# SLIDEDroid: A SECURE LIGHTWEIGHT IDENTITY FOR THE ANDROID PLATFORM

31st Crypto Day, 17/18 October 2019

Tim Ohlendorf and Wolfgang Studier

Fraunhofer

AISEC

# Methodology


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

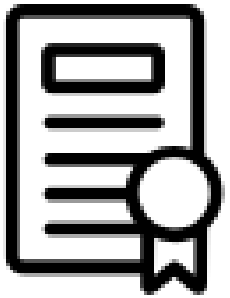
## KeyMaster

TEE

SE

(ROBO)

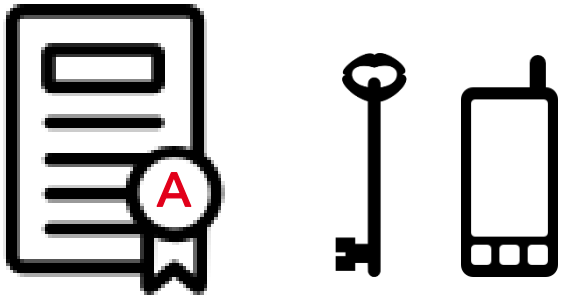
## SafetyNet Attestation



Software based

(CERT, KEY)

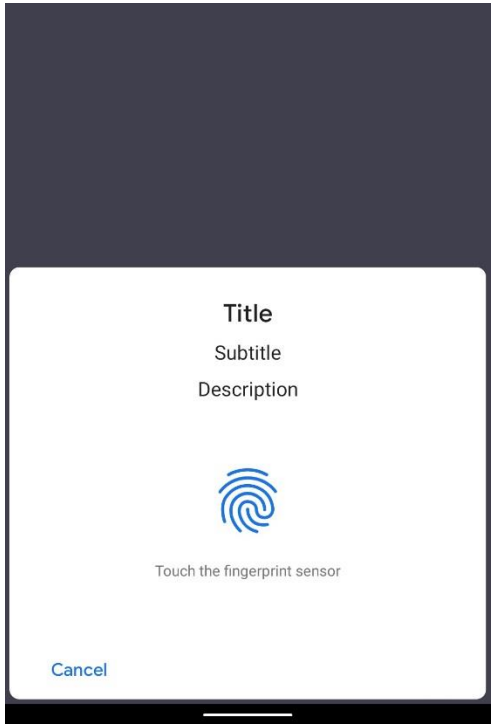
## Key & ID Attestation




TEE/SE based

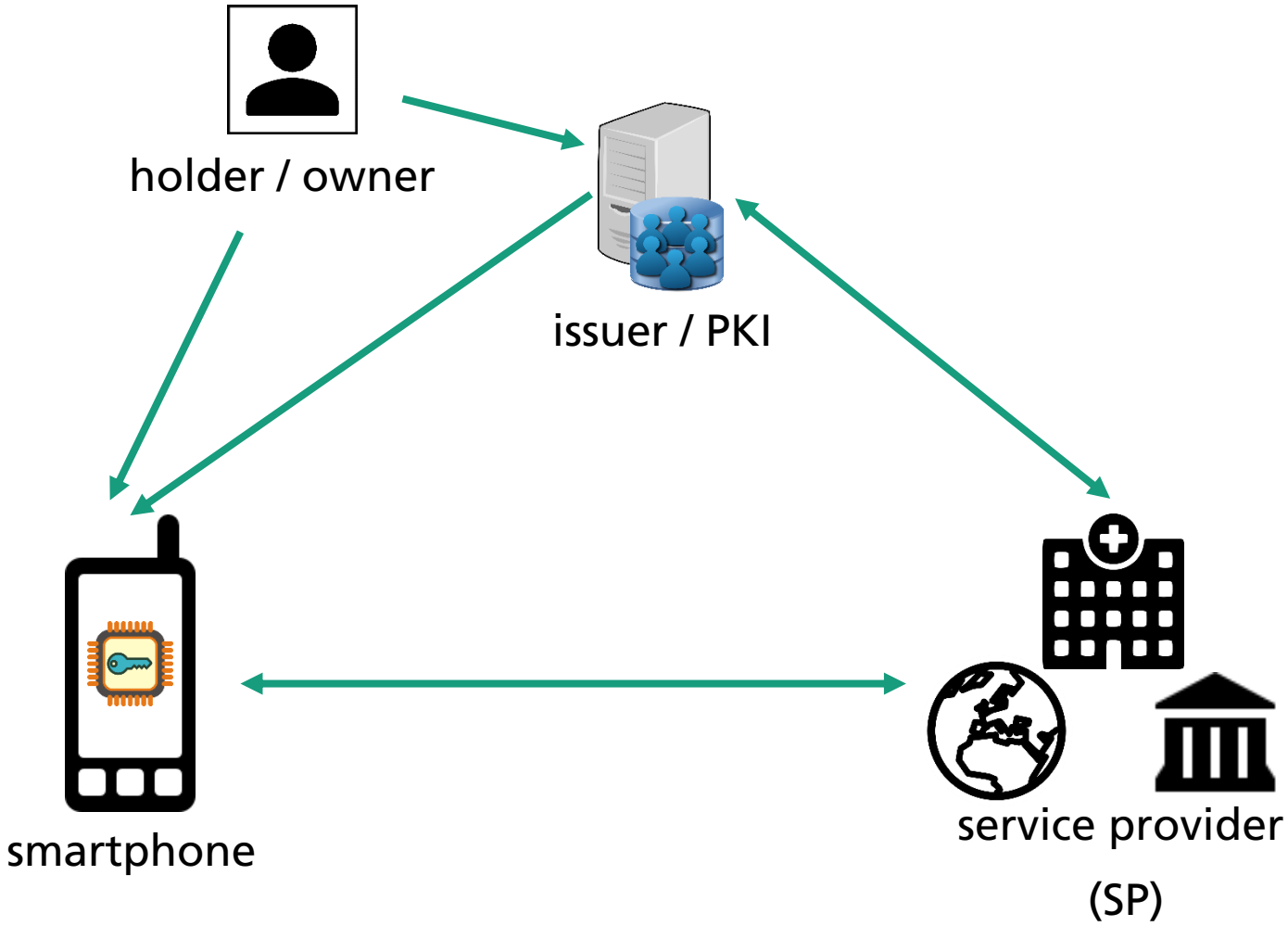
(CERT, KEY)

## Biometric Prompt




current problems
assessment of existing technology
reference architecture
PoC
security & privacy aspects

# Proposed Architecture



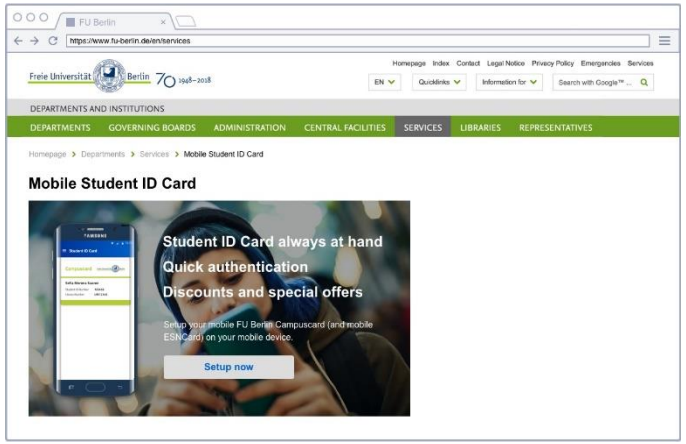

- derived eID
- PKI-based infrastructure
- certificates with identity attributes (X.509)
- mTLS for identification & authentification
- secure deployment mechanism
- only standardized HW security components used


current problems
assessment of existing technology
reference architecture
PoC
security & privacy aspects

# Proof-of-Concept: Student ID Card

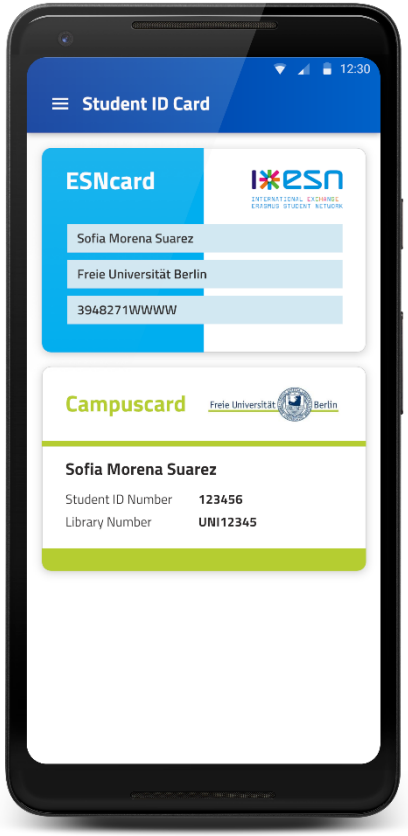
StudIES+
Co-financed by the Connecting Europe Facility of the European Union

## eID Derivation

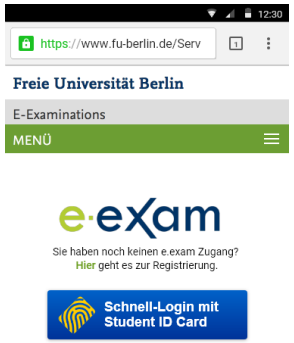


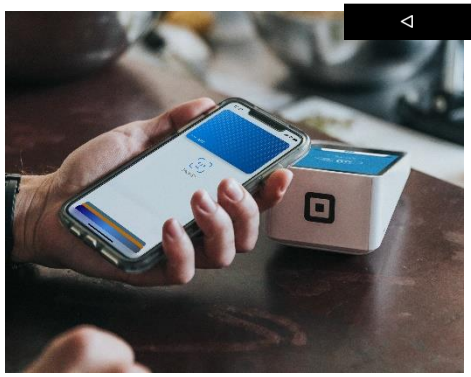


## Management & Maintenance




## Identification & Authentication

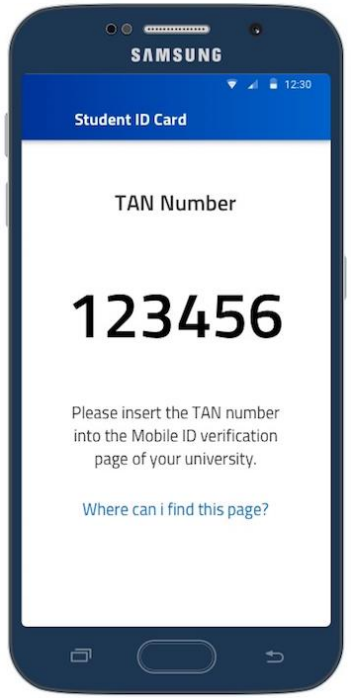


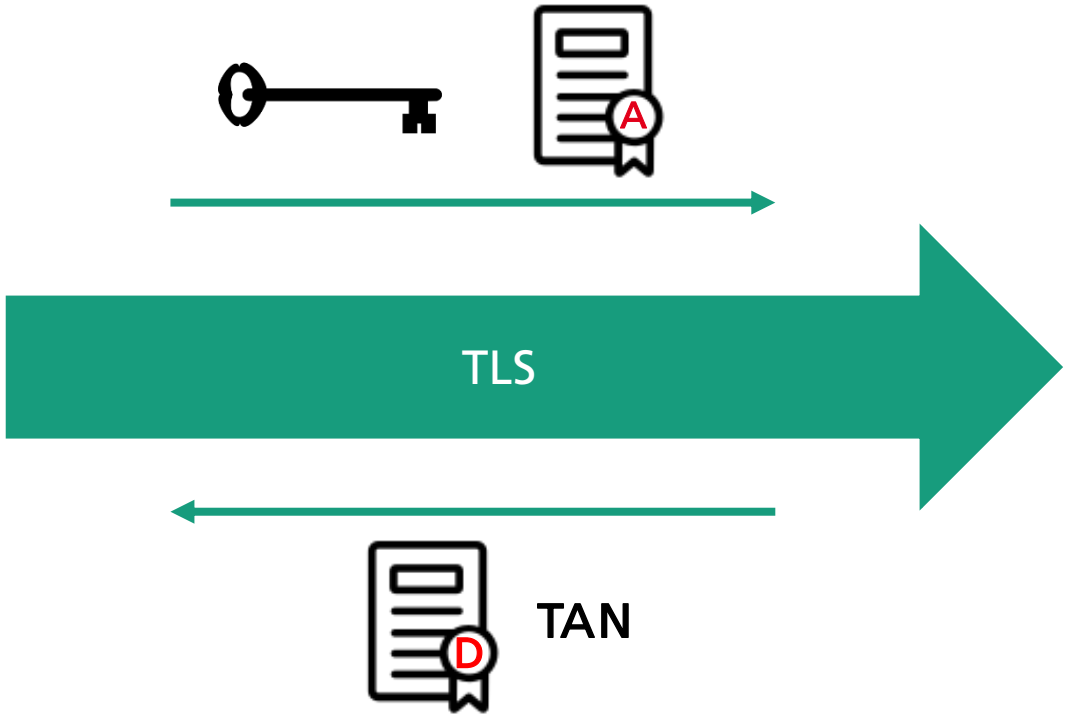





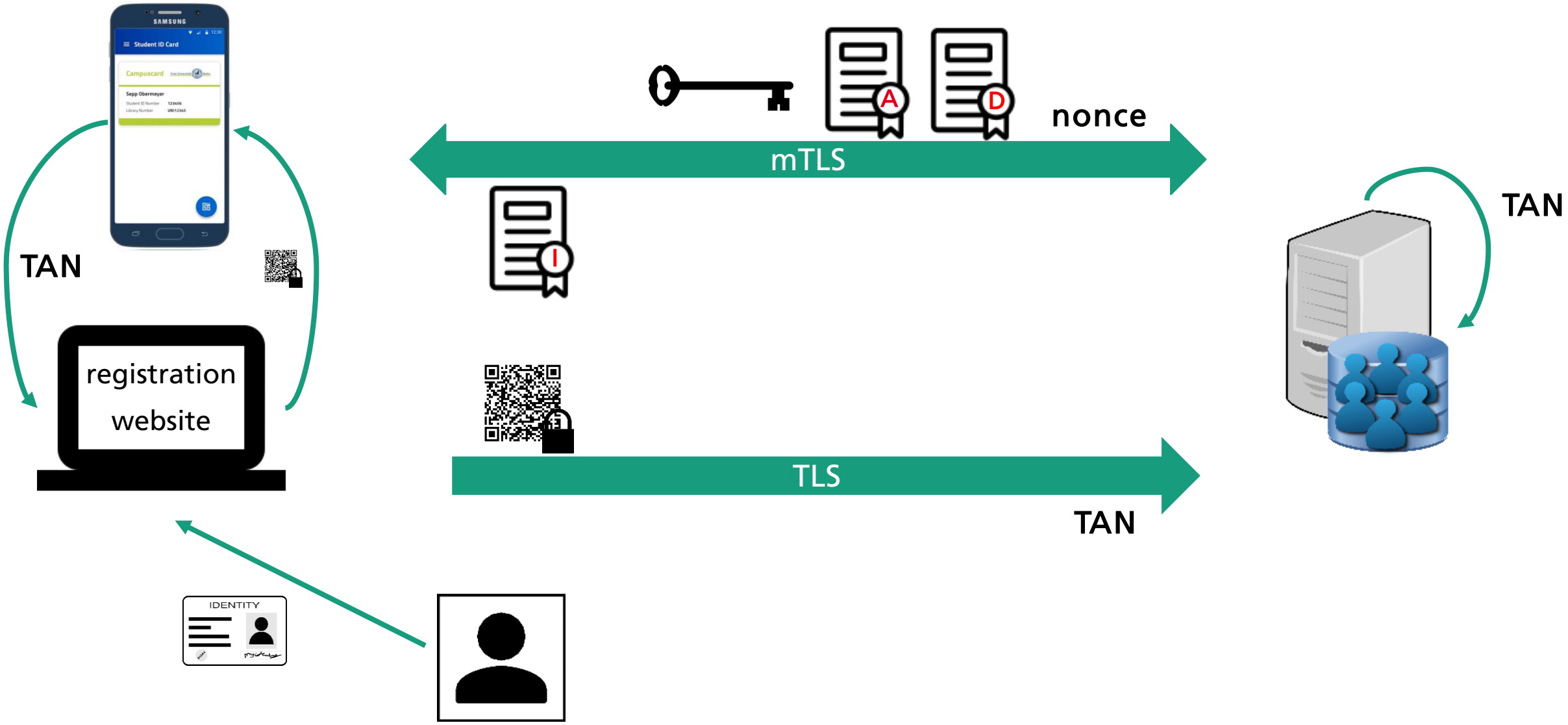
Fraunhofer AISEC

# Student ID Card Deployment: Provisioning process

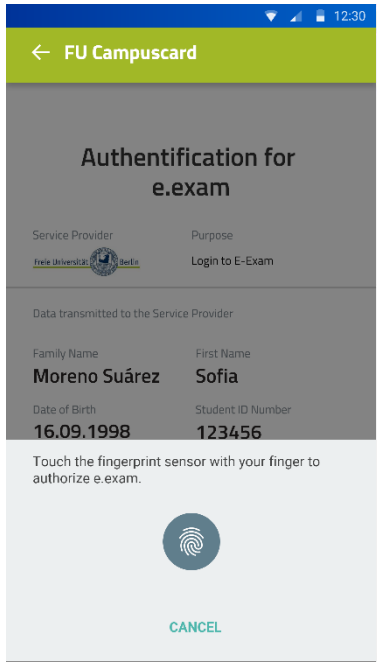


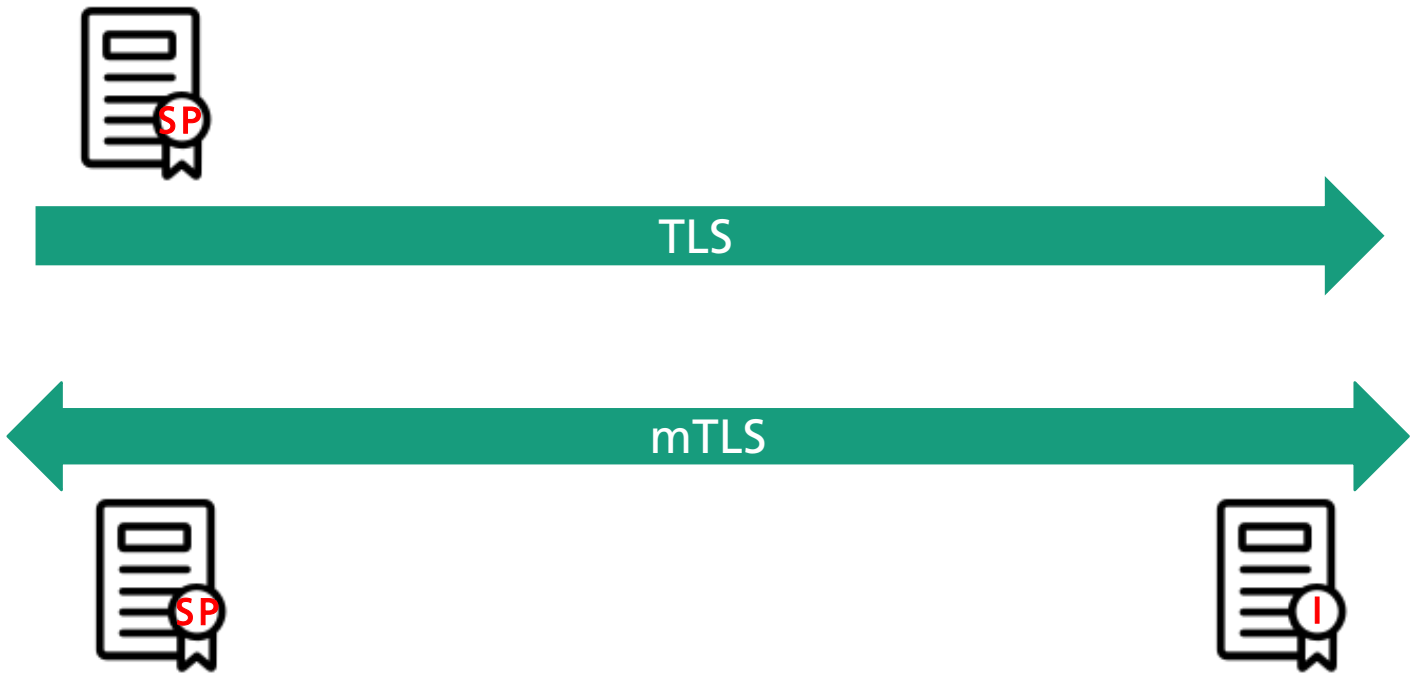




# Student ID Card Deployment: Personalization process



# Student ID Card: Identification /Authentication process

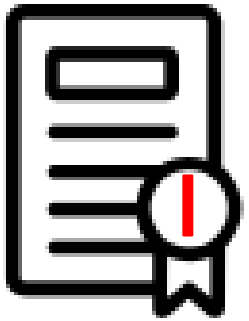





Fraunhofer AISEC

# Student ID Card: Hashed Attributes



…

| | |
|---|---|
| name: | hash(name\|$salt_1$) |
| surename: | hash(surename\|$salt_2$) |
| date of birth: | hash(d.o.b.\|$salt_3$) |
| student ID: | hash(student ID\|$salt_4$) |

…

| | |
|---|---|
| name: | (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

# Contact US

**Tim Ohlendorf**
tim.ohlendorf@aisec.fraunhofer.de

**Wolfgang Studier**
wolfgang.studier@aisec.fraunhofer.de

**Secure Systems Engineering**
Fraunhofer AISEC
Berlin, Germany

# Resources


- TZH17 Daniel Träder, Alexander Zeier, and Andreas Heinemann. Design and Implementation Aspects of Mobile Derived Identities. In: Open Identity Summit 2017 (2017).
- OSM19 Tim Ohlendorf, Wolfgang Studier, and Marian Margraf. Digitale Identitäten auf dem Smartphone. In: Datenschutz und Datensicherheit-DuD, Band 43 (2019)
- ROBO https://developer.android.com/distribute/tools/promote/brand.html, Google Inc.
- CERT https://thenounproject.com/icon/89083/, Nice and Serious
- KEY https://svgsilh.com/image/149030.html, svgsilh.com
- LAPTOP http://togotv.dbcls.jp/ja/togopic.2017.26.html, DataBase Center for Life Science