Smart-eID – Sicherheitskonzept

@ TeleTrusT-Konferenz 2021

Datum: 25.11.2021
Ort: Berlin
Verfasser: Dr. Matthias Schwan (Technology – Mobile Security)

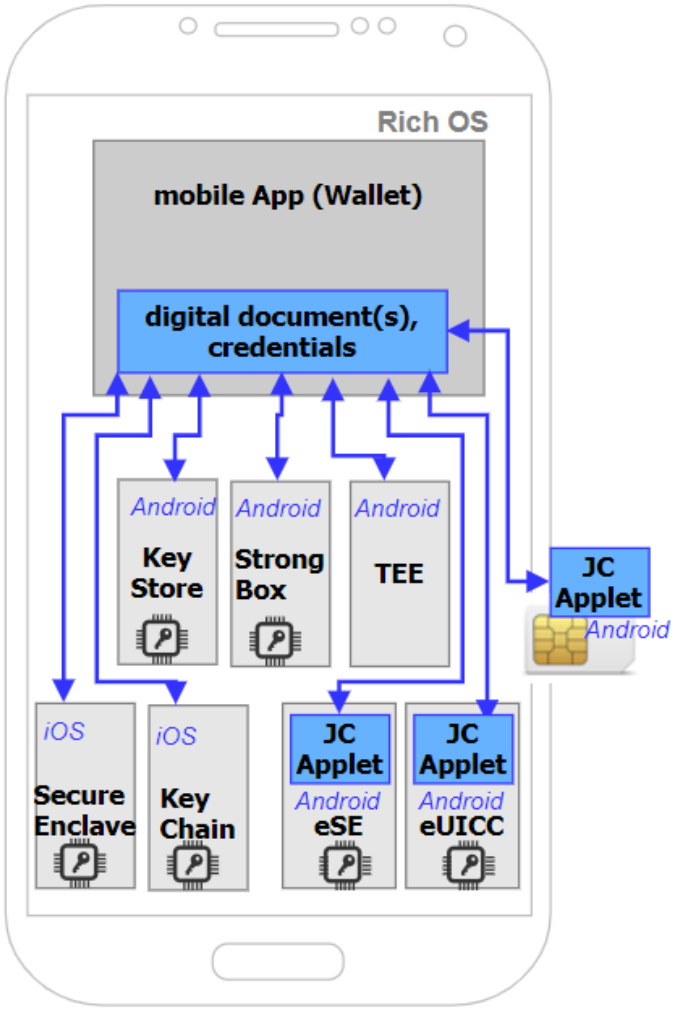
1. **Elektronische ID-Dokumente**
2. **Anforderungen für mobile ID-”Dokumente”**
3. **Smart-eID: Trusted Service Manager (Demo)**
4. **Internationale Standardisierungs-Aktivitäten**

eID-Dokumente

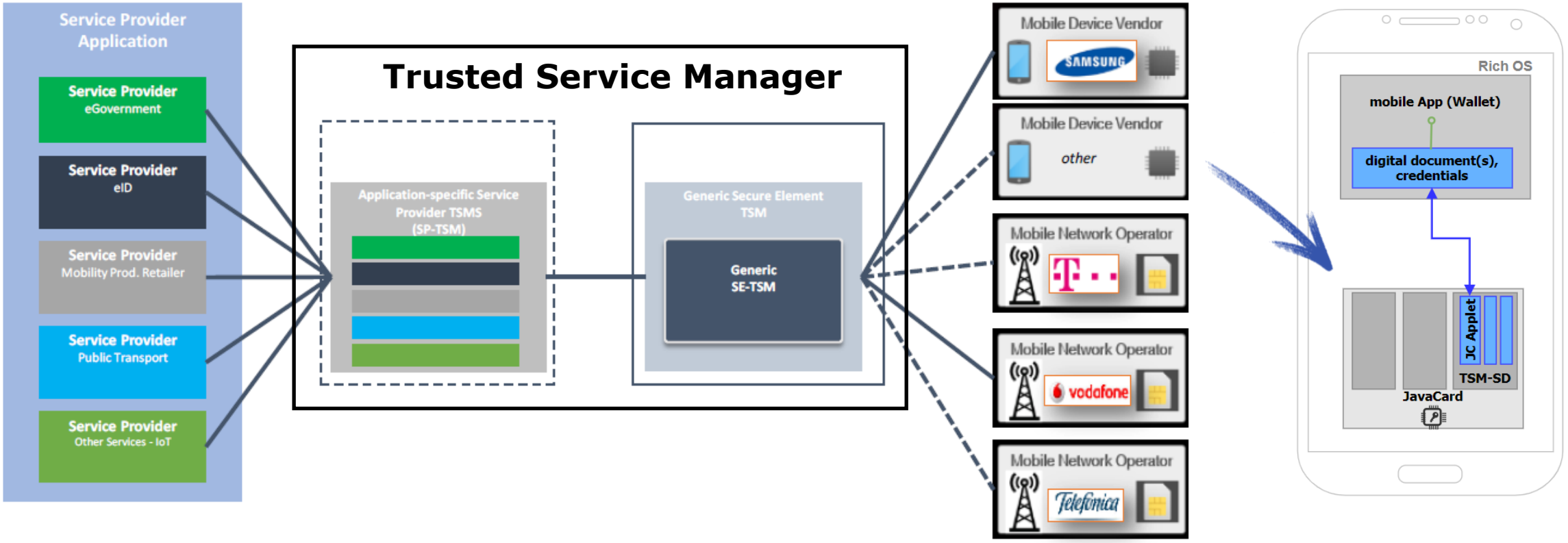
- Chip des elektronischen ID-Dokuments enthält elektronische Daten
- Chip ist physisch mit dem ID-Dokument verbunden
- Elektronische Daten sind durch kryptografische Mittel an den Chip gebunden
- Klonschutz durch Chip-Architektur (in der Regel sicherheitszertifiziert)
- Elektronisches ID-Dokument ist Authentifizierungsfaktor des **"Besitzes"**

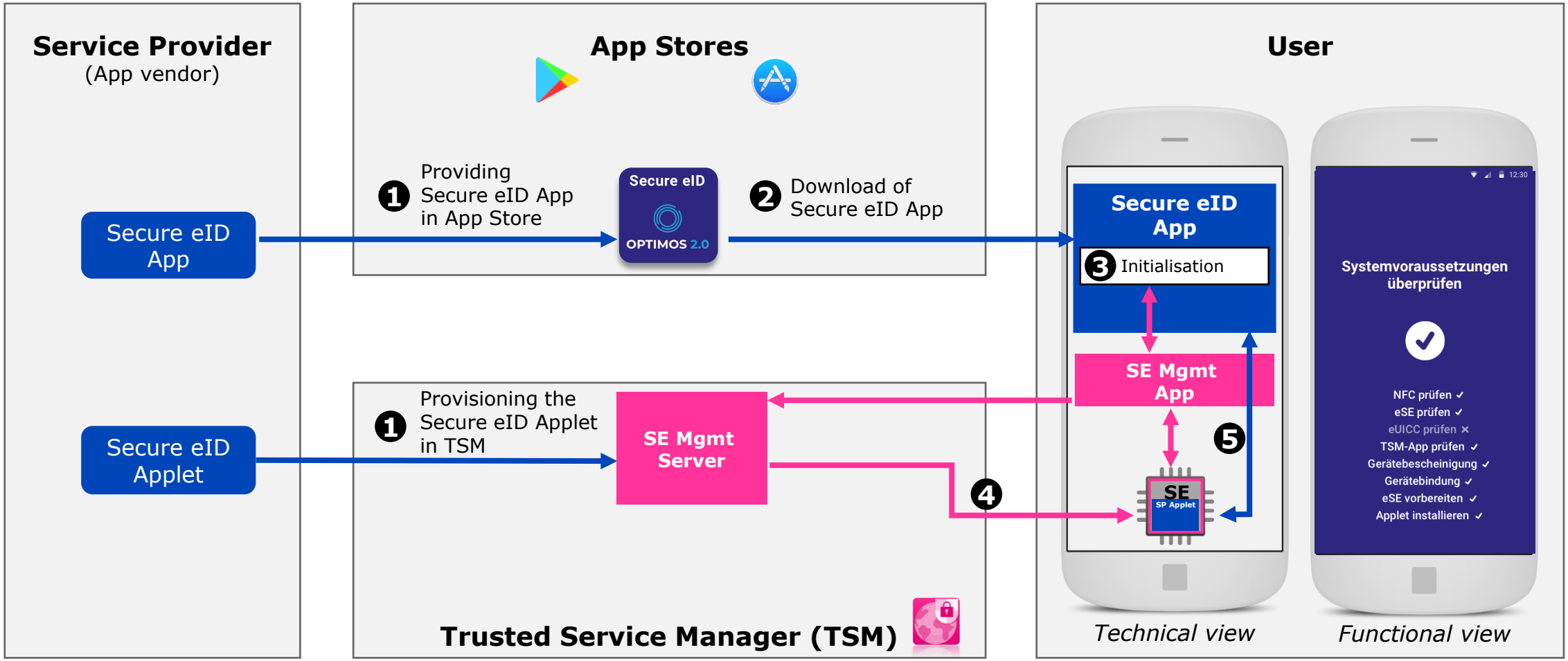
Mobile eID-Dokumente

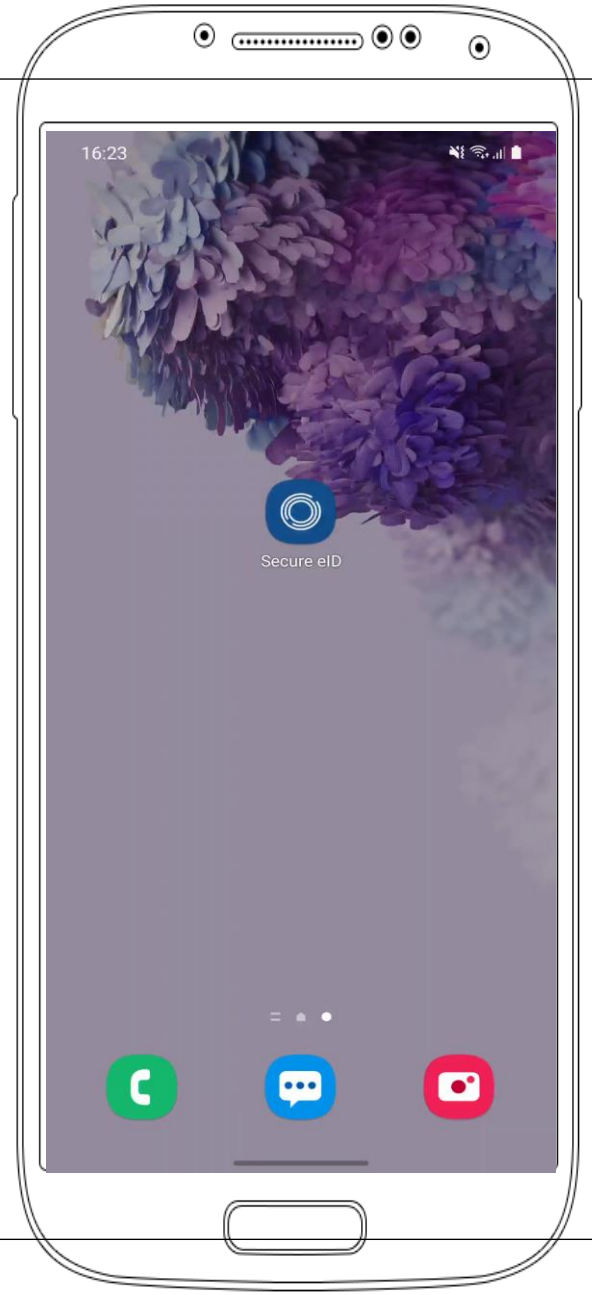
- Mobiles Gerät wird zum "Faktor des Besitzes"
- Mobiles Gerät übernimmt die Rolle des Chips in elektronischen ID-Dokumenten
- (Online-)Identifizierung erfordert kein elektronisches ID-Dokument, sondern ein mobiles Gerät
- Wo und wie ist das kryptografische Material zu speichern, um Kopier- und Manipulationsschutz zu gewährleisten?



- Mobiles Gerät wird zum „Faktor des Besitzes”
- **Sicherheitsanforderung:**
  - manipulationssichere Speicherung der kritischen Daten
  - Zugriffsschutz für kritische Daten (zweiter Authentisierungsfaktor: Wissen / Biometrie)
- **Datenschutzanforderung:**
  - Sichere Speicherung der persönlichen Daten (wenn im Mobilegerät abgelegt)
- **Vertrauenswürdigkeit** des Ausstellers in die verwendete Technologie
- Anforderungen sind unabhängig von ID-Technologie, z.B.
  - Mobiler Führerschein nach ISO 18013-5
  - Digitaler Reisepass nach ICAO Doc 9303
  - eIDAS-Token nach ANSSI/BSI TR-03110
  - Gesundheitskarten nach gematik-Spezifikationen
  - SSI-Credentials nach W3C Spezifikationen


Service Provider Application
Service Provider eGovernment
Service Provider eID
Service Provider Mobility Prod. Retailer
Service Provider Public Transport
Service Provider Other Services - IoT
Trusted Service Manager
Application-specific Service Provider TSMS (SP-TSM)
Generic Secure Element TSM
Generic SE-TSM
Mobile Device Vendor
SAMSUNG
Mobile Device Vendor
other
Mobile Network Operator
Mobile Network Operator
vodafone
Mobile Network Operator
Telefónica
Rich OS
mobile App (Wallet)
digital document(s), credentials
JC Applet
TSM-SD
JavaCard


Service Provider
(App vendor)
Secure eID App
Secure eID Applet
App Stores
1 Providing Secure eID App in App Store
Secure eID
OPTIMOS 2.0
2 Download of Secure eID App
1 Provisioning the Secure eID Applet in TSM
SE Mgmt Server
Trusted Service Manager (TSM)
User
Secure eID App
3 Initialisation
SE Mgmt App
4
5
SE
SP Applet
Technical view
Systemvoraussetzungen überprüfen
NFC prüfen
eSE prüfen
eUICC prüfen
TSM-App prüfen
Gerätebescheinigung
Gerätebindung
eSE vorbereiten
Applet installieren
Functional view

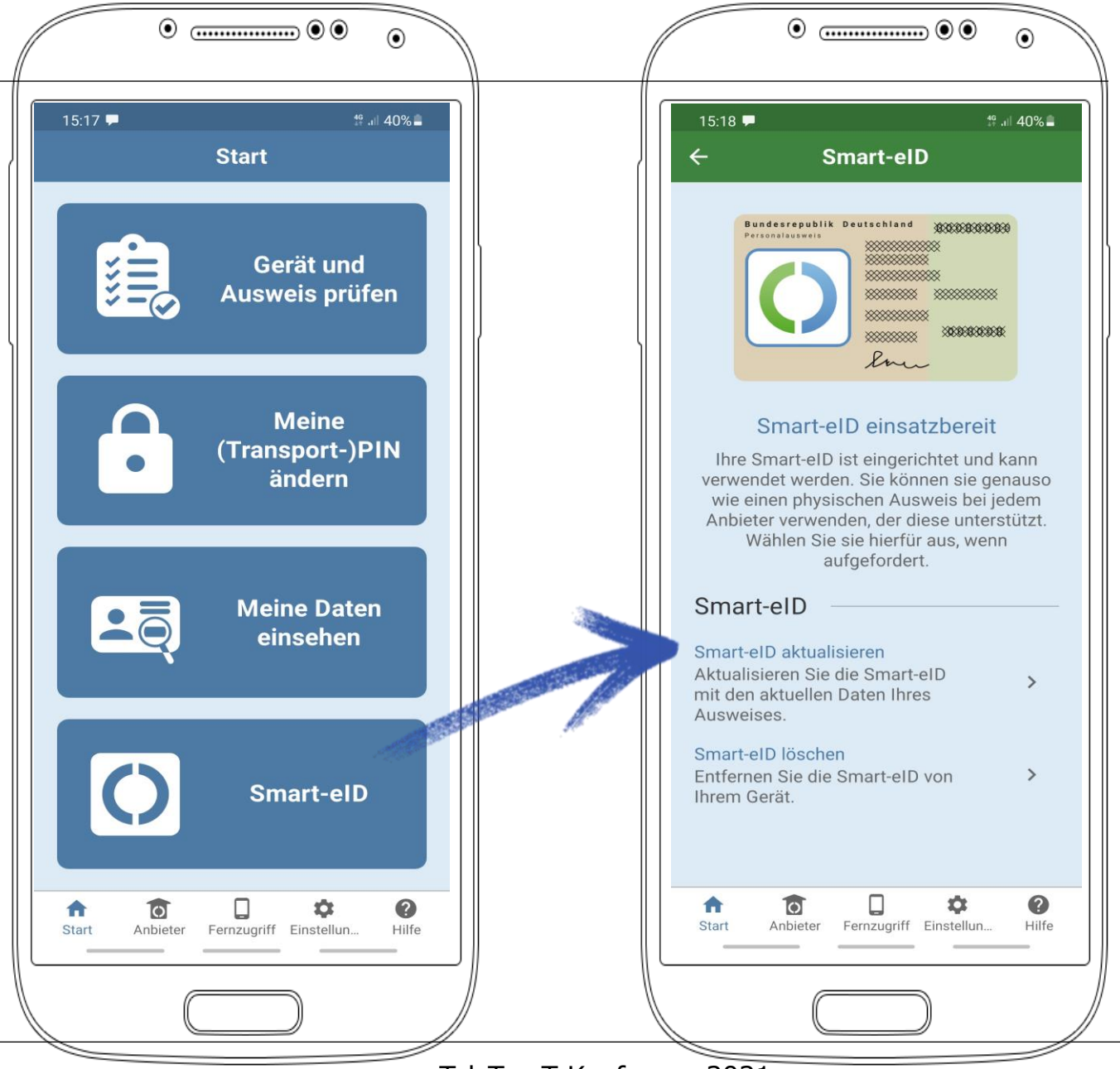


- Beispiel der Installation der “Secure-eID-App” mit der Installation des JavaCard Applets in das embedded Secure Element (eSE) eines Samsung Galaxy S20

- Bitte achten Sie auf die letzte Checkbox bzgl. der benötigten Zeit

OPTIMOS 2.0

Personalausweis
mit Online-Ausweisfunktion



bundesdruckerei.

Standardisierung

- **ISO/JTC1 SC17/WG3**
  - ICAO Technical Report "Digital Travel Credentials"
- **ISO/JTC1 SC17/WG4**
  - Project ISO/IEC 23220 "Building blocks for identity management via mobile devices" (Installation, Issuing and Identification procedures, Data elements, Confidence levels)
- **ISO/JTC1 SC17/WG10**
  - Project ISO/IEC 18013-5 "mobile driving license"
  - Project ISO/IEC 18013-7 "electronic vehicle registration"
- **GSMA**
  - Specification of "general purpose domain on eUICC"

Dr. Matthias Schwan
Technology – Mobile Security
Email: Matthias.Schwan@bdr.de
Phone: +49 (0)30 25 98-3417

Vielen Dank.