

# Comparison of Anonymous Credential Systems

## Motivation:

Transactions of electronic devices can be easily traced e.g. tracking of cars via road pricing systems, tracking of people's movement via access control systems or monitoring access logs of web servers. Cryptographic methods preventing this have been developed recently and are waiting to be investigated for use in practical applications.

## Project description:

The idea of this project is to compare different anonymising techniques concerning performance and privacy protection.

The algorithms should be implemented in C and/or Java and should work on different mobile and embedded devices such as smart cards and cell phones. Moreover, a proof-of-concept demonstrator should be developed that shows how anonymous authentication can be used for example with RFID based access control systems.

## Tasks:

- Understand the principles of state-of-the-art cryptographic anonymisation algorithms
- Get familiar with the develop environment and development tools
- Design and implement the algorithms plus required support services
- Write a report comparing the different algorithms and implementations



## Master Project

**Participants:** 1-2 Students

## Prerequisites:

- Experience with C & Java software development
- Crypto 1 & Crypto 2 Lectures

**Contact:** [Kurt.Dietrich@iaik.tugraz.at](mailto:Kurt.Dietrich@iaik.tugraz.at)

**Studies:**  INF  SEW  TEL  Master Thesis

The master project can be continued as master thesis.