Lehrstuhl Angewandte Informatik IV
Datenbanken und Informationssysteme
Prof. Dr.-Ing. Stefan Jablonski

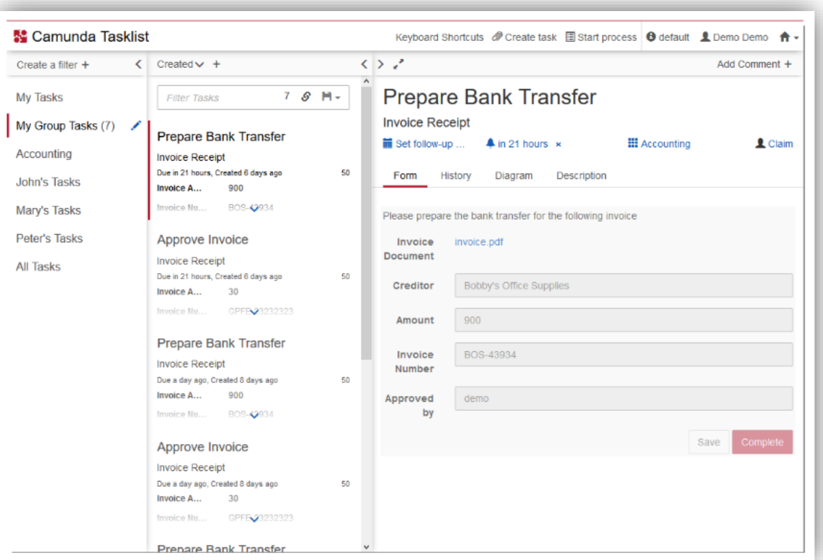
Institut für Angewandte Informatik
Fakultät für Mathematik, Physik und Informatik
Universität Bayreuth

UNIVERSITÄT
BAYREUTH

Master Thesis: Trustworthy Process Engines using Asymmetric Cryptography

Context:

Enterprises model their operational business in form of process models. On the one hand, process models help to document these processes, but on the other hand Workflow Management Systems (WFMS) are used to bring the process models to life. As an example, Camunda (Figure 1) uses process models in BPMN notation and during the execution of these processes, the participants will find the relevant tasks in their respective task list. Thereby, the workflow engine ensures a compliant execution of the process and supports the participants in their daily work. On top, the process engine logs the event history in form of an event log out of which the process can be reconstructed in detail.



Prepare Bank Transfer
Invoice Receipt
Due in 21 hours, Created 6 days ago 50
Invoice A... 900
Invoice Nu... BOS-43934

Approve Invoice
Invoice Receipt
Due in 21 hours, Created 6 days ago 50
Invoice A... 30
Invoice Nu... GPFE-23232323

Prepare Bank Transfer
Invoice Receipt
Due a day ago, Created 8 days ago 50
Invoice A... 900
Invoice Nu... BOS-43934

Approve Invoice
Invoice Receipt
Due a day ago, Created 8 days ago 50
Invoice A... 30
Invoice Nu... GPFE-23232323

Prepare Bank Transfer

Prepare Bank Transfer
Invoice Receipt

Please prepare the bank transfer for the following invoice

Invoice Document	invoice.pdf
Creditor	Bobby's Office Supplies
Amount	900
Invoice Number	BOS-43934
Approved by	demo

Figure 1: Camunda (https://docs.camunda.org/manual/webapps/tasklist/img/tasklist-dashboard.png)

Problem Statement:

Enterprises often interact with other enterprises on the market to reach a common business goal, e.g. supply chains. Consider Figure 2 for an example BPMN model, which describes the process of purchasing goods when a scarcity of resources is detected by an employee. In particular, the process models that in case of a high-value order (> 1.000 EUR), the headquarter must grant permission to submit the order. The headquarter checks, if another subsidiary of the group may have resources available. In case of accepted permission, the order may be placed. In the following, this process is to implement in a process engine like Camunda. Multiple issues will arise.

When it comes to the cross-enterprise WFMS-driven digital process execution, trust or data integrity is a decisive factor. Imagine, the employee manipulates the purchasing form, after the headquarter have granted permission by adding an extra item for instance. The process runtime environment must guarantee, that neither the data (purchasing form) nor the execution history can be manipulated afterwards.

There are several approaches, but each comes along with certain issues.

- A single workflow engine hosted by one process participant
    - The participant (e.g. employee) have power over the data and can manipulate the purchasing form secretly
- A single workflow engine, hosted externally (Azure, AWS)
    - Data protection (GDPR) or trade secret issues arise
- Multiple workflow engines, hosted per participant
    - Process engines must be kept synchronous. Event logs still can be manipulated locally, and two different (one manipulated) logs are the result.
- Blockchain-based solutions
    - Blockchains are a tamper protected data storage and research has shown that they solve the issues but may be an overkill in some situations.

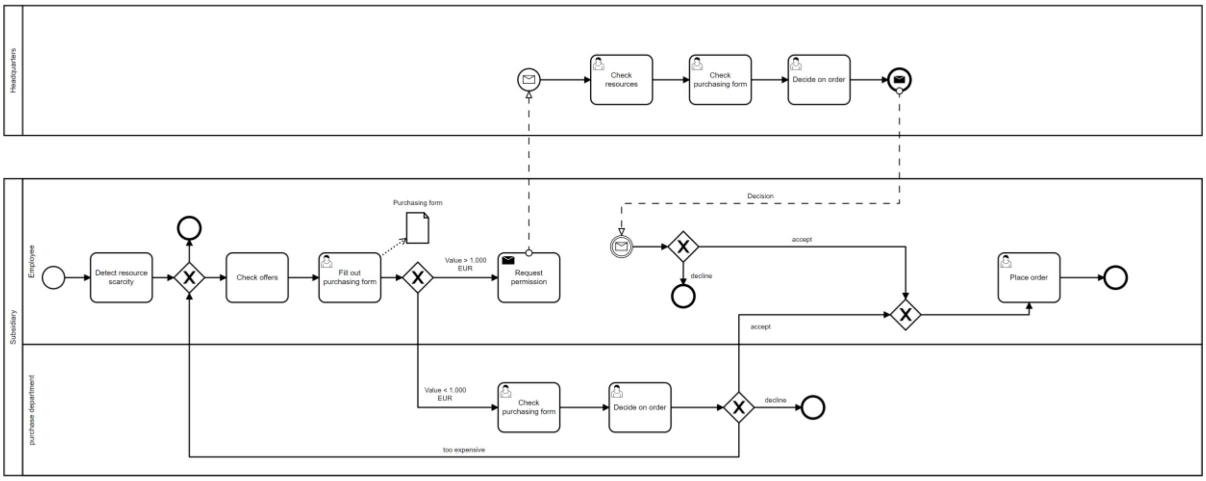


Figure 2: Example BPMN process model

Task:

The task is to get in the problem statement and fully understand the issues of automatic process execution in the B2B world. Initial steps are get used to the BPMN notation (https://www.omg.org/spec/BPMN/2.0.2/PDF), set up a Camunda instance, implement and execute an example B2B process (https://camunda.com/de/download/). The process depicted in Figure 2 may be a starting point but must be modified eventually. You can view the process using bpmn.io (https://demo.bpmn.io/) – the .bpmn file is attached. A second requirement is asymmetric cryptography, especially the public-private key infrastructure (RSA), digital signatures and key exchange (Diffie-Hellman).

Having acquired the fundamentals, the student designs an architecture, how tamper-protected process execution over a manipulable data storage can be implemented using asymmetric cryptography. The architecture includes also soft requirements like useable key management.

For the evaluation, the student also reenacts the manipulation of B2B process execution with the infrastructures depicted above and shows, that the new solution counteracts the fraud.

Goal:

The goal of the thesis is a software system for B2B process execution including an asymmetric cryptography module for integrating tamper protected task execution. Amongst others, the thesis is evaluated in terms of the architecture, usability and functional scope of the software as well as the scientific methods and the application of them in the written report.

The student is free in terms of implementing a plug-in for existing engines (e.g. Camunda) or building the software from the scratch using “BPM-libraries” (e.g. jBPM).