# Distributed Trust Management: Assignment 2

| |
|---|
| Deadline: 8 January 2013 |
| How to submit the assignment:<br>– send a pdf file with the solution by email (n.zannone at tue dot nl) |
| For any question send me an email |

## Questions

1. Write a UCON policy supporting the following scenario.

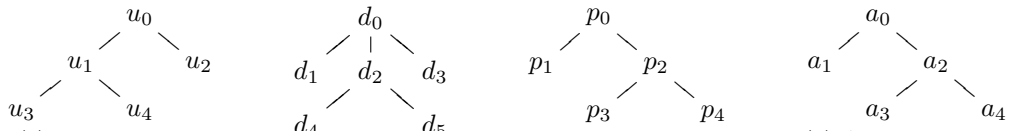
   A Dutch service provider offers pay-per-use services within the Netherlands. A user should be registered with the service provider in order to access a service. Registration is required when a user requests a service for the first time. Moreover, a user can access a service only if he has sufficient credit. The cost of the service is subtracted from the credit of the user after the usage of the service. There can be only 10 simultaneous usages of the same service.

2. Define the purpose hierarchy, role hierarchy, and access purpose authorizations in Purpose-based Access Control for the following scenario.

   Medical staff of a hospital can read patients' medical records for providing medical treatment. A doctor can treat a patient if he has worked at least three years in the hospital or he has at least five years of experience. However, only psychiatrists can read psychiatric notes in patients' medical records in order to make a psychiatric evaluation. Administrative staff can access patient information for billing purposes. In addition, receptionists (who are part of the administrative staff) can access patients' demographic information and doctors' schedule for managing appointments. Administrative staff can only access patients' information within the hospital network.

3. Let *pol* be an EPAL policy and the hierarchies in Figure 1 be user hierarchy, data hierarchy, purpose hierarchy and action hierarchy, with

$$pol = \begin{cases} \langle (u_2, d_2, p_1, a_1)(+, true, o_1) \rangle \\ \langle (u_0, d_1, p_2, a_2)(\circ, true, o_2) \rangle \\ \langle (u_2, d_0, p_4, a_3)(-, true, o_3) \rangle \\ \langle (u_1, d_0, p_3, a_3)(+, true, o_4) \rangle \end{cases}$$




(a) User Hierarchy (b) Data Hierarchy (c) Purpose Hierarchy (d) Action Hierarchy

Figure 1: Hierarchies

   Evaluate the following access requests against *pol*:

   $req_1 = (u_4, d_4, p_1, a_4)$
   $req_2 = (u_2, d_1, p_2, a_2)$
   $req_3 = (u_1, d_2, p_2, a_1)$
   $req_4 = (u_3, d_1, p_3, a_3)$

4. Given the XACML policy and access request below, determine the access response. Justify the answer. **Hint:** If an attribute from the request context does not match the target of the Rule/Policy/PolicySet, then the attribute is considered missing. If the attribute is missing, then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

   - If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")

- If MustBePresent is "True", then a missing attribute results in "Indeterminate".

Access Request

```
<Request>
  <Subject>
    <Attribute
        AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>
          Alice
      </AttributeValue>
    </Attribute>
    <Attribute
        AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>
          manager
      </AttributeValue>
    </Attribute>
    <Attribute
        AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>
          accountant
      </AttributeValue>
    </Attribute>
   </Subject>
   <Resource>
    <Attribute
        AttributeId="urn:oasis:names:tc:xacml:2.0:subject:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>
         financialrecord
      </AttributeValue>
    </Attribute>
  </Resource>
  <Action>
    <Attribute
       AttributeId="urn:oasis:names:tc:xacml:2.0:subject:action-id"
       DataType="http://www.w3.org/2001/XMLSchema#string">
     <AttributeValue>
         read
     </AttributeValue>
    </Attribute>
  </Action>
  <Environment/>
</Request>
```

```
<PolicySet PolicySetId="PS"
    xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides">
  <Target>
    <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
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true" />
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
  <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">financialrecord</AttributeValue>
            <ResourceAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
    <Rule Effect="Deny" RuleId="R1">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#time">08:00</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time"
                  MustBePresent="true" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
```

```
  </Rule>
  <Rule Effect="Deny" RuleId="R2">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
    </Target>
  </Rule>
  <Rule Effect="Permit" RuleId="R3">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
```

```
    <Target />
    <Rule Effect="Deny" RuleId="R4">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    </Rule>
    <Rule Effect="Permit" RuleId="R5">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">08:00</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```