Privacy-preserving Techniques for EU Digital Identity Wallets

Advisor: **Stefan More**

Motivation

The emerging Self-Sovereign Identity (SSI) and Decentralized Identity models indicate a shift in how individuals control and share their personal data. In this model, data is stored within Digital Identity Wallets, e.g., on the user's phone. Using this wallets, individuals have autonomy over their identity data without intermediaries.

However, with this empowerment comes an elevated responsibility: ensuring the privacy of such data. As users engage with various online services, they present and expose snippets of their identity from digital identity wallets, creating potential avenues for unintended data leakage or malicious exploitation.

Privacy-preserving exist to mitigate this issue.

Goals and Tasks

- Investigate current privacy proposals for EU wallets
- Develop a prototype for Austria's demo wallet
- Validate and evaluate the proposed mechanism

Literature

- C. Paquin, G.-V. Policharla, et al.
  Crescent: Stronger Privacy for Existing Credentials
  https://eprint.iacr.org/2024/2013
- M. Frigo and abhi shelat
  Anonymous credentials from ECDSA
  https://eprint.iacr.org/2024/2010
- J. Miranda et al.
  Specification for ZKP Implementation in EUDI Wallet
  https://s.2904.cc/arf-zkp

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE

Prerequisites

- Interest in privacy
- Programming skills (e.g., Kotlin)

Advisor Contact

smore@tugraz.at