XACML Architecture

See the following topics for information on XACML and also on the architecture of XACML.

- Introducing XACML
- Why XACML
- XACML system architecture
- XACML terminology
- XACML engine architecture
- XACML policy language structure and syntax
- Improvements in XACML 3.0
- XACML 2.0 and XACML 3.0 samples

Introducing XACML

XACML (eXtensible Access Control Markup Language) is an XML-based language for access control that has been standardized by the Technical Committee of the OASIS consortium. XACML is popular as a fine grain authorization mechanism among the community. However, there are aspects of XACML which surpass it being just a fine grain authorization mechanism.

Although XACML was introduced as a standard by OASIS in 2003, not many organisations that have been adapted it yet. This is because most of the organizations have not shown interest in moving towards a XACML solution for authorization. The following may be some reasons for this:

- Many software designer and developers do not have a clear understanding on the importance and advantages of XACML.
- It is a bit hard to implement a XACML solution rather than a typical JDBC or hard coded authorization system.
- Performances of XACML-based authorization system may be less than adequate.
- Complexity of defining and managing XACML policies.

However, current market trends indicate that there are some motivation for XACML-based authorization systems. This section includes some architectural and implementation details on XACML with an existing XACML engine.

If you are interested in going into the depth in XACML, You can find XACML specifications and other information here.

To summarize, XACML describes both an access control policy language, request/response language and reference architecture. The policy language is used to express access control policies (who can do what when). The request/response language expresses queries about whether a particular access should be allowed (requests) and describes answers to those queries(responses). The reference architecture proposes a standard for deployment of necessary software modules within an infrastructure to allow efficient enforcement of policies.

Why XACML

Most of the organizations still use legacy systems with inbuilt authorization logic. Sometimes, one organization contains a large number of information systems and applications that each system or application uses for their own process of authorization. Today, authorization has become more complex because users within organizations as well as outside the organization need access to shared data and have the need to collaborate efficiently. Therefore It has been very hard to manage those legacy, custom authorization systems. However, XACML offers a solution to this problem.

When we think about a traditional authorization system, it would mostly look like as follows:

- Authorization logics are hard coded into the programming source code
- Authorization logics are stored in a databases that could be only readable and understandable by the underlying application

The following are the some goals that current organizations are looking at from an authorization system.
Can business managers (who should determine how access controls would be implemented) define and modify authorization logics?
Can we find new IT technicians to manage these legacy systems? Especially when people who developed the system, left the organization
Can authorization logics be modified without any source code changes in an dynamic way?
Is authorization system capable for evaluating following rule? “X resource can be accessed by the Users who are from example.com domain and whose age is greater than 21 years old”
If we are going to implement a new information system with the organization, can we re-use the authorization logics of a legacy system?
Can achieve find-grant authorization without defining large number of static combinations?
Is authorization systems capable of answering following questions: “Can a user, Bob, transfer X amount from Y current account at 1.00pm?”

As we can understand, the above goals can not be achieved from a traditional authorization system. However XACML (eXtensible Access Control Markup Language) based authorization solution can provide all of these goals. This is because XACML:

- is a standard which is ratified by OASIS standards organization.
- is a policy language implemented using XML.
- supports Attribute Based Access Control (ABAC) and evaluation can be done with the additional data retrieved from Policy Information Point (PIP) which is defined by the XACML reference architecture.

### Note

**Attribute Based Access Control(ABAC)**

ABAC is an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, object, environment attributes etc.). This model supports Boolean logic, in which rules contain "IF, THEN" statements about who is making the request, the resource, and the action. For example: IF the requestor is a manager, THEN allow read/write access to sensitive data.

- contains reference architecture which is provided to externalize the authorization system. The Policy Decision Point (PDP) offers authorization as a service in your infrastructure. Authorization algorithms can be removed from the application logic and applications can query the PDP via their own Policy Enforcement Points (PEP).
- provides fine-grained authorization with higher level of abstraction by means of policies and rules.
- supports dynamic evaluation of policies by using the Policy Information Point (PIP).
- can publish multiple policies into external PDPs.

### XACML system architecture

Policy Decision Point (PDP) evaluates policies against access requests provided by Policy Enforcement Points (PEP). To provide the decisions, PDP may also need to query a Policy Information Point (PIP) to gather descriptive attributes about the user or any other missing attribute in the request. Policy Administration Point (PAP) is used to manage the PDP and PIP functionality.
**XACML terminology**

The XACML reference architecture illustrated above is comprised of the following four 'building blocks'.

- **Policy Enforcement Point (PEP)**: The system entity that performs access control by making decision requests and enforcing authorization decisions. Basically this is the entity that sends the XACML request to the Policy Decision Point (PDP) and receives an authorization decision.
- **Policy Decision Point (PDP)**: The system entity that evaluates an applicable policy and returns an authorization decision.
- **Policy Information Point (PIP)**: The system entity that acts as a source of attribute values. Basically if there are missing attributes in the XACML request that is sent by PEP, PIP would find them for the PDP to evaluate the policy.
- **Policy Administration Point (PAP)**: The system entity that creates a policy or policy set and manages them.

**XACML engine architecture**

The WSO2 Identity Server is a major player in the XACML and open source world. The Identity Server supports XACML 3.0, which is based on Balana XACML implementation. As the source code, distribution and documentation are available for free, it is possible to analyze and understand the architecture behind it. You can find source code from here. This section provides some information regarding the architecture of the XACML engine (or the entitlement engine) of the WSO2 Identity Server.

The XACML engine of the WSO2 Identity Server has two major components, i.e., PAP and PDP. This section focuses on Policy Decision Point (PDP) only.

The following diagram represents the component architecture of the PDP.
The following information provides more details on the various components available in the PDP architecture.

**Entitlement Admin Service**

All PDP configurations have been exposed via this API as a Web service. You need to have certain privilege to access this API. The following functions can be done by calling this API.

- Invalidating caches
- Refreshing policy, attribute, resource finder modules
- Retrieving PDP configurations
- Includes the function for testing the Test PDP with a given sample request or a sample request with given policies

**Entitlement Service**

Actual XACML authorization API has been exposed via this API as a Web service. This service supports the following three communication methods with PEP.

- SOAP-based Web service
- Thrift binary protocol (this is much faster than SOAP)
- WS-XACML (This is the standard way but not popular)

**Balana PDP**
This is the core of the engine. Balana PDP has been initialized with all the attribute finders, resource finders and policy finder modules that have been plugged with WSO2 Identity Server.

**Balana Test PDP**

This is same as Balana PDP. However, this instance has been initialized with the PAP policy store. It means, policies that are defined by PAP can be evaluated by using this PDP instance. There is no policy caching or decision caching with this. Therefore this can be only used for testing your policies in the PAP store. Web service API for Balana Test PDP has been exposed via the Entitlement Admin Service with method name “doTestRequest()”.

**Carbon Policy Finder**

This module finds policies from different policy stores to evaluate a XACML request. The following is a high level diagram of how this works.

Any number of policy finder modules can be plugged with the Carbon policy finder. You need to implement the CarbonPolicyFinderModule interface to write a new module and register it using the entitlement.properties configuration file. By default, WSO2 Identity Server is shipped with a Carbon registry-based policy finder module that can retrieve policies from a registry collection, where the collection path is configurable using a property value in the entitlement.properties configuration file.
All modules would be initialized and policies would be loaded into memory when the Carbon policy finder is used. Loaded policies are kept as a policy collection where you can use your own implementation to access them. A written policy collection implementation can be registered using the entitlement.properties configuration file. The default implementation uses an in-memory cache and creates an effective policy for a given XACML request.

Therefore, the Carbon policy finder always finds effective policies from the policy collection where it is recommended to be kept in-memory. However, if any update in the policy store happens, the Carbon policy finder can be re-initialized automatically by the module that you have written, or you can re-initialize it using the Web service API (Entitlement Admin Service). Also you can manually do it using the Identity Server Management Console.

When you are writing a new module, you need to consider the following in addition to policy retrieving and re-initializing.

- Policy ordering - The order which policies are evaluated.
- Policy combining algorithm

**Note**

There are **Policy Combining Algorithms** which are used by **Policy Sets** and **Rule Combining Algorithms** which are used by **Policies**. Each of the algorithms mentioned below has its Policy Combining algorithm and its Rule Combining algorithms as follows:

- Standard combining algorithms defined in XACML 3.0:
  - urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable
  - urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable
  - urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:only-one-applicable
  - urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny

These algorithms are explained in detail as follows,

- **Deny Overrides:**
  This combining algorithm combines decisions in such a way that if any decision is a Deny, then that decision wins.
  Deny overrides is one of the safest combining algorithms since it favors a Deny decision. However, if none of the children return a Deny decision, then the combining algorithm will never produce a Deny.

- **Permit Overrides:**
  This combining algorithm combines decisions in such a way that if any decision is a Permit, then that decision wins.

  The permit overrides combining algorithm can be interesting when:

  At least one child must return a Permit for access to be granted overall regardless of restrictions.
One wants to return all the reasons why access is being denied. This is what one could call a "greedy deny overrides". For instance if the reason for not being able to view a resource is that (a) you are not the owner and (b) you are in the wrong department, then we could rework the previous example as follows. When any of the deny reason triggers, the response would be denied with all the applicable reasons for access being denied:

- **Policy Set (deny overrides):** role==manager AND action==view AND resourceType==resource
  - **Policy 1 (permit overrides):**
    - Rule 1: deny if resourceOwner != userId + Advice("you are not the owner of the resource")
    - Rule 2: deny if resourceDepartment != userDepartment + Advice("you are not in the same department as the resource")
  - **Policy 2**
    - Rule 1: permit

**First Applicable:**
This combining algorithm combines decisions in such a way that the final decision returned is the first one produced either of Permit or Deny.

First applicable is useful to shortcut policy evaluation. For instance, if a policy set contains a long series of not applicable policies and one applicable policy which returns either of Permit or Deny, then if that policy comes first and does produce Permit or Deny, the PDP will stop there and not process the other siblings.

- **Deny Unless Permit | Permit Unless Deny:**
  In XACML there are 4 possible decisions: Permit, Deny, NotApplicable, and Indeterminate. Sometimes, it is desirable to hide the NotApplicable and Indeterminate decisions to only allow for Permit or Deny. It makes the PEP logic potentially simpler.

- **Only One Applicable:**
  This combining algorithm exists only for policy sets to combine policy sets and policies. It cannot be used to combine rules. With this combining algorithm, in order for either permit Permit or Deny to be returned, then only one of the children must produce a valid decision – whether Deny or Permit.

- **Ordered Deny Overrides | Ordered Permit Overrides:**
The ordered combining algorithms combine decisions in the same way as their (unordered) cousins. In addition they bring the guarantee that policies, policy sets, and rules are considered in the order in which they are defined. The need to define an ordered combining algorithm stems from the fact the XACML specification does not specify whether order matters in the deny-overrides and permit-overrides combining algorithms.

- How to retrieve referenced policies

**Carbon Attribute Finder**

This module helps to find the missing attribute for a given XACML request. The following is the high level diagram for both the Carbon attribute and resource finders.
Any number of PIP attribute finder modules can be plugged with the Carbon attribute finder. You need to implement the PIPAttributeFinder interface to write a new module and register it using the entitlement.properties configuration file. By default, WSO2 Identity Server is shipped with a DefaultAttributeFinder that communicates with the underlying user store of the Identity Server. The default user store of the Identity Server is ApacheDS where it can be changed using user-mgt.xml file. See Configuring the Realm for more information.

All modules would be initialized and supported attribute Ids are retrieved for each module. During runtime, the Carbon attribute finder checks for the support attribute Id and hands it over to the proper module to handle. A caching machine is used by the Carbon attribute finder for caching the findings or the attribute finder module itself can handle it.

**Carbon Resource Finder**

This is used to retrieve children or descendant resources of a given root level resource value. Basically it is used to fulfill the requirement of a multiple decision profile. The implementation is same as the PIP attribute finder module. By default, WSO2 Identity Server is shipped with DefaultResourceFinder (which is the implementation of PIPResourceFinder) that communicates with Carbon registry resources.

**XACML policy language structure and syntax**

In order to render an authorization decision, it must be possible to combine the two separate policies to form the single policy applicable to the request.

XACML defines three top-level policy elements:

- `<Rule>` - Element that contains a Boolean expression that can be evaluated in isolation, but that is not intended to be accessed in isolation by a PDP. So, it is not intended to form the basis of an authorization
decision by itself. It is intended to exist in isolation only within an XACML PAP, where it may form the basic unit of management.

- <Policy> - Element that contains a set of <Rule> elements and a specified procedure for combining the results of their evaluation. It is the basic unit of policy used by the PDP, and so it is intended to form the basis of an authorization decision
- <PolicySet> - Element that contains a set of <Policy> or other <PolicySet> elements and a specified procedure for combining the results of their evaluation. It is the standard means for combining separate policies into a single combined policy.

As XACML is used in Attribute Based Access Controlling, in XACML all the attributes are categorized into four main categories: But from XACML 3.0, custom categories are also supported.

- Subject
- Resource
- Action
- Environment

A Rule is the most elementary unit of policy. It may exist in isolation only within one of the major actors of the XACML domain. The main components of a Rule are as follows:

- <Target> - This defines the set of requests to which the rule is intended to apply in the form of a logical expression on attributes in the request.
- <Effect> - The effect of the rule indicates the rule-writer's intended consequence of a "True" evaluation for the rule. Two values are allowed: "Permit" and "Deny".
- <Condition> - A Boolean expression that refines the applicability of the rule beyond the predicates implied by its target. Therefore, it may be absent.
- <ObligationExpressions> - Obligation expressions may be added by the writer of the policy. When a PDP evaluates a policy containing obligation expressions, it evaluates the obligation expressions into obligations and returns certain of those obligations to the PEP in the response context.
- <AttributeSelector> - This allows the policy to specify an attribute with given identifier, category and data type. AttributeSelector on the other hand provides a mean to lookup the value of attributes using a XPath query by specifying the data type and XPath expression. Attribute selectors are then executed against the XML content that may have been sent along in the initial XACML request.

A sample XACML 3.0 policy is as follows:

```xml
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit" RuleId="permit"/>
</Policy>
```
**Improvements in XACML 3.0**

The XACML 3.0 core specification highlights the following main changes in comparison with XACML 2.0.

**Custom attribute categories**

Custom attribute categories can be defined with XACML 3.0. However, in XACML 2.0, attributes have been organized into subject, resource, environment or action. For example, consider that you want to create an attribute category called “foo” in your policy and request. You can do it with XACML 3.0 without any issue. According to the XACML 3.0 policy schema, the category of XACML element is identified by a XML attribute called "Category".

In XACML 2.0 Policy, you can define the attribute designator element as follows, However, it must be a pre-defined category such as subject, resource, environment or action.

```
<ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
```

In a XACML 3.0 Policy, you can define it as follows. Category can be any thing as it is defined as an attribute of the AttributeDesignator element.

```
<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="resource" DataType="http://www.w3.org/2001/XMLSchema#string"/>
```

**Improvements in Obligation**

In general obligation can have following,

- Obligations have an identifier, which is used to distinguish different types of obligations
- Obligations can have arguments
- Obligations apply to Permit (or Deny) decisions only

A PDP will return, as part of a Permit or Deny response, a (possibly empty) subset of the obligations that appear in the policy.

There are several improvements with Obligation in XACML 3.0 when compared to 2.0.

One of the main improvements is the introduction of **Obligation Expressions**. This adds dynamic expressions into the obligation statements. For a more indepth understanding, see the following example:

Let assume that you want to do following with the Obligation: “On deny, inform the PEP to send an email to the user”.

In XACML 2.0, you need to define the obligation element with the user email statically.

```
<Obligation ObligationId="send-email" FulfillOn="Deny">
  <AttributeAssignment AttributeId="email" DataType="http://www.w3.org/2001/XMLSchema#string">user@foo.com</AttributeAssignment>
</Obligation>
```
However, the user would not be same for each XACML request that is evaluated. Therefore it is not possible to configure the email statically in the Obligation element. Obligation can only inform PEP to send an email to user (it lets the PEP figure out the value of user’s email).

```xml
<Obligation ObligationId="send-email" FulfillOn="Deny">
    <AttributeAssignment AttributeId="text" DataType="http://www.w3.org/2001/XMLSchema#string">please send email to user</AttributeAssignment>
</Obligation>
```

However, in XACML 3.0, the email of each user can be retrieved using PIP in a dynamic manner as we can define an expression element inside the ObligationExpression. Therefore, obligation can inform PEP to send an email to user@foo.com address.

```xml
<ObligationExpression ObligationId="send-email" FulfillOn="Deny">
    <AttributeAssignmentExpression AttributeId="email" DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeDesignator AttributeId="email" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="false"/>
    </AttributeAssignmentExpression>
</ObligationExpression>
```

In XACML 2.0, obligations can only be added to policies and policy sets. However, with XACML 3.0, rules can also contain obligations. At the root of all XACML policies is a policy or a policy set. A policy represents a single access control policy, expressed through a set of rules. A policy set is a container that can hold other policies or policy sets, as well as references to policies found in remote locations.

**Introducing Advice**

Advice is a newly introduced feature with XACML 3.0. Advice is similar to obligations and it shares much of its syntax. The difference is contractual: the PEP can disregard any advice it receives. PEPs do not have to comply with advice statements; PEPs can consider or discard the statement. A common scenario is to explain why something was denied: “User bob is denied because he does not have a valid email”.

The XACML specification says that any advice returned with a decision can be safely ignored by compliant PEPs. This means that PEPs should work as described in the previous section, regardless of what the PEP does with the advice it may receive. For example, a PEP must allow access if it receives a Permit decision with no obligations, regardless of any advice in the decision.

**Improvements in Target**

Since it is possible to define custom attribute categories, there are improvements in some related elements in the XACML 3.0 policy, when compared to 2.0. With XACML 3.0, the Target element can be used to define more complex authorization logic within itself when compared with 2.0.

In XACML 2.0, the Target element contains the OR and AND relationship between the same category. However, in XACML 3.0, AllOf and AnyOf elements have been introduced to Target element. That clearly helps to define the OR and AND relationship between different categories.

As an example, let look at a Target element. In XACML 2.0, we have an AND relationship between foo1 and foo2 resources and an OR relationship between bar1 and bar2 actions. However, we cannot create an OR relationship between a foo1 resource and bar1 action. so we cannot define something such as “Target would be matched when Bob can access the foo resource or do a bar action” by using the Target element.
XACML 3.0 has an AND relationship between “foo” resource and “bar1” role and an OR relationship between “bar2 action. So we cannot define something as “Target would be matched, when Bob can access foo resource and do bar1 action or do bar2 action”.
More Functions and Algorithms

XACML3 has introduced new String functions such as:

- `urn:oasis:names:tc:xacml:3.0:function:string-starts-with`
- `urn:oasis:names:tc:xacml:3.0:function:string-ends-with`
- `urn:oasis:names:tc:xacml:3.0:function:string-contains`
- `urn:oasis:names:tc:xacml:3.0:function:string-substring`

Some improvements to other functions such as
Also improvements to existing combine algorithms (deny-overrides, permit-overrides, ordered-deny-overrides and ordered-permit-overrides) and new two combine algorithms for policy and rule combining.

• urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit
• urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-unless-permit
• urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny
• urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-unless-deny

Improvements in XPath

New XPath data type is introduced with XACML 3.0. In XACML 2.0, XPath is defined as a String and cannot define the context that the namespace prefix is going to resolve. Also XPath based multiple decisions scheme is introduced with XACML 3.0.

Improvement in XACML Request and Response

As it is possible to define custom attribute categories, many types of attribute categories can be in the XACML 3.0 request. XACML 2.0 request can contain only subject, resource, environment or action categories.

The XACML Response can contain additional data such as:

• Request attributes that are defined in the XACML response.
• Applicable policy ids for a given XACML request are defined in the XACML response.

Multiple Decision Profile

This is new profile which comes with XACML 3.0 and is not included in the XACML3 core specification. However, this is very useful for performance improvement between PEP and PDP. This is especially the case since PEP can request decisions for multiple requests in one XACML request.

Administrative Delegation Profile

This is also a new profile which comes with XACML 3.0. This allows you to define policies about who can write policies about what. For example, “Bob may issue a policy but only about resources in department X”.

XACML 2.0 and XACML 3.0 samples

The biggest difference between XACML 2.0 and XACML 3.0 for your client app is that the structure of the attributes in the authentication request has changed significantly in XACML 3.0.

In XACML 2.0, attributes were organized into subject, resource, environment, or action categories using XML element tags:
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
access_control-xacml-2.0-context-schema-os.xsd">
  <Subject>
    <Attribute
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>Julius Hibbert</AttributeValue>
    </Attribute>
  </Subject>
  <Resource>
    <Attribute
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>http://medico.com/record/patient/BartSimpson</AttributeValue>
    </Attribute>
  </Resource>
  <Action>
    <Attribute
      AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
      <AttributeValue>read</AttributeValue>
    </Attribute>
  </Action>
</Request>

In XACML 3.0, these categories are indicated using XML attributes instead of XML element tags:
The `<Subject>` element in XACML 2.0 becomes `<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">` in XACML 3.0, for example. This is the same for the resource, environment, and action categories.