TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Surname and initials:

Student number:

Examination cover sheet

(to be completed by the examiner)

Course name:Principles of data protection Course code:2IMS25

Date:30/10/2020

Start time:13:30 End time:16:30

Number of pages: 8 (Part A) + 6 (Part B) + 1 (Attachment 1) + 4 (Attachment 2)

Number of questions:6

Maximum number of points/distribution of points over questions:10

Method of determining final grade:Final exam

Answering style: formulation, order, argumentation, multiple choice:open questions

Exam inspection:

Other remarks:

INSTRUCTIONS FOR STUDENTS AND INVIGILATORS (to be indicated by examinor)

Write in black or blue. Pencil only allowed for drawings.

Permitted examination aids (to be supplied by students):

☐ Computer

☐ Calculator Graphic

☐ Calculator

☐ Lecture notes/book

☐ One A4 sheet of annotations

☐ Dictionaries. If yes, please specify:

Important:

- an exam >90 minutes consists of a Part A and a Part B. Part A needs to be collected after 90 minutes, before handing out part B. Ensure students are aware of this
- students that started on part B of the exam, are only allowed to hand it in and leave the room after the simultaneously conducted online exam part B has started. This is 11.05 (morning), 15.35 (afternoon)
- examinees are only permitted to visit the toilets under supervision
- it is not permitted to leave the examination room within 15 minutes of the start and within the final 15 minutes of the examination, unless stated otherwise
- 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
- examinees are not permitted to share examination aids or lend them to each other

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

The final grade will be announced no later than fifteen working days after this examination took place. Final grades of first-year bachelor study components in Q4 will be announced within 5 working days. Final test grades of bachelor study components in the interim period will be announced no later than 5 working days before the 1st of September.

Exercises

1	2	3

Surname, First name

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

Principles of data protection (2IMS25)
Exam 30/10/2020 (OnCampus - Part B)
30 October 2020 15:00 - 16:30

Chinese Wall

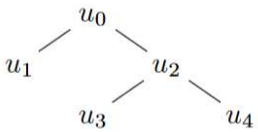
1.5p **1**

1. Explain the goal of the Chinese Wall model and describe the main concepts and properties of the model.
2. Explain the main differences between the Chinese Wall model and the Bell-LaPadula model.

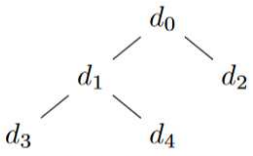
EPAL

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

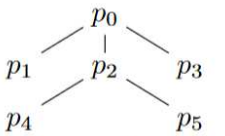
$$pol = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_2\}) \rangle \\ \langle (u_2, d_2, p_2, a_0)(\circ, true, \{o_3\}) \rangle \\ \langle (u_3, d_1, p_4, a_3)(-, true, \{o_4\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\})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



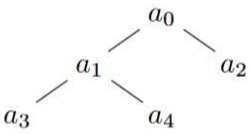
(a) User Hierarchy



(b) Data Hierarchy



(c) Purpose Hierarchy



(d) Action Hierarchy

1.5p **2** Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_2, p_1, a_3)$
$req_2 = (u_2, d_4, p_2, a_0)$
$req_3 = (u_0, d_5, p_1, a_2)$
$req_4 = (u_2, d_2, p_4, a_3)$

XACML

2p **3** Given the XACML policy and access request below, determine the access response.

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 have not occurred in the evaluation.

This page is left blank intentionally

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">
                Bob
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                nurse
            </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:permit-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>
      <AnyOf>
        <AllOf>
          <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                radiology
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:department"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </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">
                   nurse
               </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>
      </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">
                doctor
            </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="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
  <Target />
  <Rule Effect="Deny" RuleId="R3">
    <Target>
      <AnyOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

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