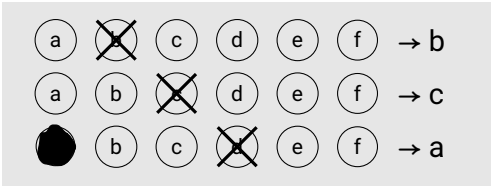
Exercises

1	2	3	4	5	6	7

1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6
7	7	7	7	7	7	7
8	8	8	8	8	8	8
9	9	9	9	9	9	9
0	0	0	0	0	0	0

Surname, First name

2IMS25 Principles of data protection
Final exam



Fill in your answer(s) to the multiple-choice questions as shown above (circles = one correct answer).

Particular Ans on paper exam instructions

- Write in a black or blue pen.
- You answer open-ended questions by using the text box. Provide your answers on the papers inside the answer box underneath a question. **If you need more space for your answers, use the extra space at the end of the exam, and clearly indicate there which question you continue answering. In the text box of the particular question, clearly state that you proceed with your answer on a different page.**
- Hand in all pages. Do not remove the staple. If you remove it anyhow, check that you hand in all pages.

Dear student,

You're about to take an exam. Write down your name and your student ID at the appropriate places above. Make sure that you enter your student ID by fully coloring the appropriate boxes. On the examination attendance card, you fill in the PDF number. You can find the correct number on the top of the first page of your exam (e.g. 1234.pdf).

Please read the following information carefully:

Date exam: 8/11/2023
Start time 09.00
End time: 12.00 (+30 minutes for time extension students)

Number of questions: 6
Maximum number of points/distribution of points over questions: 10
Method of determining the final grade: Final exam
Answering style: formulation, order, foundation of arguments, multiple choice:

Permitted examination aids:
None

Important:

- You are only permitted to visit the toilets under supervision
- Examination scripts (fully completed examination paper, stating name, student number, etc.) must always be handed in
- The house rules must be observed during the examination
- The instructions of subject experts and invigilators must be followed
- Keep your work place as clean as possible: put pencil case and breadbox away, limit snacks and drinks
- You are not permitted to share examination aids or lend them to each other
- Do not communicate with any other person by any means

During written examinations, the following actions will in any case be deemed to constitute fraud or attempted fraud:

- using another person's proof of identity/campus card (student identity card)
- having a mobile telephone or any other type of media-carrying device on your desk or in your clothes
- using, or attempting to use, unauthorized resources and aids, such as the internet, a mobile telephone, smartwatch, smart glasses etc.
- having any paper at hand other than that provided by TU/e, unless stated otherwise
- copying (in any form)
- visiting the toilet (or going outside) without permission or supervision

First-year bachelor students: The final grade for this exam will be announced no later than fifteen working days after the date of this exam, unless this exam takes place in Q4 or the interim period. For Q4 final exams, grades will be announced within five working days after the end of the Q4 final test period. For interim period final exams, grades will be announced no later than five working days before September 1.
All other students: Generally, the final grade for this exam will be announced no later than fifteen working days after the date of this examination. Specifically for bachelor exams administered in the interim period, exam grades will be announced no later than five working days before September 1.

You can start the exam now, good luck!

DAC

1.5p **1** Storing permissions in an access matrix is typically not a practical solution in real-world systems. Discuss what the underlying problems are and explain which approaches can be adopted to implement an access matrix in a practical way along with their advantages and disadvantages

MAC

Let *HIGH*, *MEDIUM*, and *LOW* be integrity levels (ordered from the highest to the lowest), and *Navy* and *Army* two categories. Consider the following subjects and objects along with their integrity class:

Subject	**Integrity**
Colonel	$(HIGH, \{Navy\})$
Major	$(MEDIUM, \{Navy\})$
Captain	$(MEDIUM, \{Army, Navy\})$
Soldier	$(LOW, \{Army\})$

Object	**Integrity**
Army position	$(HIGH, \{Army\})$
Fleet position	$(HIGH, \{Navy\})$
Number of army units	$(MEDIUM, \{Army\})$
Number of navy units	$(MEDIUM, \{Navy\})$
Cost of army units	$(LOW, \{Army\})$
Cost of navy units	$(LOW, \{Navy\})$

0.3p **2a** Draw the lattice of classifications.

1.2p **2b** Answer the following questions based on the Biba model with low-watermark for subjects:

1. Can the colonel read the number of army units?
2. Can the colonel change the fleet position after he reads the number of army units?
3. Can the major change the number of navy units after the colonel changes it?
4. Can the captain read the fleet position after he reads the cost of army units?
5. Can the captain change the number of army units after he reads the number of navy units?
6. Can the soldier read the fleet position after he changes the cost of army units?

Justify your answer and provide the new integrity classes of the subject(s) and object(s) if they change.

Hint:

- Changing an object requires 'write' rights over the object.

UCON

1.5p **3** Represent $RBAC_1$ in UCON.

RT

1p **4a** Consider the following RT_0 policy.

$A.t \longleftarrow A.t.s$
$A.t \longleftarrow K.t$

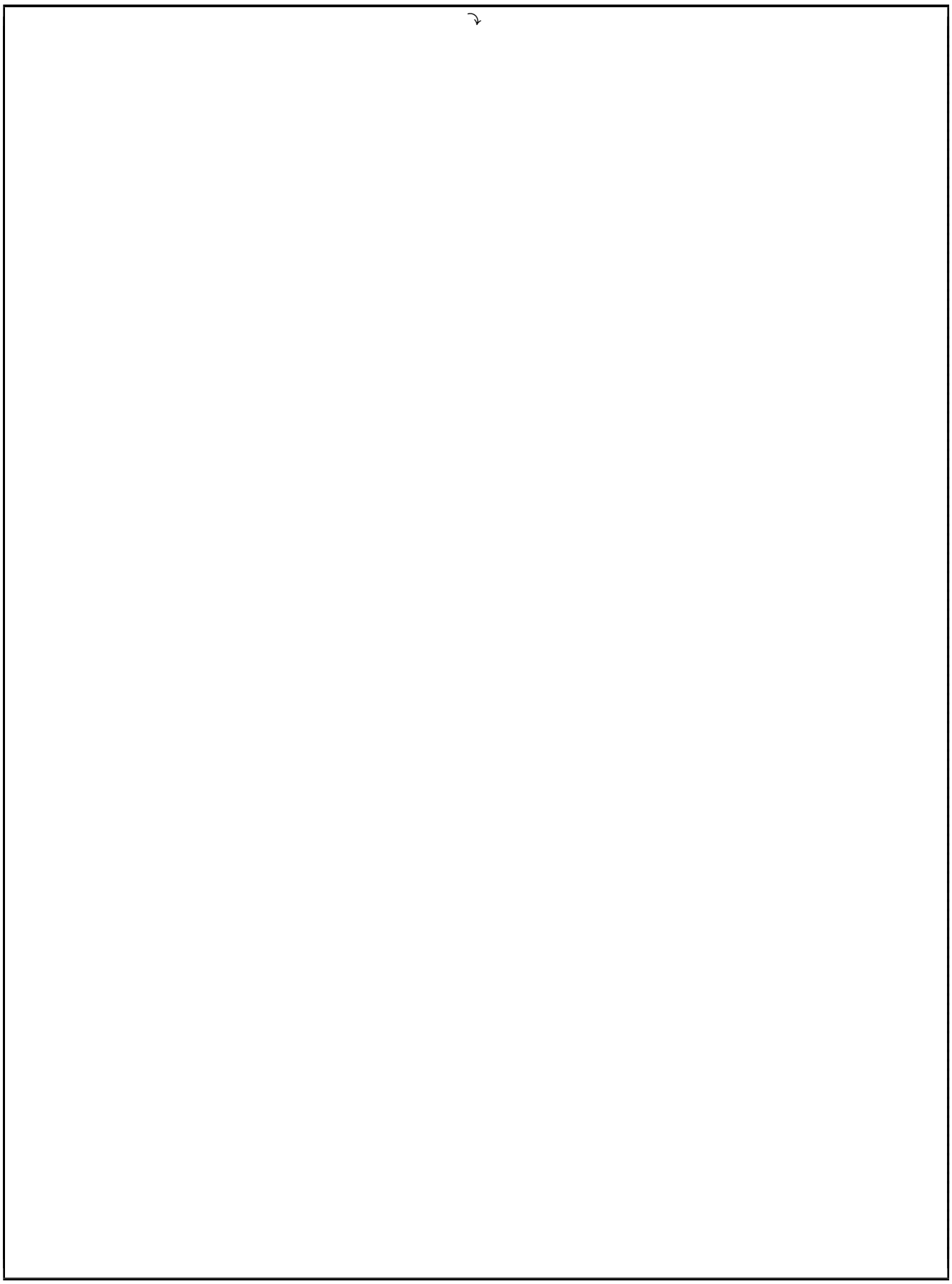
$K.t \longleftarrow K.t.s$
$K.t \longleftarrow D$
$K.t \longleftarrow E$

$L.t \longleftarrow D$
$L.s \longleftarrow E$

$D.s \longleftarrow L$
$D.s \longleftarrow M$
$D.s \longleftarrow H$

$H.t \longleftarrow W$
$H.s \longleftarrow Z$
$Z.s \longleftarrow W$

1. Find all principals populating $A.t$ (which means, compute $[[A.t]]$).
2. Write down the graph generated by the top-down algorithm when computing the semantics of $A.t$. (the top-down algorithm is also known as the "backward algorithm").

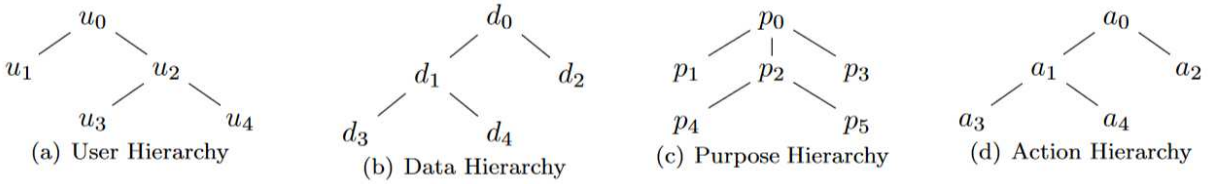


1p **4b** Consider the linked role $A.t \longleftarrow A.t.s$. Explain its semantics both in words and with a formula.

EPAL

Let *pol* be an EPAL policy defined over the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy in the figure below.

$$pol = \begin{cases} \langle (u_0, d_1, p_0, a_2)(\circ, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_2\}) \rangle \\ \langle (u_2, d_2, p_2, a_0)(\circ, true, \{o_3\}) \rangle \\ \langle (u_3, d_1, p_4, a_3)(-, true, \{o_4\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_6\} \end{cases}$$



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

1.5p **5** Evaluate the following access requests against *pol*:

$req_1 = (u_0, d_4, p_4, a_2)$
$req_2 = (u_2, d_4, p_2, a_5)$
$req_3 = (u_4, d_3, p_5, a_2)$
$req_4 = (u_4, d_2, p_4, a_3)$

XACML

2p **6** Given the XACML policy and access request below, determine the access response. Provide the policy graph illustrating the evaluation.

Hint: If an attribute is missing (i.e., it is not provided in the request), 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 an error. Recall that rule evaluation and some combining algorithms are defined over the extended Indeterminate set ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). Decisions in the extended Indeterminate set indicate the potential decision(s) (Permit or Deny) that would have returned if an error had not occurred in the evaluation.

Extra space

7

Access Request

```
  <Request>
    <Attributes
         Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Charlie
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                radiologist
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                PatientRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                read
            </AttributeValue>
         </Attribute>
    </Attributes>
  </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:3.0:policy-combining-algorithm:deny-overrides">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               PatientRecord
           </AttributeValue>
           <AttributeDesignator
               MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
               AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:first-applicable">
    <Target />
    <Rule Effect="Deny" RuleId="R1">
      <Target>
        <AnyOf>
          <AllOf>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   radiologist
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   write
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
          <AllOf>
            <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   cardiologist
```

```
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 14:00
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                 DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
</Rule>
<Rule Effect="Permit" RuleId="R2">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               cardiologist
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Match>
        <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
               14:00
           </AttributeValue>
           <AttributeDesignator MustBePresent="true"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
               DataType="http://www.w3.org/2001/XMLSchema#time"/>
        </Match>
      </AllOf>
      <AllOf>
        <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               radiologist
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
```

```
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 14:00
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                 DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Rule Effect="Deny" RuleId="R3">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 radiologist
             </AttributeValue>
             <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-overrides">
  <Target />
  <Rule Effect="Permit" RuleId="R4">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 radiologist
             </AttributeValue>
             <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
```

```
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 read
             </AttributeValue>
             <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:action"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Rule Effect="Permit" RuleId="R5">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                radiologist
             </AttributeValue>
             <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 14:00
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                 DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </Match>
        </AllOf>
      </AnyOf>
    </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>
```