an "http://www.w3.org/2001/XMLSchema#boolean". The  
315 function SHALL return "True" if and only if the following conditions are met.

316 • The number of name components in the second argument SHALL be the same as the  
317 number in the first argument and each component in the second argument SHALL be  
318 identical to the corresponding component in the first argument. (Any port values in either  
319 argument SHALL be ignored.)

320 Otherwise, it SHALL return "False".

321

## 322 2.2 Resource Attributes

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

### 325 2.2.1 Resource-id

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

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

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

### 330 2.2.2 Resource-location

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

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

333 Allowable `DataTypes` for this attribute are: <http://www.w3.org/2001/XMLSchema#anyURI>,  
334 `urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-value`,  
335 `urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value`, and  
336 `urn:ogc:def:dataType:geoxacml:1.0:geometry`. This attribute denotes the logical and/or  
337 physical location of the requested resource.

## 338 2.3 Access Subject Attributes

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

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

### 341 2.3.1 Subject-ID

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

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

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

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

### 347 2.3.2 Subject-Security-Domain

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

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

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

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

### 353 2.3.3 Authentication-Time

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

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

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

### 358 2.3.4 Authentication-Method

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

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

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

### 363 2.3.5 Request-Time

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

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

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

### 368 2.3.6 IP Address

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

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

372 The `DataType` of this attribute is `urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-value`.

### 373 2.3.7 DNS Name

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

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

## 377 2.4 Recipient Subject Attributes

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

379 `urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject`

### 380 2.4.1 Subject-ID

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

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

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

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

### 386 2.4.2 Subject-Security-Domain

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

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

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

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

## 392 2.5 Requesting Machine Attributes

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

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

### 395 2.5.1 Subject-ID

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

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

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

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

## 402 2.6 Recipient Machine Attributes

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

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

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

### 406 2.6.1 Subject-ID

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

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

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



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

## 415 2.6.2 Removable-Media

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

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

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

## 420 2.7 Codebase Attributes

### 421 2.7.1 Authorized-Application

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

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

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

## 425 2.8 Action Attributes

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

### 428 2.8.1 Action-ID

429 The following action attribute values correspond to the action-id identifier:

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

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

432 The following action-id attributes are defined.

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

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

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

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

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

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

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

440 Additional action-IDs can be defined as needed.

### 441 2.8.2 Action-Protocol

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

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

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

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

446 The list below contains a number of common protocols which can be used to construct DLP and NAC  
447 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)

448 **2.8.3 Action-Method**

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

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

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

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

GET
PUT
POST
HEAD
DELETE
OPTIONS

455

456 **2.9 Obligations**

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

463 The obligation should conform to following structure:

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

465 **2.9.1 Encrypt**

466 The Encrypt obligation shall be designated with the following identifier:

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

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

472

473 The following is an example of the Encrypt obligation:

```
474 <ObligationExpressions>  
475 <ObligationExpression  
476   ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"  
477   FulfillOn="Permit"/>  
478 </ObligationExpression>  
479 </ObligationExpressions>
```

## 480 2.9.2 Log

481 The Log obligation shall be designated with the following identifier:

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

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

489

490 The following is an example of the Log obligation:

```
491 <ObligationExpressions>  
492 <ObligationExpression  
493   ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:log"  
494   FulfillOn="Permit"/>  
495 </ObligationExpression>  
496 </ObligationExpressions>
```

## 497 2.9.3 Marking

498 Marking classification values shall be designated with the following identifier:

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

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

506

507 The following is an example of the marking obligation:

```
508 <ObligationExpressions>  
509 <ObligationExpression  
510   ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"  
511   FulfillOn="Permit">  
512 <AttributeAssignmentExpression  
513   AttributeId="urn:oasis:names:tc:xacml:3.0:example:attribute:text">  
514 <AttributeValue  
515   DataType="http://www.w3.org/2001/XMLSchema#string"  
516   >Copyright 2011 Acme</AttributeValue>  
517 </AttributeAssignmentExpression>  
518 </ObligationExpression>  
519 </ObligationExpressions>
```

---

## 520 **3 Identifiers**

521 This profile defines the following URN identifiers.

### 522 **3.1 Profile Identifier**

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

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

---

## 526 4 Examples (non-normative)

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

### 528 4.1 DLP use cases

#### 529 4.1.1 Prevent sensitive data from being read/modified by unauthorized 530 users

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

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

536

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	webserver1.acme.com

537

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

538

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

539

Action Attributes	Values
Action-ID	Read, Update

#### 540 4.1.1.1 Description

541 This sample policy can be summarized as follows:

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

543

544 **Rule:** This rule is only applicable if Resource-ID contains “confidential.acme.com”

545 Then if

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

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

548 Action-ID = “Read” OR “Update” THEN

549 PERMIT

550

551 **Obligation:**

## 4.1.1.2 Sample Implementation in XACML 3.0

```

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

```

```

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

```

672

## 673 4.1.2 Prevent sensitive data from being emailed to unauthorized users

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

677

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	webserver1.acme.com

678

Access Subject Attributes	Values
Subject-ID	Alice



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

679

Recipient Subject Attributes	Values
Subject-ID	<a href="mailto:Bob@Wileycorp.com">Bob@Wileycorp.com</a>
Subject-Security-Domain	Wileycorp.com

680

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

681

Action Attributes	Values
Action-ID	Email-send

#### 682 4.1.2.1 Description

683 This sample policy can be summarized as follows:

684

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

687

688 **Rule:** This rule is only applicable if Action-ID = "Email-send"

689 Then if

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

691 Recipient-Subject.Subject-ID contains "@[Aa][Cc][Mm][Ee]\.[Cc][Oo][Mm]" AND

692 Recipient-Subject.Subject-Security-Domain = "acme.com" AND

693 Requesting-machine.Subject-ID matches "\*.acme.com" THEN

694 PERMIT

695

696 **Obligation:**

697 On PERMIT mark AND encrypt the resource

#### 698 4.1.2.2 Sample Implementation in XACML 3.0

```

699 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
700   PolicyId="urn:oasis.names.tc.xacml.dlp nac.policies.useCase412"
701   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
702   applicable"
703   Version="1.0">
704   <Description>4.1.2 Prevent sensitive data from being emailed to unauthorized
705   users</Description>
706   <Target>
707     <AnyOf>
708       <AllOf>
709         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
710           <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
711             >webserver1.acme.com</AttributeValue>
712           <AttributeDesignator
713             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
714             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
715             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
716             MustBePresent="false"/>

```

```

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

```

```

790     <AttributeDesignator
791         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
792         DataType="urn:oasis:names:tc:xacml:2.0:data-type:dnsName-value"
793         Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-
794 machine"
795         MustBePresent="false"
796     />
797 </Match>
798
799     </AllOf>
800 </AnyOf>
801 </Target>
802 <ObligationExpressions>
803 <ObligationExpression
804     ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"
805     FulfillOn="Permit">
806     <AttributeAssignmentExpression
807         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
808         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
809         <AttributeDesignator
810             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
811             DataType="http://www.w3.org/2001/XMLSchema#anyURI"
812             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
813             MustBePresent="false"
814         />
815     </AttributeAssignmentExpression>
816 </ObligationExpression>
817 <ObligationExpression
818     ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"
819     FulfillOn="Permit">
820     <AttributeAssignmentExpression
821         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
822         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
823         <AttributeDesignator
824             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
825             DataType="http://www.w3.org/2001/XMLSchema#anyURI"
826             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
827             MustBePresent="false"
828         />
829     </AttributeAssignmentExpression>
830 </ObligationExpression>
831 </ObligationExpressions>
832 </Rule>
833 </Policy>
834

```

835

### 836 4.1.3 Prevent sensitive data from being transferred via web-mail

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

840

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	webserver1.acme.com

841

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

842

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

Subject-ID	<a href="mailto:Alice@big-email-service.com">Alice@big-email-service.com</a>
Subject-Security-Domain	big-email.service.com

843

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

844

Action Attributes	Values
Action-Protocol	HTTP(S)

#### 845 4.1.3.1 Description

846 This sample policy can be summarized as follows:

847

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

850

851 **Rule:** This rule is only applicable if Action-Protocol contains "HTTP"

852 Then if

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

854 Recipient-Subject.Subject-ID contains @[Aa][Cc][Mm][Ee].[Cc][Oo][Mm]" AND

855 Recipient-Subject.Subject-Security-Domain = "acme.com" AND

856 Requesting-Machine.Subject-ID matches "\*.acme.com" THEN

857 PERMIT

858

859 **Obligation:**

860 On PERMIT mark AND encrypt the resource.

#### 861 4.1.3.2 Sample Implementation in XACML 3.0

```

862 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
863   PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase413"
864   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
865   applicable"
866   Version="1.0">
867   <Description>4.1.3 Prevent sensitive data from being transferred via web-
868   mail</Description>
869   <Target>
870     <AnyOf>
871       <AllOf>
872         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
873           <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
874             >webserver1.acme.com</AttributeValue>
875           <AttributeDesignator
876             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
877             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
878             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
879             MustBePresent="false"/>
880         </Match>
881         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
882           <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
883             >confidential.acme.com</AttributeValue>
884           <AttributeDesignator
885             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"

```

```

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

```

```

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

```

995

#### 4.1.4 Prevent sensitive data from being copied/printed from one computer to another

996

997

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.

998

999

1000

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	fortress.acme.com

1001

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

1002

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

1003

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

1004

Action Attributes	Values
Action-ID	Copy or Print

#### 1005 4.1.4.1 Description

1006 This sample policy can be summarized as follows:

1007

1008 **Target:** This policy is only applicable to Resource-location = "fortress.acme.com"

1009 AND Resource-ID contains "confidential.acme.com"

1010

1011 **Rule:** This rule is only applicable if Action-ID = "Copy" or "Print"

1012 Then if

1013 Requesting-Machine.Subject-ID = Recipient-Machine.Subject-ID

1014 PERMIT

1015

1016 **Obligation:**

1017 On PERMIT mark AND encrypt the resource.

#### 1018 4.1.4.2 Sample Implementation in XACML 3.0

```

1019 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
1020   PolicyId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase414"
1021   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
1022   applicable"
1023   Version="1.0">
1024   <Description>4.1.4 Prevent sensitive data from being copied/printed from one computer
1025   to another</Description>
1026   <Target>
1027     <AnyOf>
1028       <AllOf>
1029         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
1030           <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1031             >fortress.acme.com</AttributeValue>
1032           <AttributeDesignator
1033             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
1034             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1035             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1036             MustBePresent="false"/>
1037         </Match>
1038         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
1039           <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
1040             >confidential.acme.com</AttributeValue>
1041           <AttributeDesignator
1042             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1043             DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1044             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1045             MustBePresent="false"
1046           />
1047         </Match>
1048       </AllOf>
1049     </AnyOf>
1050   </Target>
1051   <Rule
1052     Effect="Permit"
1053     RuleId="urn:oasis:names:tc:xacml:dlp_nac.policies.useCase414.copyOrPrint">
1054     <Description>This rule is only applicable if Action-ID = "Copy" or
1055     "Print"</Description>
1056     <Target>
1057       <AnyOf>

```



```

1058 <AllOf>
1059   <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1060     <AttributeValue
1061       DataType="http://www.w3.org/2001/XMLSchema#string">Copy</AttributeValue>
1062     <AttributeDesignator
1063       AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1064       DataType="http://www.w3.org/2001/XMLSchema#string"
1065       Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1066       MustBePresent="false"
1067     />
1068   </Match>
1069 </AllOf>
1070 <AllOf>
1071   <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1072     <AttributeValue
1073       DataType="http://www.w3.org/2001/XMLSchema#string">Print</AttributeValue>
1074     <AttributeDesignator
1075       AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1076       DataType="http://www.w3.org/2001/XMLSchema#string"
1077       Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1078       MustBePresent="false"
1079     />
1080   </Match>
1081 </AllOf>
1082 </AnyOf>
1083 </Target>
1084 <Condition>
1085   <Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:ipAddress-value-equal">
1086     <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-one-and-
1087 only" >
1088       <AttributeDesignator
1089         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
1090         DataType="urn:oasis:names:tc:xacml:2.0:data-type:ipAddress-value"
1091         Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-
1092 machine"
1093         MustBePresent="false"
1094       />
1095     </Apply>
1096     <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-one-and-
1097 only" >
1098       <AttributeDesignator
1099         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
1100         DataType="urn:oasis:names:tc:xacml:2.0:data-type:ipAddress-value"
1101         Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-machine"
1102         MustBePresent="false"
1103       />
1104     </Apply>
1105   </Apply>
1106 </Condition>
1107 <ObligationExpressions>
1108 <ObligationExpression
1109   ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:marking"
1110   FulfillOn="Permit">
1111   <AttributeAssignmentExpression
1112     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1113     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1114   <AttributeDesignator
1115     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1116     DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1117     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1118     MustBePresent="false"
1119   />
1120   </AttributeAssignmentExpression>
1121 </ObligationExpression>
1122 <ObligationExpression
1123   ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:encrypt"
1124   FulfillOn="Permit">
1125   <AttributeAssignmentExpression
1126     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1127     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1128   <AttributeDesignator
1129     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1130     DataType="http://www.w3.org/2001/XMLSchema#anyURI"

```

1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138

```
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"  
MustBePresent="false"  
/>  
</AttributeAssignmentExpression>  
</ObligationExpression>  
</ObligationExpressions>  
</Rule>  
</Policy>
```

1139

## 1140 4.1.5 Prevent sensitive data from being transferred to removable media

1141 Acme security policy prohibits the transfer of sensitive data to removable media, such as CDs,  
1142 DVDs, and USB drives. Any attempt to copy data to removable media must fail. Sample attributes  
1143 and values are provided below:

1144

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	webserver1.acme.com

1145

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

1146

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

1147

Recipient Machine Attributes	Values
Removable-media	true

1148

Action Attributes	Values
Action-ID	Copy or Print

### 1149 4.1.5.1 Description

1150 This sample policy can be summarized as follows:

1151

1152 **Target:** This policy is only applicable to Resource-location = "webserver1.acme.com"  
1153 AND Resource-ID contains "confidential.acme.com"

1154

1155 **Rule:** This rule is only applicable if Action-ID = "Copy"

1156 Then if

1157 Access-Subject.Subject-Security-Domain = "acme.com" AND

1158 Requesting-Machine.Subject-ID matches "\*.acme.com" AND

1159 Recipient-Machine.Removable-Media = "TRUE" THEN

1160 DENY

#### 1161 4.1.5.2 Sample Implementation in XACML 3.0

```
1162 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"  
1163   PolicyId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase415"  
1164   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-  
1165   applicable"  
1166   Version="1.0">  
1167   <Description>4.1.5 Prevent sensitive data from being transferred to removable  
1168   media</Description>  
1169   <Target>  
1170     <AnyOf>  
1171       <AllOf>  
1172         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">  
1173           <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"  
1174             >webserver1.acme.com</AttributeValue>  
1175           <AttributeDesignator  
1176             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"  
1177             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"  
1178             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"  
1179             MustBePresent="false"/>  
1180         </Match>  
1181         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">  
1182           <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string  
1183             >confidential.acme.com</AttributeValue>  
1184           <AttributeDesignator  
1185             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"  
1186             DataType="http://www.w3.org/2001/XMLSchema#anyURI"  
1187             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"  
1188             MustBePresent="false"  
1189           />  
1190         </Match>  
1191       </AllOf>  
1192     </AnyOf>  
1193   </Target>  
1194   <Rule  
1195     Effect="Deny"  
1196     RuleId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase415.copy">  
1197     <Description>Rule: This rule is only applicable if Action-ID = Copy</Description>  
1198     <Target>  
1199       <AnyOf>  
1200         <AllOf>  
1201           <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
1202             <AttributeValue  
1203               DataType="http://www.w3.org/2001/XMLSchema#string">Copy</AttributeValue>  
1204             <AttributeDesignator  
1205               AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"  
1206               DataType="http://www.w3.org/2001/XMLSchema#string"  
1207               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
1208               MustBePresent="false"  
1209             />  
1210           </Match>  
1211           <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
1212             <AttributeValue  
1213               DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>  
1214             <AttributeDesignator  
1215               AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-  
1216               domain"  
1217               DataType="http://www.w3.org/2001/XMLSchema#string"  
1218               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-  
1219               subject"  
1220               MustBePresent="false"  
1221             />  
1222           </Match>  
1223           <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-match">  
1224             <AttributeValue  
1225               DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-pattern"  
1226               >*.acme.com</AttributeValue>  
1227             <AttributeDesignator  
1228               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"  
1229               DataType="urn:oasis:names:tc:xacml:2.0:data-type:dnsName-value"  
1230               Category="urn:oasis:names:tc:xacml:1.0:subject-category:requesting-  
1231               machine"
```

```

1232         MustBePresent="false"
1233     />
1234 </Match>
1235 <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
1236     <AttributeValue
1237         DataType="http://www.w3.org/2001/XMLSchema#boolean">true</AttributeValue>
1238     <AttributeDesignator
1239         AttributeId="urn:oasis:names:tc:xacml:3.0:subject:removable-media"
1240         DataType="http://www.w3.org/2001/XMLSchema#boolean"
1241         Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-
1242 machine"
1243         MustBePresent="false"
1244     />
1245 </Match>
1246 </AllOf>
1247 </AnyOf>
1248 </Target>
1249 </Rule>
1250 </Policy>

```

1251

## 4.1.6 Prevent sensitive data from being transferred to disallowed URLs

1252

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:

1253

1254

1255

1256

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	webserver1.acme.com

1257

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

1258

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

1259

Recipient Machine Attributes	Values
Subject-ID	cloudstoragesite.com

1260

Action Attributes	Values
Action-Protocol	HTTP

### 4.1.6.1 Description

1261

This sample policy can be summarized as follows:

1262

1263

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

1264

1265

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

1266

1267 Then if  
1268 Action-Protocol contains "HTTP" OR  
1269 Action-Protocol contains "FTP" THEN  
1270 DENY  
1271  
1272 **Obligation:**  
1273 On DENY log transfer attempt.

#### 1274 4.1.6.2 Sample Implementation in XACML 3.0

```
1275 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"  
1276   PolicyId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase416"  
1277   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-  
1278   applicable"  
1279   Version="1.0">  
1280   <Description>4.1.6 Prevent sensitive data from being transferred to disallowed  
1281   URLs</Description>  
1282   <Target>  
1283     <AnyOf>  
1284       <AllOf>  
1285         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">  
1286           <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"  
1287             >webserver1.acme.com</AttributeValue>  
1288           <AttributeDesignator  
1289             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"  
1290             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"  
1291             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"  
1292             MustBePresent="false"/>  
1293         </Match>  
1294       </AllOf>  
1295     </AnyOf>  
1296   </Target>  
1297   <Rule  
1298     Effect="Deny"  
1299     RuleId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase416.confidentialDomain">  
1300     <Description>This rule is only applicable if Resource-ID contains  
1301     "confidential.acme.com"</Description>  
1302     <Target>  
1303       <AnyOf>  
1304         <AllOf>  
1305           <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">  
1306             <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string  
1307               >confidential.acme.com</AttributeValue>  
1308             <AttributeDesignator  
1309               AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"  
1310               DataType="http://www.w3.org/2001/XMLSchema#anyURI"  
1311               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"  
1312               MustBePresent="false"  
1313             />  
1314           </Match>  
1315         </AllOf>  
1316       </AnyOf>  
1317     </AnyOf>  
1318     <AllOf>  
1319       <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
1320         <AttributeValue  
1321           DataType="http://www.w3.org/2001/XMLSchema#string">HTTP</AttributeValue>  
1322         <AttributeDesignator  
1323           AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-protocol"  
1324           DataType="http://www.w3.org/2001/XMLSchema#string"  
1325           Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"  
1326           MustBePresent="false"  
1327         />  
1328       </Match>  
1329     </AllOf>  
1330   </AllOf>  
1331   <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```

1332     <AttributeValue
1333         DataType="http://www.w3.org/2001/XMLSchema#string">FTP</AttributeValue>
1334     <AttributeDesignator
1335         AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-
1336 protocol"
1337         DataType="http://www.w3.org/2001/XMLSchema#string"
1338         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1339         MustBePresent="false"
1340     />
1341 </Match>
1342 </AllOf>
1343 </AnyOf>
1344 </Target>
1345 <ObligationExpressions>
1346 <ObligationExpression
1347     ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:log-transfer-
1348 attempt"
1349     FulfillOn="Deny">
1350 <AttributeAssignmentExpression
1351     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1352     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1353 <AttributeDesignator
1354     AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1355     DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1356     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1357     MustBePresent="false"
1358 />
1359 </AttributeAssignmentExpression>
1360 <AttributeAssignmentExpression
1361     AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1362     Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
1363 <AttributeValue
1364     DataType="http://www.w3.org/2001/XMLSchema#string">Transfer</AttributeValue>
1365 </AttributeAssignmentExpression>
1366 </ObligationExpression>
1367 </ObligationExpressions>
1368 </Rule>
1369 </Policy>

```

1370

#### 1371 4.1.7 Prevent sensitive data from being copied from one resource to 1372 another

1373 Acme security policy prohibits copying proprietary information from one resource to another. Alice  
1374 attempts to copy sensitive data from one resource to a new one she just created. The request  
1375 fails. Sample attributes and values are listed below.

1376

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	webserver1.acme.com

1377

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

1378

Action Attributes	Values
Action-ID	Copy

#### 1379 4.1.7.1 Description

1380 This sample policy can be summarized as follows:

1381

1382 **Target:** This policy is only applicable if Resource-location = "webserver1.acme.com"

1383 AND Resource-ID contains "confidential.acme.com"

1384

1385 **Rule:** This rule is only applicable if Action-ID = "Copy"

1386 Then if

1387 Access-Subject.Subject-Security-Domain = "acme.com"

1388 DENY

1389

1390 **Obligation:**

1391 On DENY log copy attempt.

1392

#### 1393 4.1.7.2 Sample Implementation in XACML 3.0

```
1394 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
1395   PolicyId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase417"
1396   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
1397   applicable"
1398   Version="1.0">
1399   <Description>4.1.7 Prevent sensitive data from being copied from one resource to
1400   another</Description>
1401   <Target>
1402     <AnyOf>
1403       <AllOf>
1404         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
1405           <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1406             >webserver1.acme.com</AttributeValue>
1407           <AttributeDesignator
1408             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
1409             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1410             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1411             MustBePresent="false"/>
1412         </Match>
1413         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
1414           <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#string
1415             >confidential.acme.com</AttributeValue>
1416           <AttributeDesignator
1417             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1418             DataType=http://www.w3.org/2001/XMLSchema#anyURI"
1419             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1420             MustBePresent="false"
1421             />
1422         </Match>
1423       </AllOf>
1424     </AnyOf>
1425   </Target>
1426   <Rule
1427     Effect="Deny"
1428     RuleId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase417.copy">
1429     <Description>This rule is only applicable if Action-ID contains "Copy"</Description>
1430     <Target>
1431       <AnyOf>
1432         <AllOf>
1433           <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1434             <AttributeValue
1435               DataType="http://www.w3.org/2001/XMLSchema#string">Copy</AttributeValue>
1436             <AttributeDesignator
1437               AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
```



```

1438         DataType="http://www.w3.org/2001/XMLSchema#string"
1439         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1440         MustBePresent="false"
1441     />
1442 </Match>
1443 </AllOf>
1444 </AnyOf>
1445 <AnyOf>
1446     <AllOf>
1447         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1448             <AttributeValue
1449                 DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
1450             <AttributeDesignator
1451                 AttributeId="urn:oasis:names:tc:xacml:3.0:subject:subject-security-domain"
1452                 DataType="http://www.w3.org/2001/XMLSchema#string"
1453                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
1454                 MustBePresent="false"
1455             />
1456         </Match>
1457     </AllOf>
1458 </AnyOf>
1459 </Target>
1460 <ObligationExpressions>
1461     <ObligationExpression
1462         ObligationId="urn:oasis:names:tc:xacml:3.0:dlp-nac:obligation:log-transfer-
1463 attempt"
1464         FulfillOn="Deny">
1465         <AttributeAssignmentExpression
1466             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1467             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
1468         <AttributeDesignator
1469             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1470             DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1471             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1472             MustBePresent="false"
1473         />
1474         </AttributeAssignmentExpression>
1475         <AttributeAssignmentExpression
1476             AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1477             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
1478         <AttributeDesignator
1479             AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
1480             DataType="http://www.w3.org/2001/XMLSchema#string"
1481             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1482             MustBePresent="false"
1483         />
1484         </AttributeAssignmentExpression>
1485     </ObligationExpression>
1486 </ObligationExpressions>
1487 </Rule>
1488 </Policy>

```

1489

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

1490  
1491

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.

1495

Resource Attributes	Values
Resource-ID	<a href="http://confidential.acme.com/eyes-only.xml">http://confidential.acme.com/eyes-only.xml</a>
Resource-location	webserver1.acme.com

1496

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

1497

Codebase Attribute	Values
Authorized-application	<a href="#">false</a>

1498

Action Attributes	Values
Action-Protocol	HTTP

#### 1499 4.1.8.1 Description

1500 This sample policy can be summarized as follows:

1501

1502 **Target:** This policy is only applicable to Resource-location = "webserver1.acme.com"  
 1503 AND Resource-ID contains "confidential.acme.com"

1504

1505 **Rule:** This rule is only applicable if Action-Protocol contains "HTTP"

1506 Then if

1507 Access-Subject.Subject-Security-Domain = "acme.com" AND Authorized-application = false

1508 DENY

1509

1510 **Obligation:**

1511 On DENY log attempt to use an authorized application

#### 1512 4.1.8.2 Sample Implementation in XACML 3.0

```

1513 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
1514   PolicyId="urn:oasis:names:tc:xacml:dlp_nac:policies:useCase418"
1515   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
1516   applicable"
1517   Version="1.0">
1518   <Description>4.1.8 Prevent sensitive data from being read/modified by unauthorized
1519   applications</Description>
1520   <Target>
1521     <AnyOf>
1522       <AllOf>
1523         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:dnsName-value-equal">
1524           <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1525             >webserver1.acme.com</AttributeValue>
1526           <AttributeDesignator
1527             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
1528             DataType="urn:oasis:names:tc:xacml:3.0:data-type:dnsName-value"
1529             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1530             MustBePresent="false"/>
1531         </Match>
1532         <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:anyURI-contains">
1533           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"
1534             >confidential.acme.com</AttributeValue>
1535           <AttributeDesignator
1536             AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
1537             DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1538             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1539             MustBePresent="false"
1540           />
1541         </Match>
1542       </AllOf>
1543     </AnyOf>
1544   </Target>
1545   <RuleDef>
1546     <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:deny"
1547       <AttributeValue DataType="boolean" >false</AttributeValue>
1548     </Match>
1549   </RuleDef>
1550 </Policy>

```

```

1541         </Match>
1542     </AllOf>
1543 </AnyOf>
1544 </Target>
1545 <Rule
1546     Effect="Deny"
1547     RuleId="urn:oasis.names.tc.xacml.dlp_nac.policies.useCase418.httpProtocol">
1548     <Description>This rule is only applicable if Action-Protocol contains
1549 HTTP</Description>
1550     <Target>
1551         <AnyOf>
1552             <AllOf>
1553                 <Match MatchId="urn:oasis.names.tc.xacml:1.0:function:string-equal">
1554                     <AttributeValue
1555                         DataType="http://www.w3.org/2001/XMLSchema#string">HTTP</AttributeValue>
1556                     <AttributeDesignator
1557                         AttributeId="urn:oasis.names.tc.xacml:3.0:dlp-nac:action:action-
1558 protocol"
1559                         DataType="http://www.w3.org/2001/XMLSchema#string"
1560                         Category="urn:oasis.names.tc.xacml:3.0:attribute-category:action"
1561                         MustBePresent="false"
1562                     />
1563                 </Match>
1564                 <Match MatchId="urn:oasis.names.tc.xacml:1.0:function:string-equal">
1565                     <AttributeValue
1566                         DataType="http://www.w3.org/2001/XMLSchema#string">acme.com</AttributeValue>
1567                     <AttributeDesignator
1568                         AttributeId="urn:oasis.names.tc.xacml:3.0:subject:subject-security-
1569 domain"
1570                         DataType="http://www.w3.org/2001/XMLSchema#string"
1571                         Category="urn:oasis.names.tc.xacml:1.0:subject-category:access-subject"
1572                         MustBePresent="false"
1573                     />
1574                 </Match>
1575                 <Match MatchId="urn:oasis.names.tc.xacml:1.0:function:boolean-equal">
1576                     <AttributeValue
1577                         DataType="http://www.w3.org/2001/XMLSchema#boolean">>false</AttributeValue>
1578                     <AttributeDesignator
1579                         AttributeId="urn:oasis.names.tc.xacml:3.0:codebase:authorized-
1580 application"
1581                         DataType="http://www.w3.org/2001/XMLSchema#boolean"
1582                         Category="urn:oasis.names.tc.xacml:1.0:subject-category:codebase"
1583                         MustBePresent="false"
1584                     />
1585                 </Match>
1586             </AllOf>
1587         </AnyOf>
1588     </Target>
1589     <ObligationExpressions>
1590         <ObligationExpression
1591             ObligationId="urn:oasis.names.tc.xacml:3.0:dlp-nac:obligation:log-transfer-
1592 attempt"
1593             FulfillOn="Deny">
1594             <AttributeAssignmentExpression
1595                 AttributeId="urn:oasis.names.tc.xacml:1.0:resource:resource-id"
1596                 Category="urn:oasis.names.tc.xacml:3.0:attribute-category:resource">
1597                 <AttributeDesignator
1598                     AttributeId="urn:oasis.names.tc.xacml:1.0:resource:resource-id"
1599                     DataType="http://www.w3.org/2001/XMLSchema#anyURI"
1600                     Category="urn:oasis.names.tc.xacml:3.0:attribute-category:resource"
1601                     MustBePresent="false"
1602                 />
1603                 </AttributeAssignmentExpression>
1604                 <AttributeAssignmentExpression
1605                     AttributeId="urn:oasis.names.tc.xacml:1.0:action:action-id"
1606                     Category="urn:oasis.names.tc.xacml:3.0:attribute-category:action">
1607                     <AttributeValue
1608                         DataType="http://www.w3.org/2001/XMLSchema#string">access</AttributeValue>
1609                     </AttributeAssignmentExpression>
1610                 </ObligationExpression>
1611             </ObligationExpressions>
1612     </Rule>
1613 </Policy>

```

## 1614 4.2 NAC use case examples

### 1615 4.2.1 Prevent traffic flow between network resources, based on protocol

1616 Acme security policy prohibits sensitive data from being transferred using unsecure protocols.  
1617 Alice attempts to retrieve a document resource on a server using the ftp protocol, in which case  
1618 the attempt fails.

1619

Resource Attributes	Values
Resource-location	<a href="http://192.168.0.1">192.168.0.1</a>

1620

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

1621

Action Attributes	Values
Action-Protocol	FTP

#### 1622 4.2.1.1 Description

1623 This sample policy can be summarized as follows:

1624

1625 **Target:** This policy is only applicable if Subject-ID ends with "O=Acme,C=US"

1626

1627 **Rule:**

1628 If Action-Protocol = "FTP"

1629 DENY

#### 1630 4.2.1.2 Sample Implementation in XACML 3.0

```
1631 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"  
1632   PolicyId="urn:oasis.names.tc.xacml.dlp nac.policies.useCase421"  
1633   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-  
1634   applicable"  
1635   Version="1.0">  
1636   <Description>4.2.1 Prevent traffic flow between network resources, based on  
1637   protocol</Description>  
1638   <Target>  
1639     <AnyOf>  
1640       <AllOf>  
1641         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-match">  
1642           <AttributeValue DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"  
1643             >O=Acme,C=US</AttributeValue>  
1644           <AttributeDesignator  
1645             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"  
1646             DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"  
1647             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"  
1648             MustBePresent="false"/>  
1649         </Match>  
1650       </AllOf>  
1651     </AnyOf>  
1652   </Target>  
1653   <Rule  
1654     Effect="Deny"  
1655     RuleId="urn:oasis.names.tc.xacml.dlp nac.policies.useCase421.ftpProtocol">  
1656     <Description>This rule is only applicable if Action-Protocol equals  
1657     FTP</Description>
```

```

1658     <Target>
1659       <AnyOf>
1660         <AllOf>
1661           <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1662             <AttributeValue
1663               DataType="http://www.w3.org/2001/XMLSchema#string">FTP</AttributeValue>
1664             <AttributeDesignator
1665               AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-
1666 protocol"
1667               DataType="http://www.w3.org/2001/XMLSchema#string"
1668               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1669               MustBePresent="false"
1670             />
1671           </Match>
1672         </AllOf>
1673       </AnyOf>
1674     </Target>
1675 </Rule>
1676 </Policy>
1677

```

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

1678 Acme security policy restricts access to certain secure access zones based on an authenticated  
1679 subject DN of a user when using certificate-based authentication and the destination IP address.  
1680 Alice, a contractor at Acme, attempts access a server containing sensitive data within a secure  
1681 access zone, but is denied based on her subject-id OU value.  
1682  
1683

Resource Attributes	Values
Resource-location	<a href="#">10.0.0.1</a>

1684

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

1685

Action Attributes	Values
Action-Protocol	HTTP
Action-Method	GET

### 4.2.2.1 Description

1686 This sample policy can be summarized as follows:  
1687  
1688

1689 **Target:** This policy is only applicable to resource type *Resource-location* = 10.\d\*\.\d\*\.\d\*

1690  
1691 **Rule:** This rule is only applicable if Subject-ID ends with "O=Employee,O=Acme,C=US"

1692 Then if

1693 Action-Protocol = "HTTP" AND

1694 Action-Method = "GET"

1695 THEN

1696 PERMIT

### 4.2.2.2 Sample Implementation in XACML 3.0

```

1697 <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
1698

```

```

1699     PolicyId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase422"
1700     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
1701 applicable"
1702     Version="1.0">
1703     <Description>4.2.2 Restrict users to certain network resources, based on subject-
1704 id</Description>
1705     <Target>
1706         <AnyOf>
1707             <AllOf>
1708                 <Match MatchId="urn:oasis:names:tc:xacml:3.0:function:ipAddress-match">
1709                     <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-
1710 pattern"
1711                         >10.0.0.0-10.255.255.255</AttributeValue>
1712                     <AttributeDesignator
1713                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-location"
1714                         DataType="urn:oasis:names:tc:xacml:3.0:data-type:ipAddress-value"
1715                         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
1716                         MustBePresent="false"/>
1717                     </Match>
1718                 </AllOf>
1719             </AnyOf>
1720         </Target>
1721     <Rule
1722         Effect="Permit"
1723         RuleId="urn.oasis.names.tc.xacml.dlp_nac.policies.useCase422.employee">
1724         <Description>This rule is only applicable if subject-id ends with
1725 O=Employee,O=Acme,C=US</Description>
1726         <Target>
1727             <AnyOf>
1728                 <AllOf>
1729                     <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-match">
1730                         <AttributeValue DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
1731                             >O=Employee,O=Acme,C=US</AttributeValue>
1732                         <AttributeDesignator
1733                             AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
1734                             DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"
1735                             Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
1736                             MustBePresent="false"/>
1737                         </Match>
1738                     <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1739                         <AttributeValue
1740                             DataType="http://www.w3.org/2001/XMLSchema#string">HTTP</AttributeValue>
1741                         <AttributeDesignator
1742                             AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-protocol"
1743                             DataType="http://www.w3.org/2001/XMLSchema#string"
1744                             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1745                             MustBePresent="false"/>
1746                     <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
1747                         <AttributeValue
1748                             DataType="http://www.w3.org/2001/XMLSchema#string">GET</AttributeValue>
1749                         <AttributeDesignator
1750                             AttributeId="urn:oasis:names:tc:xacml:3.0:dlp-nac:action:action-method"
1751                             DataType="http://www.w3.org/2001/XMLSchema#string"
1752                             Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
1753                             MustBePresent="false"/>
1754                     </Match>
1755                 </AllOf>
1756             </AnyOf>
1757         </Target>
1758     </Rule>
1759 </Policy>

```

1760

## 1761 5 Conformance

1762 Conformance to this profile is defined for *policies* and *requests* generated and transmitted within and  
1763 between XACML systems.

### 1764 5.1 IP Address and DNS Name Datatypes and Functions

1765 Conformant XACML *policies* and *requests* SHALL use the IP Address and DNS Name datatypes and  
1766 functions defined in Section 2 for their specified purpose and SHALL NOT use any other identifiers for the  
1767 purposes defined by attributes in this profile. Conformant XACML PDPs SHALL implement these  
1768 datatypes and functions. The following table lists the datatypes and functions that must be supported.

1769 Note: “M” is mandatory “O” is optional.

1770

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

1771

### 1772 5.2 Category Identifiers

1773 Conformant XACML *policies* and *requests* SHALL use the category identifiers defined in Section 2 for  
1774 their specified purpose and SHALL NOT use any other identifiers for the purposes defined by categories  
1775 in this profile. The following table lists the categories that must be supported.

1776 Note: “M” is mandatory “O” is optional.

1777

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

1778

1779 **5.3 Attribute Identifiers**

1780 Conformant XACML *policies* and *requests* SHALL use the attribute identifiers defined in Section 2 for  
 1781 their specified purpose and SHALL NOT use any other identifiers for the purposes defined by attributes in  
 1782 this profile. The following table lists the attributes that must be supported.

1783 Note: “M” is mandatory “O” is optional.

1784

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

1785 **5.4 Attribute Values**

1786 Conformant XACML *policies* and *requests* SHALL use attribute values in the specified range or patterns  
 1787 as defined for each attribute in Section 2 (when a range or pattern is specified).

1788 NOTE: In order to process conformant XACML *policies* and *requests* correctly, *PIP* and  
 1789 *PEP* modules may have to translate native data values into the datatypes and formats  
 1790 specified in this profile.

1791

---

## Appendix A. Acknowledgments

1792 The following individuals have participated in the creation of this specification and are gratefully  
1793 acknowledged:

1794 **Participants:**

1795 John Tolbert, The Boeing Company  
1796 Richard Hill, The Boeing Company  
1797 Crystal Hayes, The Boeing Company  
1798 David Brossard, Axiomatics AB  
1799 Hal Lockhart, Oracle  
1800 Steven Legg, ViewDS

1801 **Committee members during profile development:**

---

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

1802

## 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.

1805