XACML Profile for Requests for Multiple Resources

Working Draft 02, 4 June 2004

Document identifier:

xacml-profile-multiple-resources-1.0-draft-02

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=xacml

Editor:

Anne Anderson, Sun Microsystems (anne.anderson@sun.com)

Contributors:

Frank Siebenlist, Argonne National Laboratory
Daniel Engovatov, BEA
Tim Moses, Entrust
Michiharu Kudo, IBM
Michael McIntosh, IBM
Anthony Nadalin, IBM
Rebekah Lepro, NASA Ames
Steve Anderson, Open Network
Simon Godik, OverXeer
Bill Parducci, OverXeer
Seth Proctor, Sun Microsystems
Polar Humenn, Syracuse University

Abstract:

This document provides a profile for requesting access to more than one resource in a single XACML Request Context.

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.

Committee members should send comments on this specification to the xacml@lists.oasis-open.org list. Others should subscribe to and send comments to the xacml-comment@lists.oasis-open.org list. To subscribe, send an email message to xacml-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

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 XACML TC web page (http://www.oasis-open.org/committees/xacml/).

For any errata page for this specification, please refer to the XACML Profile for Requests for Multiple Resources section of the XACML TC web page (http://www.oasis-open.org/committees/xacml/).

Table of Contents

1 Introduction

{Non-normative}

The ***policy*** evaluation performed by an XACML ***Policy Decision Point***, or ***PDP***, is defined in terms of a single requested ***resource*** in the XACML Specification [XACML]. For efficiency, however, a ***Policy Enforcement Point***, or ***PEP***, may want to submit a single ***Authorization Decision Request*** that bundles requests for multiple ***resources***. This profile describes three ways in which a ***PEP*** can request multiple ***Authorization Decisions*** in a single ***Authorization Decision Request***. It also describes how the result of each ***Authorization Decision*** is represented in the bundled response ***context*** that is returned to the ***PEP***.

Support for each of the three mechanisms described in this profile is optional for compliant XACML implementations.

1.1 Terminology

Access - Performing an action

Access control - Controlling ***access*** in accordance with a ***policy***

Action - An operation on a ***resource***

Applicable policy - The set of ***policies*** and ***policy sets*** that governs ***access*** for a specific ***decision request***

Attribute - Characteristic of a ***subject***, ***resource, action*** or ***environment*** that may be referenced in a ***predicate*** or ***target*** (see also – ***named attribute***)

Authorization decision - The result of evaluating ***applicable policy,*** returned by the ***PDP*** to the ***PEP.*** A function that evaluates to "Permit”, “Deny”, “Indeterminate” or “NotApplicable", and (optionally) a set of ***obligations***

Context - The canonical representation of a ***decision request*** and an ***authorization decision***

Decision request - The request by a ***PEP*** to a ***PDP*** to render an ***authorization decision***

Hierarchical resource – A resource that is organized as a tree or forest (Directed Acyclic Graph) of individual resources called ***nodes.***

Node – An individual resource that is part of a ***hierarchical resource.***

Obligation - An operation specified in a ***policy*** or ***policy set*** that should be performed by the ***PEP*** in conjunction with the enforcement of an ***authorization decision***

Policy - A set of ***rules,*** an identifier for the ***rule-combining algorithm*** and (optionally) a set of ***obligations.*** May be a component of a ***policy set***

Policy decision point (PDP) - The system entity that evaluates ***applicable policy*** and renders an ***authorization decision***. This term is defined in a joint effort by the IETF Policy Framework Working Group and the Distributed Management Task Force (DMTF)/Common Information Model (CIM) in [RFC3198]. This term corresponds to "Access Decision Function" (ADF) in [ISO10181-3].

Policy enforcement point (PEP) - The system entity that performs ***access control***, by making ***decision requests*** and enforcing ***authorization decisions***. This term is defined in a joint effort by the IETF Policy Framework Working Group and the Distributed Management Task Force (DMTF)/Common Information Model (CIM) in [RFC3198]. This term corresponds to "Access Enforcement Function" (AEF) in [ISO10181-3].

Resource - Data, service or system component

1.1. Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF [RFC2119]

> "they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)"

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

The phrase ***{Normative, but optional}*** means that the described functionality is optional for compliant XACML implementations, but, if the functionality is claimed as being supported according to this Profile, then it SHALL be supported in the way described.

2 Requests for multiple resources

{Normative, but optional}

A single XACML request ***context*** MAY represent a request for ***access*** to multiple ***resources***. The syntax and semantics of such requests are specified in this section.

The `<Result>` elements produced by evaluating a request for ***access*** to multiple ***resources*** SHALL be identical to those that would be produced from a series of requests, each requesting ***access*** to exactly one of the ***resources.*** Each such resource is called an ***Individual Resource.*** The conceptual request ***context*** that corresponds to each `<Result>` element is called an ***Individual Resource Request.*** The `ResourceId` value in `<Result>` element is the `<AttributeValue>` of the ***resource attribute*** with `AttributeId` "`urn:oasis:names:tc:xacml:2.0:resource:resource-id`" in the ***Individual Resource Request.*** This Profile does NOT REQUIRE that the implementation of the evaluation of a request for ***access*** to multiple ***resources*** conform to the preceding model or that actual ***Individual Resource Requests*** be constructed. The Profile REQUIRES only that the `<Result>` elements SHALL be the same as if the preceding model were used.

Three ways of specifying requests for ***access*** to multiple ***resources*** are described in the following Sections. Each way of specifying requests describes the ***Individual Resource Requests*** that correspond to the `<Result> elements` in the response ***context.***

A single XACML request ***context*** MAY use more than one of these ways.

2.1 XPath expression in resource-id

{Normative, but optional}

This syntax SHALL be used only with ***resources*** that are XML documents.

An XACML request ***context*** `<Resource>` element MAY contain an ***attribute*** with an `AttributeId` of "`urn:oasis:names:tc:xacml:2.0:resource:resource-id`" and a `DataType` of "`urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression`", such that the `<AttributeValue>` evaluates to a nodeset that represents multiple ***nodes*** in the `<ResourceContent>` element. In this case, the `<Resource>` element SHALL NOT include an ***attribute*** with `AttributeId` "`urn:oasis:names:tc:xacml:2.0:resource:scope`".

Such a request ***context*** SHALL be interpreted as a request for ***access*** to the multiple ***nodes*** in the nodeset represented by the `<AttributeValue>` of the "`resource-id`" ***attribute***. Each such ***node*** SHALL represent an ***Individual Resource.***

Each ***Individual Resource Request*** SHALL be identical to the original request ***context*** with one exception: the `<Resource>` element SHALL contain a single "`resource-id`" ***attribute*** with a `DataType` of "`urn:oasis:names:tc:xacml:2.0:data-type:xpath-expression`" and an `<AttributeValue>` that SHALL be an XPath expression that evaluates to a single ***node*** in the `<ResourceContent>` element of the `<Resource>.` That node SHALL be the ***Individual Resource***. If the "`resource-id`" ***attribute*** in the original request ***context*** contained an `Issuer`, the "`resource-id`" ***attribute*** in the ***Individual Resource Request*** SHALL contain the same `Issuer`.

2.2 Scope Attribute in <Resource>

{Normative, but optional}

This syntax MAY be used with any ***hierarchical resource [Hierarchical]***, regardless of whether it is an XML document or not.

An XACML request ***context*** `<Resource>` element MAY contain a ***resource attribute*** with an `AttributeId of "urn:oasis:names:tc:xacml:2.0:resource:scope" and a DataType of` "http://www.w3.org/2001/XMLSchema#string". The <AttributeValue> for this ***attribute*** SHALL be either "Immediate", "Children", or "Descendants". If the ***resource*** is an XML document, then the <ResourceContent> element SHALL be included in the <Resource> element and SHALL contain the entire XML document of which the requested elements are a part. If the ***resource*** is an XML document, and the "scope" ***attribute*** is used, then the XPath expression used in the <AttributeValue> element of the "resource-id" ***attribute*** SHALL evaluate to a nodeset containing exactly one ***node***.

Such a request ***context*** SHALL be interpreted as a request for ***access*** to a set of ***nodes*** in a hierarchy relative to the single ***node*** specified in the "resource-id" ***attribute***. If the value of the "scope" ***attribute*** is "Immediate", the ***Individual Resource*** is the one ***node*** indicated by the "resource-id" ***attribute***. If the value of the "scope" ***attribute*** is "Children", the ***Individual Resources*** are the one ***node*** indicated by the "resource-id" attribute and all of its immediate child ***nodes***. If the value of the "scope" ***attribute*** is "Descendants", the ***Individual Resources*** are the one ***node*** indicated by the "resource-id" attribute and all of its descendant ***nodes***.

Each ***Individual Resource Request*** SHALL be identical to the original request ***context*** with one exception: the <Resource> element SHALL represent a single ***Individual Resource.*** This <Resource> element SHALL be at least one "resource-id" ***attribute,*** and all values for these ***attributes*** SHALL be unique, normative identities of the ***Individual Resource*.** If the "resource-id" ***attribute*** in the original request ***context*** contained an Issuer, the "resource-id" ***attributes*** in the ***Individual Resource Request*** SHALL contain the same Issuer.

Neither XACML nor this Profile specifies how the ***PDP*** obtains the information required to determine which ***nodes*** are children or descendants of a given ***node,*** except in the case of an XML document, where the information is obtained from the <ResourceContent> element.

2.3 Multiple <Resource> elements

{Normative, but optional}

This syntax MAY be used with any ***resource*** or ***resources***, whether they are XML documents or not and whether they are ***hierarchical resources*** [Hierarchical] or not.

An XACML request ***context*** MAY contain multiple <Resource> elements.

Such a request ***context*** SHALL be interpreted as a request for ***access*** to all ***resources*** specified in the individual <Resource> elements. Each <Resource> element SHALL represent one ***Individual Resource.***

Each ***Individual Resource Request*** SHALL be identical to the original request ***context*** with one exception: exactly one of the original <Resource> elements SHALL be present.

Note that the semantics for multiple <Resource> elements are very different from the semantics for multiple <Subject> elements in a request ***context***.

3 References

[Hierarchical]	A. Anderson, *XACML Profile for Hierarchical Resources,* *http://www.oasis-open.org/committees/xacml.*
[RFC2119]	S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, IETF RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt.
[XACML]	T. Moses, ed., *OASIS eXtensible Access Control Markup Language (XACML) Version 2.0, http://www.oasis-open.org/committees/xacml*

A. Revision History

	Date	By Whom	What
01	25 May 2004	Anne Anderson	Original specification, which was part of the Hierarchical Resources specification.
02	4 Jun 2004	Anne Anderson	Formatted multiple resource requests as a separate profile from hierarchical resources; made each feature normative but optional.

B. Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

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

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 RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.