

Surname and initials: \_\_\_\_\_

Student number: \_\_\_\_\_

## Examination cover sheet

(to be completed by the examiner)

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

Date: 18/1/2021

Start time: 18:00 End time: 21.45

Number of pages: 7 (Part A) + 5 (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 examiner)

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 1<sup>st</sup> of September.

**Exercises**

1	2	3
---	---	---

**Surname, First name**

---

**Principles of data protection (2IMS25)**  
Exam 18/1/2021 (OnCampus - Part B)

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

## Purpose- based Access Control

- 1.5p 1 Explain the steps (along with their goals) of the access decision making process in Purpose-based Access Control.

## Decision reduction

- 1.5p 2 Consider an operator  $\alpha$  defined over the six-valued decision set  $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$  defined as follows:

$\alpha$	<b>P</b>	<b>D</b>	<b>NA</b>	<b>I(P)</b>	<b>I(D)</b>	<b>I(PD)</b>
<b>P</b>	P	P	P	P	P	P
<b>D</b>	D	D	D	D	D	D
<b>NA</b>	I(P)	I(D)	NA	I(P)	I(D)	I(PD)
<b>I(P)</b>	I(P)	I(P)	I(P)	I(P)	I(P)	I(P)
<b>I(D)</b>	I(D)	I(D)	I(D)	I(D)	I(D)	I(D)
<b>I(PD)</b>	I(PD)	I(PD)	I(PD)	I(PD)	I(PD)	I(PD)

Given the four-valued decision set  $\mathcal{D}_4 = \{P, D, NA, I\}$  and the two-valued decision set  $\mathcal{D}_2 = \{P, D\}$ , consider the decision reductions  $\rho_{64} : \mathcal{D}_6 \rightarrow \mathcal{D}_4$  and  $\rho_{42} : \mathcal{D}_4 \rightarrow \mathcal{D}_2$  defined as follows:

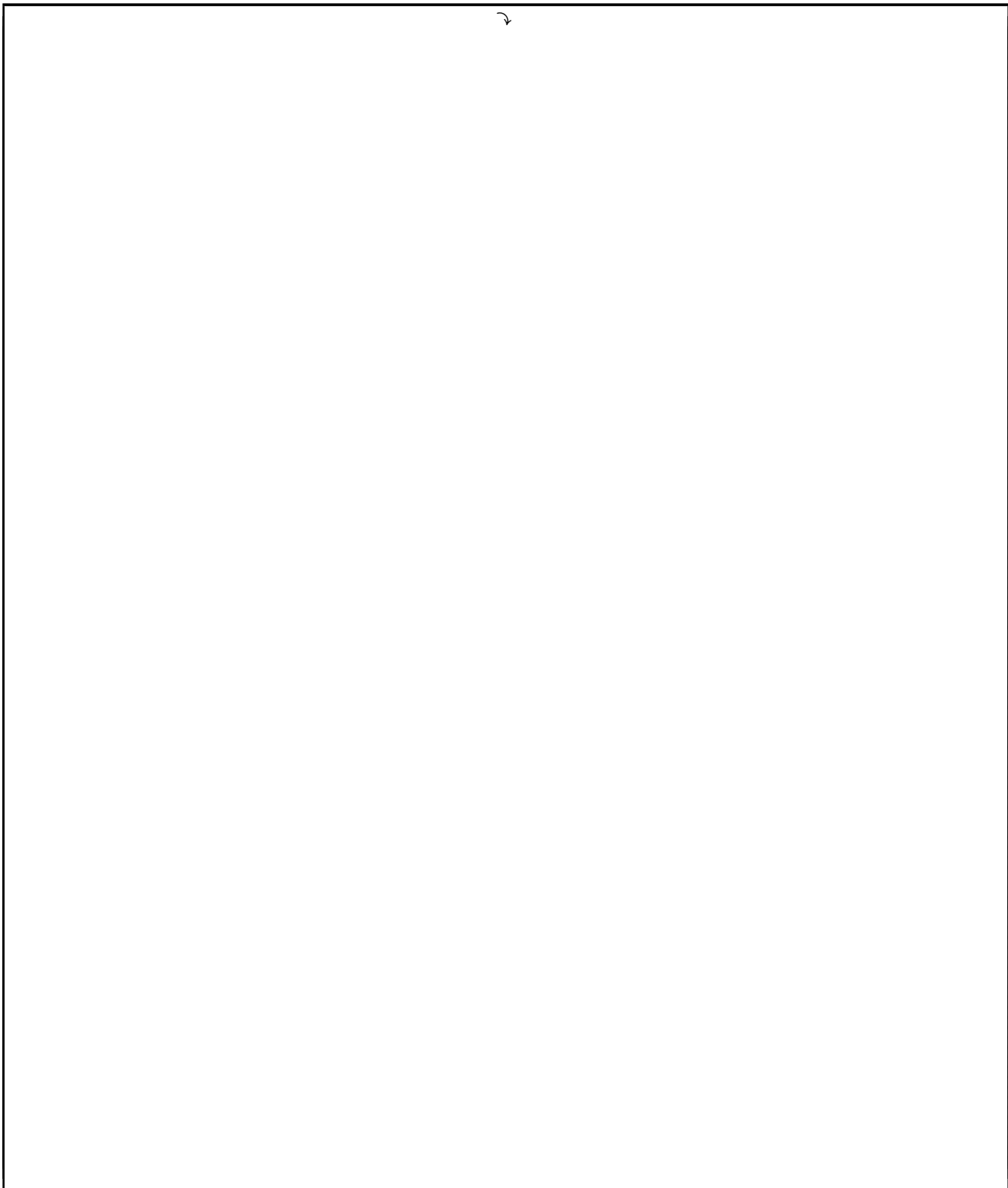
$$\rho_{64}(d) = \begin{array}{ll} P & \text{if } d = P \\ D & \text{if } d = D \\ NA & \text{if } d = NA \\ I & \text{if } d \in \{I(P), I(D), I(PD)\} \end{array}$$

$$\rho_{42}(d) = \begin{array}{ll} P & \text{if } d = P \\ D & \text{if } d \in \{D, NA, I\} \end{array}$$

</br>

1. Explain when a decision reduction is safe with respect to an operator.
2. Determine whether decision reductions  $\rho_{64}$  and  $\rho_{42}$  are safe with respect to  $\alpha$ . Justify the answer.
3. Explain whether it is possible to determine the safety of  $\rho_{62}$  (defined as the concatenation of  $\rho_{64}$  and  $\rho_{42}$ , i.e.  $\rho_{62} = \rho_{64} \circ \rho_{42}$ ) with respect to  $\alpha$  based on the one of  $\rho_{64}$  and  $\rho_{42}$ .





## 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.

1. If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicySet is "Not Applicable")
2. 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.

# Principles of Data Protection (2IMS25): Exam 18/1/2021

## 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>
```

# Principles of Data Protection (2IMS25): Exam 18/1/2021

```
<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">
            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>
    <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny">
      <Target />
      <Rule Effect="Permit" 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>
      </Policy>
    </PolicySet>
```



```

<Rule Effect="Deny" 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">
              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="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:time-greater-than">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                  15:00
                </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>
        <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"
                >
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
  </AnyOf>
</Rule>

```

```

        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:permit-overrides">
    <Target />
    <Rule Effect="Deny" 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="true"
            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>

```