TSCP

TRANSGLOBAL SECURE
COLLABORATION PROGRAM

Feedback on

XACML 3.0 Draft Public review 04

Document Version: 1.1

Date: 28 June, 2012

Prepared by:

Jean-Paul Buu-Sao, TSCP
Jean-Paul.Buu-Sao@tscp.org

Context

TSCP (www.tscp.org) is a cooperative forum in which leading Aerospace & Defense companies and key government agencies work together to establish and maintain an open standards-based framework that can be used to enable secure collaboration and assured information sharing between parties, irrespective of the tools they choose to use.

TSCP intends to use XACML as a standard representation for policies exchanged across organizations, as well as is considering XACML as a key enabler for authorization engines within organizations. The feedback, that this document formulates, addresses both use-cases, shortened as “interchange” and “execution”, use-cases.

Feedback

Support for an explicit policy-binding by reference

TSCP suggests adding to the standard the concept of policy-reference resource attribute. This clarifies the semantics of this attribute (interchange use-case) and can improve the performance of PDP’s (execution use-case)

XACML rules specify the conditions under which a given policy must apply, using the construct {`Target` / `AnyOf` / `AllOf` / `Match` / `AttributeDesignator`, `AttributeValue`}. The attributes, that are used for this determination, can be of any source (Subject, Resource, Environment, custom), of any type, in any number, and in any combination. This provides for a great flexibility, which indeed is all very positive. This model, that we name “policy-binding by inference”, can be contrasted with the model of “policy-binding by reference”, whereas the determination of the applicable policy is explicitly provided as a particular Resource attribute, which calls out the Policy Identifier. The resource contains the references of all the policies that must apply, making the policy selection process deterministic and unambiguous.

The primary use-case, that key organizations of the Aeronautical & Defense sector are considering, is the one of information labeling: security labels applied to documents explicitly contain the references of all the policies that must apply. This use-case can indeed be “simulated” under the current XACML 2.0 specification, by considering policy-binding reference as just another resource attribute.

However, implementations of XACML PDP’s that are aware that a particular resource-attribute designates a policy-reference can gain from some key system benefits:

- Integrity: a reference that corresponds to no known policy identifier reveals a loss of integrity;
- Flexibility: it is possible to update a policy without affecting all the resources under this policy;
- Performance: the policy references speed the process of policy selection;
- Predictability: there is no need to arbitrate between policy candidates, as all applicable policies are explicitly called out.

We suggest that XACML 3.0 incorporates the support for an explicit policy-binding by reference. This could, for example, be achieved by the addition of an `AttributeDesignator` category, such as: `urn:oasis:names:tc:xacml:3.0:resource-category:policyId`. In a “policy-binding by reference” model, the Target of a XACML policy would contain a match condition on a resource attribute, which category is policyId, and which constant value would be the identifier of the policy itself.

Support for parameterized policies

TSCP suggests adding the support for parameterized policies, which mostly benefits the “interchange” use-case, by allowing reuse and helping change-management.

XACML rules specify attributes, which need to be evaluated, as the tuple {AttributeDesignator, AttributeValue} whereas the AttributeDesignator indicates the source of the attribute, and the AttributeValue, its associated type and actual, constant, value. There are cases where it is desirable to resolve the value at the time of authorization, in a late-bound manner: in these cases, the rule specifies that the actual value of a given attribute needs to be resolved, given an attribute identifier, much in the same way attribute designators currently work.

To clarify the proposal, here is a slightly modified version of the Medi Corp example 1 (per 4.1.1 of the XACML 3.0 draft):

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
           xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17
           http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-schema-wd-17.xsd"
           PolicyId="urn:oasis:names:tc:xacml:3.0:example:SimplePolicy1"
           Version="1.0"
           RuleCombiningAlgId="identifier:rule-combining-algorithm:deny-overrides">
    <Description>
        Medi Corp access control policy
    </Description>
    <Target/>
    <Rule
      RuleId= "urn:oasis:names:tc:xacml:3.0:example:SimpleRule1"
  Effect="Permit">
        <Description>
            Any subject with an e-mail name in the {urn:example:com:permitted-domain}
            can perform any action on any resource.
        </Description>
        <Target>
            <AnyOf>
                <AllOf>
                    <Match
                      MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
                        <AttributeValue
                          ParameterId="urn:example:com:permitted-domain"
                          DataType=http://www.w3.org/2001/XMLSchema#string/>
                        <AttributeDesignator
                          MustBePresent="false"
                          Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                          DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
                    </Match>
                </AllOf>
            </AnyOf>
        </Target>
    </Rule>
</Policy>
```

The difference with the original example, found in XACML 3.0 draft, is the addition of the ParameterId attribute on the AttributeValue element. The presence of this attribute means that the actual value of the attribute must be retrieved at authorization time (given the parameter identifier). We suggest that this principle of parameterization be generalized, so than any `AttributeValue` that is member of a `string-bag` function, could be benefit from it; this would allow the parameterization of rules articulating sets.

Policies containing parameterized `AttributeValue` elements become in effect policy templates. Policy templates, that supply the rules, cannot be executed, and can only be referred to by other, non-parameterized policies, that supply the parameters of the template. TSCP would like to discuss further how this construct could be articulated, if this is of interest to the XACML TC.

We provide an example of use of this capability: organizations of the Aeronautical & Defense sector need to manage a large volume of export-control licenses. Taken the US as an illustration, the ITAR (International Traffic in Arms Regulations) mandates that organizations must export goods and services under licenses called Technical Assistance Agreements (TAA). Each TAA specifies the values of the parameters that are used in the ITAR access rules. The lack of support for parameterized rules implies that PAP and PDP must manage one policy-rule per TAA. The problem is that there are tens of thousands of TAA's for a given business context, and a vast majority of them only differ by only a few attribute constant values.

The support for parameterized rules, as proposed, would allow the PAP to administering a small number of ITAR policy templates, which only contain the rules. Additionally this allows organizations to cleanly track evolving regulations, without having to redistribute tens of thousands individual TAA access rules.

Examples

In order to illustrate the proposal we provide examples of simplified policies:

<u>Without parameterized policies:</u>

- Example 1: TAA-1.1
- Example 2: TAA-1.2

(Note how example 1 and example 2 are very similar)

<u>With parameterized policies:</u>

- Example 3: generic policy template for TAA
- Example 4: policy data for TAA-1.1
- Example 5: policy data for TAA-1.2

(Note that example 4 and example 5 only contain the differences between two TAA)

Example 1

The policy TAA-1.1 contains the following rule:

“Subjects from organization {Curtiss | Packard} who are {US | GB} nationals and who work on {DetailedDesign | Simulation} are permitted {any} access to resources under policy urn:curtiss:ba:taa:taa-1.1”

```
<Policy PolicyId="TAA-1.1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
  <Description>Policy for Business Authorization category TAA-1.1</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match
         MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
           DataType="http://www.w3.org/2001/XMLSchema#string">urn:curtiss:ba:taa:taa-1.1</AttributeValue>
          <AttributeDesignator
           MustBePresent="true"
           Category="urn:oasis:names:tc:xacml:1.0:resource:policy-id"
           AttributeId="urn:oasis:names:tc:xacml:1.0:resource:policy-id"
           DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit">
    <Description />
    <Target>
      <Actions>
        <Action>
          <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <ActionAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string" />
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Any</AttributeValue>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Curtiss</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Packard</AttributeValue>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/OrganizationID"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">US</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">GB</AttributeValue>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/Nationality"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
```

```
          <AttributeValue 
DataType="http://www.w3.org/2001/XMLSchema#string">DetailedDesign</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Simulation</AttributeValue>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/Work-Effort" 
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AndFunction" functionId="urn:oasis:names:tc:xacml:1.0:function:and" />
    </Condition>
  </Rule>
</Policy>
```

Example 2

The policy TAA-1.2 contains the following rule:

“Subjects from organization {Curtiss | Spad} who are {US | FR} nationals and who work on {Integration | Simulation} are permitted {any} access to resources under policy urn:curtiss:ba:taa:taa-1.2”

```
<Policy PolicyId="TAA-1.2" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
  <Description>Policy for Business Authorization category TAA-1.2</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match 
         MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue 
           DataType="http://www.w3.org/2001/XMLSchema#string">urn:curtiss:ba:taa:taa-1.2</AttributeValue>
          <AttributeDesignator 
           MustBePresent="true" 
           Category="urn:oasis:names:tc:xacml:1.0:resource:policy-id" 
           AttributeId="urn:oasis:names:tc:xacml:1.0:resource:policy-id" 
           DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit">
    <Description />
    <Target>
      <Actions>
        <Action>
          <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <ActionAttributeDesignator 
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" 
              DataType="http://www.w3.org/2001/XMLSchema#string" />
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Any</AttributeValue>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Curtiss</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Packard</AttributeValue>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/OrganizationID"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">US</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">GB</AttributeValue>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/Nationality"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Integration</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Simulation</AttributeValue>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/Work-Effort"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AndFunction" functionId="urn:oasis:names:tc:xacml:1.0:function:and" />
    </Condition>
  </Rule>
</Policy>
```

Example 3

The policy-template ITAR-TAA contains the following rule:

“Subjects from organization {param=organizations} who are {param=nationals} nationals and who work on {param=workEfforts} are permitted {any} access to resources"

```
<Policy PolicyId="urn:us:ddtc:itar:taa" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:deny-overrides">
  <Description>Policy for generic ITAR TAA</Description>
  <Target>
    <AnyOf>
      <AllOf>
        <Match
         MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
           ParameterId="PolicyId"
           DataType="http://www.w3.org/2001/XMLSchema#string"/>
          <AttributeDesignator
           MustBePresent="true"
           Category="urn:oasis:names:tc:xacml:1.0:resource:policy-id"
           AttributeId="urn:oasis:names:tc:xacml:1.0:resource:policy-id"
           DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit">
    <Description />
    <Target>
      <Actions>
        <Action>
          <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
            <ActionAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string" />
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Any</AttributeValue>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue ParameterId="organizations" DataType=http://www.w3.org/2001/XMLSchema#string/>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/OrganizationID"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue ParameterId="nationals" DataType=http://www.w3.org/2001/XMLSchema#string/>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/Nationality"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AtLeastMemberOf" functionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-
one-member-of">
        <Apply functionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue ParameterId="workEfforts" DataType=http://www.w3.org/2001/XMLSchema#string/>
        </Apply>
        <AttributeDesignator AttributeId="http://schemas.tscp.org/2012-03/claims/Work-Effort"
DataType="http://www.w3.org/2001/XMLSchema#string" />
      </Apply>
      <Apply xsi:type="AndFunction" functionId="urn:oasis:names:tc:xacml:1.0:function:and" />
    </Condition>
  </Rule>
</Policy>
```

Example 4

The policy TAA-1.1 provides the parameter data which, together with the referred policy-template, produces the rule:

“Subjects from organization {Curtiss | Packard} who are {US | GB} nationals and who work on {DetailedDesign | Simulation} are permitted {any} access to resources under policy urn:curtiss:ba:taa:taa-1.1”

```
<Policy PolicyId="urn:curtiss:ba:taa:taa-1.1" PolicyTemplateId=" urn:us:ddtc:itar:taa " >
  <Description>Policy instance TAA-1.1, that refers to ITAR-TAA policy-template</Description>
  <Parameters>
    <Parameter ParameterId="organizations">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Curtiss</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Packard</AttributeValue>
    </Parameter>
    <Parameter ParameterId="nationals">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">US</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">GB</AttributeValue>
    </Parameter>
    <Parameter ParameterId="workEfforts">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">DetailedDesign</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Simulation</AttributeValue>
    </Parameter>
  </Parameters>
</Policy>
```

Example 5

The policy TAA-1.2 provides the parameter data which, together with the referred policy-template, produces the rule:

“Subjects from organization {Curtiss | Spad} who are {US | FR} nationals and who work on {Integration | Simulation} are permitted {any} access to resources under policy urn:curtiss:ba:taa:taa-1.2”

```
<Policy PolicyId="urn:curtiss:ba:taa:taa-1.2" PolicyTemplateId=" urn:us:ddtc:itar:taa " >
  <Description>Policy instance TAA-1.2, that refers to ITAR-TAA policy-template</Description>
  <Parameters>
    <Parameter ParameterId="organizations">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Curtiss</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Spad</AttributeValue>
    </Parameter>
    <Parameter ParameterId="nationals">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">US</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">FR</AttributeValue>
    </Parameter>
    <Parameter ParameterId="workEfforts">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Integration</AttributeValue>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Simulation</AttributeValue>
    </Parameter>
  </Parameters>
</Policy>
```