



LDAP profile for distribution of XACML policies

Working draft 01, 17 October 2003

Document identifier: oasis-xacml-v2.0-LDAP_profile-wd-01

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

Send comments to: xacml-comment@lists.oasis-open.org

Editors:

Tim Moses, Entrust

Contributors:

Abstract:

This working draft describes how to distribute XACML policies using LDAP.

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, subscribe to the xacml-comment@lists.oasis-open.org list and send comments there. To subscribe, send an email message to xacml-comment-digest-subscribe@lists.oasis-open.org

Copyright (C) OASIS Open 2003 All Rights Reserved.

22	Table of contents	
23	1. Introduction (non-normative)	3
24	1. Directory information tree (normative)	3
25	2. Directory schema (normative)	4
26	2.1 Object Class Definitions	4
27	2.1.1. XACML Target Info	4
28	2.1.2. XACML Policy Info	4
29	2.1.3. XACML Policy Instance	5
30	2.2 Attribute Definitions	5
31	2.2.1. XACML Target	5
32	2.2.2. XACML Attribute Name	5
33	2.2.3. XACML Attribute Value	5
34	2.2.4. XACML Policy Data	6
35	2.2.5. XACML Policy Id	6
36	2.2.6. XACML Policy	6
37	2.3 Matching Rule Definitions	6
38	3. Policy posting (normative)	7
39	4. Policy retrieval (normative)	7
40	5. Policy validation (normative)	7
41	6. Policy combination (normative)	7
42	7. Security considerations (non-normative)	7
43	Appendix A. Revision history	8
44	Appendix B. Notices	9
45		
46		

1. Introduction (non-normative)

XACML <Policy> and <PolicySet> elements may be distributed from the **PAP** to the **PDP** by means of an LDAP repository. In this case, conformant implementations behave as described in this specification.

1. Directory information tree (normative)

The XACML <Target> element conforms to the data model shown in Figure 1. XACML does not specify the attribute names and distinguished values used in the data model, but these MUST be agreed between the **PAP** and the **PDP**.

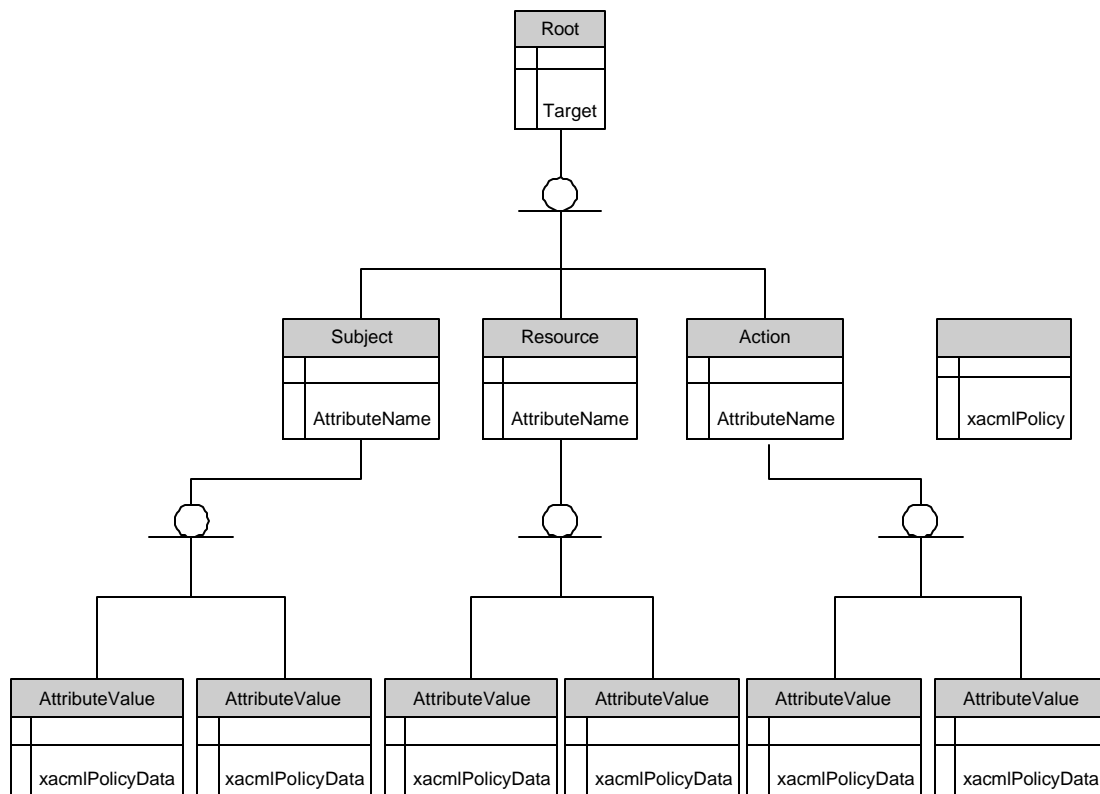


Figure 1 – Directory information tree

The Directory Information Tree of the LDAP repository MUST be congruent with that of the **target** data model. The **PAP** is REQUIRED to ensure that all policies of the domain are available from a directory entry. The **PAP** is REQUIRED to ensure that all policies applicable to a particular distinguished subject attribute value, resource attribute value or action attribute value are available from, or referenced by, the corresponding directory entry. In the case of a reference, it SHALL identify the directory entry from which the policy can be retrieved.

2. Directory schema (normative)

This directory schema defines three structural object classes:

- **xacmlTargetInfo**;
- **xacmlPolicyInfo**; and
- **xacmlPolicyInstance**.

xacmlTargetInfo is used to partition the DIT according to the components of an XACML *target*.

xacmlPolicyInfo is used for adding XACML policy data to the directory entries associated with distinguished attribute values of resources, actions and/or subjects, as determined from the *target* data model. It defines a directory attribute, called **xacmlPolicyData**, to contain the associated policies or references to entries containing the associated policies.

In addition, XACML policies MAY be stored in policy-specific entries where they can be referenced from the directory entries of the distinguished attribute values of resources, actions and/or subjects, as described above. For this purpose, the schema defines a structural object class, called **xacmlPolicyInstance**, and a directory attribute, called **xacmlPolicyId**, to contain the string used to name the entry in the directory. The **xacmlPolicy** directory attribute is used in these entries to contain the policy itself.

2.1 Object Class Definitions

The following object classes are defined.

2.1.1. XACML Target Info

The **xacmlTargetInfo** object class is used for defining entries for the components of the target.

```
xacmlTargetInfo OBJECT-CLASS ::= {  
  SUBCLASS OF {top}  
  KIND auxiliary  
  MUST CONTAIN {xacmlTarget}  
  MAY CONTAIN {xacmlAttributeName}  
  ID id-???-oc-xacmlTargetInfo }
```

The **xacmlTarget** directory attribute is used to name the entry and position it in the DIT.

2.1.2. XACML Policy Info

The **xacmlPolicyInfo** object class is used for defining entries of objects that hold XACML policy data.

```
xacmlPolicyInfo OBJECT-CLASS ::= {  
  SUBCLASS OF {top}  
  KIND auxiliary  
  MUST CONTAIN {xacmlAttributeValue}  
  MAY CONTAIN {xacmlPolicyData}  
  ID id-???-oc-xacmlPolicyInfo }
```

The **xacmlAttributeValue** directory attribute is used to name the entry and position it in the DIT.

2.1.3. XACML Policy Instance

The **xacmlPolicyInstance** object class is used for defining entries of objects that hold only a single XACML policy statement.

```
xacmlPolicyInstance    OBJECT-CLASS ::= {  
  SUBCLASS OF    {top}  
  KIND            structural  
  MUST CONTAIN   {xacmlPolicyId}  
  MUST CONTAIN   {xacmlPolicy}  
  ID             id-???-oc-xacmlPolicyObject }
```

The **xacmlPolicyId** directory attribute is used to name the entry and position it in the DIT.

2.2 Attribute Definitions

The following directory attributes are defined.

2.2.1. XACML Target

The **xacmlTarget** directory attribute SHALL contain an enumeration of the components of the XACML *target*.

```
xacmlTarget            ATTRIBUTE ::= {  
  WITH SYNTAX          XacmlTargetSyntax  
  ID                   id-???-at-xacmlPolicy }  
XacmlTargetSyntax ::= ENUMERATION {  
  Subject              [0]  
  Resource              [1]  
  Action               [2] }
```

2.2.2. XACML Attribute Name

The **xacmlAttributeName** directory attribute is a multi-valued attribute containing XACML attribute names.

```
xacmlAttributeName    ATTRIBUTE ::= {  
  WITH SYNTAX          XacmlAttributeNameSyntax  
  ID                   id-???-at-xacmlPolicy }  
XacmlAttributeNameSyntax ::= UTF8String }
```

2.2.3. XACML Attribute Value

The **xacmlAttributeValue** directory attribute is a single-valued attribute containing an XACML attribute value.

```
xacmlAttributeValue    ATTRIBUTE ::= {  
  WITH SYNTAX          XacmlAttributeValueSyntax  
  ID                   id-???-at-xacmlPolicy }  
XacmlAttributeValueSyntax ::= UTF8String }
```

2.2.4. XACML Policy Data

The **xacmlPolicyData** directory attribute is a multi-valued attribute containing XACML policy information.

```
xacmlPolicyData  ATTRIBUTE ::= {  
  WITH SYNTAX    XacmlPolicySyntax  
  ID             id-???-at-xacmlPolicyData }  
XacmlPolicySyntax ::= SEQUENCE {  
  policyRef      [0]    UTF8String OPTIONAL,  
  policyData     [1]    UTF8String OPTIONAL  
  -- at least one of the optional elements must be present-- }
```

If **policyRef** is present, then it SHALL contain the value of the relative distinguished name of the entry that contains the policy.

If **policyData** is present, then it SHALL contain a SAML assertion, which, in turn, contains an XACML <policy> or <policySet> element.

2.2.5. XACML Policy Id

It is RECOMMENDED That the **xacmlPolicyId** directory attribute contain a single XACML policyId attribute.

```
xacmlPolicyId    ATTRIBUTE ::= {  
  WITH SYNTAX    UTF8String  
  EQUALITY MATCHING RULE    xacmlPolicyIdMatch  
  ID             id-???-at-xacmlPolicyId }
```

2.2.6. XACML Policy

The **xacmlPolicy** directory attribute SHALL contain a single SAML assertion, which, in turn, contains an XACML <Policy> or <PolicySet> element.

```
xacmlPolicyId    ATTRIBUTE ::= {  
  WITH SYNTAX    UTF8String  
  ID             id-???-at-xacmlPolicy }
```

2.3 Matching Rule Definitions

The **xacmlPolicyIdMatch** matching rule compares for equality a presented value with an attribute value of type **xacmlPolicyId**.

```
xacmlPolicyIdMatch  MATCHING-RULE ::= {  
  SYNTAX    UTF8String  
  ID       id-???-at-policyNameMatch }
```

This rule returns TRUE if the presented value is equal to the stored value of the **xacmlPolicyId** directory attribute.

3. Policy posting (normative)

If the **PAP** posts policies in entries named by **xacmlPolicyId** values, then the ascending portion of the entry's DN MUST be agreed between the **PAP** and the **PDP** using an unspecified method.

It is RECOMMENDED that **PAPs** use the `PolicyId` attribute value as the **policyRef** attribute value.

4. Policy retrieval (normative)

Given a target definition, a **PDP** MUST retrieve all **xacmlPolicyData** values from the corresponding entries in the DIT. It SHALL eliminate duplicate **PolicyRef** values and retrieve all **xacmlPolicy** attributes from the entries identified by the **PolicyRef** values.

The **PDP** is REQUIRED to confirm that the retrieved policy is applicable to the **decision request** (i.e., the request **context**) that it is processing.

5. Policy validation (normative)

The **PDP** MUST validate the retrieved SAML assertions by verifying signatures and validity intervals.

6. Policy combination (normative)

A **PDP** MUST verify that it has retrieved all applicable policies, by an unspecified method.

The **PDP** MUST combine all the retrieved policies into a single `<PolicySet>` element, using a combining algorithm that has been agreed between the **PAP** and the **PDP**.

7. Security considerations (non-normative)

If an entry were to be deleted from, or replaced in, the DIT, then the **PDP** would not retrieve all the policies associated with the target. This could cause it to render an incorrect decision. Therefore, the **PDP** must be able to detect this condition and render an "Indeterminate" decision.

Appendix A. Revision history

Version	When	By whom	Changes
WD 01	17 Oct 2003	Tim Moses	Initial draft

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

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.

Copyright (C) OASIS Open 2003. All Rights Reserved.

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 paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document 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 RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.