IAIK | Institute of Applied Information Processing and Communications

Lightweight Trust Verification on Constrained Devices using Zero-Knowledge Proofs

Advisor: **Stefan More**

Motivation

Electronic credentials can be used to authorize a person to access a resource. The entity verifying the credentials uses a policy to decide if the credentials provided by the user are trustworthy, and thus if access should be granted. This entity can not only be a person or website, but also a device.

Sometimes the device executing such a policy has limited computational resources – think about an access gate or car sharing. Additionally, it is not always possible to connect to the Internet during verification.

Goals and Tasks

In this project we look into one strategy to free the verifying device from the heavy task of executing a policy. By using **lightweight zero-knowledge proofs** we let the user do the work by themselves.

- Understand SSI concepts
  and the concept of a policy language
- Construct a suitable zero-knowledge proof
- Implement prototype of idea
- Perform benchmarks and compare approaches

Literature

- G. Noble et al.
  Verifiable Credentials Data Model 1.0
  W3C Recommendation
  https://www.w3.org/TR/vc-data-model
- A. Abraham et al.
  Revocable and Offline-Verifiable Self-Sovereign Identities
  Trustcom 2020
- xjsnark: A high-level framework for developing efficient zk-SNARK circuits
  https://github.com/akosba/xjsnark

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Java programming
- Understanding of cryptography
- Basic understanding of blockchains/distributed ledgers is beneficial

Advisor / Contact

stefan.more@iaik.tugraz.at