XACML – Proposal for Policy Model Regarding Subject Semantics

October 15, 2001
V 0.1
Author: Michiharu Kudo

Status of this Document

This document is created to present to XACML policy model sub-committee a proposal of subject semantics.

1. Overview

I propose that the subject semantics should mean only a subject who submitted an access request (Initiator in [ISO]). Other usage of subject such as a person to whom the authorization is granted should be distinguished from the Initiator. In this proposal, the subject semantics are defined in three different XACML specification stages: policy model, policy language, and PDP specification.

- In a policy model, subject semantics are defined as general as possible, for example logical expression using attribute type-value pairs.
- In a policy language, subject semantics are represented in more application-specific ways primarily for readability purpose as well as in logical expression.
- PDP specification presents how to retrieve subject related information into PDP and associate it to each language primitive.

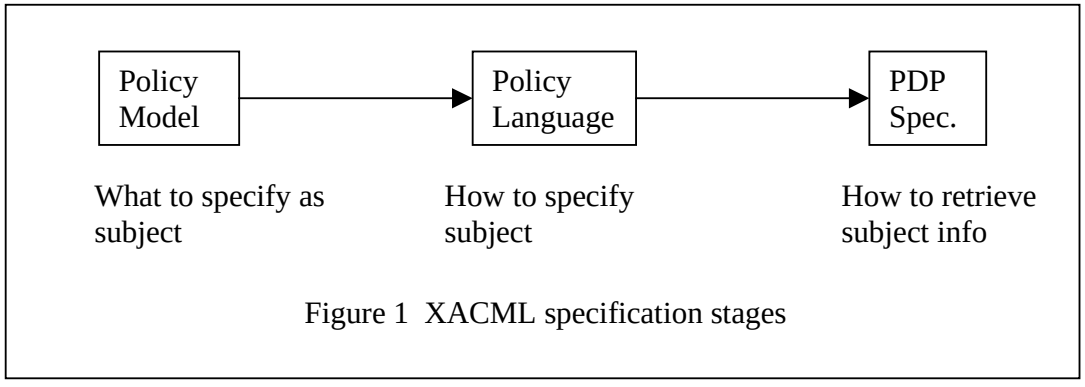

Figure 1 XACML specification stages

2. Subject Semantics in Policy Model

Subject primitive represents conditions on an Initiator (a requesting subject) for applying the specific access control policy. The semantics are represented as logical expression using Initiator's attribute type-value pairs (conjunctive and disjunctive expression.) In the policy model, we do not care about how to retrieve those information. For example, a subject who belongs to a marketing group, who is activating a manager role, and who holds a X.509 certificate issued from VeriSign is represented as Ex1:

Ex1: (group = "marketing" AND role = "manager" AND X509.Issuer = "VeriSign")
Ex2: ((group = "development" AND role = "manager") OR group = "marketing")
Ex3: "*"

"*" implies every Initiator.

Policy model may contain another subject information such as a person to whom the authorization is granted. The policy model should provide a model primitive to represent such an entity. For example, Grantee primitive may be introduced. The semantics are represented in the same manner as Subject.

Grantee:

Ex4: (X509.Issuer = "VeriSign" AND X509.dn = "Alice")

3. Subject Semantics in Policy Language

In general, we should at least provide a language primitive for logical expression as policy model defines. Examples are:

<formula>group="marketing"</formula>

and

<formula type="equal"><type>group</type><value>marketing</value></formula>

It would be better to provide a simpler way for specifying subject. Examples are:

<group>marketing</group>

and

<subject group="marketing"/>

XACML should be as flexible as it allows each application to define local schema for the simple way of specifying subject.

It may be the case that a PDP application is not focusing every attributes that are possibly used in authorization policies but much smaller set of attributes. For example, if the application uses group and

role attributes much often than X509.Issuer attribute, then it could be reasonable to specify subject as follows:

Ex1:

```
<subject>
    <group>marketing</group>
    <role>manager</role>
    <formula type="equal"><type>X509.Issuer</type><value>VeriSign</value></formula>
</subject>
```

It would be better to specify logical expression in more iutuitive way. The following example represents Ex2 in different way assuming that each element within a subject element is conjunctively connected and subject elements in parallel are disjunctively connected.

Ex2:

```
<subject>
    <group>development</group>
    <role>manager</role>
</subject>
<subject>
    <group>marketing</group>
</subject>
```

Finally, "*" could be mapped to the following since "*" implies there is no conditions for subject:

Ex3:

```
<subject>
  <all/>
</subject>
```

or

```
<subject/>
```

4. Subject Semantics in PDP Specification

In PDP specification, we should present how to retrieve subject related information (attributes etc.) and associate it to each language primitive. Some of the subject information can be obtained from an access request. Other subject-related information may not be. Following is the possibility:

1. Access request contains subject-related information in SAML assertion
2. Access request contains subject-related information outside the SAML assertion
3. PDP asks PIP for subject-related information (attribute authority, LDAP, etc.)

4. PDP locally maintains subject-related information

Figure 2 illustrates relationship among authorization components. The first two items are contained in the access request in Figure 2. The third item is contained in the subject-related information from PIP. The last item is not drawn in the figure.

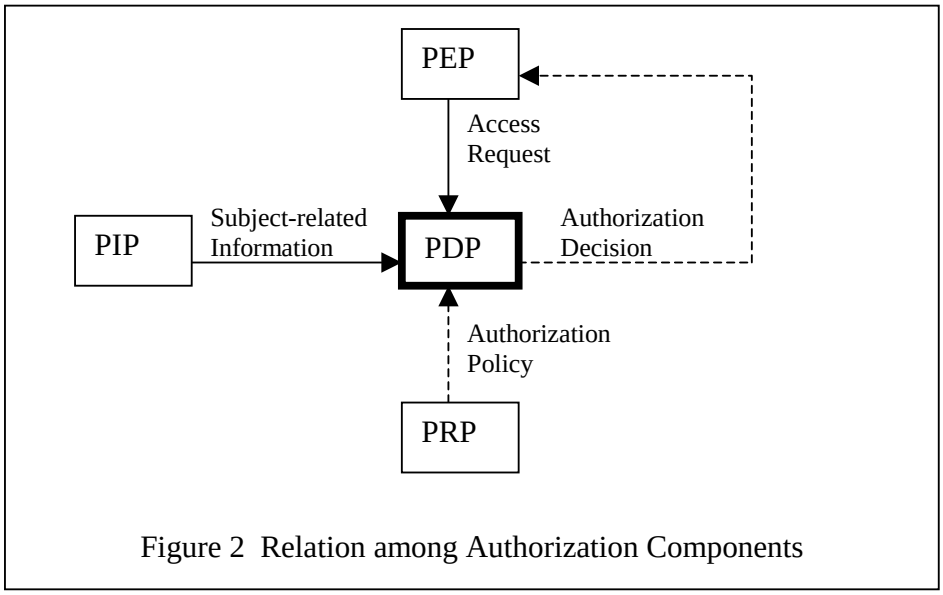

Figure 2 Relation among Authorization Components

References

[ISO] ISO/IEC 10181-3, Access Control Framework