Distributed Trust Management; Exam 19/4/2013

Questions

1. **(1.5 points)** Recall commands $CREATE$, $CONFER_{read}$, $CONFER_{*read}$ [1], $REVOKE_{read}$ [2], $TRANSFER_{read}$. Given initial state $Q = (S, O, A)$ with $S = \{s_1, s_2, s_3\}$, $O = \emptyset$ and $A = \emptyset$, and the sequence of commands α

   $CREATE(s_2, o)$
   $CREATE(s_1, s_4)$
   $CONFER_{*read}(s_1, s_4, o)$
   $TRANSFER_{read}(s_4, s_3, o)$
   $REVOKE_{read}(s_2, s_4, o)$
   $REVOKE_{read}(s_2, s_3, o)$
   $CONFER_{*read}(s_2, s_1, o)$
   $TRANSFER_{read}(s_1, s_4, o)$
   $TRANSFER_{read}(s_4, s_3, o)$
   $REVOKE_{read}(s_1, s_3, o)$

   Determine the state Q after the execution of α. Does α leak access privileges? (Consider only s_3 to be untrusted) Justify the answer.

2. **(1.5 points)** Mandatory Access Control

   (a) Explain the main differences between the Bell LaPadula (BLP) model and Biba model. Explain under which condition(s) the two models can be combined.

   (b) Consider two security levels, high (denoted by S_H) and low (S_L), and two integrity levels, high (I_H) and low (I_L). Fill in the table below with the permissions where the first colomn indicates the clearance of the subject and the first row indicates the classification of the object, using the combined BLP+Biba model. Use the following symbols: 'r for read, 'w for write, 'rw for read and write, '$-$ for no permission.

	S_L, I_L	S_L, I_H	S_H, I_L	S_H, I_H
S_L, I_L				
S_L, I_H				
S_H, I_L				
S_H, I_H				

3. **(2 points)** In the trust management language RT there are two locations where credentials may be stored: at the issuer and at the subject.

   (a) Would it be possible to store all credentials at the issuer? Motivate your answer.

   (b) Give a reason why it may be better to store some credentials at the subject and some other credential at the issuer.

   (c) What undesirable fact can happen if you are not careful in choosing the locations where credentials should be stored? Can you give an example of a (small) RT policy illustrating the problem?

4. **(1.5 points)** Write a UCON policy supporting the following scenario.

   A Dutch service provider offers pre-paid services within the Netherlands. The services are available only during working days. There can be only 20 simultaneous usages of the same service. In case there are more requests than the ones that the system can satisfy, the service execution invoked by the user with less credit is stopped.

[1] Equal to $CONFER_{read}$ but grants $*read$.
[2] Using this command $*read$ is also revoked.

5. **(1.5 points)** Explain the difference between data-centric protection (at the application level) and link-centric protection (at the transport level). Which technology is a better choice to provide end-to-end data confidentiality in a distributed system with many intermediaries that should be used to re-route but not 'see' the data in the clear. What are the existing technologies/standards that can be used to provide data-centric protection?

6. **(2 points)** Given the XACML policy and access request below, determine the access response. Do the same exercise, in the case the policy combining algorithm of policy set PS is *permit-overrides*.
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#string">
        <AttributeValue>
            John
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
          DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>
            nurse
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
          DataType="http://www.w3.org/2001/XMLSchema#time">
        <AttributeValue>
            10:00
        </AttributeValue>
      </Attribute>
     </Subject>
     <Resource>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:resource:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
           medRecord
        </AttributeValue>
      </Attribute>
    </Resource>
    <Action>
      <Attribute
         AttributeId="urn:oasis:names:tc:xacml:2.0:action:action-id"
         DataType="http://www.w3.org/2001/XMLSchema#string">
       <AttributeValue>
           read
       </AttributeValue>
      </Attribute>
    </Action>
    <Environment/>
  </Request>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides"
    PolicySetId="PS">
  <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" />
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
  <Policy PolicyId="P1"
          RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
    <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" />
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
    <Rule Effect="Permit" 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">Hard token</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-method"
                  DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true" />
            </SubjectMatch>
          </Subject>
        </Subjects>
        <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" />
          </ActionMatch>
        </Action>
      </Actions>
    </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">nurse</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#anyURI">medRecord</AttributeValue>
            <ResourceAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
                DataType="http://www.w3.org/2001/XMLSchema#anyURI" />
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="O1" />
    <Obligation FulfillOn="Deny" ObligationId="O2" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
        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:anyURI-equal">
          <AttributeValue
             DataType="http://www.w3.org/2001/XMLSchema#anyURI">medRecord</AttributeValue>
          <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
             DataType="http://www.w3.org/2001/XMLSchema#anyURI" />
        </ResourceMatch>
      </Resource>
    </Resources>
  </Target>
  <Rule Effect="Deny" 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">nurse</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-less-than">
          <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#time">14:00</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>
    <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" />
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
</Rule>
<Rule Effect="Permit" 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">nurse</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">14:00</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="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">nurse</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">Hard token</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-method"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="O3" />
      <Obligation FulfillOn="Deny" ObligationId="O4" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="O5" />
    <Obligation FulfillOn="Deny" ObligationId="O6" />
  </Obligations>
</PolicySet>
```