SLIDEDroid: A SECURE LIGHTWEIGHT IDENTITY FOR THE ANDROID PLATFORM

31st Crypto Day, 17/18 October 2019
Tim Ohlendorf and Wolfgang Studier
Methodology

current problems → assessment of existing technology → reference architecture → PoC → security & privacy aspects
current problems → assessment of existing technology → reference architecture → PoC → security & privacy aspects
Current Problems of Mobile eIDs

- „local storage“ approaches:
  - no security
  - software-based security
  - hardware-backed security
    - Secure Element
    - Trusted Execution Environment

- „cloud-based“ approaches:
  - only "auth_token" on device
  - identity attributes at IdP

➤ security / privacy vs. usability / market coverage

(Träder et al. [TZH17], Ohlendorf et al. [OSM19])
current problems → assessment of existing technology → reference architecture → PoC → security & privacy aspects
Student ID Card: Android Platform Security Features

KeyMaster

![Android Logo] (ROBO)

SafetyNet Attestation

![Certificate and Mobile Phone] (CERT, KEY)

Software based

Key & ID Attestation

![Certificate, Key, and Mobile Phone] (CERT, KEY)

TEE/SE based

Biometric Prompt

![Biometric Prompt Image]
Proposed Architecture

- derived eID
- PKI-based infrastructure
- certificates with identity attributes (X.509)
- mTLS for identification & authentification
- secure deployment mechanism
- only standardized HW security components used
current problems → assessment of existing technology → reference architecture → PoC → security & privacy aspects
Proof-of-Concept: Student ID Card

eID Derivation

Management & Maintenance

Identification & Authentication
Student ID Card Deployment: Provisioning process

- TAN Number: 123456
- Insert TAN number into the Mobile ID verification page of your university.
- Where can I find this page?
- TLS
- TAN
Student ID Card Deployment: Personalization process

TAN

registration website

mTLS

nonce

TAN

TLS

TAN
Student ID Card: Identification /Authentication process

- **mTLS**
- **TLS**

1. Touch the fingerprint sensor with your finger to authorize the exam.
Student ID Card: Hashed Attributes

... name: hash(name|salt_1)
surname: hash(surname|salt_2)
date of birth: hash(d.o.b.|salt_3)
student ID: hash(student ID|salt_4)
...

ame: (name, salt_1)
student ID: (student ID, salt_4)
current problems → assessment of existing technology → reference architecture → PoC → security & privacy aspects
Security & Privacy Aspects

security
+ local eID
+ standardized, well-established protocols
+ hardware-backed security
- local MITM attacker scenario
- no secure I/O

privacy
+ data economy
- unique ID
- user tracking (TLS 1.2)
- bruteforcing of attributes
- SP can sell verified identity attributes
current problems → assessment of existing technology → reference architecture → PoC → security & privacy aspects
Conclusion & Future Work

- current solutions → security / privacy vs. usability / market coverage
- SLIDEDroid secure lightweight identity solution for Android
- Proof-of-Concept → Student ID Card
- security / privacy evaluation → still some shortcomings remain
- analyze shortcomings and suggest possible solutions
- evaluate SLIDE on iOS
Secure Systems Engineering
Fraunhofer AISEC
Berlin, Germany
Resources


- **CERT**  [https://thenounproject.com/icon/89083/](https://thenounproject.com/icon/89083/), Nice and Serious

- **KEY**  [https://svgsilh.com/image/149030.html](https://svgsilh.com/image/149030.html), svgsilh.com