

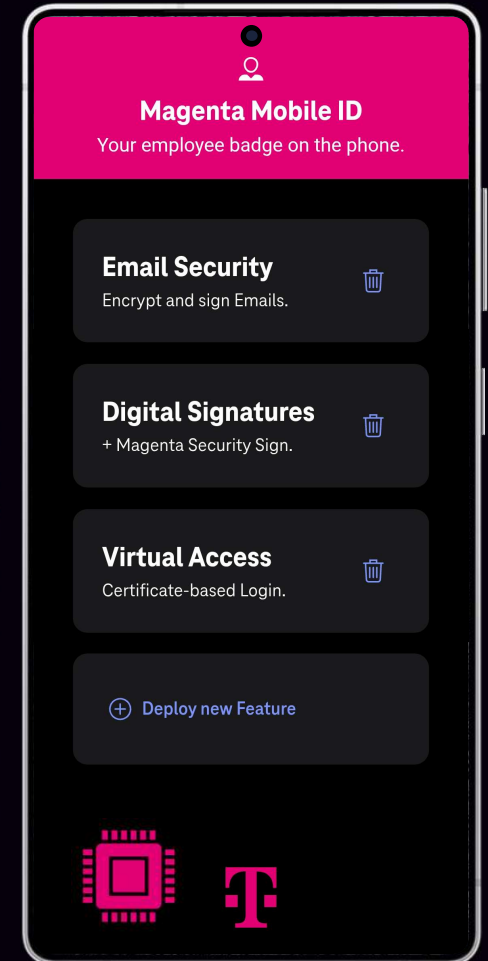
Omnisecure 2026

From **Smart Cards** towards
Samsung Mobile Devices

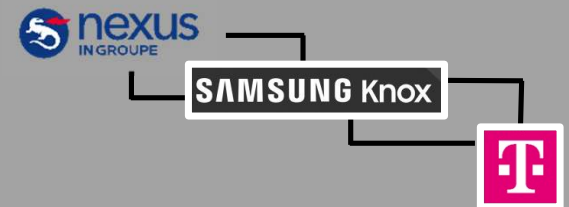
Berlin, 19. Januar 2026



SAMSUNG



First have a look on the basics:
Smartcard vs. eSE



SAMSUNG

Security



eSE powered Security

The eSE provides higher security than smart cards. It is a physical chip integrated directly into the device, offering a secure environment for long-term secrets.

Cryptographic protection mechanisms: Robust protection against attacks.

Isolated environment: Protection against malware and software-based threats.

Biometric authentication: Additional security through fingerprint and face recognition.



SAMSUNG

Usability



eSE improves usability

The eSE in Samsung smartphones simplifies the use of sensitive services directly from the smartphone, without additional hardware and integrated into Samsung Android One UI.

Easy handling: Seamless use of services via NFC for access controls.

No additional carriers: Always available as long as the smartphone is within range.

Simple integration: Simplified integration through SDK integration (UCM SDK) for partners.



SAMSUNG

Productivity



eSE enables productivity

The eSE also contributes to increased productivity by supporting a variety of features and applications that simplify users' daily lives and work processes.

Fast authentication to services: Efficiency improvement through quick authentication to services.

Support for business applications: Secure mobile solutions for enterprises.

Scalability: Versatile use from personal to business application cases.



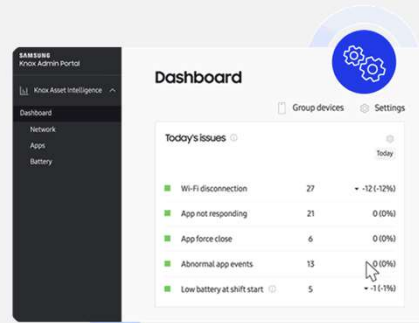
Tools available to deploy & manage Samsung Smartphones

SAMSUNG Knox Suite

Cloud based Plattform



Knox Mobile Enrollment



Knox Asset Intelligence



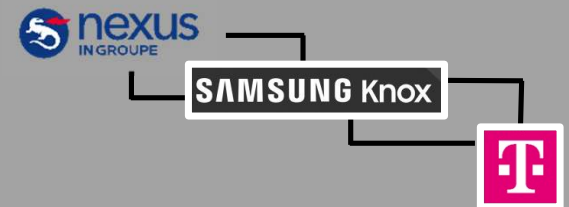
Knox E-FOTA



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.

And now to customer view:
**All of our business customers are
facing ever greater challenges**



Complexity of digital processes

Business goes mobile

Digital company sovereignty

Cyber Resilience Act (CRA)

A large number of mobile devices in company use & BYOD

Secure digitization of business processes

Industrial espionage (also) on smartphones

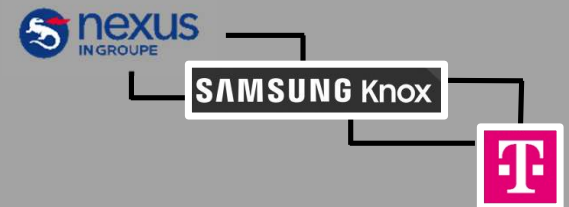
Protection of sensitive data on mobile devices

Increasing cyberattack on mobile systems

... and much more

Therefore, a high secured solution is needed for that brings secure mobile services to the smartphone.

The best basis for that are Secure Elements and Samsung Knox!



Benefits of Secure Elements based Solutions

Business Benefits for Enterprises

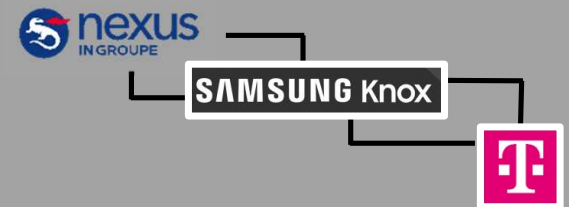
- Builds trust with customers and partners through **certified security**
- **Simplifies compliance with CRA, GDPR, and BSI** requirements
- **Reduces audit and lifecycle costs** via centralized SE management
- **Enables scalable identity solutions** for mobile and desktop
- **Provides future-proof foundation** for EUDI-Wallet, SSO, and company systems and underlines digital sovereignty

Hardware vs. Software-only Security

| Aspect | Software-only | Secure Element (Hardware) |
|------------------------------|------------------------------|--|
| Protection against tampering | Vulnerable to root/jailbreak | Physically isolated, tamper-resistant |
| Key management | Stored in RAM/filesystem | Stored in SE, not extractable |
| Certificate security | OS-dependent | BSI-compliant, VS-NfD capable |
| Update capability | Yes, but easily attackable | Yes, with secure lifecycle management |
| Compliance and trust | Limited | High acceptance in industry and government |

Secure Elements – hardware-based security for digital sovereignty!

And what about Applications?



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



Mobile enterprise ID



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**).
VS-NfD compliancy via Samsung Knox Native

SAMSUNG Knox

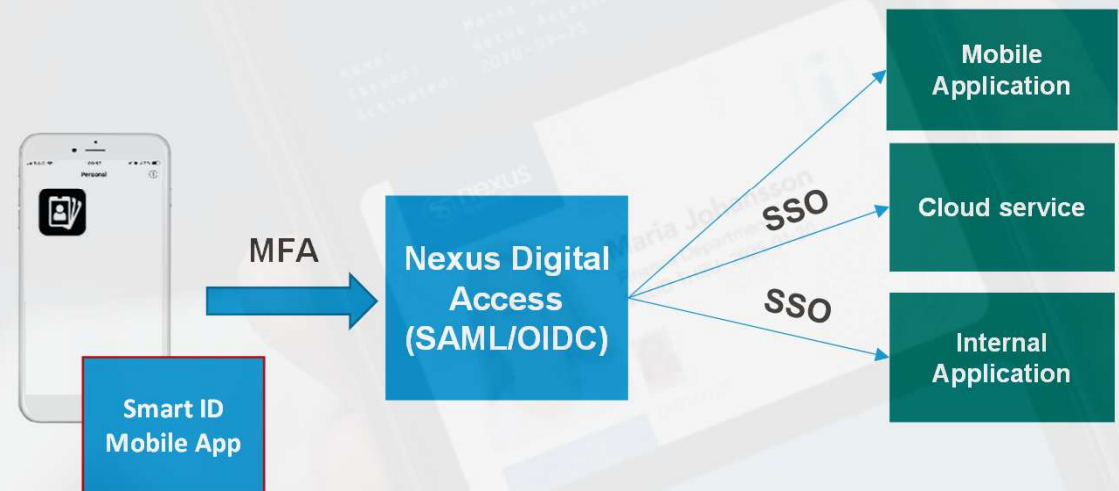


Physical ID

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

Single-Sign-On with Mobile ID

- Smart ID Mobile App is high-secure and convenient Multi-Factor-Authentication
- Keys + Certificates are enrolled and managed securely
- Use PIN, Face ID or Fingerprint as second factor on your smart phone
- No dedicated hardware token needed, therefore easy to enroll also for contractors
- PKI-based MFA allows to (in contrast to FIDO2) enforce global policies, and lifecycle management (revocation, renewal etc.)
- Increase security and usability in contrast to OTP-based solutions

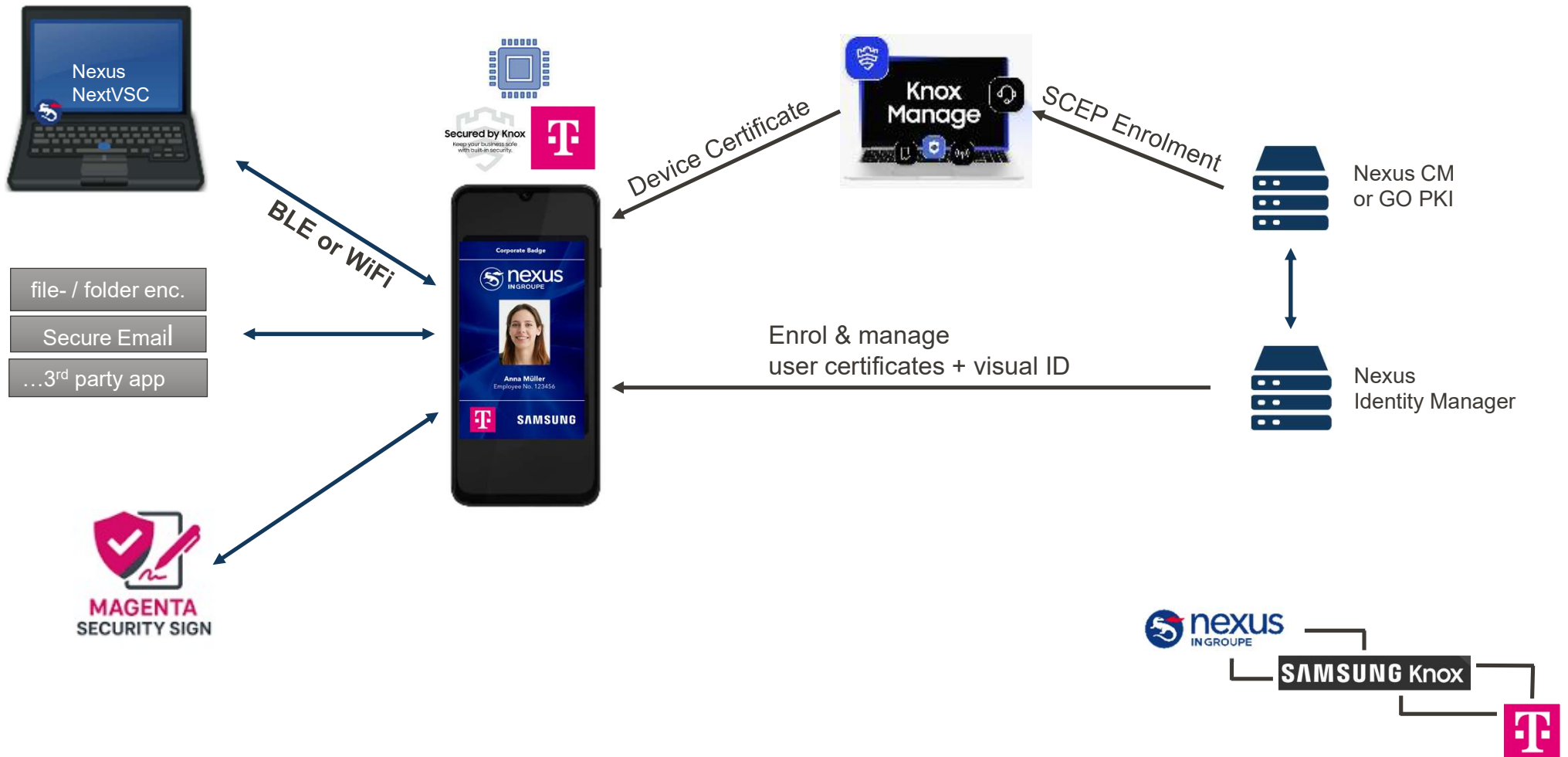


Nexus NextVSC

- Connect Smart Phone via Bluetooth-low-energy (BLE) or IP/WiFi with Windows Workstation
- Nexus client component emulates smart phone a minidriver-based smart card in Windows
- All typical smart card use cases by using Smart ID Mobile App on the smart phone instead plugging in a card

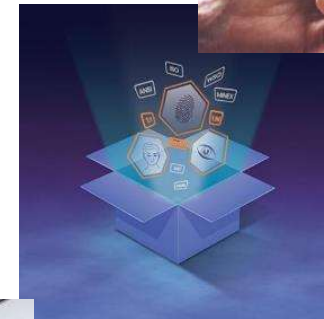
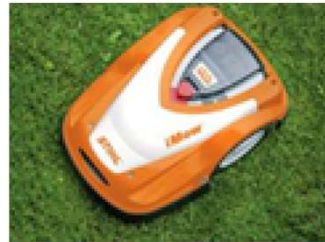
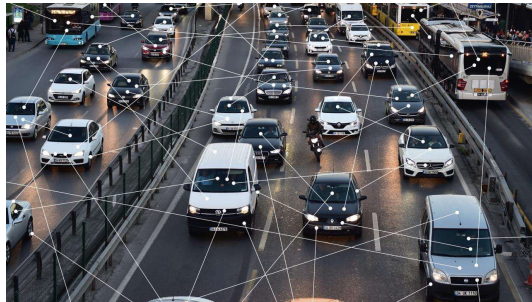


Secure Identities on mobile



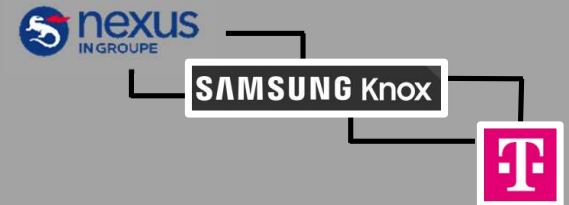


Identities for Citizens, Workforce, Workplace and IoT



From Smart Cards towards Samsung Mobile Devices –
OMNISECURE 2026

**All Secure Element Solutions need
a feasible infrastructure for the
lifecycle Management of Secure
Elements in the field.
And we have one ...**



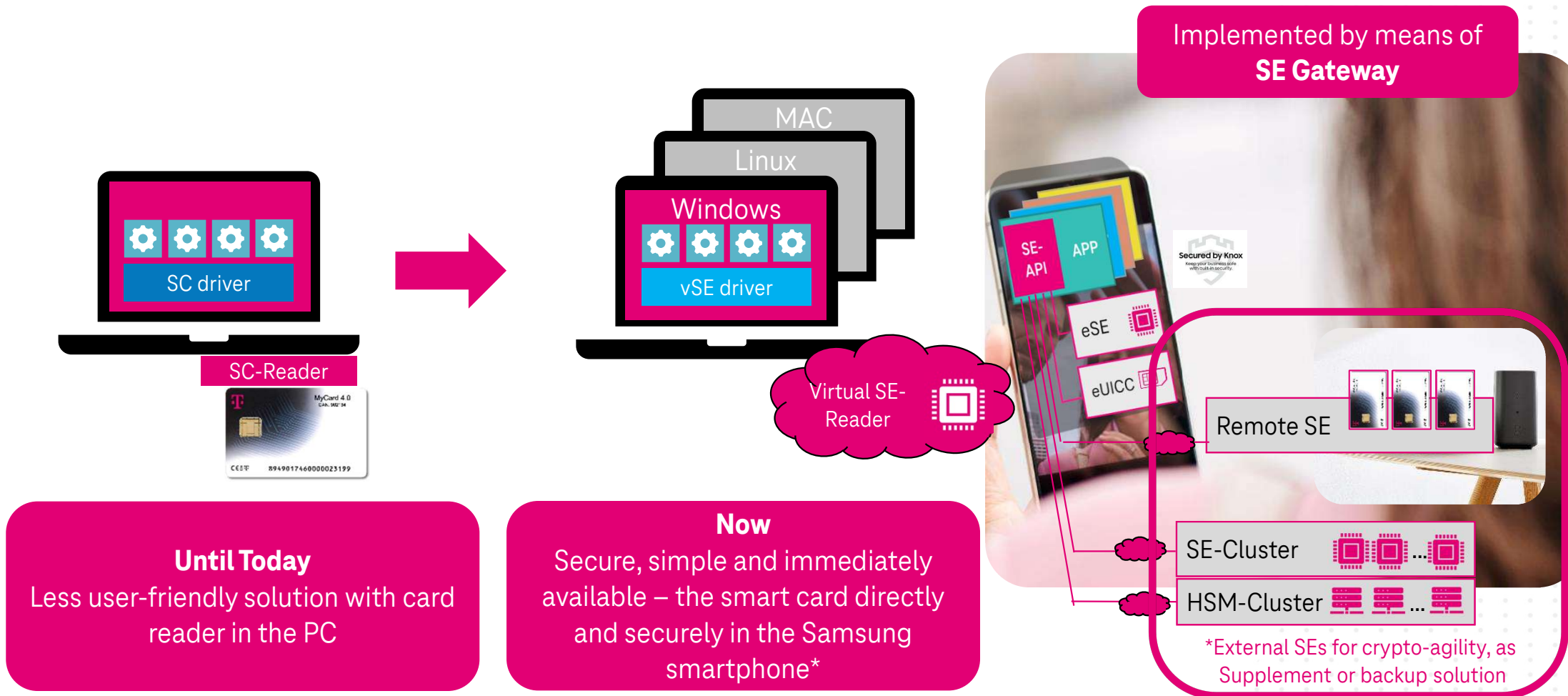
... namely ...



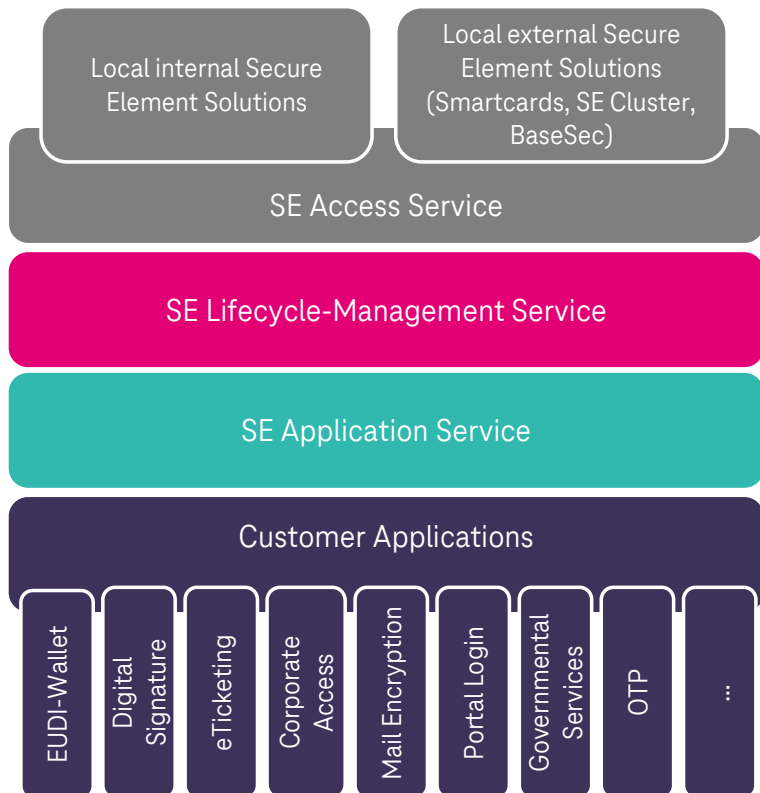
T's Secure Element Gateway

.. a management system to enable virtual physical Smartcard functionalities in Smartphones!

The SE-Gateway enables future proof Solutions



Basis is the Secure Element Gateway Secure Bridge to Smartcard Applications



What we offer:

Universal Access to Physical Secure Elements

Whether embedded in smartphones (preferred), PCs, or external devices – we connect them all.

Lifecycle Management for your Applications

Deploy, update, and manage your own smartcard-based apps and applets with ease.

Application Services for Trusted Use Cases

Corporate Badge, Qualified Electronic Signature (QES), EUDI Wallet, eTicketing, ... and many more.

Full sovereignty in digital identities

The SE-Gateway is unique

- It enhances lifecycle management of **Secure Elements** with advanced functions and is operated in Deutsche Telekom's Sovereign Cloud in Germany.
- Developed entirely by Telekom Security, it **enables secure mobile services**, remote updates, and supports the high standards of the **Cyber Resilience Act (CRA)**.
- It lays the foundation for **scalable, resilient solutions in sensitive environments** – as a future-proof security anchor.

Innovative and secure – future-oriented –
ready to go – 100% made in Europe!

From Smart Cards towards Samsung Mobile Devices – OMNISECURE 2026

Magenta Security – Secure Element (SE) Gateway



The SE Gateway manages a large number of secure elements in and out of mobile devices

AUTHADA



SEs have been tested as a security anchor for the EUDI wallet in the SPRIND competition

SAMSUNG Knox



Together with Samsung and Nexus, we offer virtual smart cards and other services

The SE Gateway, Samsung Knox and Nexus PKI systems create the foundation to make hardware security on Samsung devices usable for a wide range of applications!

EUDI-Wallet

SE-based security anchor on mobile devices as the basis for mobile ID cards such as driver's license and ID card

1



Critical infrastructure

SE-based security anchor as a virtual smart card for digital identities and to secure networked devices & processes

2



Secure company solutions

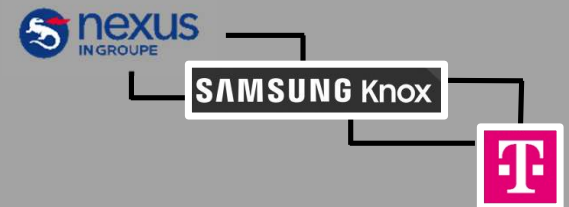
SE-based security anchor for the implementation of new measures, e.g. in sensitive areas

3



Our SE gateway provides a **basis for long-term investment** and future security, as it enables remote updates and keeps components and Secure Elements "up-to-date"!*

*This is particularly relevant in view of the Cyber Resilience Act (CRA)!



Our portfolio – a selection

ID card systems



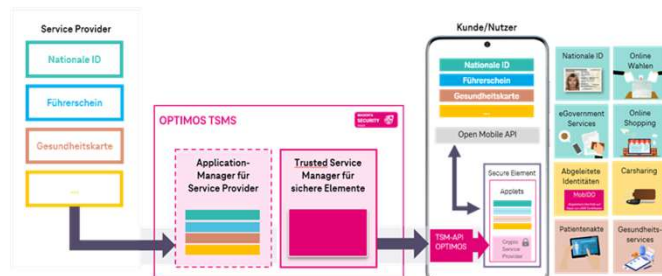
Cash registers



Smart Metering SE



SE-Gateway



Authority radio



TCOS
Telekom Chipcard Operating System

Your contact at Samsung Electronics



Nima Baharian-Shiraz
Senior PreSales Consultant

nima.bs@samsung.com

Your contact at Nexus



Michael Leuchtner
Senior Solution Architect

michael.leuchtner@ingroupe.com

Your contact at Telekom Security



Christian Stengel
Lead Architect Identity Security

christian.stengel@telekom.de

