MUNI
FI

lasaris LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

Forensic-Ready Risk Management for Software Systems

Lukas Daubner, Sofija Maksović
daubner@mail.muni.cz

Faculty of Informatics, Masaryk University, Brno

March 31, 2022

Why Forensic Readiness?

- Digital forensic investigation is:
  - Laborious
  - Costly
  - Time-consuming
  - Delicate
- Success is never assured
  - Data might be unavailable, corrupted, or tampered
  - Error in evidence handling jeopardies the process
- Data might me misleading

What is Forensic Readiness?

- Original definition
  - Maximizing the usefulness of incident evidence data
  - Minimizing the cost of forensics during an incident response
- Systematic preparation for forensic investigation
- Proactive measures
  - Opposed to actual investigation, which is reactive

What is Forensic Readiness?

- Approached as a set of general guidelines
  - Collection of evidence
  - Handling of evidence
  - Presentation of evidence
  - Staff training
  - Escalation policies

- Increases likelihood of successful investigation

Forensic Readiness in Software Engineering

- Prepare software system during its development
  - A.k.a. forensic-by-design
- Capable of:
  - Conducting digital forensic processes in a forensically sound way
  - **Producing forensically sound evidence**
- High-level non-functional requirement
- Measures for the failure of security measures

MUNI C4E

Forensic Readiness in Software Engineering

- It is true that software systems produce a lot of data
  - Logs
  - Documents
  - Database records
- But can we trust them?
- Are they complete?
- Will they help us during the investigation?

MUNI C4E

Forensic-Ready Software Systems -

Requirements

- What exactly should be implemented?
- We need some guideline to identify the requirements
- In other words, for what investigation should we prepare for?
- We can consider the reason for investigation as a risk

MUNI C4E

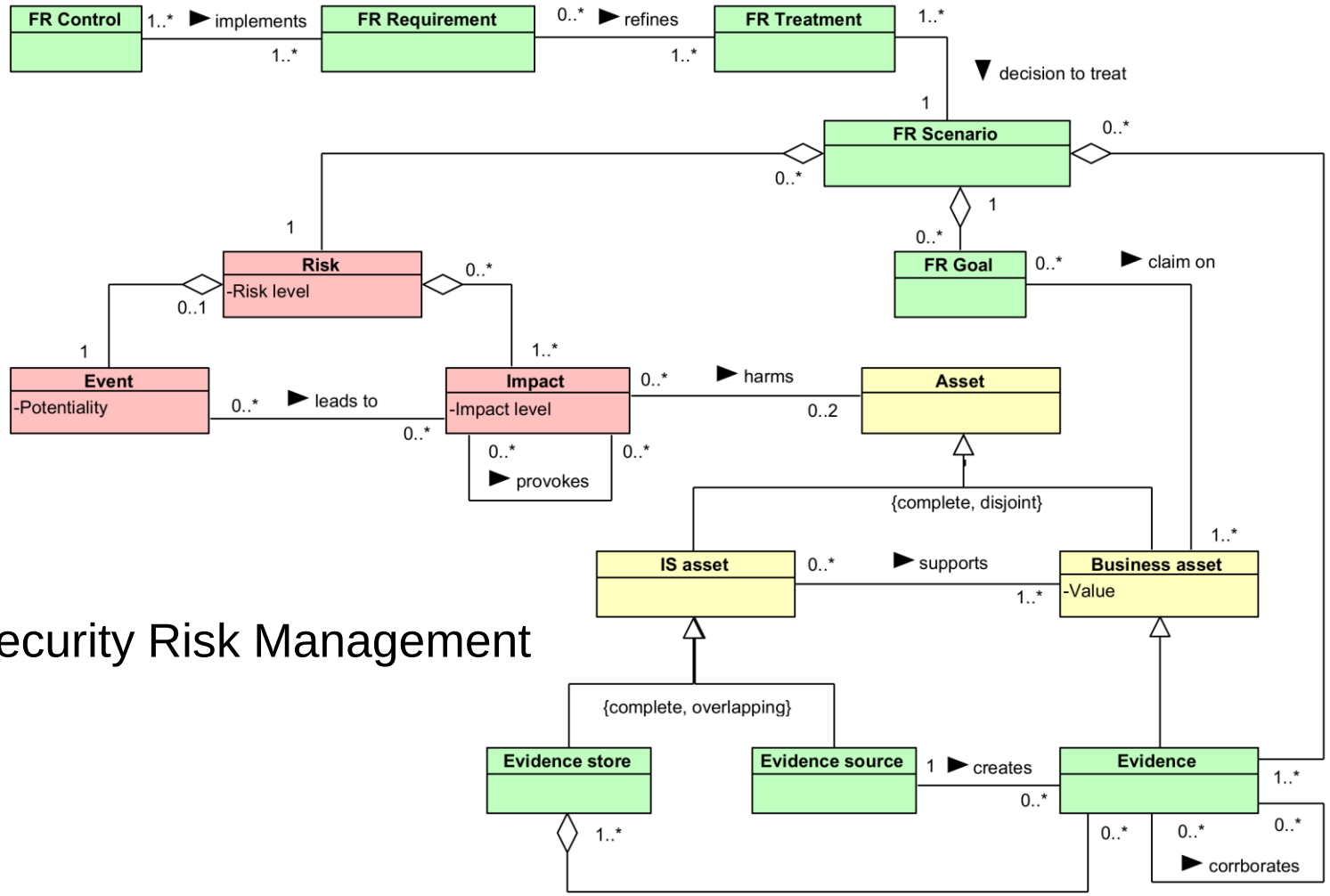
Forensic-Ready Risk Management

- Risk management has been discussed within forensic readiness
  - However, there is a very little methodological support
- The focus here is to conceptualize the process
  - What do we have (assets, evidence)
  - What do we need from forensic readiness (goals)
  - What are the threats to the system (risks)
  - What it fits together (scenarios)
  - What to do with it (decisions)
  - What to implement (requirements, controls)

MUNI C4E

Forensic-Ready Risk Management

Domain Model



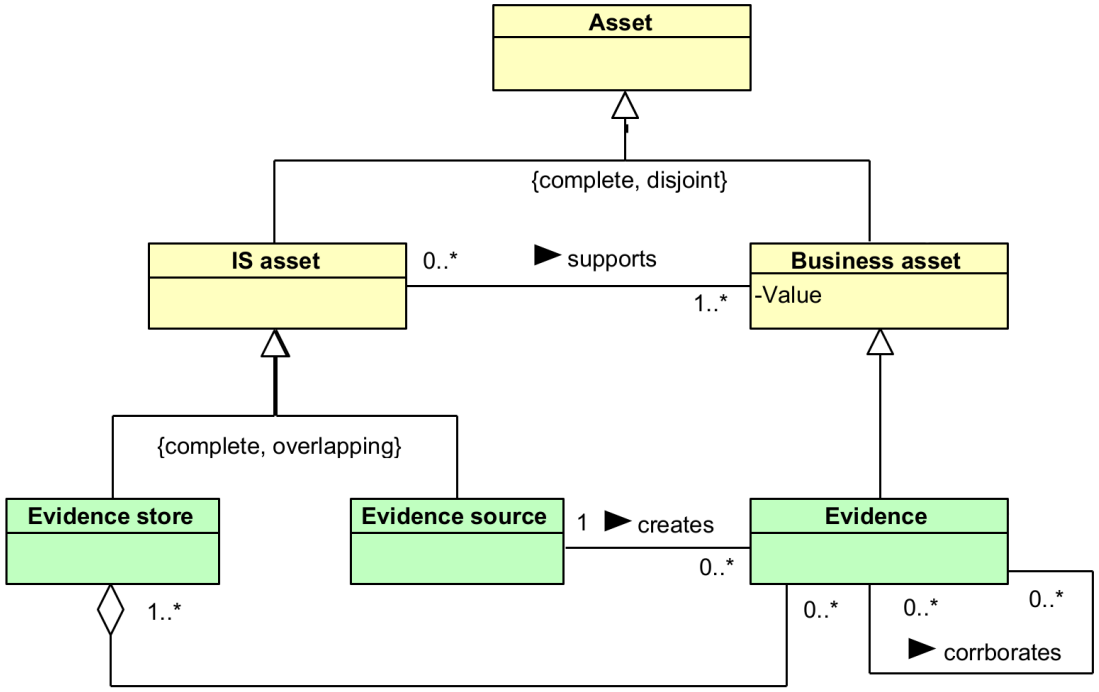
- Based on ISSRM
  - Information System Security Risk Management

MUNI C4E

Forensic-Ready Risk Management

Asset-Related Concepts

- Anything of value
  - Business asset
  - IS asset
- Potential Evidence
  - Data that have value to the organization
- Evidence Source
  - Where the evidence come from
- Evidence Store
  - Where can you find it, if you need it

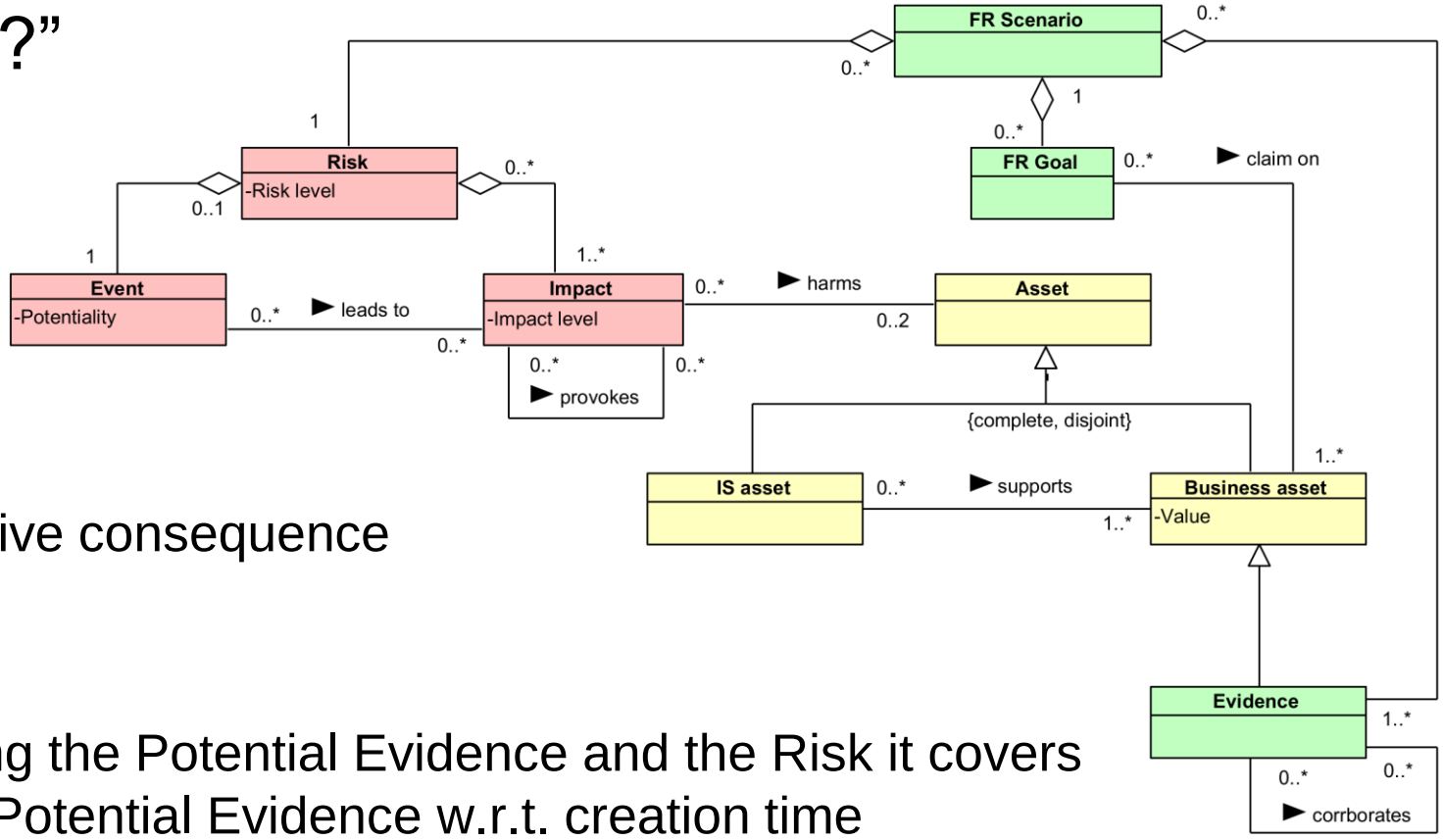


MUNI C4E

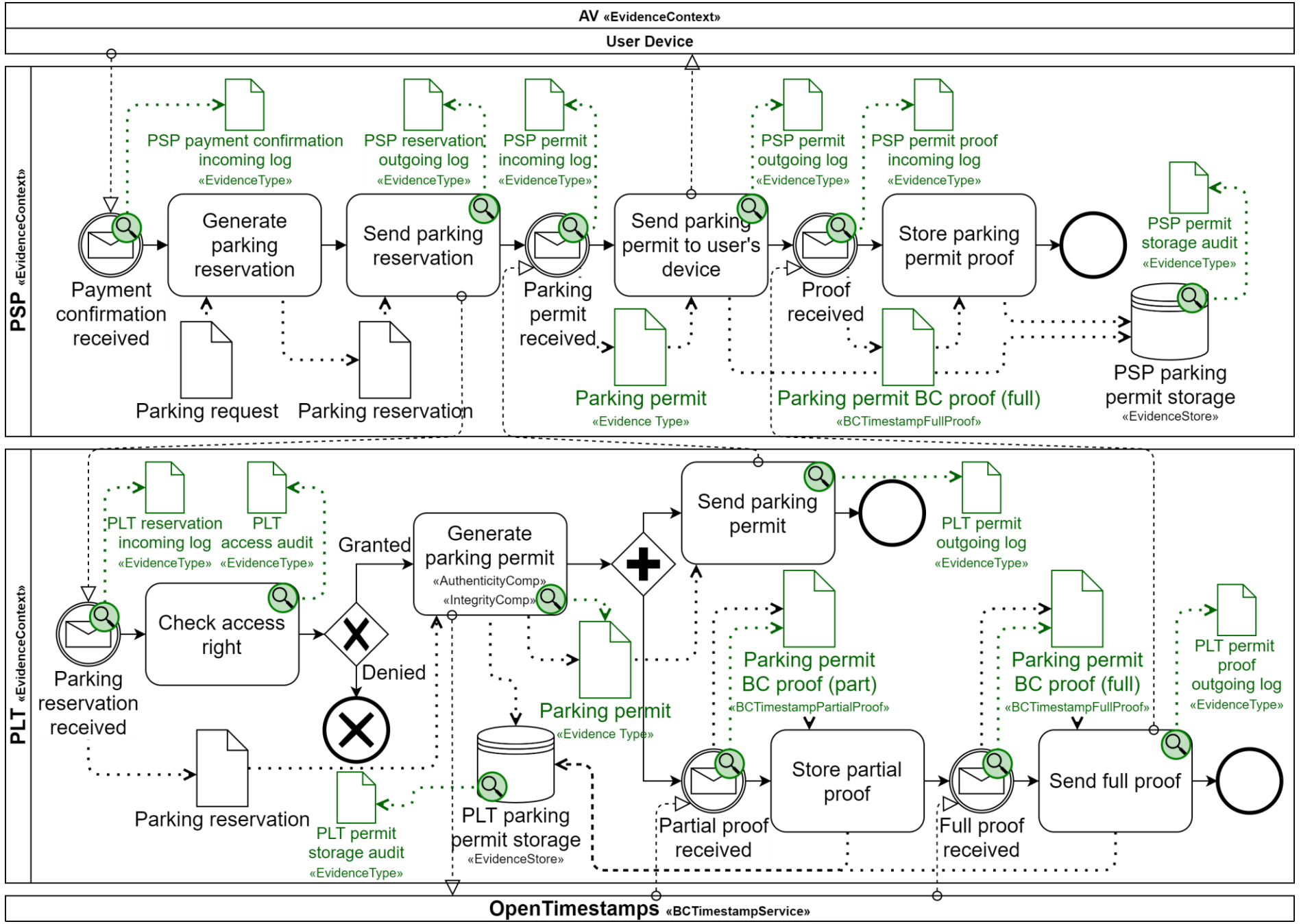
Forensic-Ready Risk Management

Risk-Related Concepts

- Goal – Answer to “Why?”
  - Prove an impact of a risk
  - Handling disputes
  - Demonstrate compliance
  - Support evidence release
- Risk
  - Undesired occurrence + negative consequence
- Scenario
  - How is a Goal addressed, using the Potential Evidence and the Risk it covers
  - It creates a partial ordering of Potential Evidence w.r.t. creation time



MUNI C4E

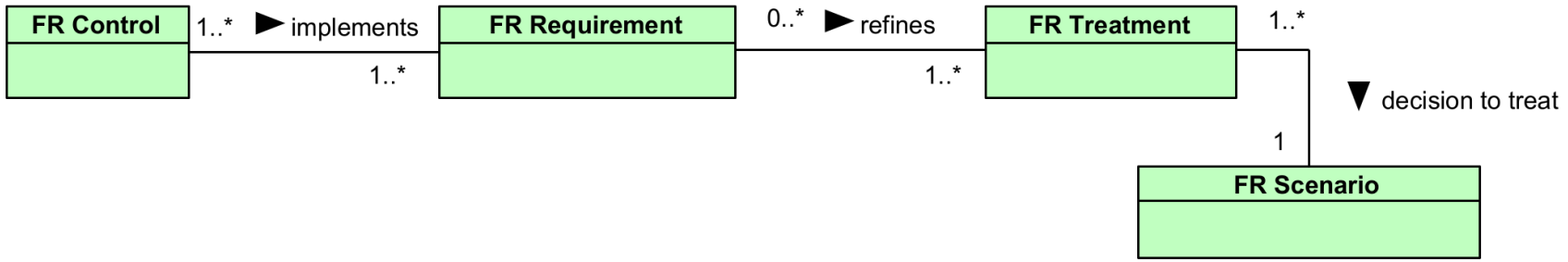

AV «EvidenceContext»
User Device
PSP «EvidenceContext»
PSP payment confirmation incoming log
«EvidenceType»
PSP reservation outgoing log
«EvidenceType»
PSP permit incoming log
«EvidenceType»
PSP permit outgoing log
«EvidenceType»
PSP permit proof incoming log
«EvidenceType»
Payment confirmation received
Generate parking reservation
Send parking reservation
Parking permit received
Send parking permit to user's device
Proof received
Store parking permit proof
PSP permit storage audit
«EvidenceType»
Parking request
Parking reservation
Parking permit
«Evidence Type»
Parking permit BC proof (full)
«BCTimestampFullProof»
PSP parking permit storage
«EvidenceStore»
PLT «EvidenceContext»
PLT reservation incoming log
«EvidenceType»
PLT access audit
«EvidenceType»
Granted
Generate parking permit
«AuthenticityComp»
«IntegrityComp»
Send parking permit
PLT permit outgoing log
«EvidenceType»
Parking reservation received
Check access right
Denied
Parking permit
«Evidence Type»
Parking permit BC proof (part)
«BCTimestampPartialProof»
Parking permit BC proof (full)
«BCTimestampFullProof»
PLT permit proof outgoing log
«EvidenceType»
Parking reservation
PLT permit storage audit
«EvidenceType»
PLT parking permit storage
«EvidenceStore»
Partial proof received
Store partial proof
Full proof received
Send full proof
OpenTimestamps «BCTimestampService»

MUNI C4E

Forensic-Ready Risk Management

Treatment-Related Concepts

- Treatment – “What to do next”
  - Scenario Avoidance
  - Scenario Enhancement
  - Scenario Retention
  - Scenario Transfer



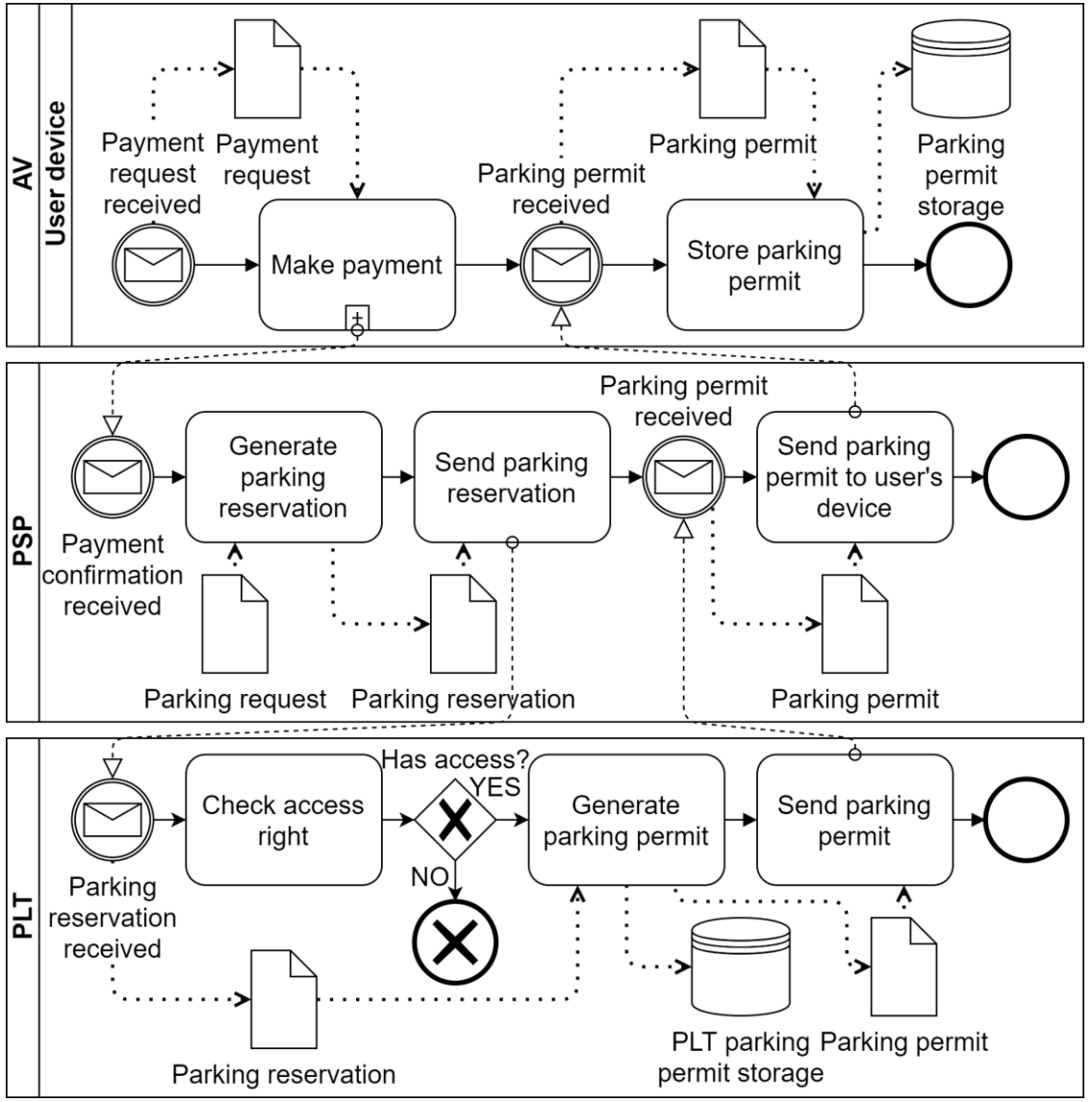
- Requirement
  - Condition to be satisfied

- Control
  - Add or modify Potential Evidence/Store/Source
  - Documentation
  - Establish or modify Policy/Practice

MUNI C4E

Hands-On Demo

- Try how the concepts fits together
- Identify and evaluate the scenarios
  - Fill in the available potential evidence
  - Think about completeness of the scenario
- Evaluate the potential evidence
  - Is it trustable?
  - Is there enough?



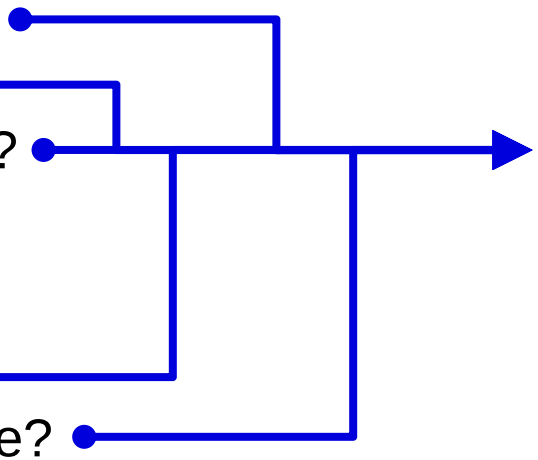
MUNI C4E

Analysis of Forensic Readiness Scenarios

- The problem is how to evaluate and prioritize what is needed.
- Scenario coverage
  - Do we have enough potential evidence?
  - Are there any blind spots?
  - Where are the evidentiary/risk hot-spots?
- Potential evidence quality
  - Is the evidence non-disputable?
  - What is the chances of having it available?
- Validity of the model

Analysis of Forensic Readiness Scenarios

- The problem is how to evaluate and prioritize what is needed.
- Scenario coverage
  - Do we have enough potential evidence?
  - Are there any blind spots?
  - Where are the evidentiary/risk hot-spots?
- Potential evidence quality
  - Is the evidence non-disputable?
  - What is the chances of having it available?
- Validity of the model



Metrics

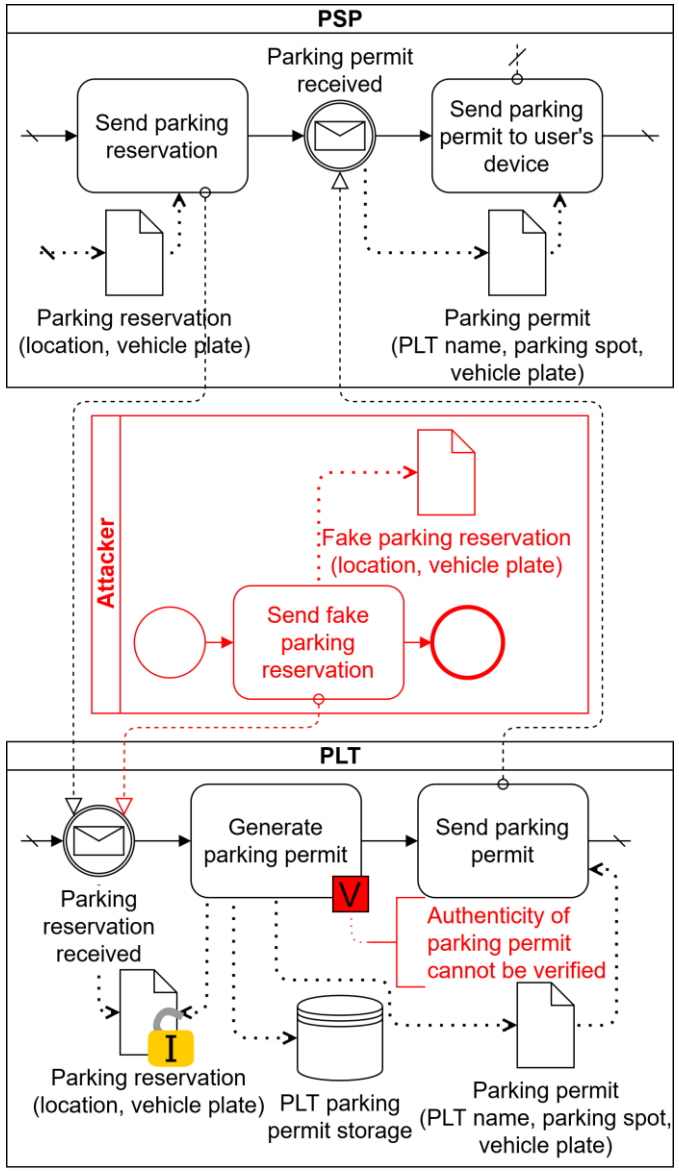
…which are not yet defined…

MUNI C4E

Analysis of Forensic Readiness Scenarios

Risk Coverage Analysis

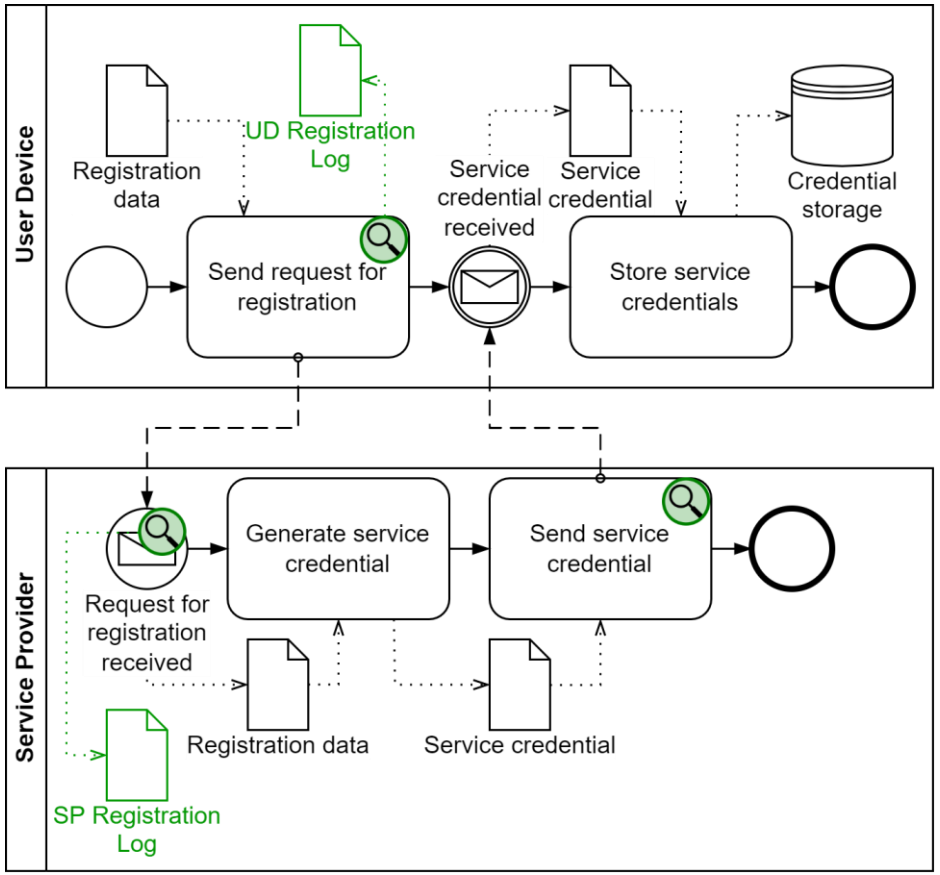
- How to be sure that we have overed everything?
  - Can we distinguish between the nominal and abnormal?
- Utilization of models
  - Forensic readiness (BPMN4FRSS)
  - Risks (Risk-Oriented BPMN)
- Simulations of the modelled scenario
  - Find the probability of potential evidence occurrence
  - Find the hot spots/indicators



Analysis of Forensic Readiness Scenarios

Validity and Hints Analysis

- Analysis of BPMN4FRSS models
- Check the model validity
- Provide hints to enhance the model
  - Cover the blind spots
  - Add evidence on strategic spots
  - Improve non-disputability

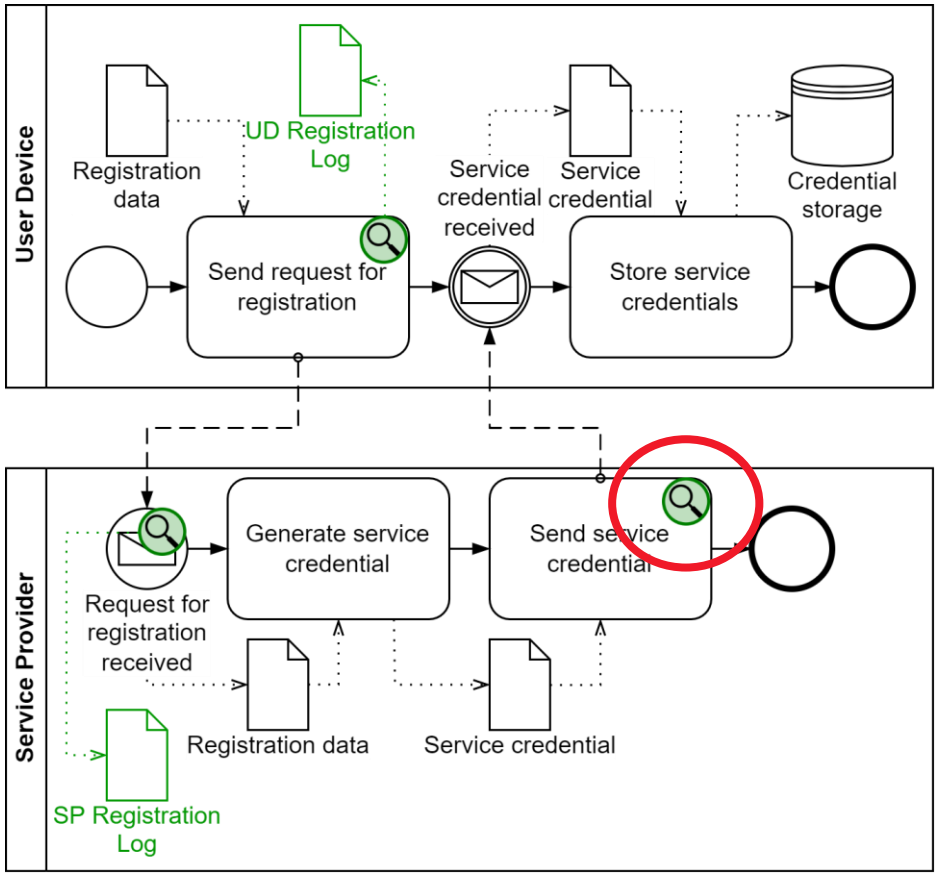


MUNI C4E

Analysis of Forensic Readiness Scenarios

Validity and Hints Analysis

- Analysis of BPMN4FRSS models
- **Check the model validity**
- Provide hints to enhance the model
  - Cover the blind spots
  - Add evidence on strategic spots
  - Improve non-disputability

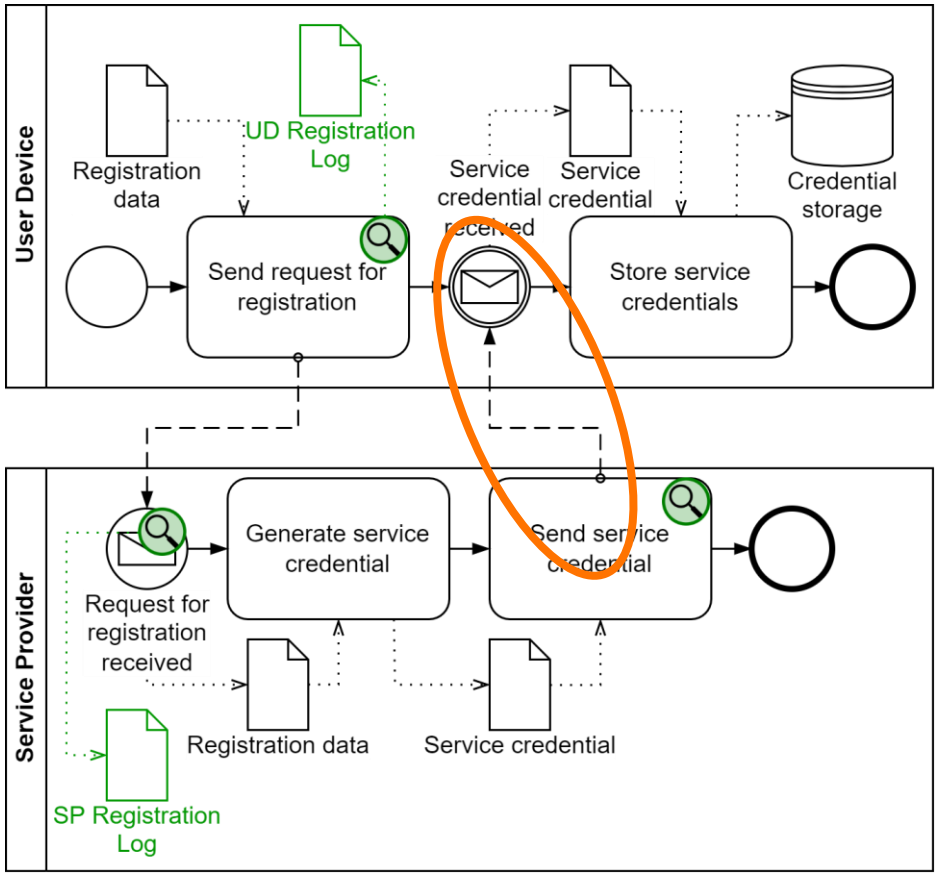


MUNI C4E

Analysis of Forensic Readiness Scenarios

Validity and Hints Analysis

- Analysis of BPMN4FRSS models
- Check the model validity
- **Provide hints to enhance the model**
  - Cover the blind spots
  - Add evidence on strategic spots
  - Improve non-disputability



MUNI C4E

Analysis of Forensic Readiness Scenarios

Validity and Hints Analysis

```
(declare-sort Task)

(declare-fun flow (Task Task) Bool)


(declare-const send Task)
(declare-const receive Task)
(declare-const alone Task)


(assert (flow send receive))
(assert (flow receive send))
(assert (forall ((x Task)) (= (flow x x) false) ))
```

```
(check-sat)
// sat

(eval (= (flow send receive) true))
// true

(eval (= (flow send send) true))
// false

(eval (= (flow send alone) true))
// (= (ite (= alone Task!val!0)
//  Task!val!0 Task!val!1) Task!val!1)
```


MUNI C4E

Conclusion

- Forensic readiness is about preparation when things go wrong
  - We need to know why, what, when, who, how
  - We need to defend against or support accusations
  - We need to show that we did everything we could
  - We need to effectively support law enforcement
- Risk management
  - Determine our current status
  - Plan and prioritize what to implement
- Analysis support, validation, verification
  - Be sure that we are going the right direction

MUNI C4E