Establishment of a Minimum Viable Self-Sovereign Identity Network

Kilian Käslin, 27.01.2020, Kick-Off Master's Thesis

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

Introduction
- Motivation: Classic Identity Management & Self-Sovereign Identity
- Introduction to Self-Sovereign Identity
- Trust Models: PGP & Self-Sovereign Identity

Problem Statement

Research Questions

Methodology

Preliminary Results
- Functional Requirements: Use Cases & User Stories
- Preliminary Architecture
- Sequence Diagram: Register & Login

Further Expected Results

Timeline

Motivation: Classic Identity Management & Self-Sovereign Identity

Centralized/Federal/User-Centric Identity

- Dependence on centralized identity providers
  - Privacy concerns
  - No absolute control over identity
- Hierarchical Trust

Self-Sovereign Identity

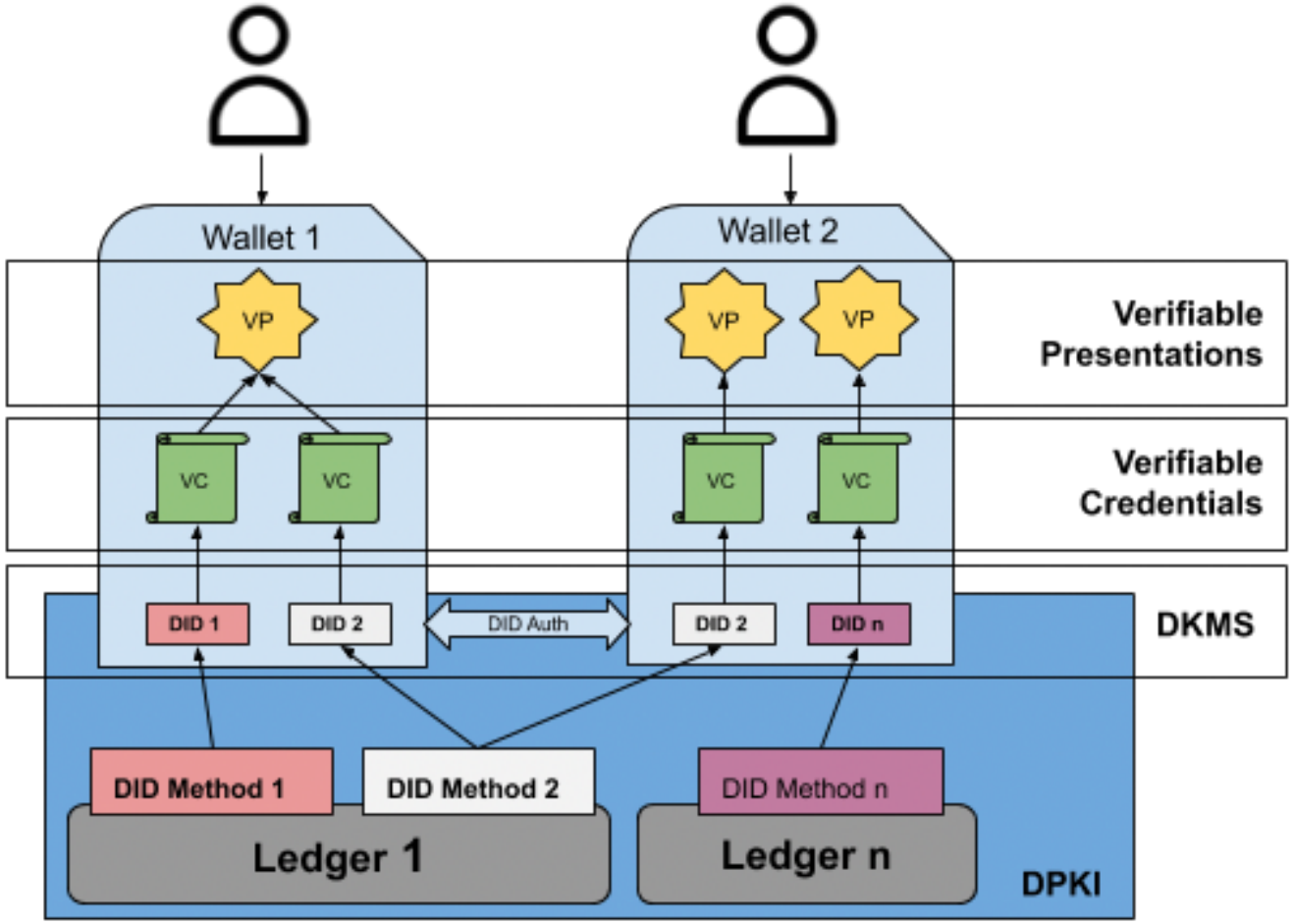
- Identity stored on decentralized database
  - More control over identity
- Attestation of claims
  - Improved control over shared data
- Decentralized Trust

Almasi P. (2019). ‘‘The Identity Revolution — Self Sovereign Powered by Blockchain‘‘.

Introduction to Self-Sovereign Identity

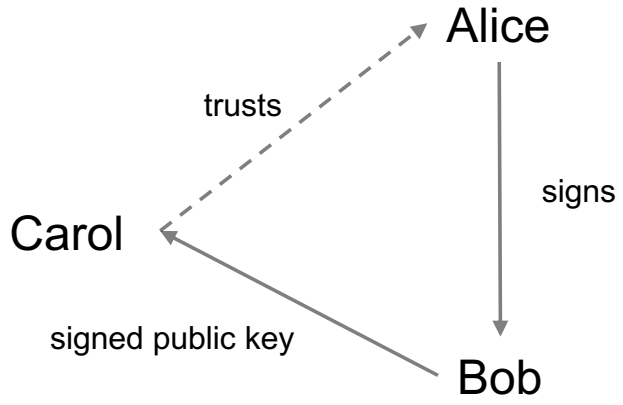
Components of SSI:

- **Web of Trust** between **actors**
- **Wallets** manage VCs, VPs, DIDs
- **Verifiable Presentations (VP)** to share data in a privacy-preserving manner
- **Verifiable Credentials (VC)** to attest personal information
- **Decentralized Key Management System (DKMS)** to manage keys and communication
- **DID Methods** to create and manage **Decentralized Identifiers (DIDs)** on a ledger to establish a **Decentralized Public Key Infrastructure** (**DPKI**)



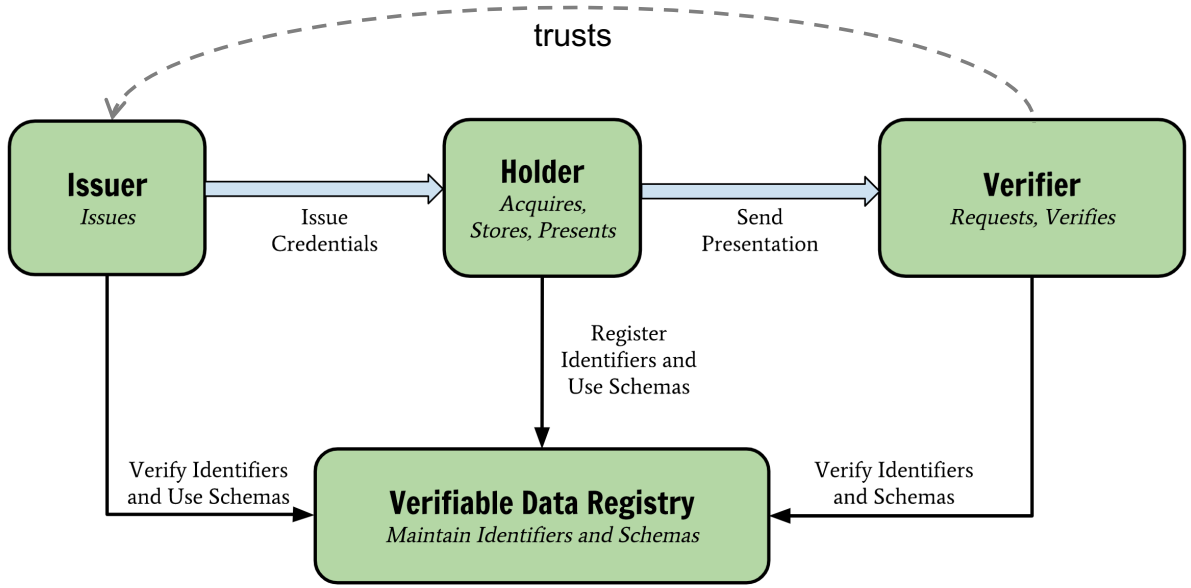
Schäfer, M. 2019. “Analysis and Evaluation of Blockchain-Based Self-Sovereign Identity Systems“.

Trust Models: PGP & Self-Sovereign Identity



PGP

- Individuals sign each others' public keys
- Carol trust Alice
- Alice signed Bob's public key
- Carol trusts Bob based on Alice's signature
- Mostly hierarchical Public Key Infrastructure



Self-Sovereign Identity

- Individuals can proof control over their public key stored on a decentralized database
- Verifier trust Issuer
- Issuer issues a Verifiable Credential (VC) with claims about Holder and a signature
- Holder sends Verifiable Presentation (VP) which Verifier can check
- Distributed Public Key Infrastructure

Abdul-Rahman, A. 1997. "The PGP Trust Model," | Sporny, M., Longley, D., and Chadwick, D. 2019. *Verifiable Credentials Data Model 1.0*.

Problem Statement

Establishment of a Minimum Viable Self-Sovereign Identity Network

- Authentication
- Access Control
- Issuance, Sharing, Proof of Claims

Research Questions

Requirements Engineering

RQ1: **Which requirements must be fulfilled by a minimum viable Self-Sovereign Identity network?**

- Which functional requirements must be fulfilled?
- How can the non-functional requirements be defined?
- Which non-function requirements must be fulfilled?
- Which limitations are induced by relying on Self-Sovereign Identity compared to other possible authentication and access control methods?

Design

RQ2: **What are the main processes that must be implemented to fulfill the requirements for a minimum viable Self-Sovereign Identity network?**

- To which extend are the processes defined by prior works?
- What are the characteristics of the processes?
- How can the processes be implemented?

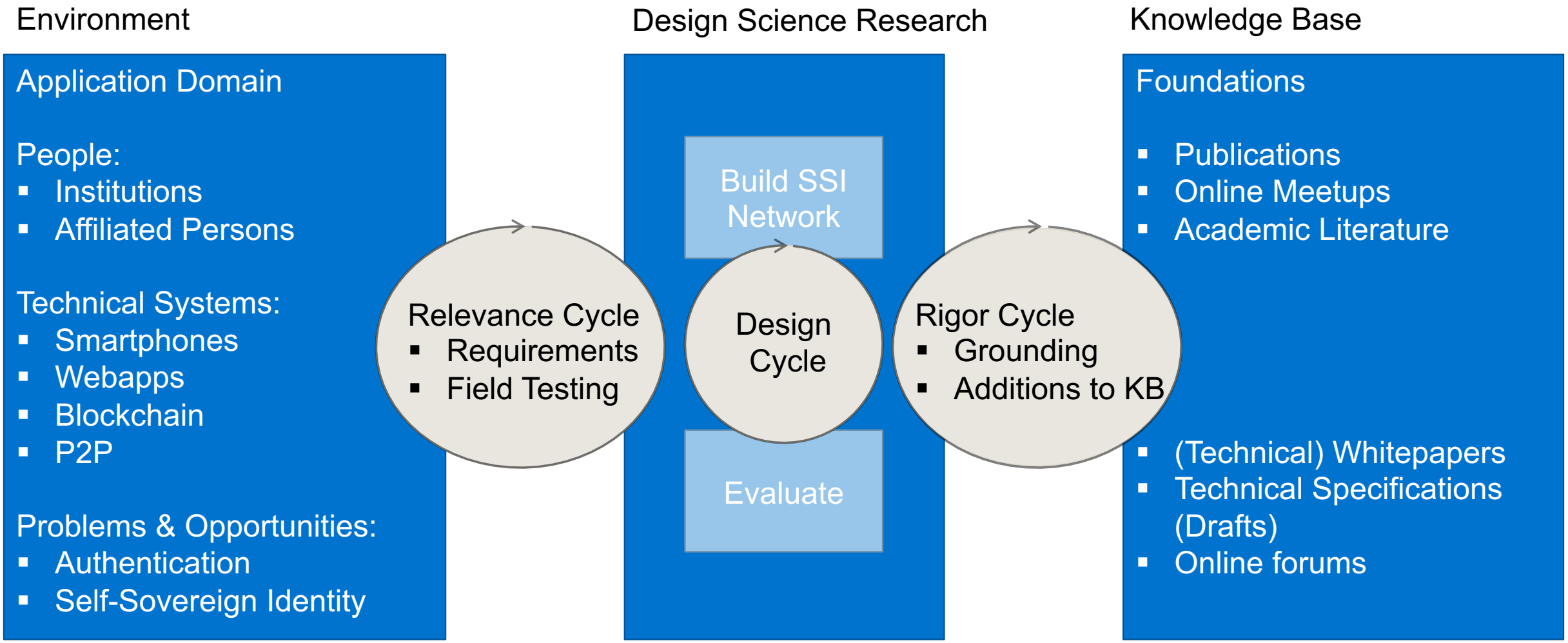
Evaluation

RQ3: **To what extend does the implemented solution fulfil the requirements for a minimum viable Self-Sovereign Identity network?**

- Which limitations does the implementation have?
- What are the differences compared to other authentication methods?

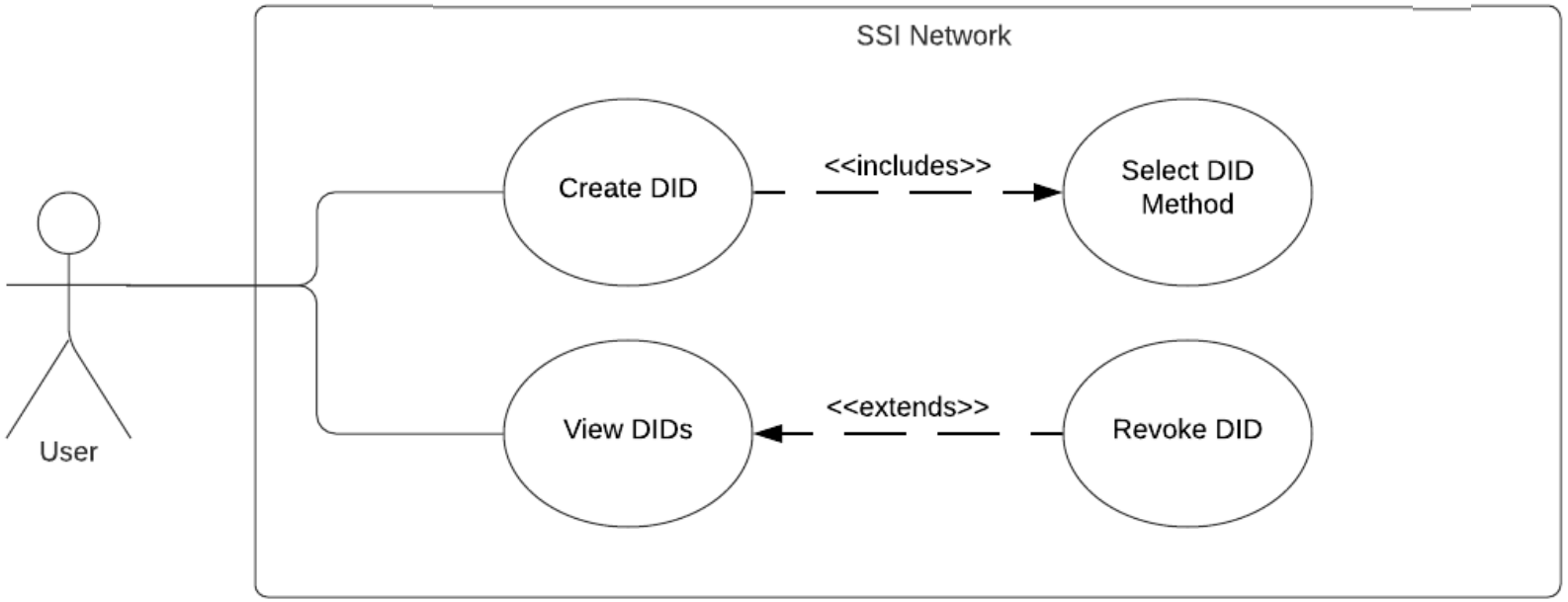
Methodology

Design Science following Alan A. Hevner



Hevner, A. R. 2007. "A Three Cycle View of Design Science Research," *Scandinavian Journal of Information Systems* (Vol. 19).

Functional Requirements – Manage DIDs

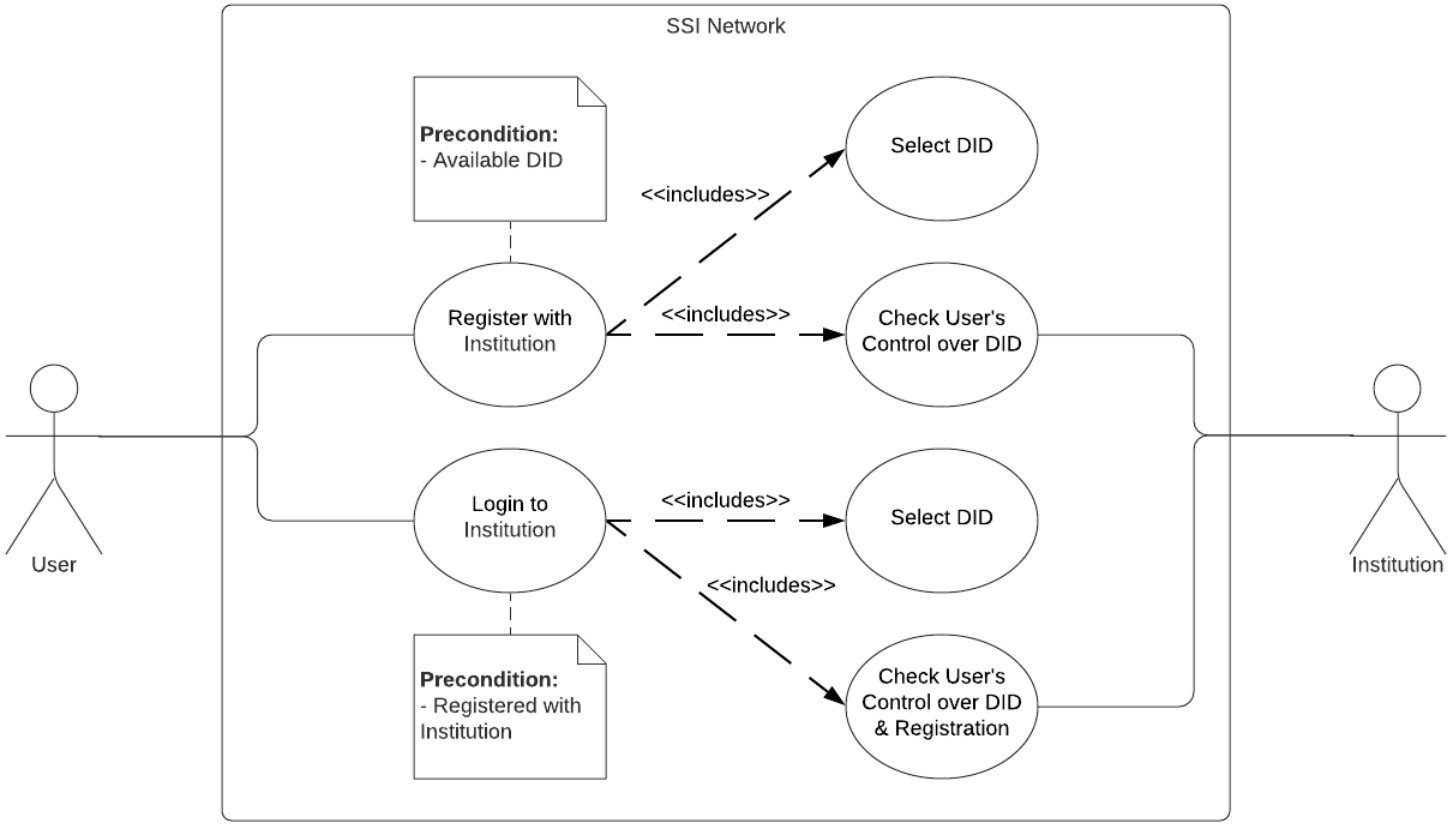


User Story

As a user I can register a DID, so that I can use it to authenticate myself.

As a user I can view my DIDs, so that I can select a DID to be revoked.

Functional Requirements – Register / Login

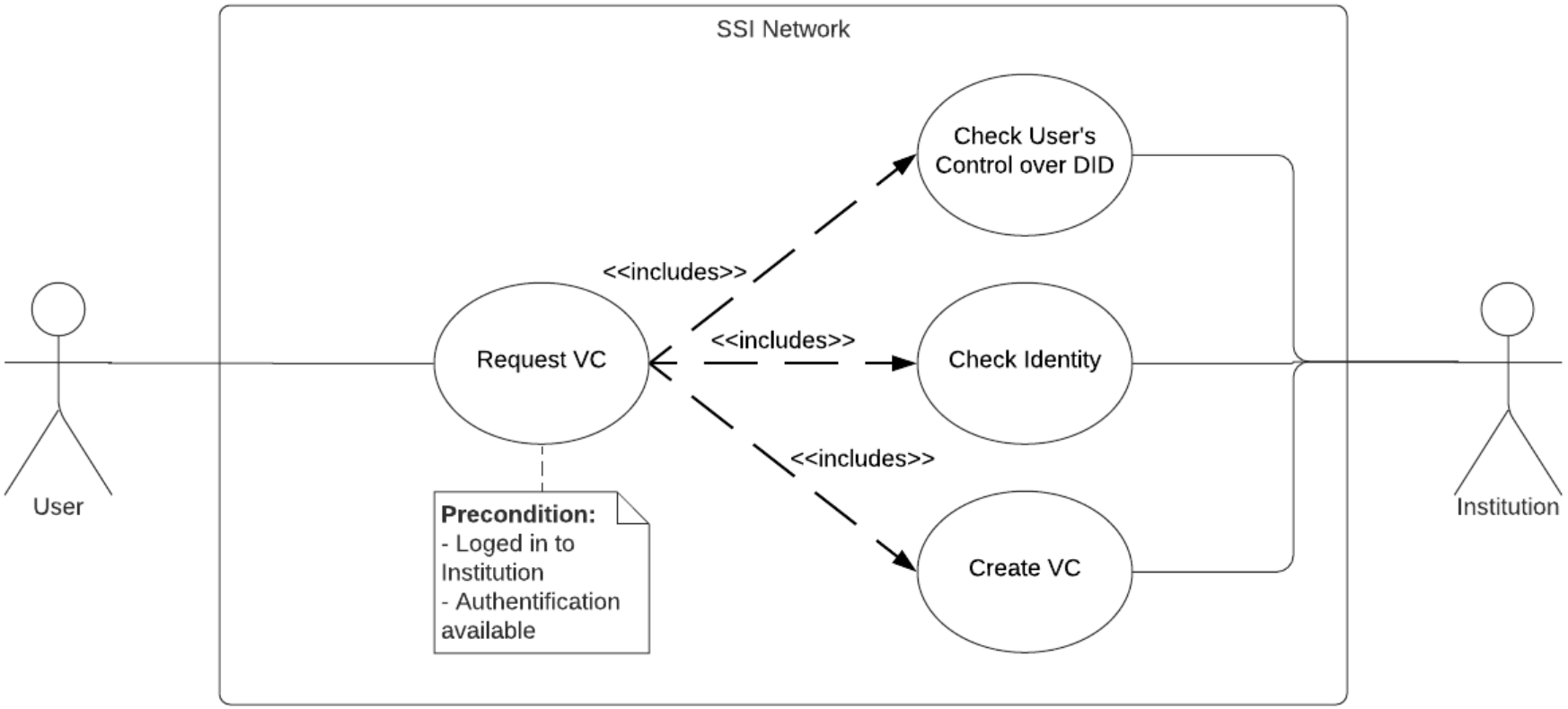


User Story

As a user I can register to Blockchain Bayern, so that I can login to Blockchain Bayern.

As a user I can login to Blockchain Bayern, so that I can use the user portal.

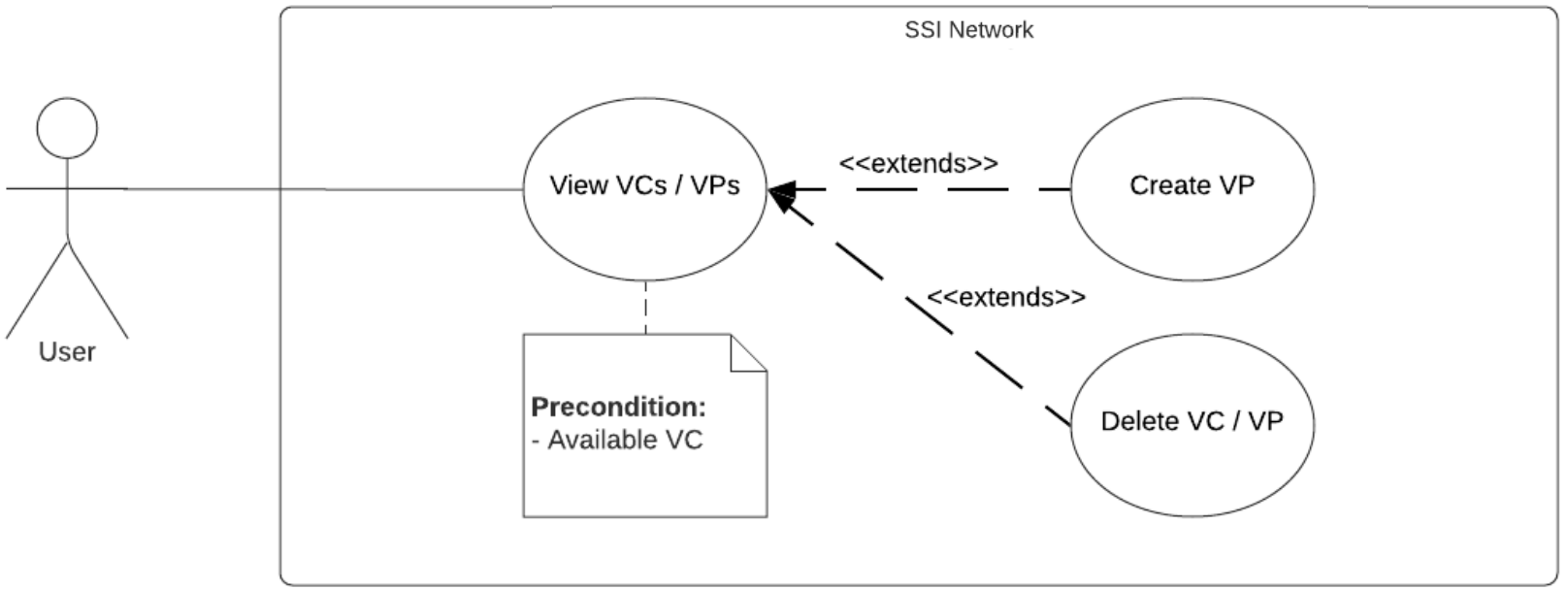
Functional Requirements – Request VC



User Story

As a user I can request a VC, so that I can use it to create VPs to pass on to third parties.

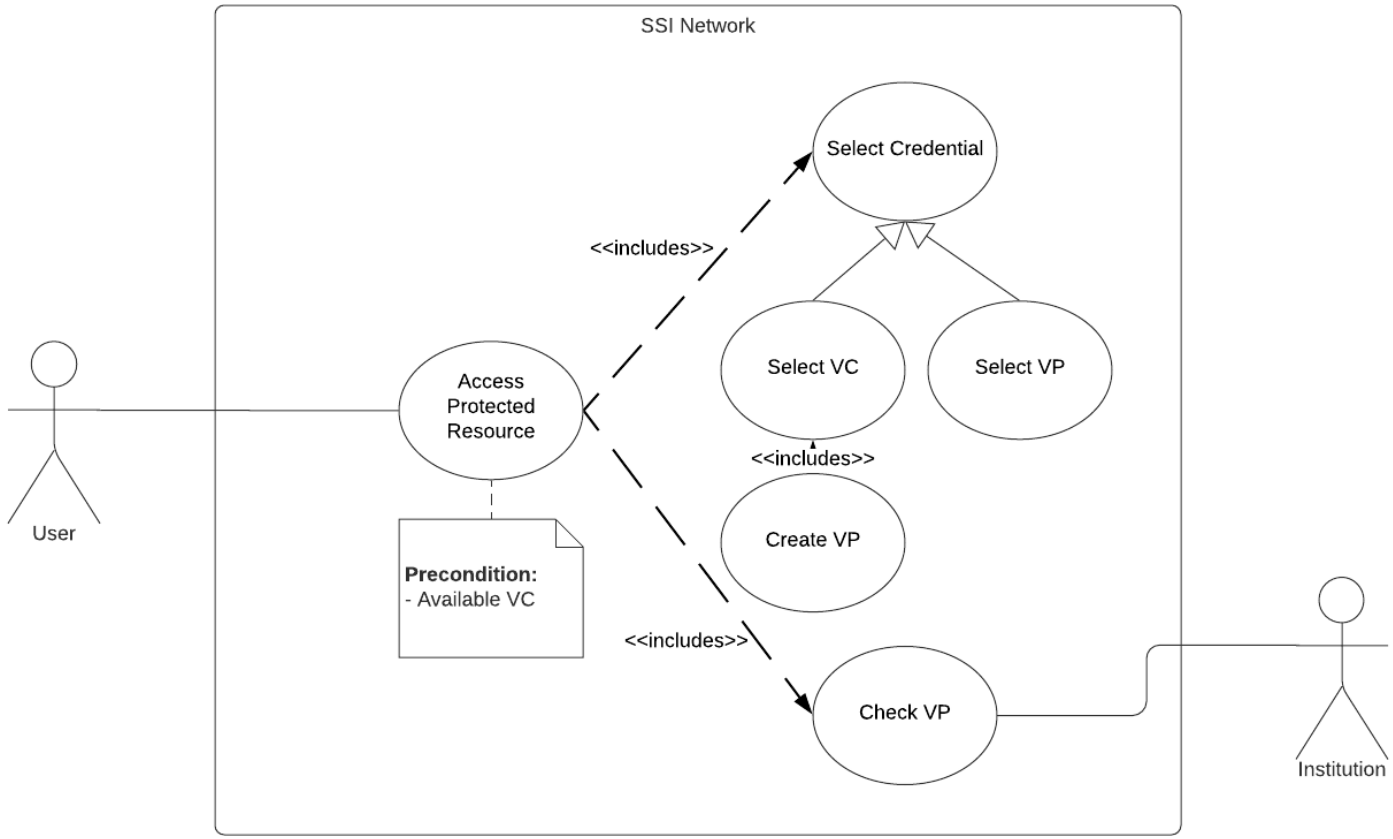
Functional Requirements – Manage VCs & VPs



User Story

As a user I can view my VCs and VPs, so that I can create new VPs to pas on to third parties and delete existing VCs and VPs.

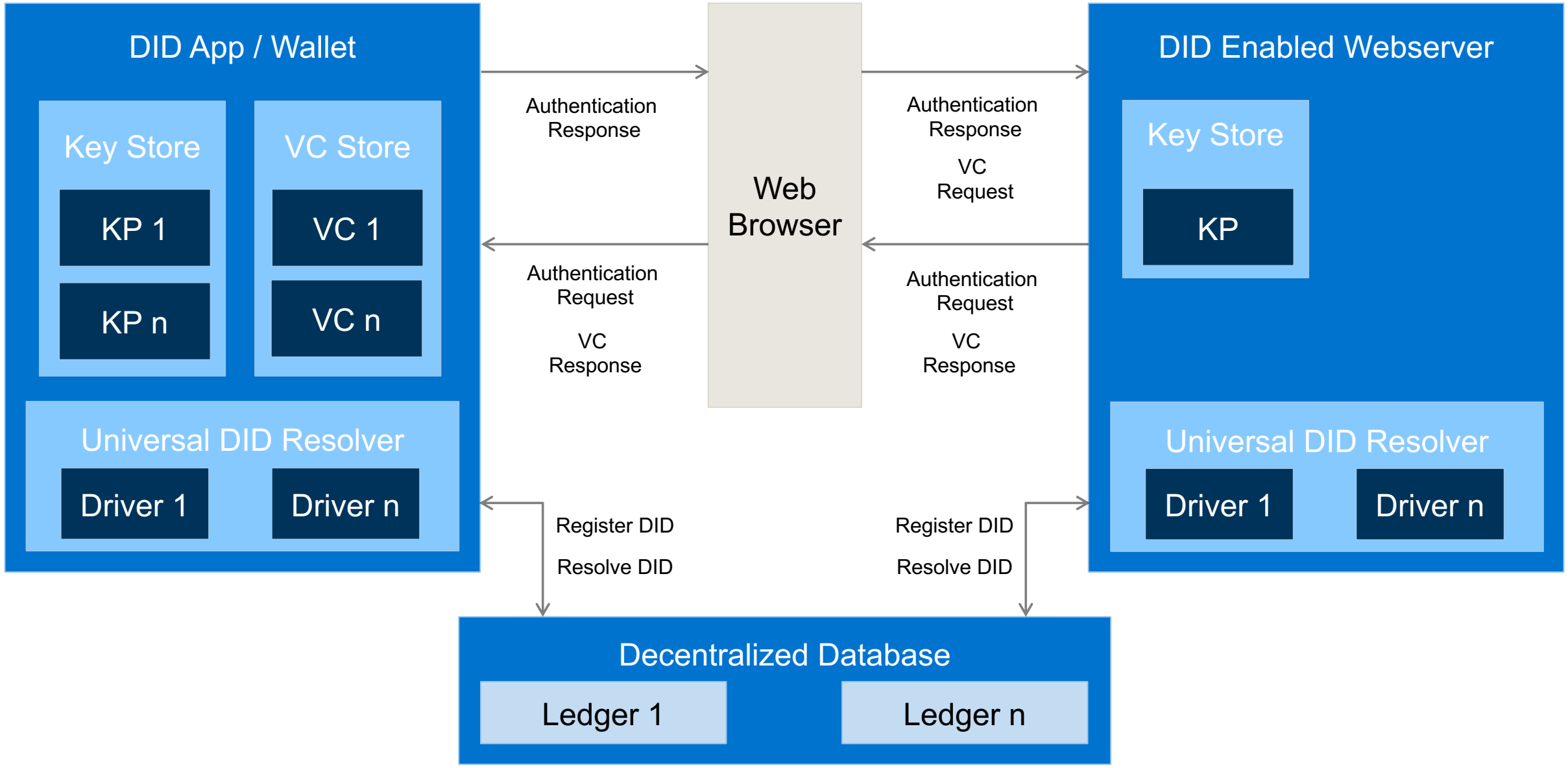
Functional Requirements – Use VCs & VPs



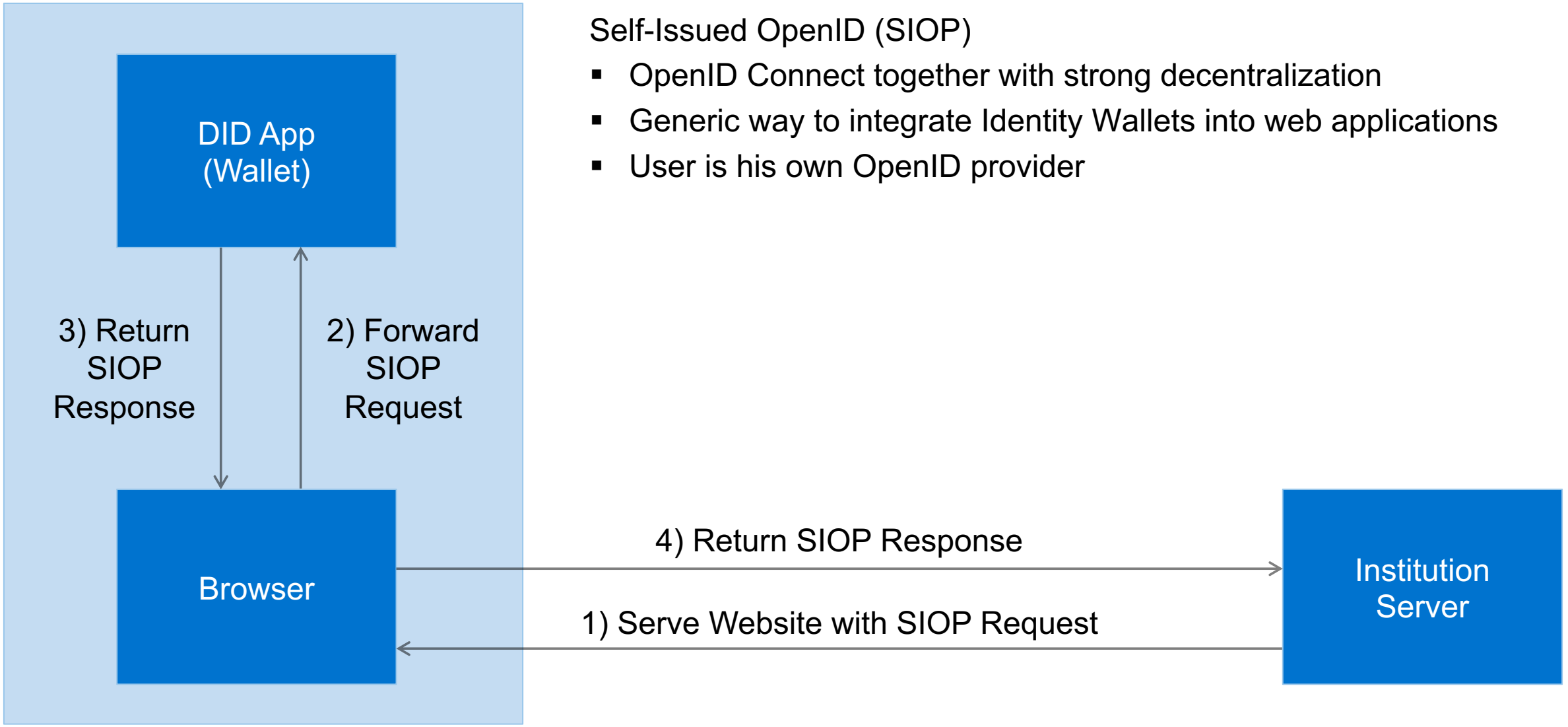
User Story

As a user I can access protected resources, so that I can view them.

Preliminary Architecture



Sequence Diagram – Register & Login



Self-Issued OpenID (SIOP)

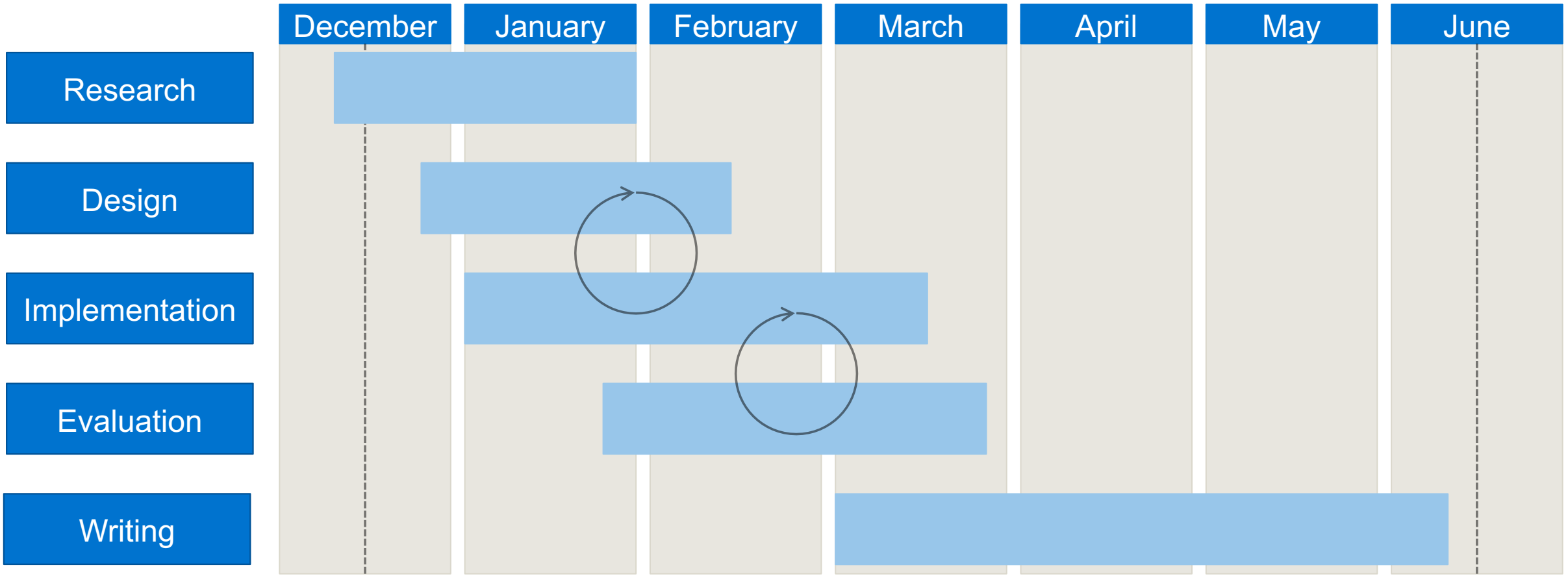
- OpenID Connect together with strong decentralization
- Generic way to integrate Identity Wallets into web applications
- User is his own OpenID provider

Terbu, O., Basart, I., Hartog, K. Den, Lundkvist, C., Stark, D., Zagidulin, D., Strockis, D., and Steele, O. 2019. “Self-Issued OpenID Connect Provider DID Profile.”

Further Expected Results

- **Non-functional Requirements**
- **Process Analysis**: Verifiable Credentials / Verifiable Presentations
- **Implementation** of a minimum viable self sovereign identity network
- **Evaluation** of the implementation against the functional and non-functional requirements
- **Comparison** of the implementation with other authentication methods

Timeline



Registration Date
15. December

Submission Date
15. June

B.Sc.

Kilian Käslin

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289. 17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de