



Digital Identities on Mobile Devices



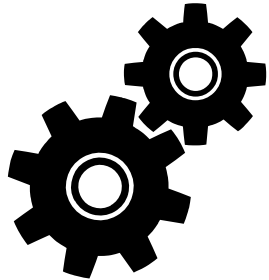
ID-Management Group

ID-Management Group

- led by Prof. Dr. Marian Margraf
- Secure Software Engineering (Fraunhofer AISEC)
- close collaboration / joint projects
- staff: ~ 20 people (research assistants, PhD students, student assistants, management staff)

Research Focus

- Post-Quantum Crypto
- Secure Coding
- Information Security Management
- Usable Security / Privacy
- Identity Management
- Cryptanalysis
- Design of Cryptosystems
- Mobile Security
- Physical Unclonable Functions



Mobile ID Concept

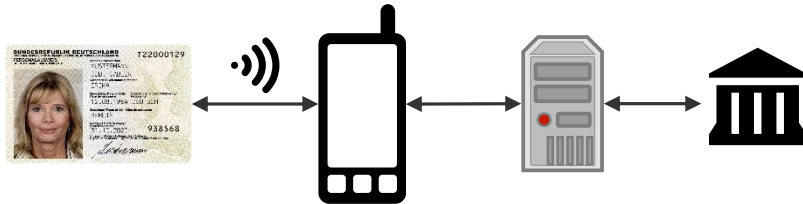
Digital Identity – Definition

“An eID is a sub-representation of a person's analog identity in the digital world.”

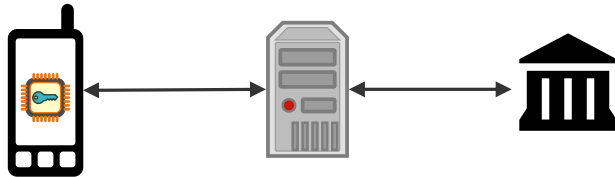
“For their holders, the aim is to be able to prove in the digital world that they are who they claim to be.”

Current Solutions & Problems

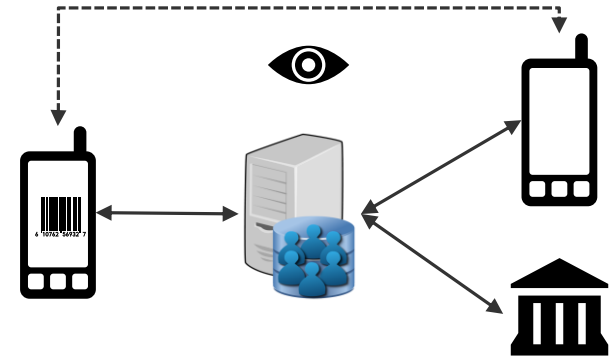
German eID



Mobile ID – OPTIMOS2



My Identity App (MIA)



various others...

Research Question

*Is it possible to **securely distribute, store and use** a digital identity, also known as an **electronic identity (eID)**, on a **smartphone**?*

- only the platform's own security mechanisms may be used
- focus lies on smartphone only

Requirements

Verification of Authenticity

Non-cloneability & Non-extractability

Proof of Holdership

Secure eID Process

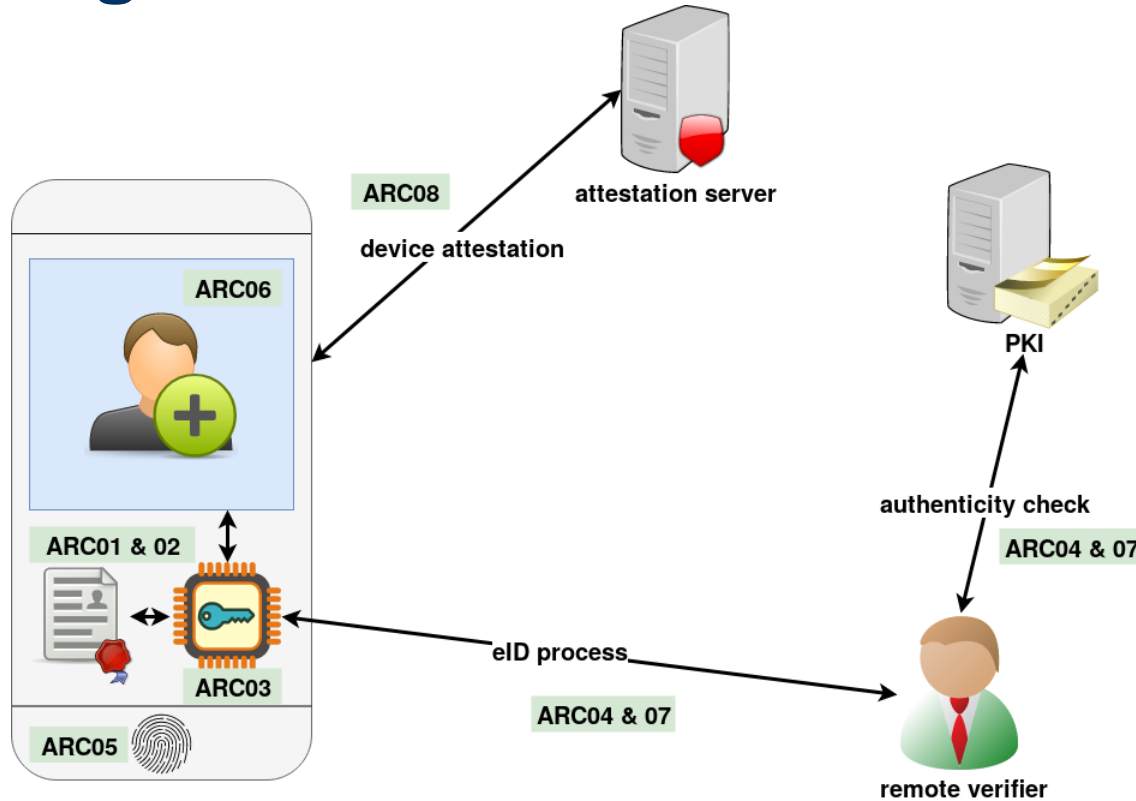


Data Minimization

Binding to Holder

Transaction Consent by Holder

High Level Architecture



- ARC01** Verification of Authenticity
- ARC02** Proof of Holdership
- ARC03** Non-cloneability & Non-extractability
- ARC04** Secure eID Process
- ARC05** Binding to Holder
- ARC06** Transaction Consent by Holder
- ARC07** Data Minimization
- ARC08** Platform Integrity

REQ -> ARC	Android	iOS
Verification of Authenticity	PKI	PKI
Proof of Holdership	KeyStore	Keychain
Non-cloneability & Non-extractability	TEE / SE via KeyStore	(Secure Enclave)
Secure eID Process	✗	✗
Binding to Holder	BiometricPromt	Touch ID / Face ID
Transaction Consent by Holder	(BiometricPromt)	(Touch ID / Face ID)
Data Minimization	X.509v3 & Hashing	X.509v3 & Hashing
Platform Integrity	SafetyNet	✗



Proof-of-Concept

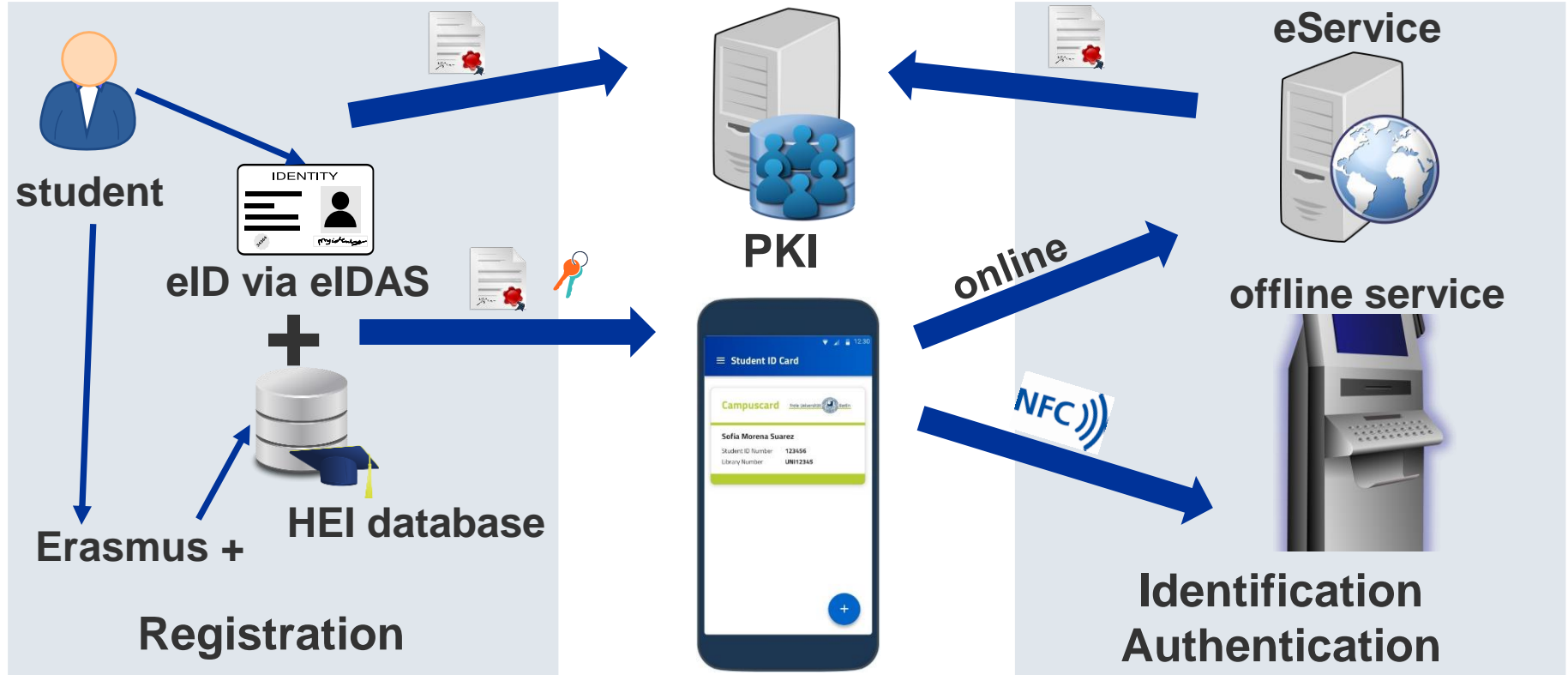
Erasmus Student eCard - Overview



Mobile student card for various **online** and **offline** use cases:

- **secure:** usage of standardized and well established protocols and security mechanisms
- **privacy-friendly:** student's attributes are stored locally on the smartphone, student decides which attributes are shared with a remote party
- **easy integration:** use as a standalone app or as a module in an existing campus app, integrate third-party cards (e.g. ESNcard, ISIC)

Erasmus Student eCard - Architecture



Short Summary

1. What is a digital identity?
2. What are the problems and challenges?
3. Reference architecture (high level & platform specific)
4. Proof-of-Concept: Erasmus Student eCard

Contact Us



Tim Ohlendorf
Research Assistant
ID-Management Group
Freie Universität Berlin
tim.ohlendorf@fu-berlin.de

Wolfgang Studier
Research Assistant
Secure Systems Engineering
Fraunhofer AISEC
wolfgang.studier@aisec.fraunhofer.de