Self-Sovereign Identity - A Proof of Concept

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Gerhard Hassenstein, Prof. Dr. Annett Laube
Expert: Dr. Andreas Spichiger

The need to establish trust and security in the digital world is currently preoccupying governments and organizations worldwide. We have developed and analyzed a prototype based on a new identity management model called self-sovereign identity (SSI).

Problem

The internet is missing an identity layer. Due to that, the unfortunate truth is that identity or the lack of it is one of the primary sources of cybercrime. Therefore, different models for identity management have been developed. Currently, we most widely use centralized or federated identity models due to the excellent user experience. Although, from a privacy and security point of view, they have serious flaws. For example, identity providers can track individuals' actions in their digital lives. Furthermore, the providers are popular targets for attacks because all user data is stored centrally. Moreover, and most importantly, individuals have lost control of their digital identities to identity providers, who can dispose of the identities at will.

Goal

The overall goal of this project was to implement a prototype based on an SSI framework. The prototype must handle a real use case regarding user authentication at the Bern University of Applied Sciences and follow the principles of SSI.

Solution

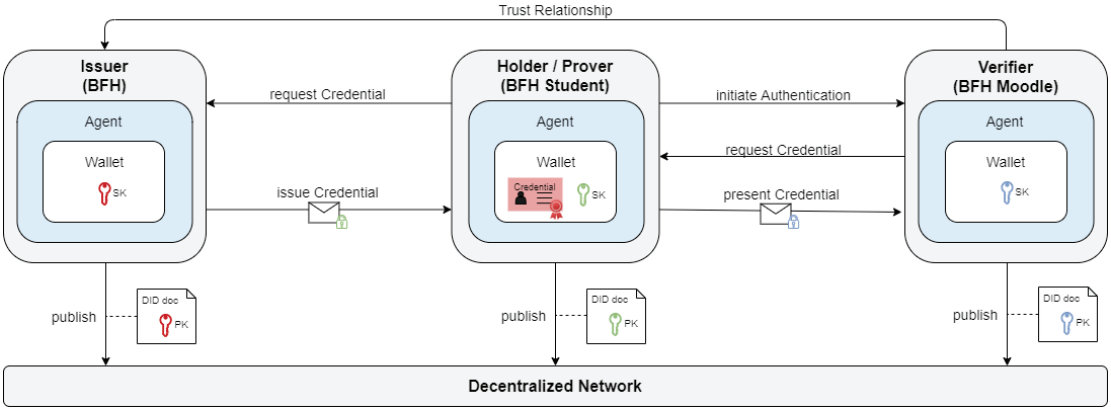
We have implemented our prototype based on the new DID Agent Framework (DAF) from ConsenSys, a company focusing on Ethereum blockchain solutions. We made sure that the prototype follows the principles of SSI. This includes that the user has sole control over his identities and that the identity management system follows a decentralized approach. The figure below illustrates the authentication process of a university member in an SSI environment. For example, students request verifiable credentials from the BFH and store them in their digital wallets. With selective disclosure requests, a BFH web service invites a student to disclose specific information (e.g., credentials). The student presents credentials in the form of a verifiable presentation to the web service, which verifies them, and authenticates the student.

Conclusion

With our prototype, we were able to show that SSI, based on the DAF, enormously improves privacy and security. However, during the analysis, we realized that not all issues are fixed yet, and a malicious issuer/verifier can still correlate user data due to the unique decentralized identifiers. Therefore, we have proposed and implemented a new approach, which uses a different identifier for each verifier.

Martin Scheck

Nicola Schlup



Self-Sovereign Identity - Overview