



1
2 **eXtensible Access Control Markup Language**
3 **(XACML) Version 3.0 Policy Distribution**
4 **Protocol Use-cases and Requirements**

5 **Working draft 01, 8 Oct 2004**

6 Document identifier: `access_control-xacml-3.0-distribution-requirements-wd-01`

7 Location: http://docs.oasis-open.org/xacml/access_control-xacml-3.0-distribution-requirements-wd-01.pdf

8 Editors:

9 Tim Moses, Entrust

10 Committee members:

11 Anne Anderson, Sun Microsystems

12 Anthony Nadalin, IBM

13 Bill Parducci, GlueCode Software

14 Daniel Engovatov, BEA Systems

15 Ed Coyne, Veterans Health Administration

16 Frank Siebenlist, Argonne National Labs

17 Hal Lockhart, BEA Systems

18 Michael McIntosh, IBM

19 Michiharu Kudo, IBM

20 Polar Humenn, Self

21 Ron Jacobson, Computer Associates

22 Seth Proctor, Sun Microsystems

23 Simon Godik, GlueCode Software

24 Steve Anderson, OpenNetwork

25 Tim Moses, Entrust

26 Abstract:

27 This document defines the use-cases and requirements for the policy distribution protocol
28 for version 3.0 of the extensible access-control markup language.

29 Status:

30 This version of the specification is a working draft of the committee. As such, it is expected
31 to change prior to adoption as an OASIS standard.

32 If you are on the xacml@lists.oasis-open.org list for committee members, send comments
33 there. If you are not on that list, you may use the following link and complete the comment
34 form:

35 http://oasis-open.org/committees/comments/form.php?wg_abbrev=xacml

36 Copyright (C) OASIS Open 2004. All Rights Reserved.

`access_control-xacml-3.0-distribution-requirements-wd-01`

37
38
39
40
41
42
43
44
45
46
47
48

Table of contents

1. Glossary (non-normative).....	3
2. Introduction (normative).....	3
3. Sequence.....	4
4. Requirements.....	5
5. Potential sources.....	5
6. Transport layer.....	6
7. References.....	6
Appendix A. Acknowledgments.....	7
Appendix B. Revision history.....	8
Appendix C. Notices.....	9

50 1. Glossary (non-normative)

51 **PRP** – Policy retrieval point. The component from which **applicable policies** may be retrieved.

52 **Topic** – The set of **decision requests** that a **PDP** is intended to answer.

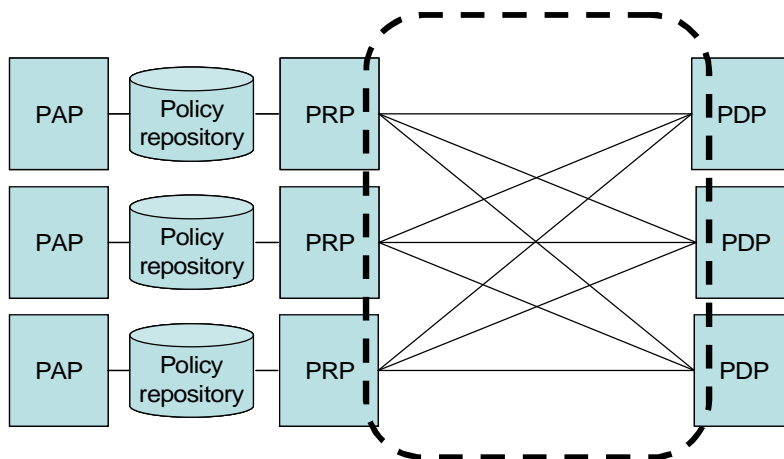
53 Other terms have the meaning defined in the glossary of [XACML].

54 2. Introduction (normative)

55 A common deployment of XACML components involves one or more **PAPs** and one or more **PDPs**.
 56 The **policies** applicable to any one of the **PDPs** may include a subset of the **policies** administered
 57 by each **PAP**. In response to a **decision request**, a **PDP** commonly executes all the **policies** it
 58 contains. Therefore, it is more efficient for a **PDP** to load only **policies** that may be applicable to
 59 the requests that it may be called upon to answer.

60 It is assumed that the **PAP** stores its **policies** in a repository and that a **PRP** offers a simple
 61 interface into the repository by which the **PDP** can locate and retrieve the **applicable policies**.

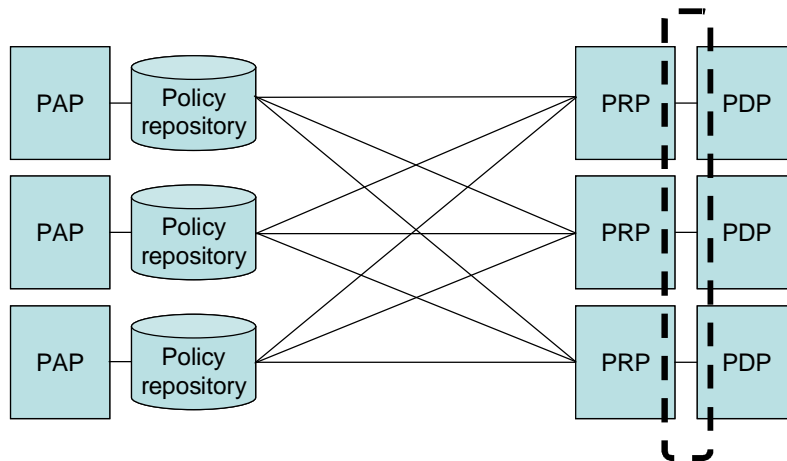
62 As shown by the dashed rectangles in Figure 1 and Figure 2, this requirements document deals
 63 with the exchange between the **PRP** and the **PDP**. Any exchanges between the repository and the
 64 **PRP** are out of scope.



65

66

Figure 1 - Context 1



67

68

Figure 2 - Context 2

69 It is assumed that there is a many-to-many relationship between the **PAP** and the **PDP**. It is further
 70 assumed that the **PAP** stores its **policies** in a repository. The **PRP** retrieves policies from the
 71 repository. The **PDP** interacts with the **PRP** to obtain the **policies** it needs.

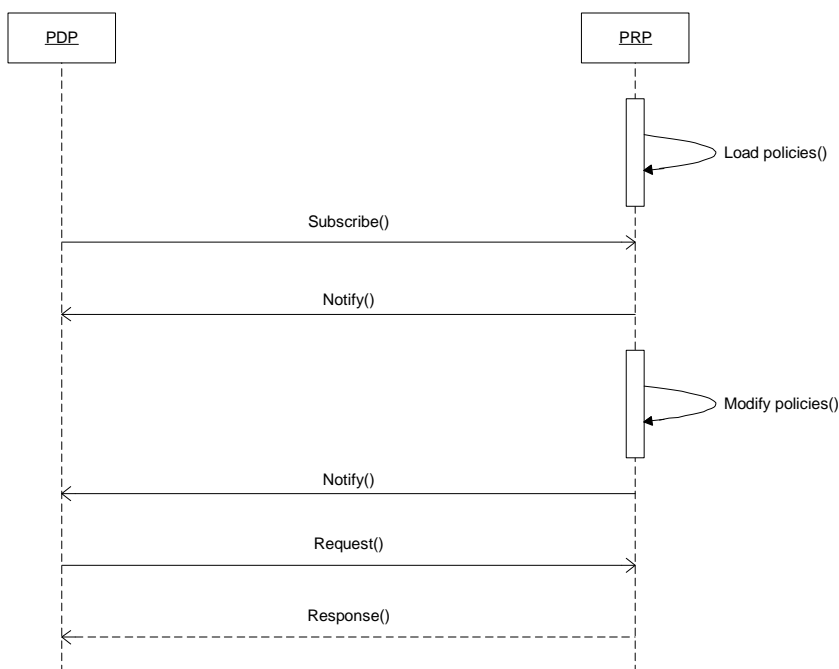
72 Figure 1 shows a one-to-one relationship between the repository and the **PRP** and a many-to-many
 73 relationship between the **PRP** and the **PDP**.

74 Figure 2 shows a many-to-many relationship between the repository and the **PRP** and a one-to-one
 75 relationship between the **PRP** and the **PDP**. Regardless, the required protocol operates between
 76 the **PRP** and the **PDP**. The protocol in operation between the repository and the **PRP** is out of
 77 scope.

78

79 **3. Sequence**

80 The protocol proceeds as shown in Figure 3.



81

82

Figure 3 - Sequence diagram

83

1. (Optionally) the **PDP** subscribes to the **PRP**, indicating that it wishes to be notified of the introduction, replacement or withdrawal of **applicable policies**.

84

85

2. (Optionally) the **PRP** notifies the **PDP** of the identities of **applicable policies** that it currently possesses.

86

87

3. (Optionally) the **PRP** notifies the **PDP** of the identities of **applicable policies** that have been introduced, replaced or withdrawn.

88

89

4. The **PDP** requests **policies** (by identity).

90

5. The **PRP** returns the requested **policies**.

91

4. Requirements

92

At the time of deployment of the PDP it is configured with a **topic**. The **PDP's** topic defines the set of **decision requests** that it is intended to answer. The **topic** conforms with the syntax of the `<xacml:Target>` element.

93

94

95

5. Potential sources

96

[SAMLProf] describes a request/response protocol for retrieving **policies** by identifier or **topic**.

97

[WS-Notification] describes a subscription/notification protocol.

98 **6. Transport layer**

99 It is expected that the protocol will be defined as a profile of an existing application protocol (such
100 as SAML), in which case it will inherit the transport-layer bindings of the host protocol.

101 **7. References**

102 **SAML** – OASIS Assertions and Protocols for the OASIS Security Assertion Markup Language
103 (SAML) V2.0, Committee Draft 02, 24 September 2004. Available at: [http://www.oasis-
open.org/committees/download.php/9455/sstc-saml-core-2.0-cd-02.pdf](http://www.oasis-
104 open.org/committees/download.php/9455/sstc-saml-core-2.0-cd-02.pdf)

105 **SAMLProf** – OASIS SAML 2.0 profile of XACML, Committee Draft 01, 16 September 2004.
106 Available at: [http://docs.oasis-open.org/xacml/access_control-xacml-2.0-saml_profile-spec-cd-
01.pdf](http://docs.oasis-open.org/xacml/access_control-xacml-2.0-saml_profile-spec-cd-
107 01.pdf)

108 **WS-Notification** – OASIS Web Services Base Notification 1.2 (WS-BaseNotification), Working
109 draft 03, 21 June 2004. Available at: [http://docs.oasis-open.org/wsn/2004/06/wsn-WS-
BaseNotification-1.2-draft-03.pdf](http://docs.oasis-open.org/wsn/2004/06/wsn-WS-
110 BaseNotification-1.2-draft-03.pdf)

111 **XACML** – OASIS eXtensible Access Control Markup Language (XACML) Version 2.0, Committee
112 Draft 02, 30 September 2004. Available at: [http://docs.oasis-open.org/xacml/access_control-xacml-
2_0-core-spec-cd-02.pdf](http://docs.oasis-open.org/xacml/access_control-xacml-
113 2_0-core-spec-cd-02.pdf)

114 **Appendix A. Acknowledgments**

115 The following individuals contributed to the development of the specification:

116

117 **Appendix B. Revision history**

Rev	Date	By whom	What
WD 01	8 Oct 2004	Tim Moses	First working draft

118

119 **Appendix C. Notices**

120 OASIS takes no position regarding the validity or scope of any intellectual property or other rights
121 that might be claimed to pertain to the implementation or use of the technology described in this
122 document or the extent to which any license under such rights might or might not be available;
123 neither does it represent that it has made any effort to identify any such rights. Information on
124 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS
125 website. Copies of claims of rights made available for publication and any assurances of licenses to
126 be made available, or the result of an attempt made to obtain a general license or permission for
127 the use of such proprietary rights by implementers or users of this specification, can be obtained
128 from the OASIS Executive Director.

129 OASIS has been notified of intellectual property rights claimed in regard to some or all of the
130 contents of this specification. For more information consult the online list of claimed rights.

131 OASIS invites any interested party to bring to its attention any copyrights, patents or patent
132 applications, or other proprietary rights which may cover technology that may be required to
133 implement this specification. Please address the information to the OASIS Executive Director.

134 Copyright (C) OASIS Open 2004. All Rights Reserved.

135 This document and translations of it may be copied and furnished to others, and derivative works
136 that comment on or otherwise explain it or assist in its implementation may be prepared, copied,
137 published and distributed, in whole or in part, without restriction of any kind, provided that the above
138 copyright notice and this paragraph are included on all such copies and derivative works. However,
139 this document itself may not be modified in any way, such as by removing the copyright notice or
140 references to OASIS, except as needed for the purpose of developing OASIS specifications, in
141 which case the procedures for copyrights defined in the OASIS Intellectual Property Rights
142 document must be followed, or as required to translate it into languages other than English.

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

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