

Motivation

Data protection is committed to the protection of personal data. If the anonymity of a person should be guaranteed during conducting a survey, the surveyor is required to perform some legal duties. Survey data can be considered anonymous if an assignment to a person is not possible or only possible under a considerable and disproportionate amount of time, expense and manpower.

The aim of this project is to establish a trust management to authenticate and authorize smartphone users for consuming a service (for example an anonymized survey), in which no third party can identify a person via his or her personal data. To make this possible, an Identity Escrow should be implemented, where users have to initially authenticate themselves and perform a cryptographic binding. This binding will be used for the anonymous authentication and verification processes when the user wants to perform a survey at a Service Provider.

This topic is scalable from bachelor's to master's thesis. We can arrange and adjust the scope according to your scheduled effort, interests, and ideas.

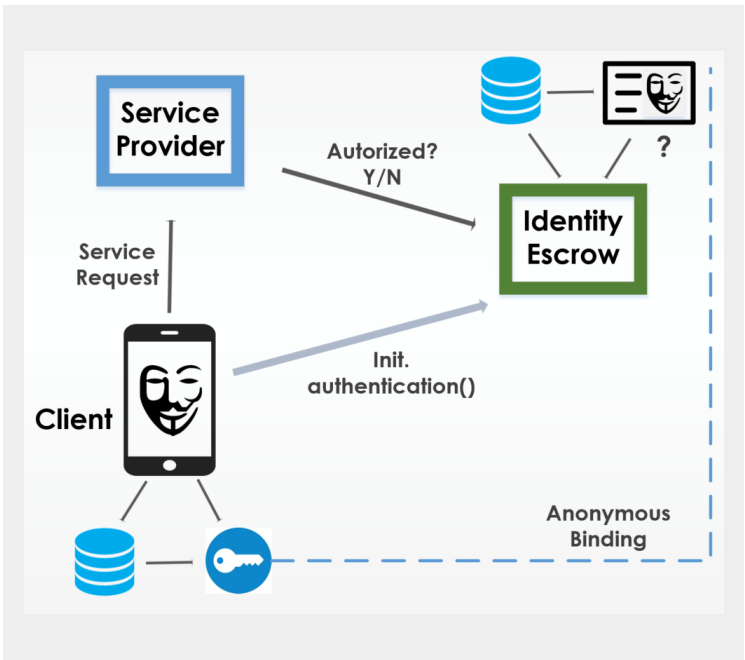
Goals and Tasks

- ▶ Create and analyze a concept for a Mobile Identity Escrow based on state-of-the-art technologies
- ▶ Implement the components (IDP, SP, client) in order to establish a minimal proof-of-concept

Literature

Jan Camenisch et al.
An Identity Escrow Scheme with Appointed Verifiers
Advances in Cryptology - CRYPTO 2001

Figure



Deliverables

- ▶ Project files (zip, cleaned)
- ▶ Documentation (pdf)
- ▶ Presentation (pdf)

Studies

- INF
- TEL
- SW

Prerequisites

- ▶ Interest in cryptography
- ▶ Interest in identity management
- ▶ Programming skills (+ mobile app development)

Advisor / Contact

kevin.theuermann@egiz.gv.at