

**SAMSUNG**

**Samsung  
Knox Native  
Solution**

**Omnisecure 2025**



# What means Native?

# Knox Native Solution Übersicht

**von...**

Crypto-MicroSD als HW-Anker



**Hoher Aufwand und Kosten**  
aufgrund additiver HW und manueller Prozesse



**Langer Freigabeprozess**  
aufgrund plattformspezifischen Dokumentationsaufwand für Partner



**...ZU**

embedded Secure Element (eSE) als HW-Anker



**Geringere Kosten** durch automatisiertem Rollout des kryptographischen Schlüssels.



**Go-to-Market beschleunigen** durch direkten Austausch



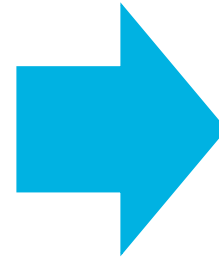
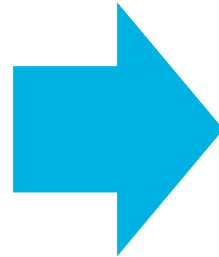
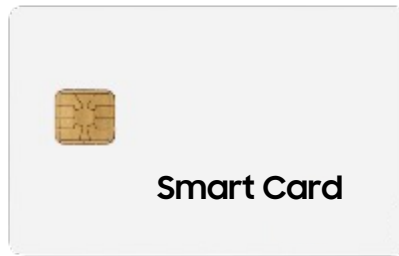
**Konsistente und native Customer Experience**



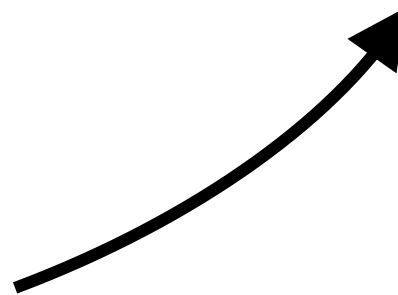
**Kryptographischer Schlüssel sicher im eSE**



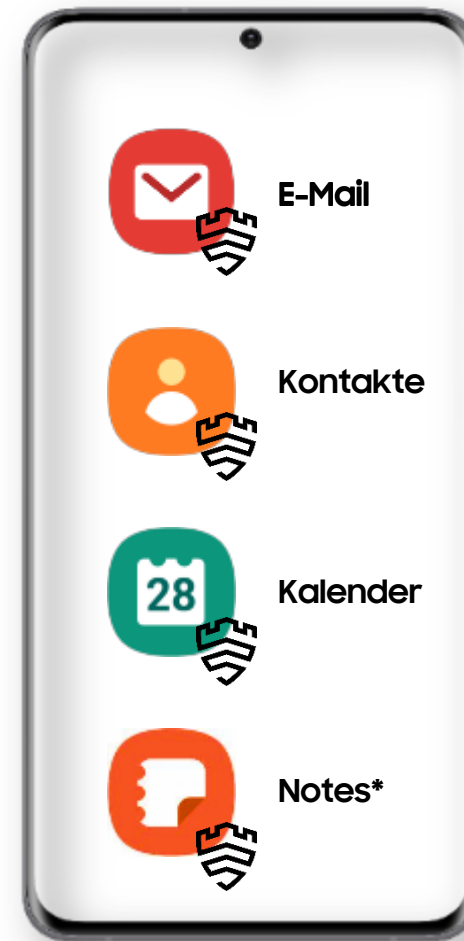
# Problem Solving



# Secure Use of Native Apps



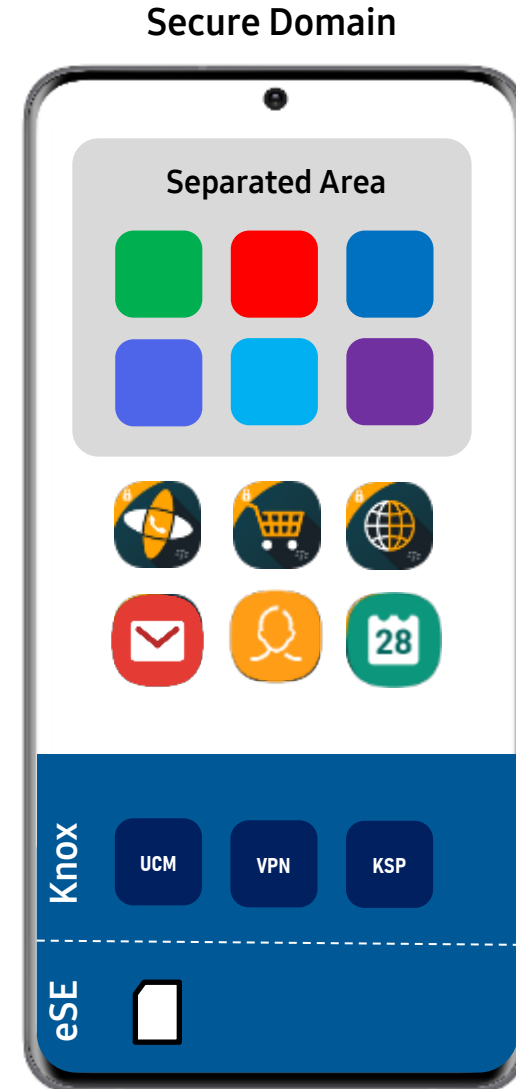
Next Security Level



# Secure Domain

A **fully managed device** in which evaluated applications can be installed, with a separate area for other applications

- **User Space encryption** according to BSI specifications, based on cryptographic keys (DAR)
- **VPN authentication** using cryptographic key (Samsung VPN Client)
- **Device PIN** = Smartcard PIN
- **Platform for solution providers** and self-developed applications





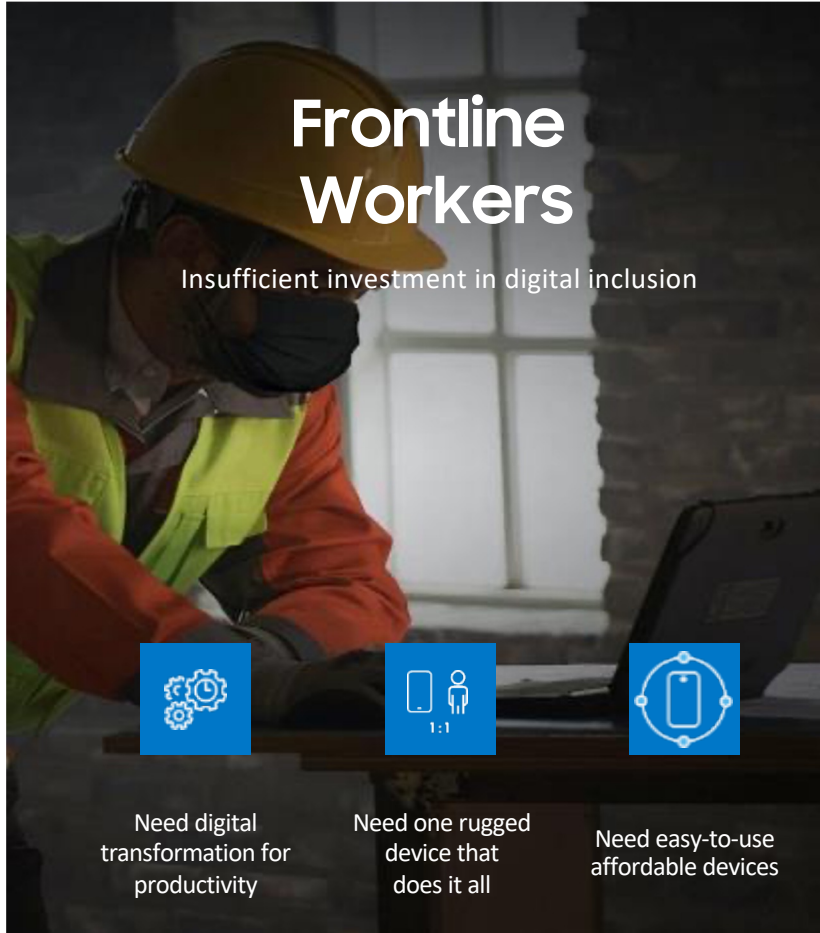
**SAMSUNG**

**1**

# Use Cases






# Advanced Solutions for Digital Acceleration



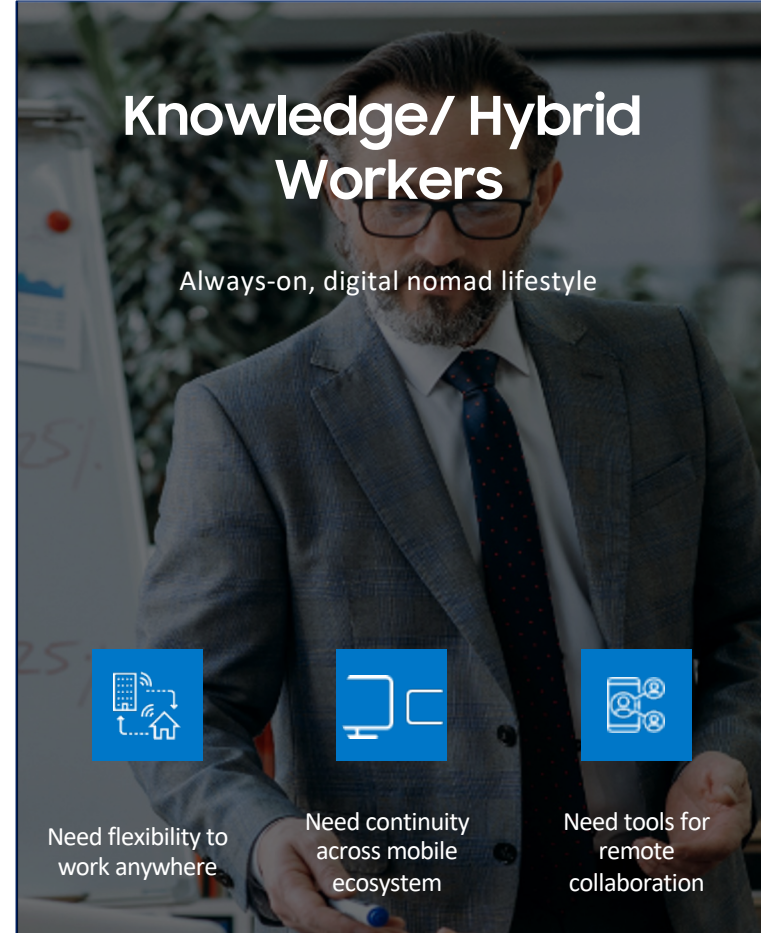
**Frontline Workers**

Insufficient investment in digital inclusion




Need digital transformation for productivity      Need one rugged device that does it all      Need easy-to-use affordable devices

The image shows a worker in a yellow hard hat and orange safety vest looking at a laptop. The background is a blurred industrial setting.



**Knowledge/ Hybrid Workers**

Always-on, digital nomad lifestyle

Need flexibility to work anywhere      Need continuity across mobile ecosystem      Need tools for remote collaboration

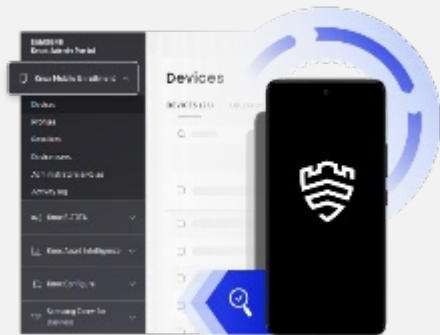
The image shows a man in a grey suit and glasses standing in front of a whiteboard. The background is a blurred office setting.



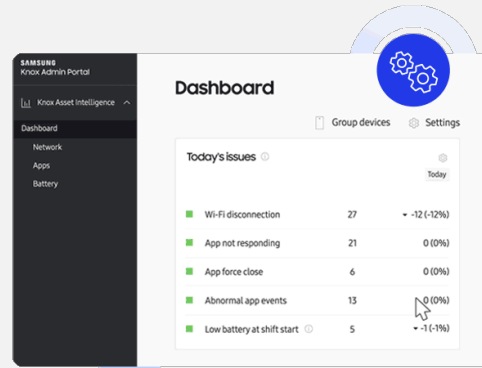
# Tools available to deploy & manage **Knox Native** Solution

## SAMSUNG Knox Suite

Cloud based Plattform



Knox Mobile Enrollment



Knox Asset Intelligence



Knox E-FOTA



Knox Manage  
or Samsung SDS EMM\*

\*For bright/dark side operation, the SDS EMM can be used instead of Knox Manage. More EMMs to follow.

# Knox Native Portfolio

Galaxy  
Z Fold5



Galaxy  
Z Flip6



Galaxy  
S24 5G EE



Galaxy  
S24 Ultra 5G



Galaxy  
S23 5G EE



Galaxy  
S23 Ultra 5G EE



Galaxy  
XCover6 Pro EE



Galaxy Tab  
Active4 Pro EE



Galaxy Tab  
Active5 EE



Galaxy Tab  
S8 + 5G EE



# New features in 2025

## Generic

- Android 15 – enhancements in: power mgt., UI, AI, Wifi7, ...
- More fine-grained policy controls (e.g. AI)

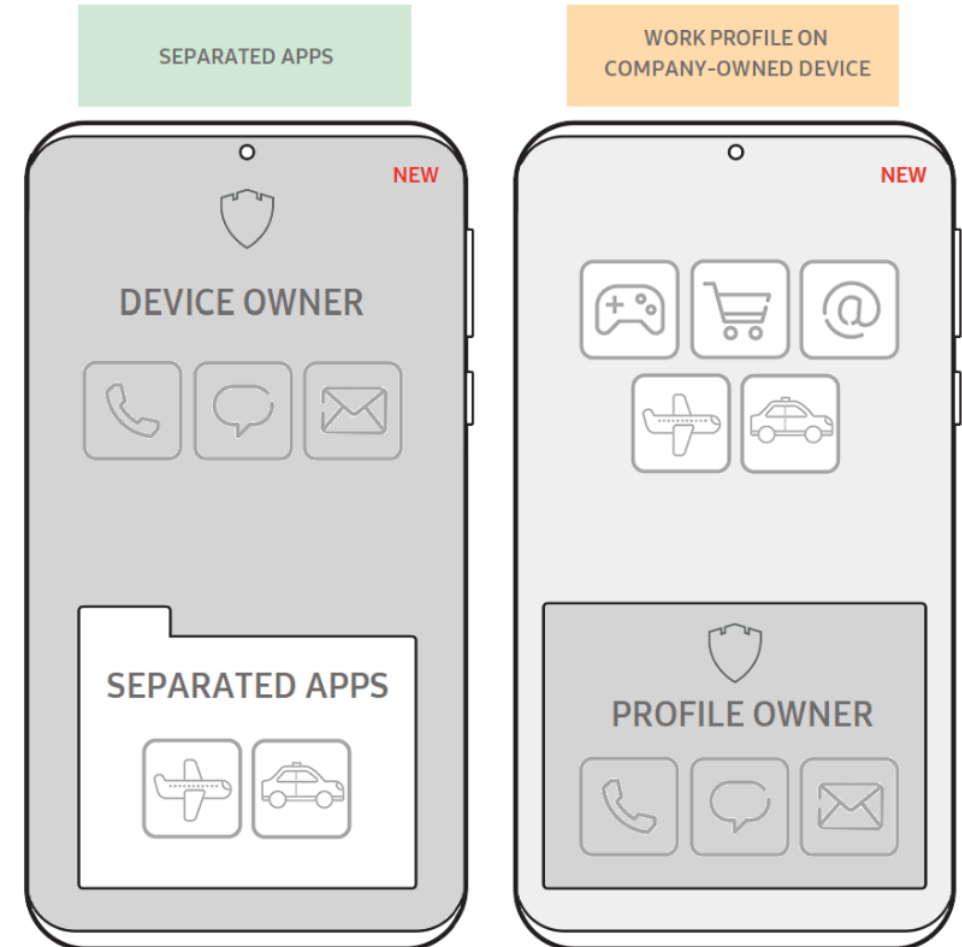
## KNS-specific

- Work Profile (WP-C) mode, in addition to Fully-Managed Separated Apps (FMSA) mode support
- Support for new devices
- SCEP certificate enrollment for approval
- DeX for approval
- Optimized rollout procedure in both modes – QR-Code-less rollout in WP-Mode
- Mandatory PIN change by user to personal value
- VPN enhancements (Support for NdB configuration, EAP-TLS, Remote ID, etc.,)
- BSI applet upgrade possible in the field
- Inject eSE randomness into kernel entropy pool
- Additional apps beyond PIM Apps – BSI App Ecosystem process



# Operational mode differences

Fully Managed with Separated Apps (FMSEA)	Work Profile on Company Owned Device (WP-C)
Secure side (VS-NfD) is the main user (base device)	Secure side (VS-NfD) is the profile user
Admin has full control over both sides	Admin has limited control over personal side, may set some device-wide policies
No personal Google Play account	Personal Google Play account to download apps on personal side
Admin must allow apps for the separated area	Admin has no control over personal apps, but can block certain apps
Device lock based on BSI applet	Profile lock based on BSI applet (separate device PIN needed)







OmniSecure 2025

CO PUBLIC  
Nexus property

# Secure Identities on mobile

- Today, everyone is using smart phones for private and business purposes
- Organizations what to get rid of cards and use mobile devices instead
- How use smart phones in our business with the same level of security as desktops?
- How to replace employee cards with smart phones?
- How can digital certificates on mobile help to work in a secure and convenient way?



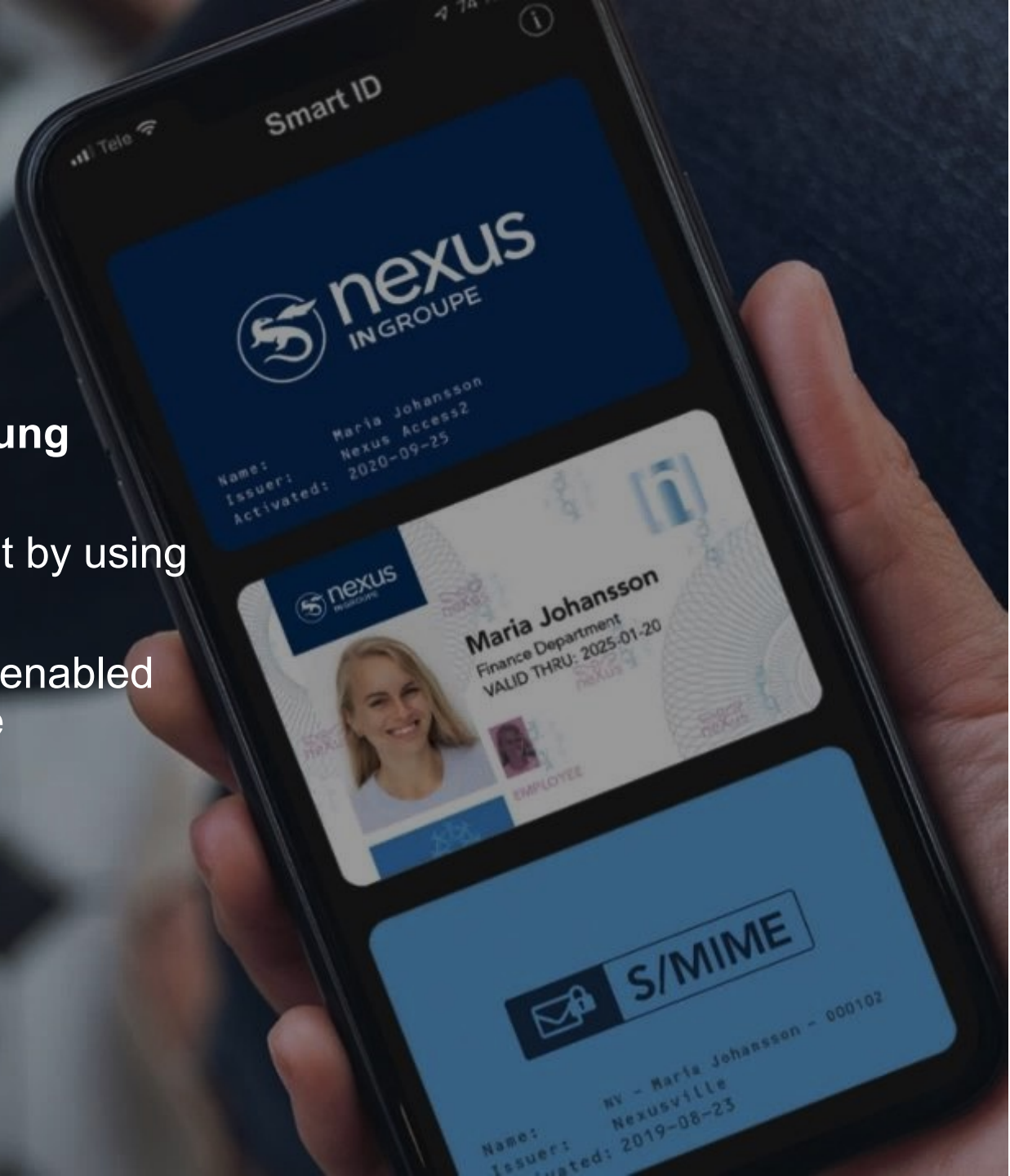
# Mobile ID use cases

- Use mobile as smart card replacement
- Combine secure smart cards with mobile use cases
- Use cases on mobile with same level of security as on Desktop
  - Encrypted email (S/MIME)
  - 2-Factor-Authentication
  - Manage and store certificates and keys in a dedicated secure environment

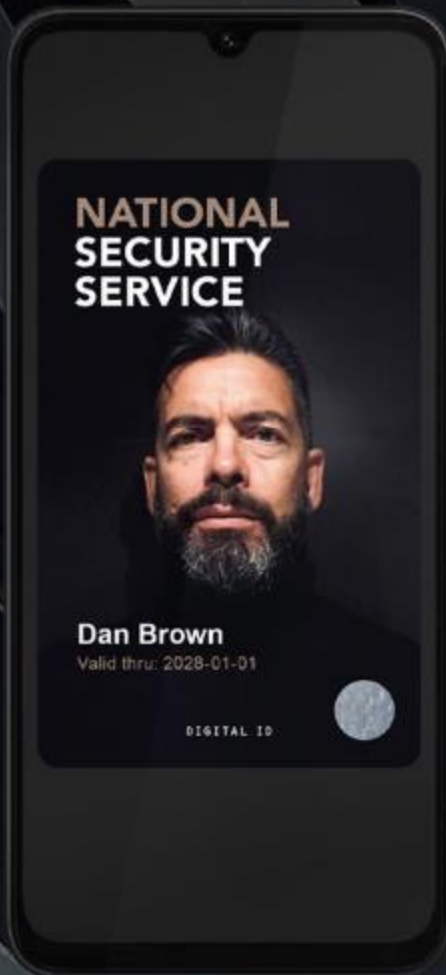


# Main objective

- Provide a complete “Mobile Corporate ID” (visual, digital + physical access) on the Samsung platform
- Smart ID Mobile App connecting to secure element by using BSI-certified Samsung Knox applet
- Providing end-to-end solution to customers: Knox-enabled Mobile app plus certificate enrollment and lifecycle management with Smart ID Identity Manager







## Visual ID

Visual representation of employee card (frontside, backside) in the mobile app

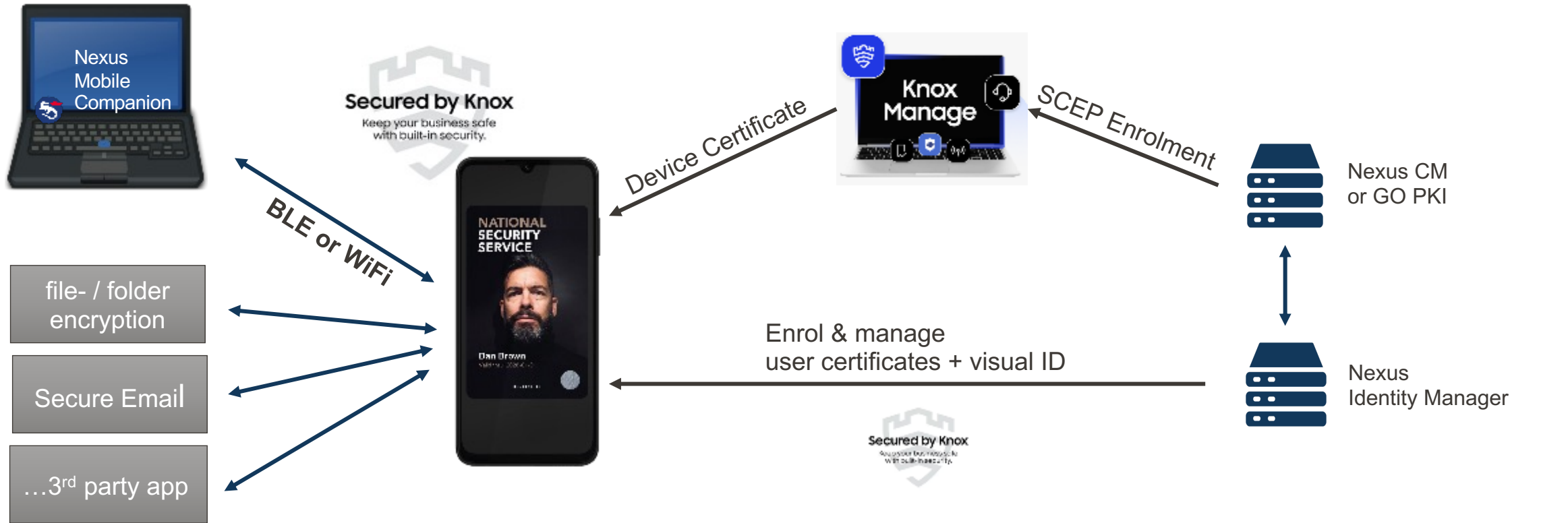
## Digital ID

Certificates for authentication, signing, encryption, stored in the secure element (eSE), via the **BSI**-certified Samsung Knox applet. VS-NfD (~ NATO-restricted) compliant

## Physical ID

Providing replacement for RFID-card via NFC channel on the mobile

# Mobile Corporate ID



TELEKOM SECURITY

Realisierung sicherer  
mobiler Services auf

**SAMSUNG Knox**



**SAMSUNG Knox**



**Unsere Business-Kunden stehen  
vor immer größeren  
Herausforderungen ...**



# Die Herausforderungen

Zunehmende  
Cyberangriff auf  
mobile Systeme

Komplexität digitaler  
Prozesse

Business  
goes mobile

Digitale  
Firmensouveränität

Cyber Resilience Act  
(CRA)

Schutz sensibler Daten  
auf mobilen  
Endgeräten

Eine Vielzahl mobiler  
Endgeräte im  
Firmeneinsatz

Industriespionage  
(auch) am Smartphone

Sichere Digitalisierung  
von  
Geschäftsprozessen

u.v.m.

**... daher ist ein Enabler auf Basis  
von **SAMSUNG Knox** erforderlich,  
der die sicheren mobilen Services  
aufs Smartphone bringt ...**

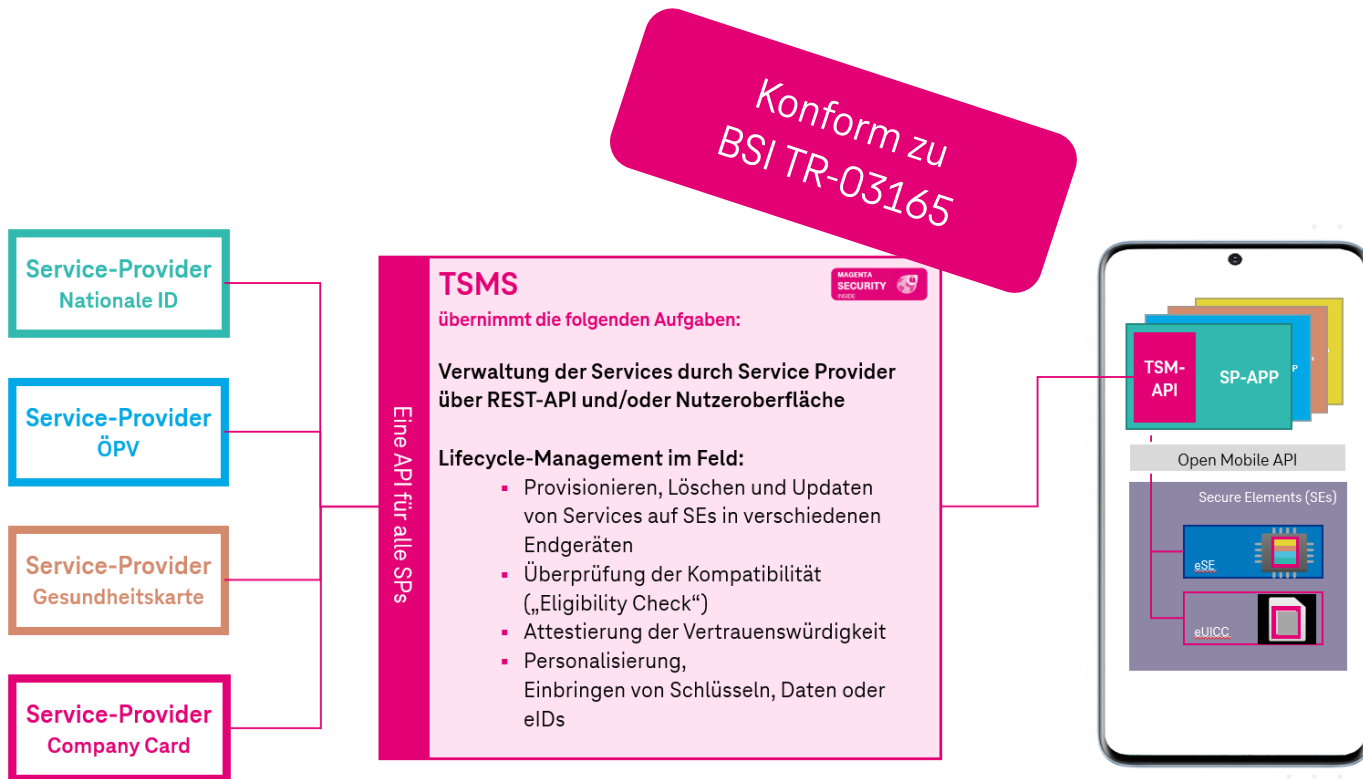
... und zwar das ...



# TSMS

Trusted Service Management System

# Das TSMS\* als Enabler sicherer mobiler Services

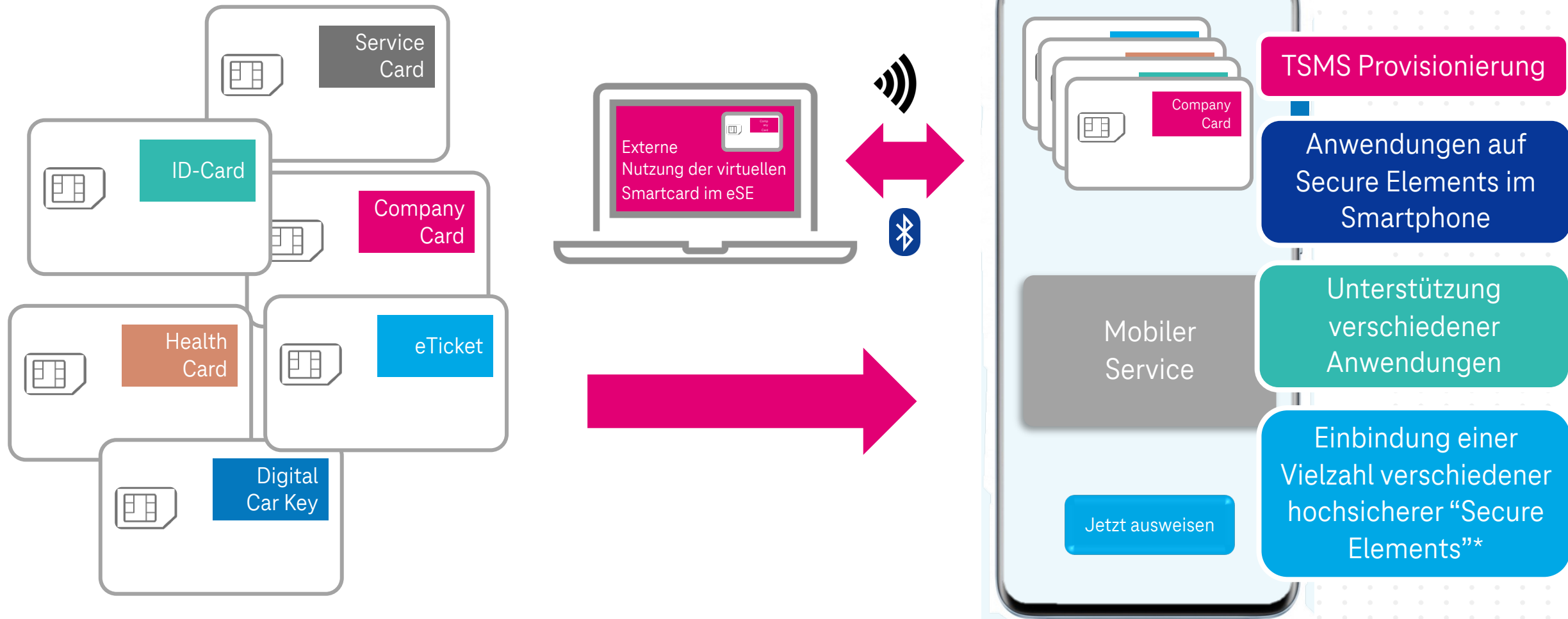


## Leistungen im Überblick

- Bereitstellung des Zugriffs auf Secure Elements und der Lifecycle Management Operationen zum Aufbringen, Updaten, Personalisieren und Löschen von Applets
- Sichere Speicherung von Schlüsseln, Daten & Co. im Secure Element
- Souveräne Kundenlösungen – TSMS als Bindeglied zwischen Service Providern und SE-Providern
- Erhöhung der Sicherheit von Services/Apps in einer Vielzahl von Anwendungsbereichen – z.B. Company Card, Autoschlüssel, Ticketing...
- Unterstützung bei der Erfüllung der Anforderungen des CRA u.a. durch hochsicheren Online-Zugriff auf die Geräte im Feld

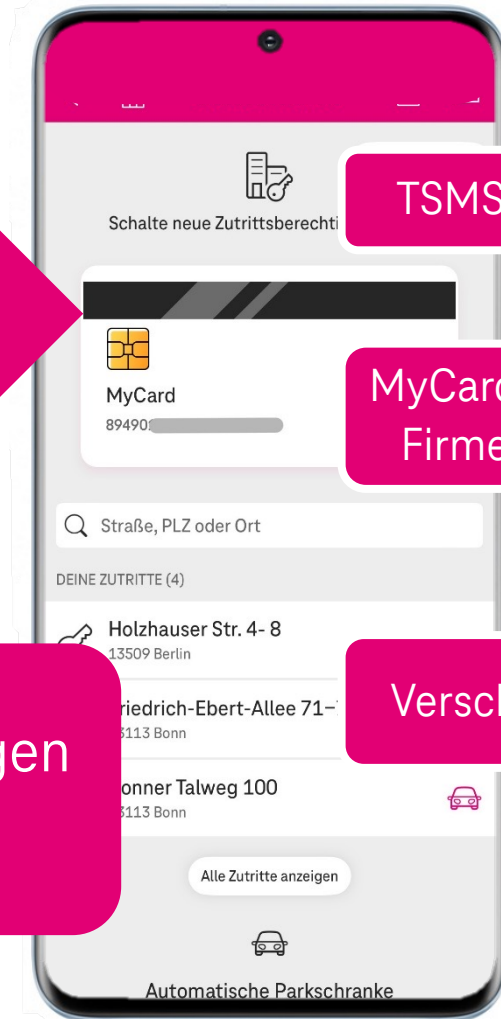
\*Trusted Service Management System

# Das TSMS aktiviert Hardware-sicherheit im Smartphone





# Company Card



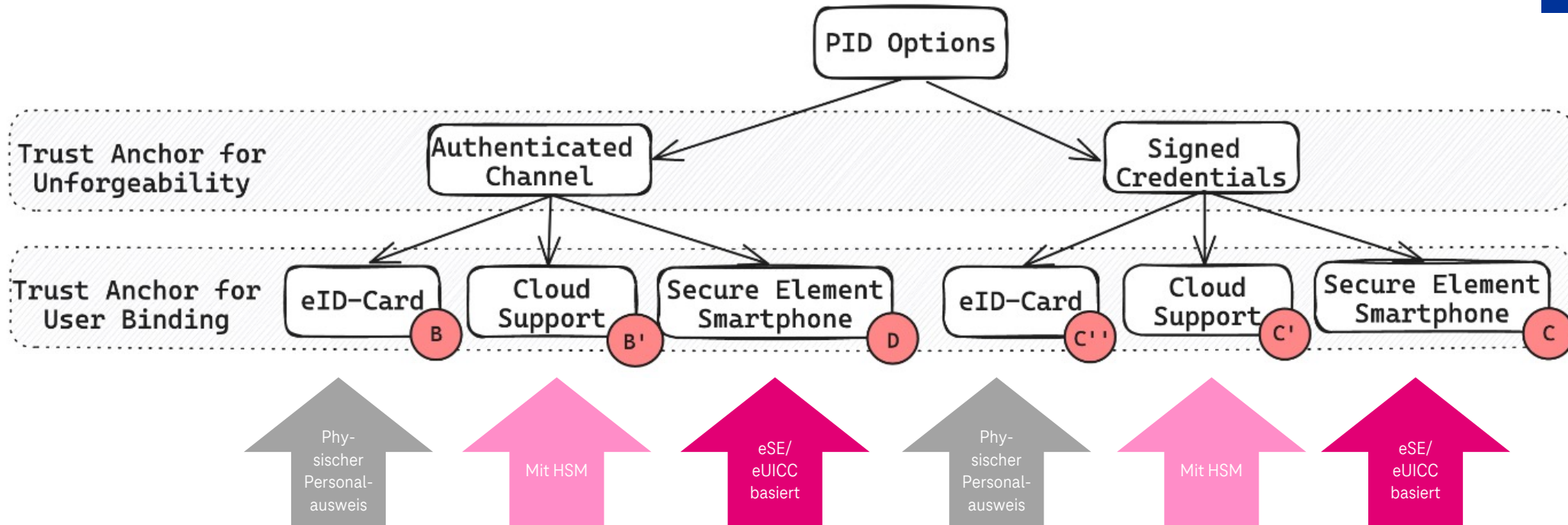
TSMS Provisionierung

MyCard oder individuelle Firmenlösung auf eSE

Verschiedene Services

Wir bringen Firmenkarten oder andere Kartenlösungen auf Smartphones

# EUDIW - Optionen nach dem deutschen ARF\*



Aber: Es gibt nur eine "high level" Regulierung zur Umsetzung von B', D, C' und C!

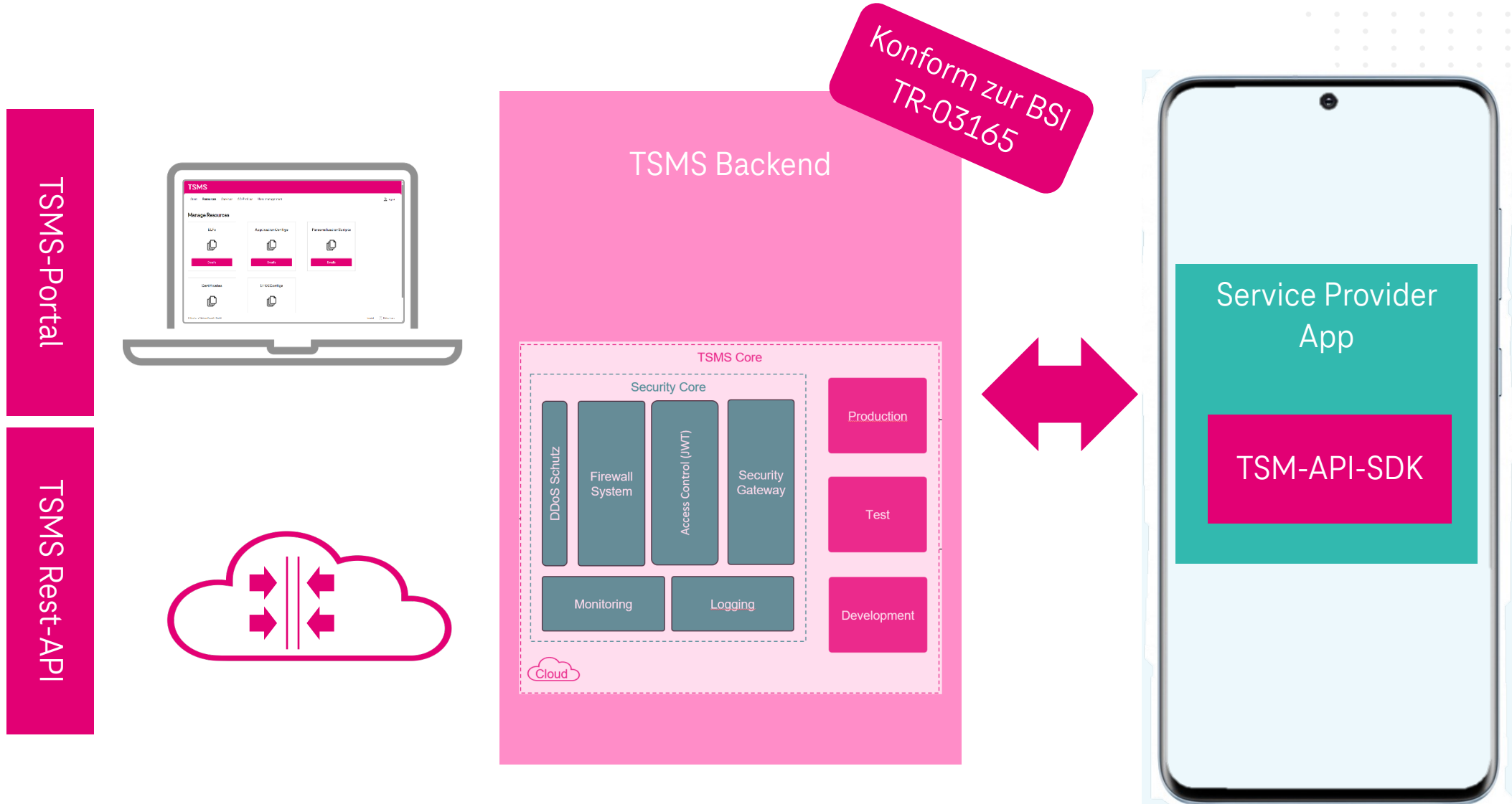
\*Architectural Reference Framework  
Basis für verschiedene Lösungen im deutschen SPRIN-D-Wettbewerb für EUDIW Prototypen

# Unser Ansatz: EUDI-Wallet auf Secure Element

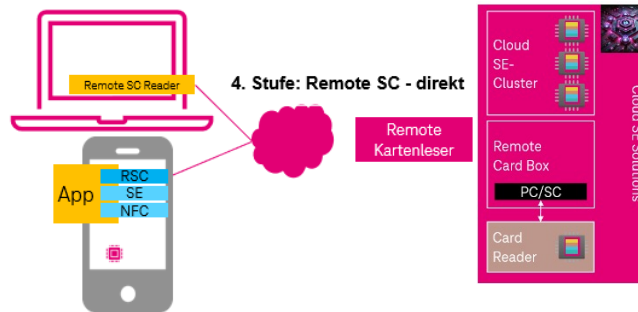
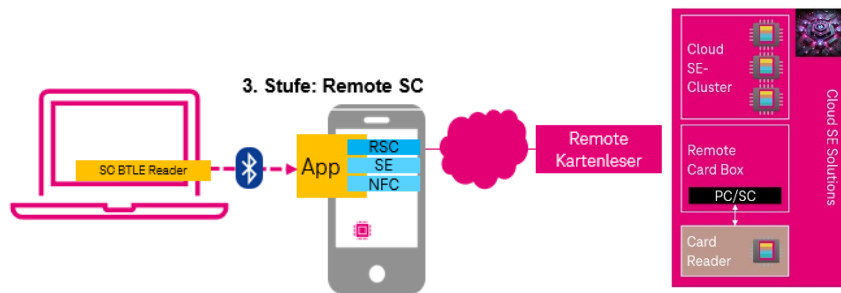
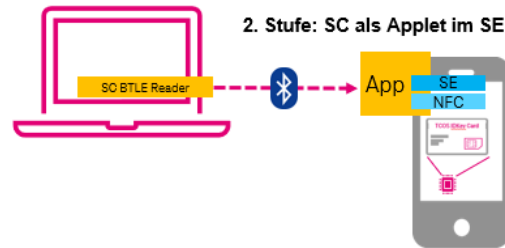
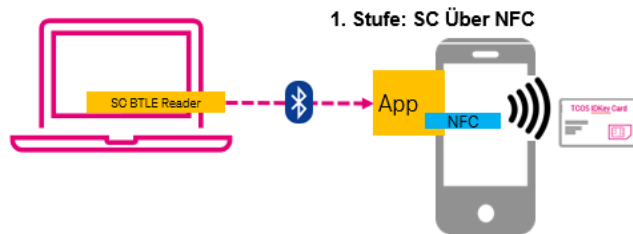


Wir enablen Secure Elements zur Absicherung der Europäischen Identitäts-Wallet!

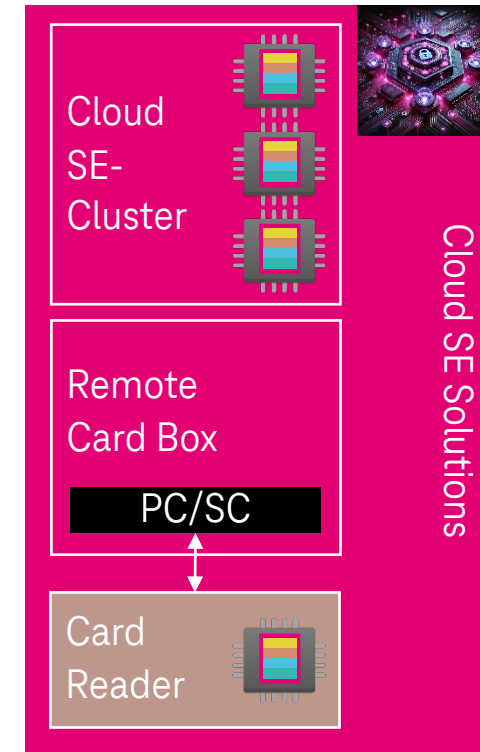
# Integrale Bestandteile des TSMS



# Weitere TSMS-Services



Virtual Smartcard Services



Cloud Services für Stufe 3+4





**Christian Stengel**

Deutsche Telekom Security



**Michael Leuchtner**

Nexus



**Nima Baharian-Shiraz**  
Senior PreSales Consultant  
Samsung Electronics GmbH  
nima.bs@samsung.com



**Stefan Schröder**  
Senior Security Expert  
Samsung Research UK  
s.schroder@samsung.com