Data Portability in Self-Sovereign Identity Applications

RQ: How can we achieve interoperability in SSI applications while ensuring usability?

1. Background

Self-Sovereign Identity

- User is the only one managing their own data.
- Uses decentralized data storage (blockchain).
- Removes the need to have an account for every service you use.

2. The problem of interoperability

Problem

 Relying parties might use another application than the Super App but must be able to communicate with it in a secure way.

Solution: Verifiable claims

- Advantage: No actual data about the user is sent.
- Disadvantage: Cannot send very extensive data.

3. Communication protocol

- Public/private key pairs are used for encryption to keep data secure.
- A registry of Trusted Issuers (TIs) maintains a list of peers that are allowed to issue certain identities.
- TIs are assigned by Trusted Accreditors, which are listed in a TA registry.
- User data and claims are stored on the device of the user, such that only they can access it.



Delft University of Technology

m.a.steenbergen@student.tudelft.nl

TrustChain SuperApp

- SSI application under development by the Delft Blockchain Lab.
- Built upon **IPv8**: A library for creating distributed applications, based on a P2P-overlay.





4. Framework design

The framework consists of two parts

- A library for the relying party.
- Easy to integrate for developers.
- Connects to IPv8 \rightarrow Becomes a peer in the network.

• An application in the SuperApp.

- Holds the TA and TI, as this is public information.
- Has an overview of requests and attestations.

5 Usability review

Improvements based on user study

- **Rephrase:** claims → requests
- **Rephrase:** attestations → Your data
- Add more information (buttons) on all the screens and the notification.
- Make the distinction between separate items clearer.
- Add more information to the requests: What data was requested?

5. Conclusions and further research

Our framework



Secure Enables interoperability Focus on usability

9:00QBBlockchain Lab
Status: PendingCCBS
Status: SuccessCCBS
Status: SuccessITU Delft
Status: SuccessSSpam account
Status: DeniedGGall&Gall
Status: SuccessGGoogle
Claims

Future work

- Research towards secure data storage.
- Use Verifiable Credentials (access requests) to allow
- peers access to this data storage.
- Our framework can be extended for this purpose, as
 - interoperability and security remain vital.

01-07-2021

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



Mock-ups of user interfaces in the Super App

	Blockchain Lab Status: Pending 22-06	2021	Driver's license B Attested by: CBS 15-06-2021
	C CBS Status: Success 22-06	-2021	Age over 18 Attested by: Rijksoverheid 14-06-2021
	Blockchain Lab Requests access to the following TU Delft enrollment	claim t	TU Delft enrollment Attested by: TU Delft 10-06-2021
	Allow access Deny a Status: Derved 20-00	szazi	Driver's license A Attested by: CBS 03-06-2021
1	G Gall&Gall Status: Success 18-00	6-2021	Albert Heijn employee Attested by: Albert Heijn 18-05-2021
ions	G Google Claims Atte	estations	Credit card possession



Blockchain-lab.org