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

Secure eID Process

Binding to Holder

Transaction Consent by Holder

Proof of Holdership

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

- eID via eIDAS
- HEI database
- PKI
- eService

Registration

Identification

Authentication
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