Data Portability in Self-Sovereign Identity Applications

Student: Merel Steenbergen
Supervisor: Martijn de Vos
Responsible professor: Johan Pouwelse

How can we transfer data from the blockchain of the SuperApp to a third party while ensuring security?

1. Background

Self-sovereign identity

- Self-sovereign identity (SSI) gives users complete control over their data.
- SSI uses decentralized data storage.
- Many believe that SSI will eventually replace the current centralized authentication methods.

TrustChain SuperApp

- Application under development by the Delft Blockchain Lab.
- Uses a blockchain to store data about users in a decentralized way.
- Includes multiple applications, such as a trading application and a music streaming service.

2. The problem of interoperability

Problems

- Other applications must be able to communicate with the SuperApp.
- The protocol must be secure to ensure the subject's privacy. No redundant data should be sent.
- SSI often makes use of verifiable claims and *attested data*, these are limited in the amount of data they can contain.

Public/private key pairs

Can be used to communicate between applications.

Advantages

- Suited for attestations: Can be used for signatures. No information about the identity of the user.
- Secure: Protocols like Pretty Good Privacy could be used.
- Decentralized: Does not require a third party to issue the keys.

Disadvantages

- Can only verify claims, not send additional data.
- Quantum computers might be able to decrypt them.

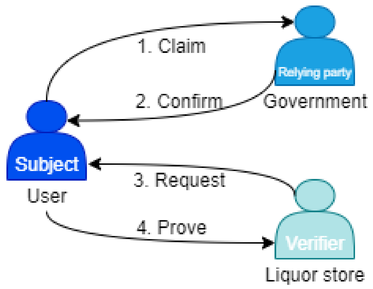
3. Sending attestations

Three parties involved:

- **Subject** to identify themself.
- **Issuer** to support the identity claim.
- **Relying party** requests identification from the subject.

The subject is in full control of the data and who gets access to it.

Flow of attested data



Example use case

1. User claims they are of legal drinking age.
2. The government attests it.
3. Liquor store requests proof of the subject's age.
4. User provides signature (attestation) that the government sent.

4. Communication protocol

5. Engineering Contribution

6. Conclusions and further research