# eXtensible Access Control Markup Language (XACML) Version 3.0 Policy Distribution Protocol Use-cases and Requirements

## Working draft 01, 8 Oct 2004

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

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


Editors:

Tim Moses, Entrust

Committee members:

Anne Anderson, Sun Microsystems
Anthony Nadalin, IBM
Bill Parducci, GlueCode Software
Daniel Engovatov, BEA Systems
Ed Coyne, Veterans Health Administration
Frank Siebenlist, Argonne National Labs
Hal Lockhart, BEA Systems
Michael McIntosh, IBM
Michiharu Kudo, IBM
Polar Humenn, Self
Ron Jacobson, Computer Associates
Seth Proctor, Sun Microsystems
Simon Godik, GlueCode Software
Steve Anderson, OpenNetwork
Tim Moses, Entrust



Abstract:

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


Status:

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

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

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

# Table of contents

# 1. Glossary (non-normative)

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

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

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

# 2. Introduction (normative)

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

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

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

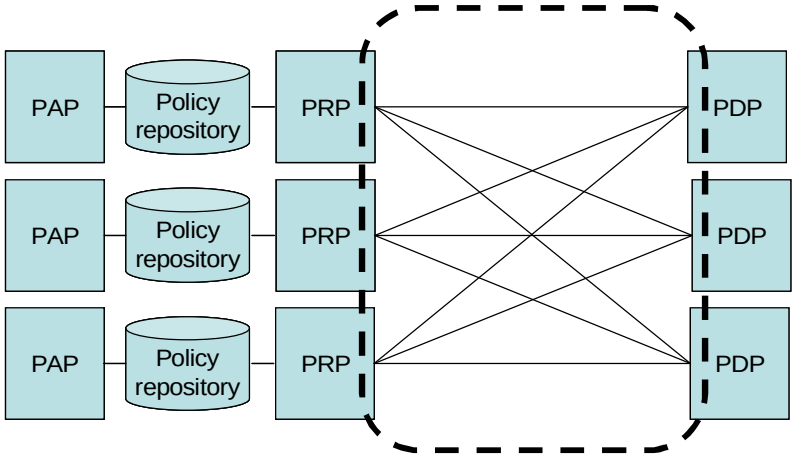


**Figure 1 - Context 1**

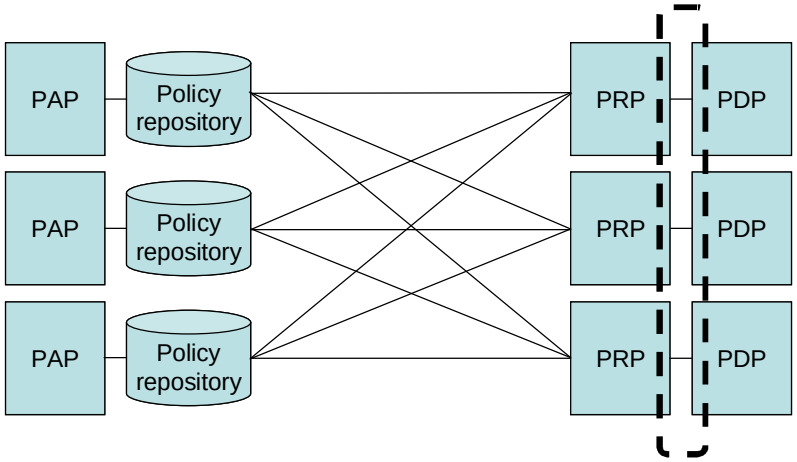


**Figure 2 - Context 2**

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

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

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

# 3. Sequence

The protocol proceeds as shown in Figure 3.

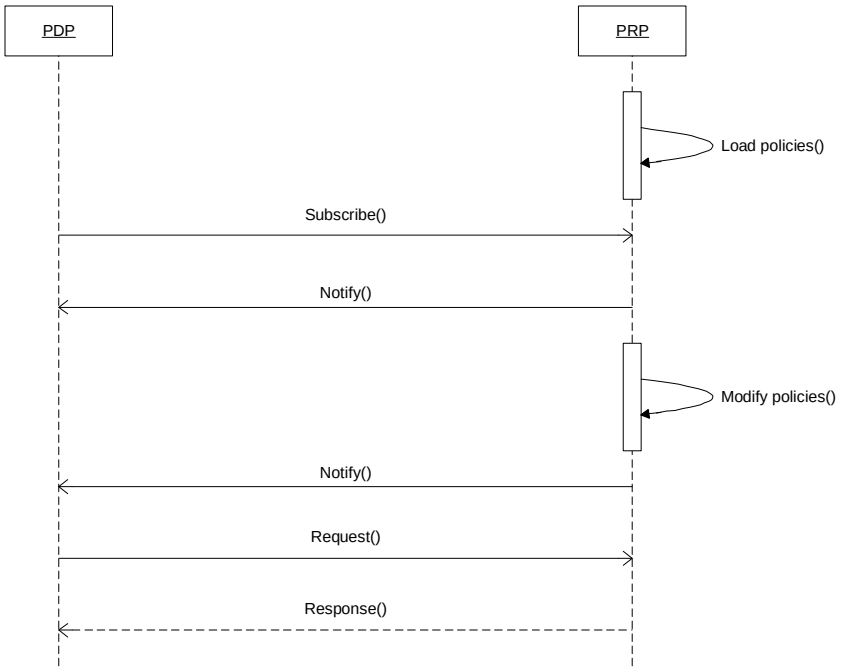


**Figure 3 - Sequence diagram**

1. (Optionally) the ***PDP*** subscribes to the ***PRP***, indicating that it wishes to be notified of the introduction, replacement or withdrawal of ***applicable policies***.
2. (Optionally) the ***PRP*** notifies the ***PDP*** of the identities of ***applicable policies*** that it currently possesses.
3. (Optionally) the ***PRP*** notifies the ***PDP*** of the identities of ***applicable policies*** that have been introduced, replaced or withdrawn.
4. The ***PDP*** requests ***policies*** (by identity).
5. The ***PRP*** returns the requested ***policies***.

# 4. Requirements

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.

# 5. Potential sources

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

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

# 6. Transport layer

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

# 7. References


**SAML** – OASIS Assertions and Protocols for the OASIS Security Assertion Markup Language (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

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

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

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

# Appendix A. Acknowledgments

The following individuals contributed to the development of the specification:

# Appendix B. Revision history

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

# Appendix C. Notices