MUNI
FI

lasaris LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

Forensic-Ready Software System Design

Lukas Daubner
daubner@mail.muni.cz

Faculty of Informatics, Masaryk University, Brno
September 9, 2021

What is Forensic-Ready Software?

a.k.a. Forensic-by-Design

- Capable of:
  - Conducting digital forensic processes in a forensically sound way
  - **Producing forensically sound evidence**
- Assisting during the investigation
- High-level, non-functional requirement
  - Evidence availability, minimality, non-repudiation, …
  - Legal compliance
  - Data provenance

MUNI C4E

What is Forensic-Ready Software?

a.k.a. Forensic-by-Design

- Preparing when security measures fail
  - The question is on **if** but **when**…
- Introducing proactive measures within the system
  - Opposed to the actual investigation, which is reactive
- Increasing the likelihood of successful investigation
  - Having the right evidence
  - Having the evidence right

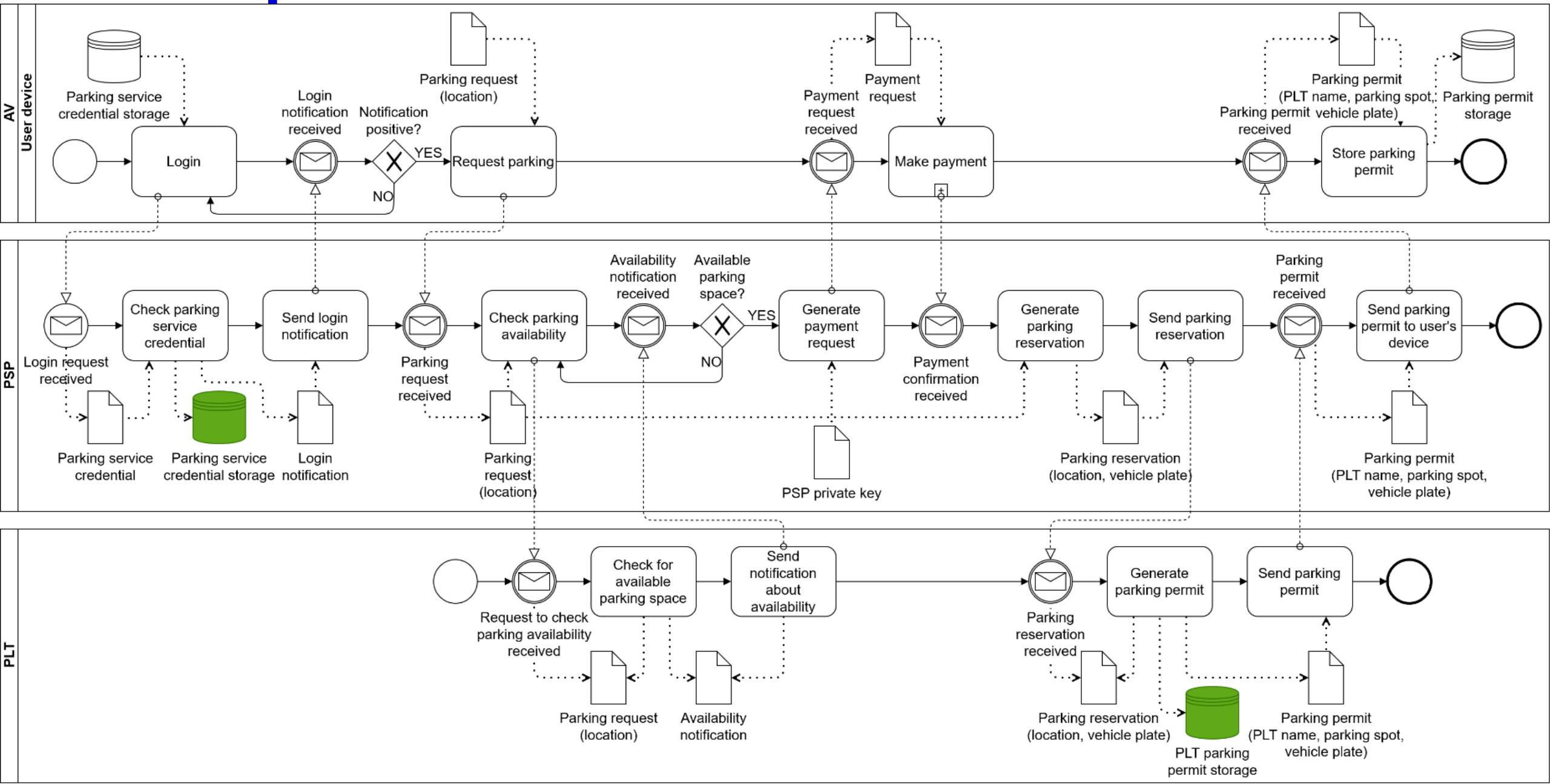
Forensic-Ready Software – Challenges

- Dealing with a huge conflict of interests
  - Service owners want running systems
  - Law enforcement wants evidence
  - Lawyers want the correct procedure
  - Investigators want useable data
- How to capture, model and reason about the systems?
- Validation and verification

MUNI C4E

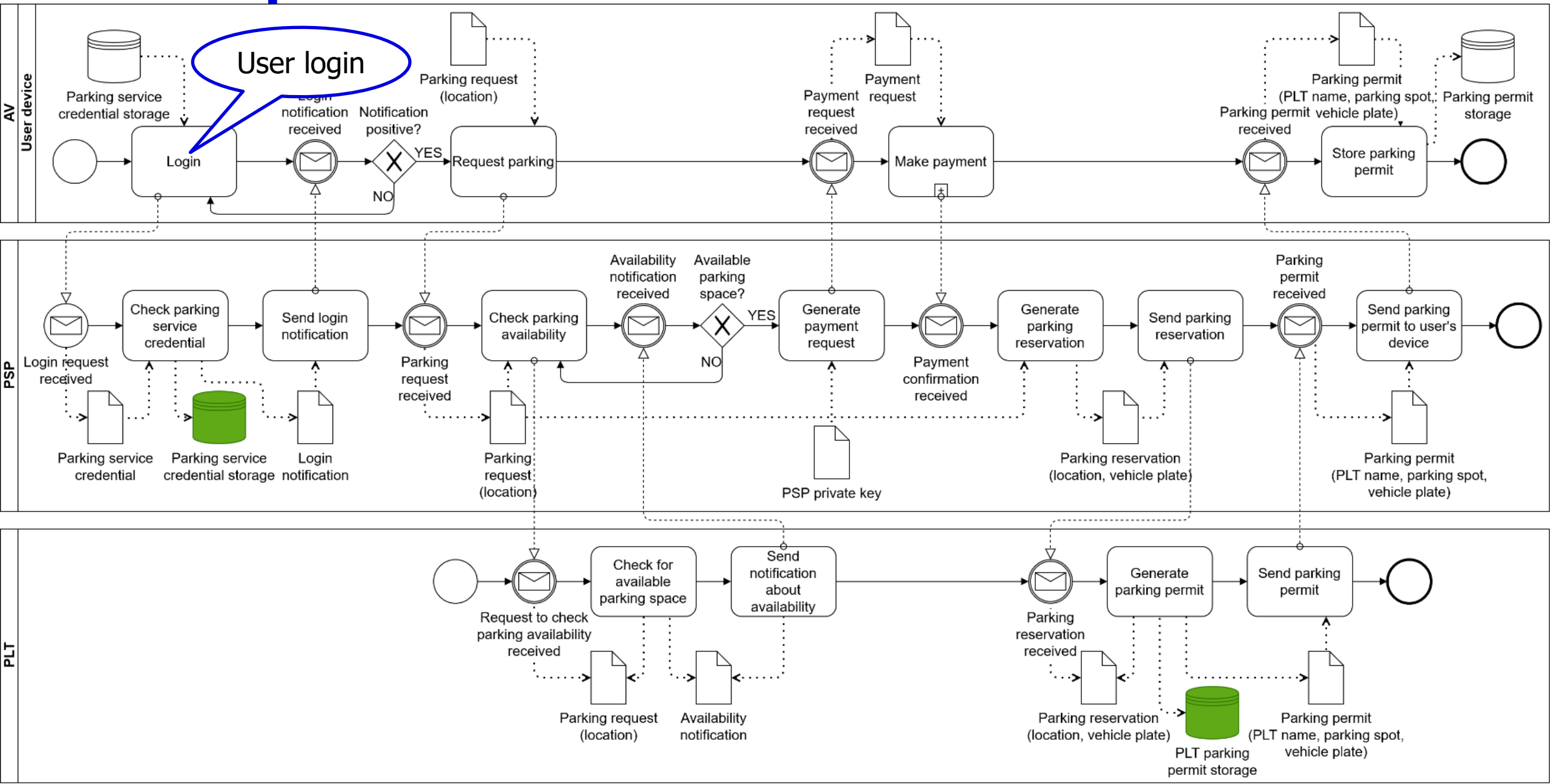
Example Scenario

Automated Valet Parking: Issuing a Permit



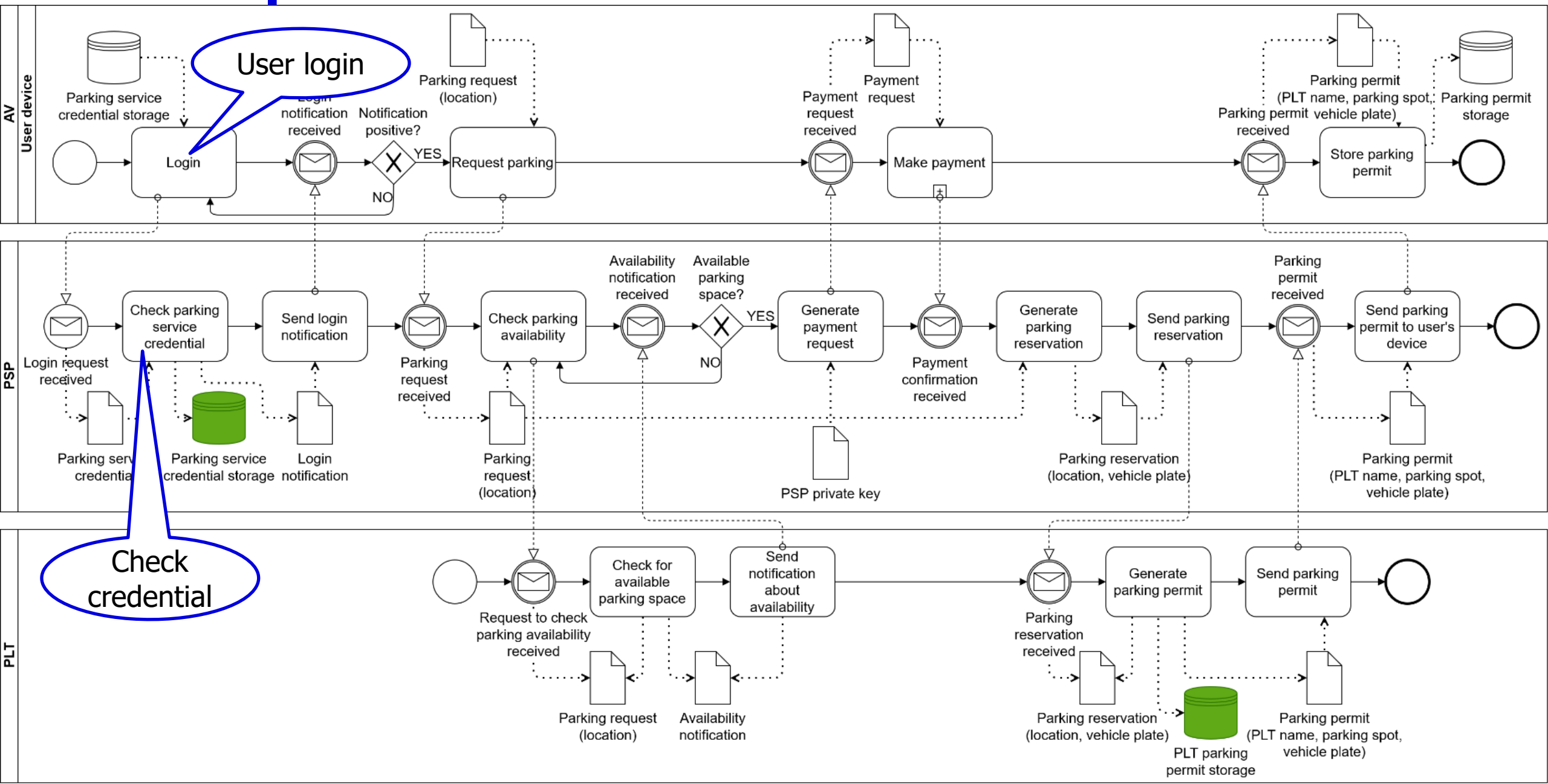
Example Scenario

Automated Valet Parking: Issuing a Permit



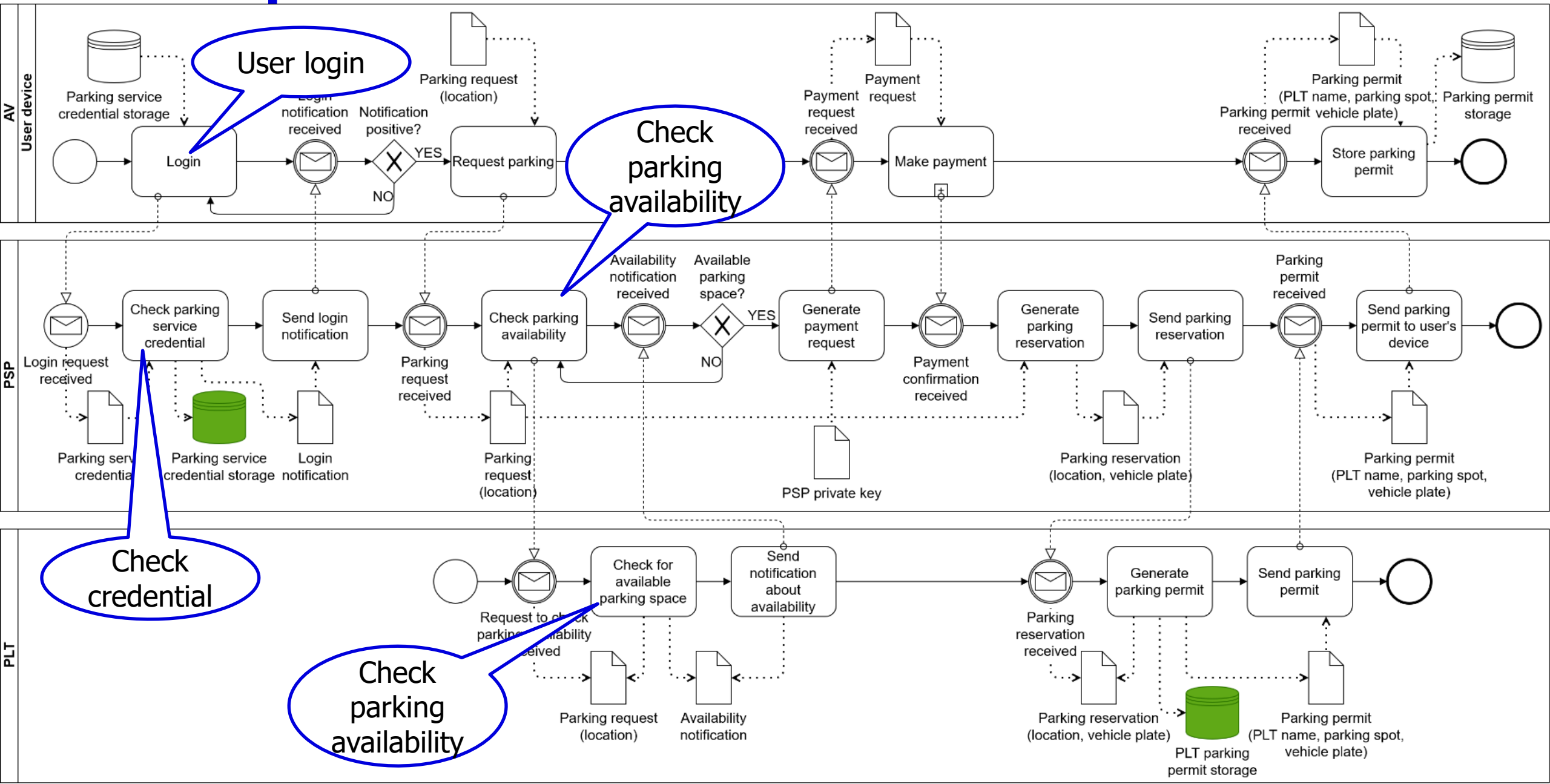
Example Scenario

Automated Valet Parking: Issuing a Permit



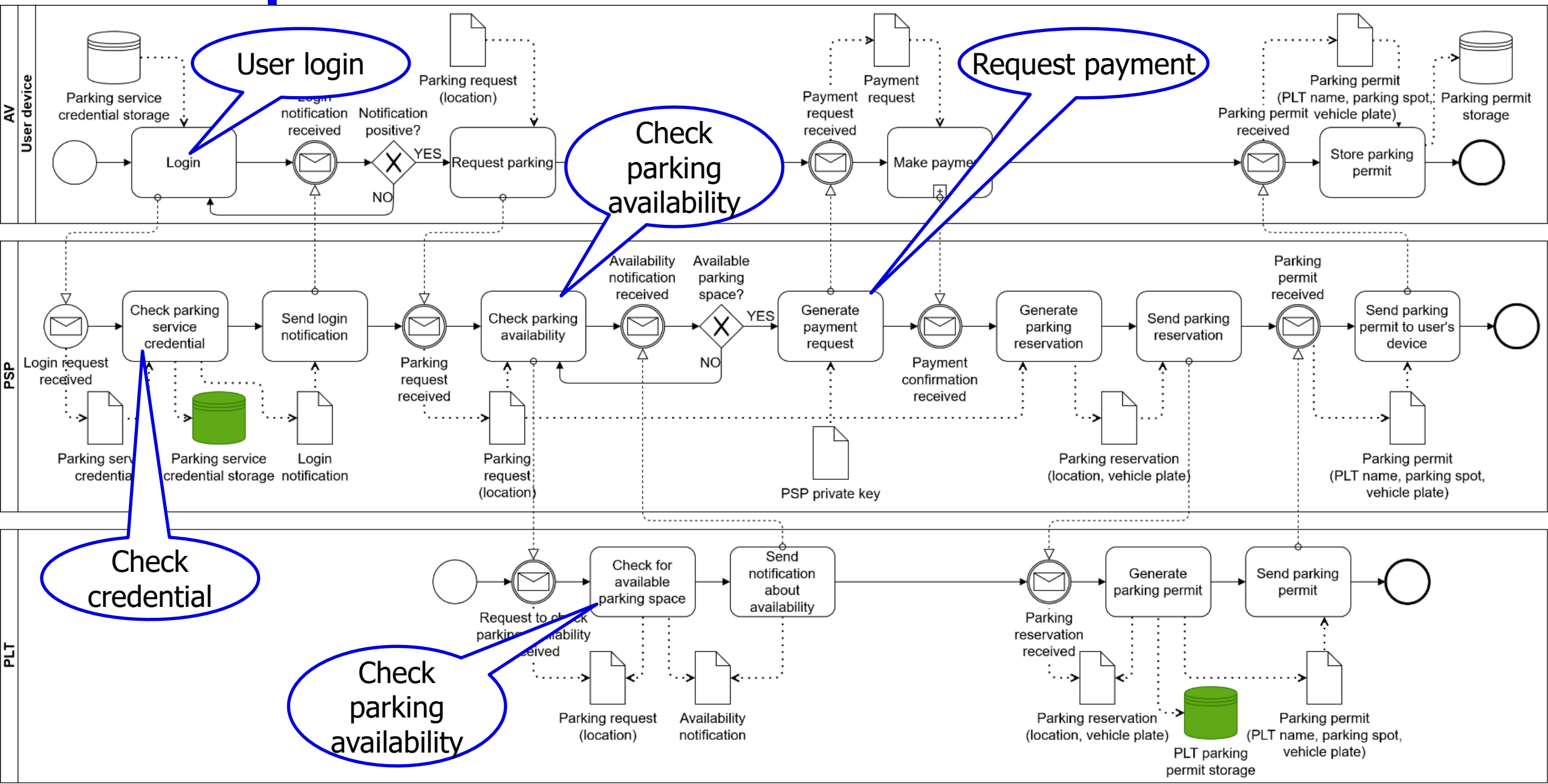
Example Scenario

Automated Valet Parking: Issuing a Permit



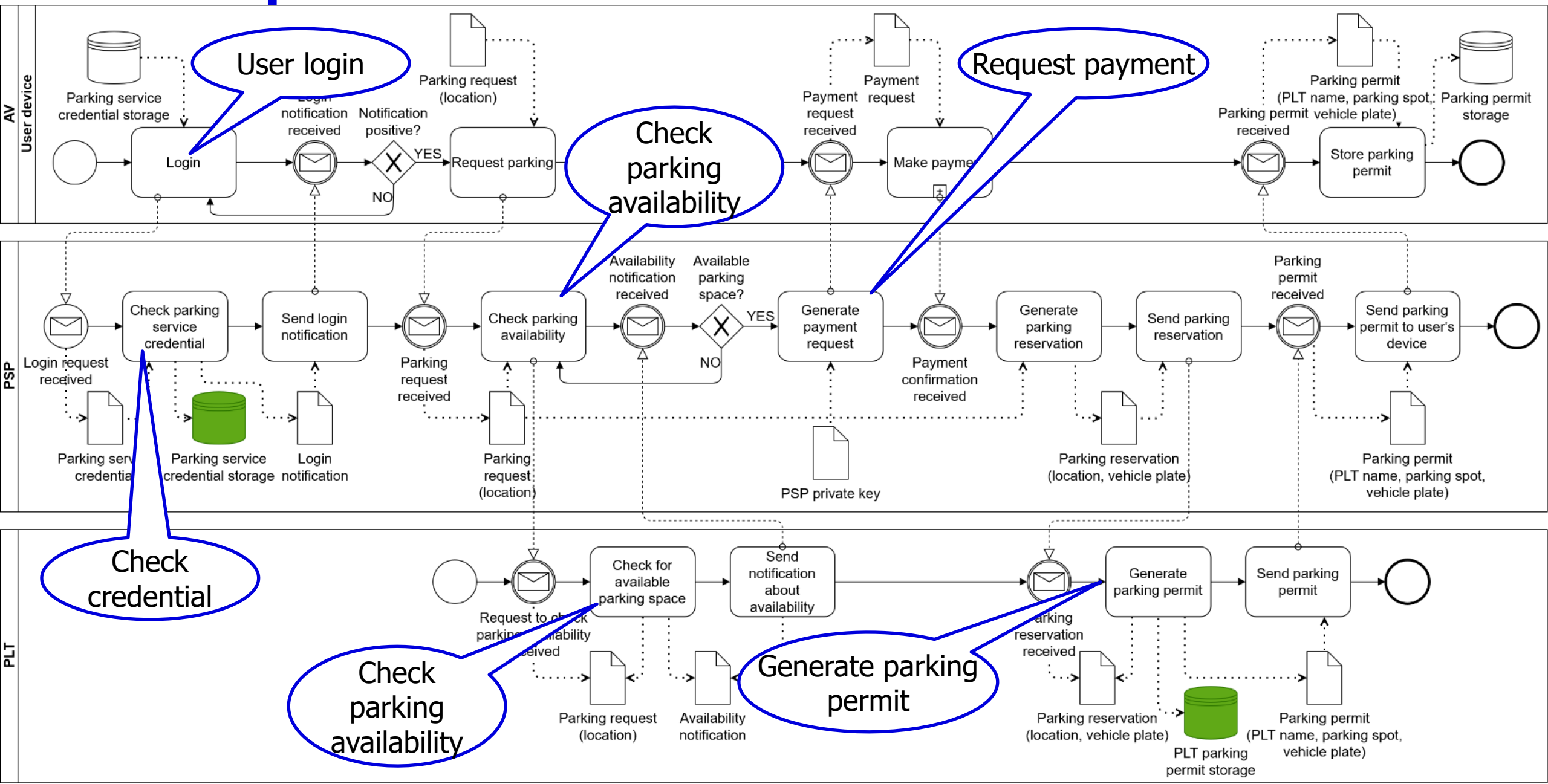
Example Scenario

Automated Valet Parking: Issuing a Permit



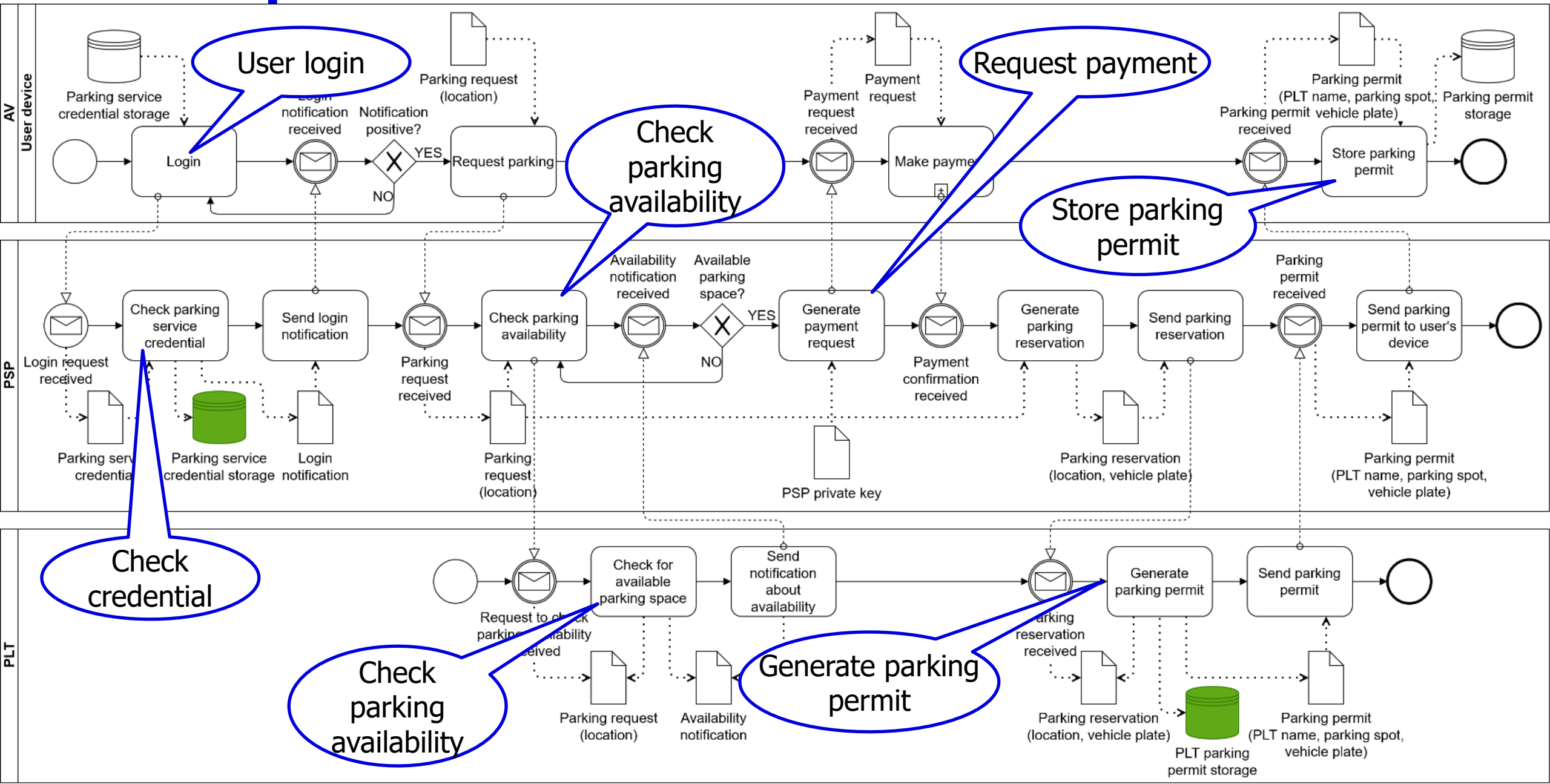
Example Scenario

Automated Valet Parking: Issuing a Permit



Example Scenario

Automated Valet Parking: Issuing a Permit



Example Scenario – Considerations

- Attacks or misuse cannot be detected in the scenario
- But if we apply security measures, the attacks can be prevented
  - Not entirely – security is never 100%
  - Sometimes measures are not implemented – cost, inference, low probability, etc.
  - Human aspect – insider attacks
  - Unforeseen attacks
- Consider the forensic readiness as an enhancement of security

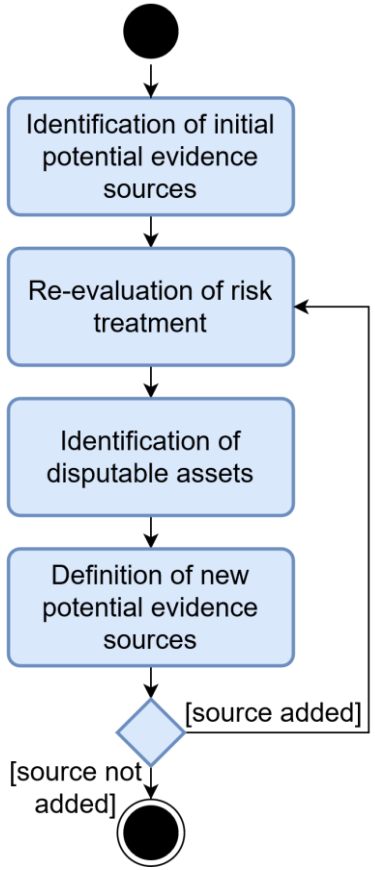
Risk-Oriented Forensic-Ready Design

- Risk management is well-known approach in cybersecurity
  - Assessing risks for the systems and their treatment
  - Modeling techniques and patterns
- Make informed decisions and reason about them
- Extension of Information Systems Security Risk Management
  - **Process** to identify the potential evidence sources to implement
  - **Modeling** to support the process and allow the reasoning

MUNI C4E

Forensic-Ready Risk Analysis Process

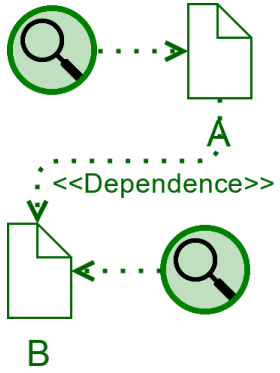
- Core of the approach
  - Helps with the identification of innate evidence sources
  - Guides the decisions whether to include evidence sources into the system
  - Considers threat of disputes, usually not covered by security risk
- Assumes and builds on previously performed security risk management



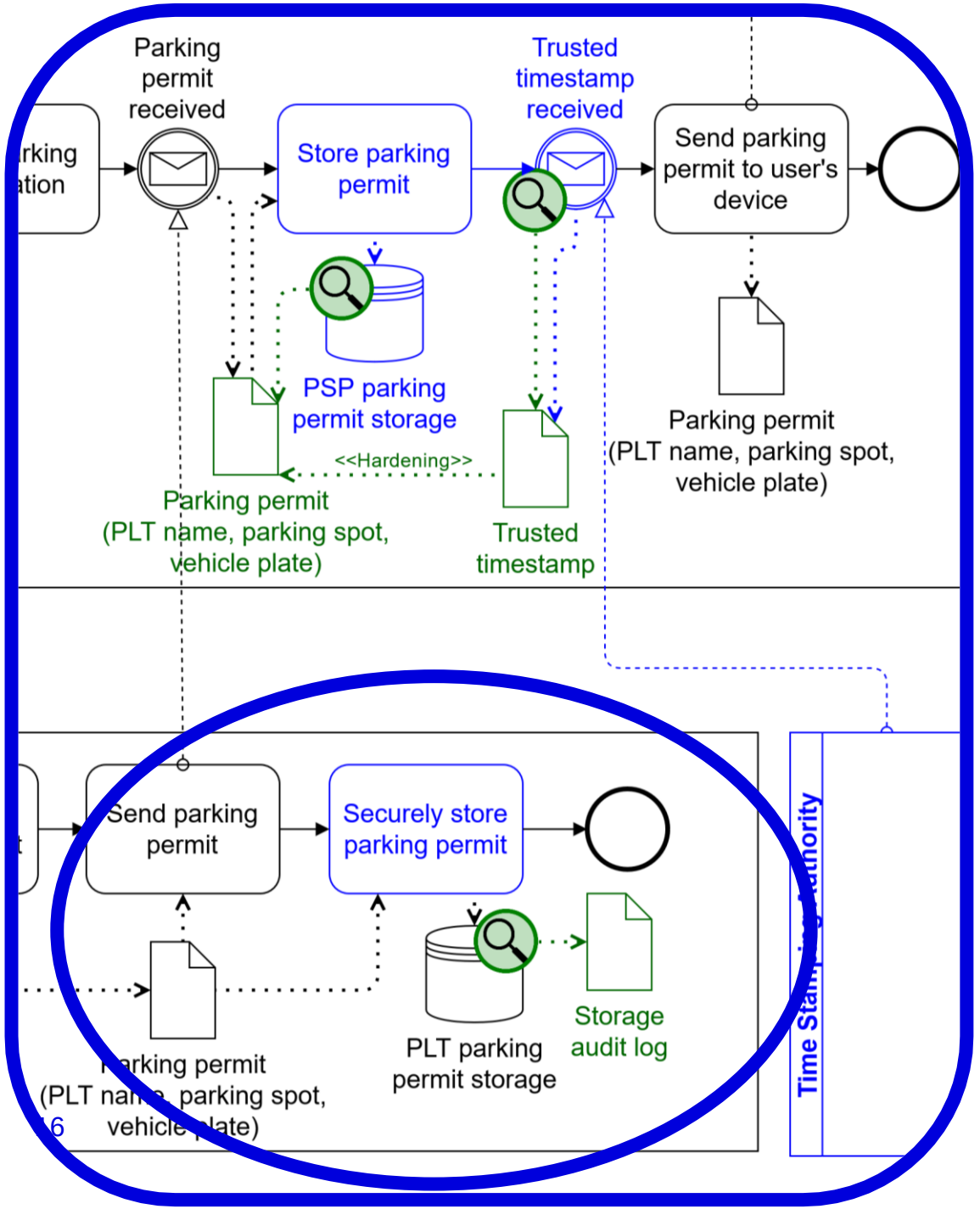
MUNI C4E

Forensic-Ready BPMN Notation

- Novel notation to capture the evidence sources
  - Including relationships and protective measures
- Complements Security Risk-Aware BPMN
  - Risk-related constructs
- Assist in the re-evaluation of risk treatment phase



MUNI C4E

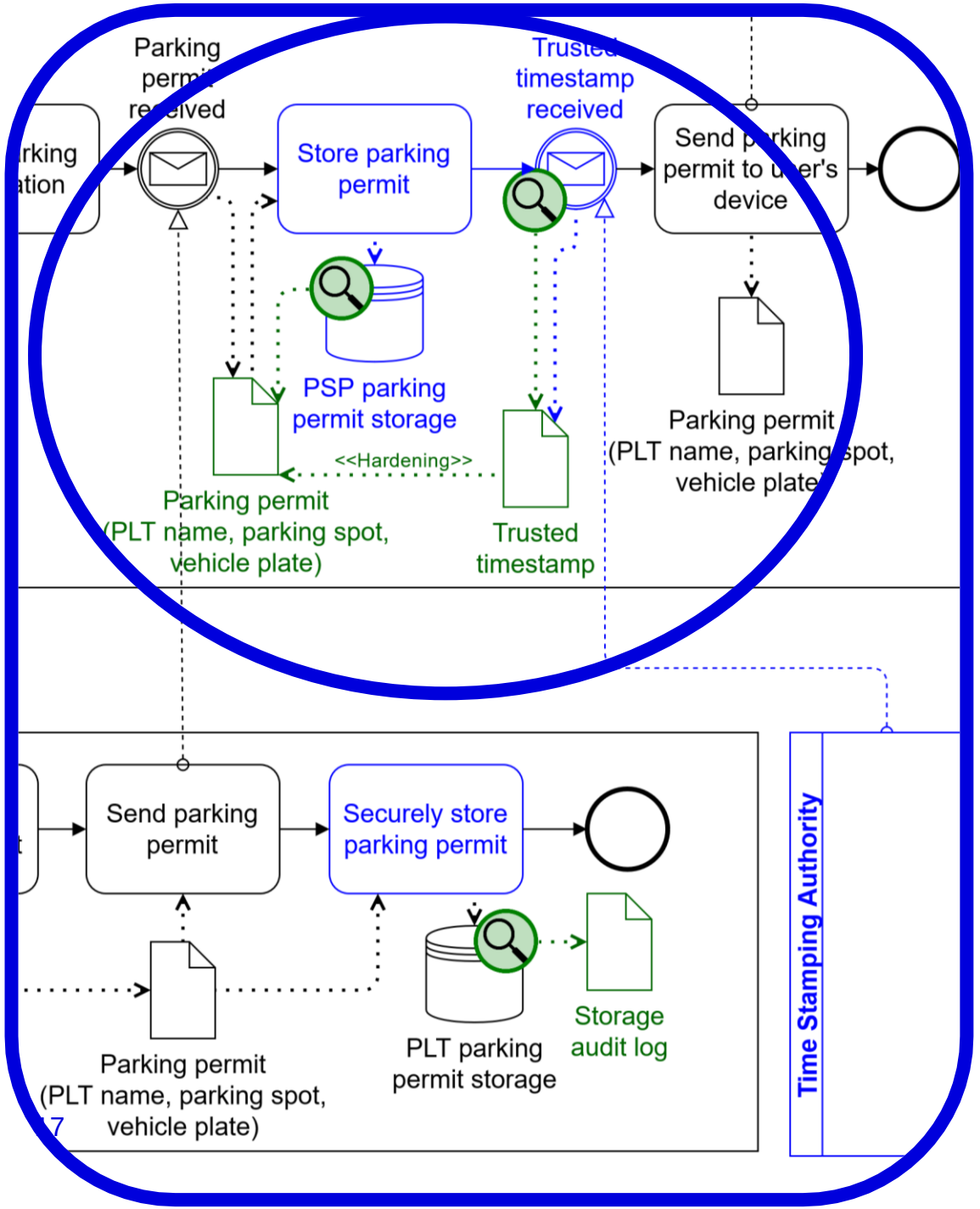


Example Scenario – Application

Parking permit fabrication (store injection)

- Risk mitigated by securing storage
  - Insider with elevated privileges can still perform the attack
- Introduced data store auditing
  - Log monitoring to detect suspicious behavior
  - Good place to make attacker noisy

MUNI C4E



Example Scenario – Application

Dispute – parking permit repudiation

- Dispute not covered by security risks
  - However, it is a business risk
- Keep issued parking ticket
  - We don't have control over user device
  - Store on multiple places
  - With proof of integrity

MUNI C4E

Future Steps

- Elaborate the initial idea of BPMN extension
- Create algorithms to analyze and verify the design
  - Both model and implementation
- Create an extension to existing modeling tool

MUNI C4E

Conclusion

- Forensic-ready software systems
  - Produce sound digital evidence and handle the potential evidence in a sound way
  - Assist the persons involved in digital forensic investigation
- Risk-based process to identify & manage forensic-ready controls
  - Guidance what to implement regarding the **security and business risks**.
- BPMN notation to assist in this process

- Idea created in collaboration with InfoSec group form University of Tartu

MUNI
C4E