Request for Change

eXtensible Access Control Markup Language (XACML)

Version 3.0 (Committee Draft 16 April 2009)

Contact

Dr. Michael Hoche <michael.hoche@eads.com>
EADS Deutschland GmbH
Defence and Communications Systems
Claude-Dornier-Straße
D-88090 Immenstaad (Germany)

Heiko Kirsch <kirschheiko@googlemail.com>
Student
University of Applied Sciences Brandenburg
Magdeburger Str. 50
D-14770 Brandenburg (Germany)

Abstract

This document describes how ontologies may be used for an authorization decision based on the eXtensible Access Control Markup Language (XACML). It is a Request for Change in addition to the XACML standard, version 3.0 (Committee draft 1 from 16th April 2009) and is submitted to the XACML Technical Committee which belongs to the Organization for the Advancement of Structured Information Standards (OASIS).

Using ontologies in XACML

Standards and methodologies in relation to the ***Semantic Web*** are very useful for authorization. According to the ***W3C*** specifiactions, ontologies are suitable for making knowledge understandable for machines. With the help of the ontologies it is possible to describe relationsships between attributes and/or attribute values. Dependencies are resolvable e.g.:

- A subject has a clearance with "*top_secret*".
- An object has a classification with "*restricted*".
- "*top_secret*" is *more_confidential_than* "*restricted*"

The orginal XACML functions and architecture specified by the OASIS standard are actually not able to resolve those questions in an easy and correct way.

We suggest to consider an ***Ontology Decision Point (ODP)*** in addition to the ***PDP*** within a prototypical implementation as shown in figure 1. This ODP should be able to resolve logical relationsships between attributes or attribute values. To describe these relations it is possible to use the ***Ressource Description Framework***, ***Ressource Description Framework Schema***, ***Web Ontolgy Language*** as shown in example 2.

To use the ODP in an autorization we suggest a special XACML function preferably based on a binary predicate called "**http://research.eads.com#string-onto-greater-or-equal**" as used in example 1. This function needs 5 arguments of datatype "**http://www.w3.org/2001/XMLSchema#string**" and delivers a result as "**http://www.w3.org/2001/XMLSchema#boolean**“. It generates a ***SPARQL-ASK-Query*** and requests the ***ODP***.

- argument 1: subject, object or environment attribute value or value definied in the policy (***SPARQL-subject***)
- argument 2: subject, object or environment attribute value or value definied in the policy (***SPARQL-object***)
- referenced ontology
- ontology namespace
- assumed relationship (***SPARQL-predicate***)

The function returns "***true***" if the assumed relation between argument 1 and argument 2 is resolvable in the referenced ontology. Otherwise it returns "***false***".

Extended data-flow model

The major actors in the XACML domain are shown in the collaboration diagram of Figure 1.

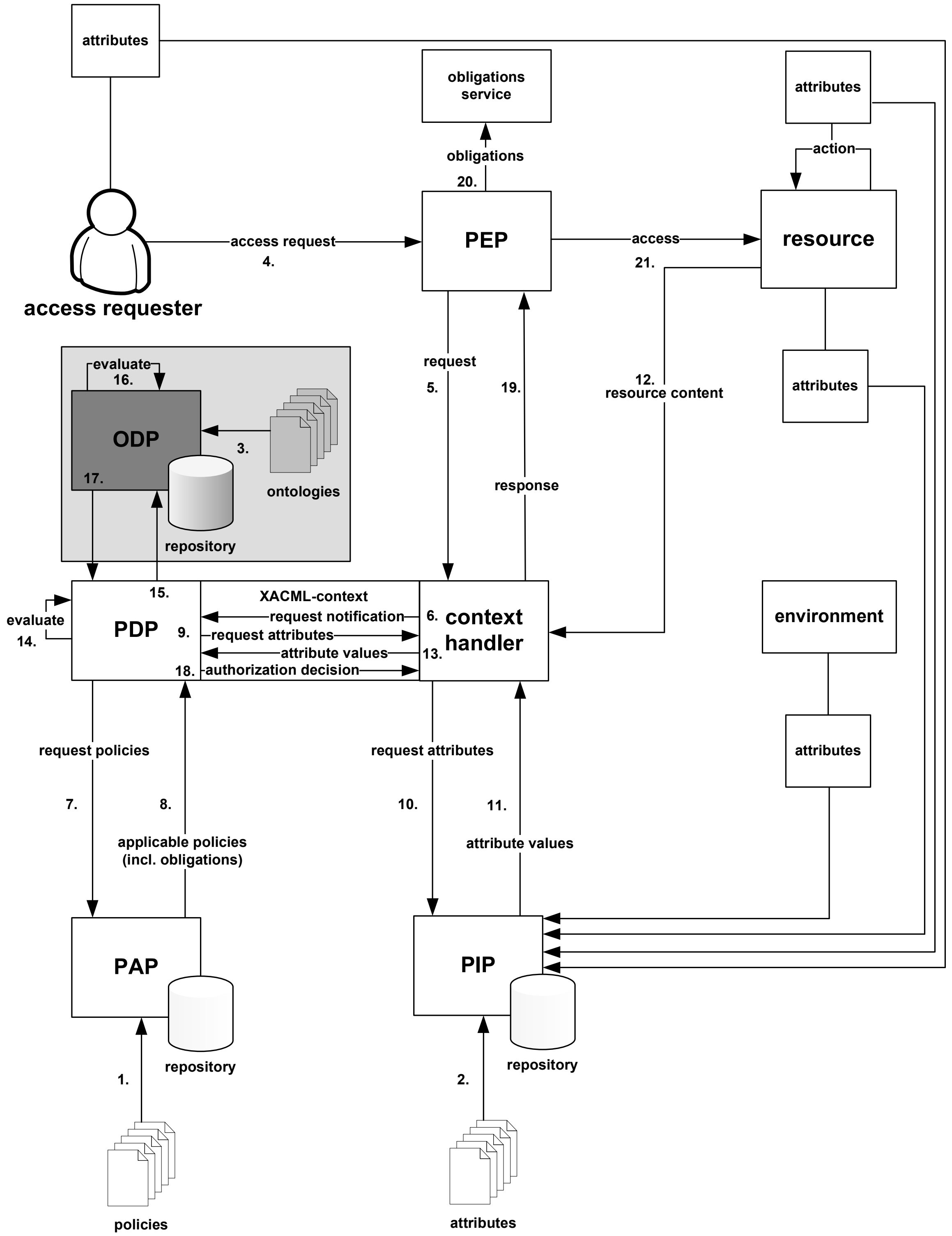

Figure 1 – Extended data-flow diagram

The model operates according to the following seeqence:

1. ***PAPs*** write ***policies*** and ***policy sets*** and make them available to the ***PDP***.
2. ***PIPs*** write ***attributes*** for the access requester, resource, action or environment and make them available to the ***context handler***.
3. ***ODPs*** write ***authorization ontologies*** for the internal reasoner and make the ODP-decision avaiable to the ***PDP***.
4. The ***access requester*** sends a request for ***access*** to the ***PEP***.
5. The ***PEP*** sends the request for ***access*** to the ***context handler*** in its native request format, optionally including ***attributes*** of the ***subjects***, ***resource***, ***action***, ***environment*** and other categories.
6. The ***context handler*** constructs an XACML request ***context*** and sends it to the ***PDP***.
7. The ***PDP*** requests ***applicable policies***.
8. The ***applicable policies*** were delivered by the ***PAP***.
9. The PDP requests any additional ***subject***, ***resource***, ***action***, ***environment*** and other categories (not shown) ***attributes*** from the ***context handler***.
10. The ***context handler*** requests the ***attributes*** from a ***PIP***.
11. The ***PIP*** obtains and returns the requested ***attributes*** to the ***context handler***.
12. Optionally, the ***context handler*** includes the ***resource*** in the ***context***.
13. The ***context handler*** sends the requested ***attributes*** and (optionally) the ***resource*** to the ***PDP***.
14. The ***PDP*** evaluates the ***policy***. If there are no ***ontology-functions*** referenced by the policy, go to step 18.
15. The ***PDP*** constructs a ***SPARQL-ASK-Query*** and sends it to the ***ODP***.
16. The ***ODP*** evaluates the the query by using a ***reasoner*** and the available ***ontologies***.
17. The ***ODP*** returns the result.
18. The ***PDP*** returns the response ***context*** (including the ***authorization decision***) to the ***context handler***.
19. The ***context handler*** translates the response ***context*** to the native response format of the ***PEP***. The ***context handler*** returns the response to the ***PEP***.
20. The ***PEP*** fulfills the ***obligations***.
21. If ***access*** is permitted, then the ***PEP*** permits ***access*** to the ***resource***; otherwise, it denies ***access***

Examples

Example 1 - XACML policy (more_confidential_policy)

```
<?xml version="1.0" encoding="UTF-8"?>

<Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        PolicyId="ontology"
        RuleCombiningAlgId=
        "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:ordered-permit-overrides">

  <Description>
     XACML-policy which uses the Ontology Decision Point
  </Description>

  <Target>

    <Subjects>
      <AnySubject/>
    </Subjects>

    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
             example.com/.*</AttributeValue>
          <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
       </ResourceMatch>
      </Resource>
    </Resources>

    <Actions>
      <AnyAction/>
    </Actions>

  </Target>

  <Rule RuleId="DefaultDeny" Effect="Deny">
  </Rule>

  <Rule RuleId="PermitCondtionsRead" Effect="Permit">

    <Target>

      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              users.example.com</AttributeValue>
            <SubjectAttributeDesignator DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"/>
          </SubjectMatch>
        </Subject>
      </Subjects>
```

```
   <Resources>
    <AnyResource/>
   </Resources>

   <Actions>
    <Action>
     <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
       read</AttributeValue>
      <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
       AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
     </ActionMatch>
    </Action>
   </Actions>

   <Environment/>

  </Target>

  <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

   <Apply FunctionId="http://research.eads.com#string-onto-greater-or-equal">

    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
     <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
       AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-clearance"/>
    </Apply>

    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
      <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
       AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-classification"/>
    </Apply>

     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
      secclass</AttributeValue>

     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
      http://www.w3.org/2001/XMLSchema#</AttributeValue>

     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
      more_confidential_than</AttributeValue>

   </Apply>

  </Condition>

 </Rule>

</Policy>
```

Example 2 - ontology (security_classification_level)

```
<?xml version="1.0"?>
<!DOCTYPE rdf:RDF [
   <!ENTITY owl "http://www.w3.org/2002/07/owl#" >
   <!ENTITY xsd "http://www.w3.org/2001/XMLSchema#" >
   <!ENTITY owl2xml "http://www.w3.org/2006/12/owl2-xml#" >
   <!ENTITY rdfs "http://www.w3.org/2000/01/rdf-schema#" >
   <!ENTITY rdf "http://www.w3.org/1999/02/22-rdf-syntax-ns#" >
]>

<rdf:RDF xmlns="http://www.w3.org/2001/XMLSchema#"
    xml:base="http://www.w3.org/2001/XMLSchema#"
    xmlns:owl2xml="http://www.w3.org/2006/12/owl2-xml#"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
    xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:owl="http://www.w3.org/2002/07/owl#">
    <owl:Ontology rdf:about="">
      <rdfs:comment>
        An OWL ontology of SecurityClassificationLevel (OWL-SecClass)
     </rdfs:comment>
   </owl:Ontology>

   <owl:ObjectProperty rdf:about="#more_confidential_than">
      <rdf:type rdf:resource="&owl;TransitiveProperty"/>
      <rdfs:domain rdf:resource="#SecurityClassificationLevel"/>
   </owl:ObjectProperty>

   <owl:Thing rdf:about="#unmarked">
      <rdf:type rdf:resource="#SecurityClassificationLevel"/>
   </owl:Thing>

   <owl:Thing rdf:about="#unclassified">
      <rdf:type rdf:resource="#SecurityClassificationLevel"/>
      <more_confidential_than rdf:resource="#unmarked"/>
   </owl:Thing>

   <owl:Thing rdf:about="#restricted">
      <rdf:type rdf:resource="#SecurityClassificationLevel"/>
      <more_confidential_than rdf:resource="#unclassified"/>
   </owl:Thing>

   <owl:Thing rdf:about="#confidential">
      <rdf:type rdf:resource="#SecurityClassificationLevel"/>
      <more_confidential_than rdf:resource="#restricted"/>
   </owl:Thing>

   <owl:Thing rdf:about="#secret">
      <rdf:type rdf:resource="#SecurityClassificationLevel"/>
      <more_confidential_than rdf:resource="#confidential"/>
   </owl:Thing>

   <owl:Thing rdf:about="#top_secret">
      <rdf:type rdf:resource="#SecurityClassificationLevel"/>
      <more_confidential_than rdf:resource="#secret"/>
   </owl:Thing>
</rdf:RDF>
```