

**SAMSUNG**

Samsung  
Knox Native  
Solution



# 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

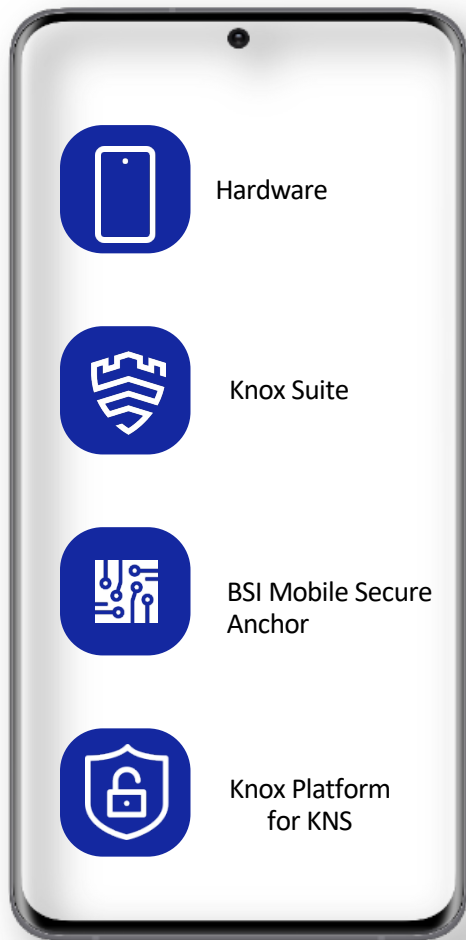


Kryptographischer Schlüssel sicher im eSE

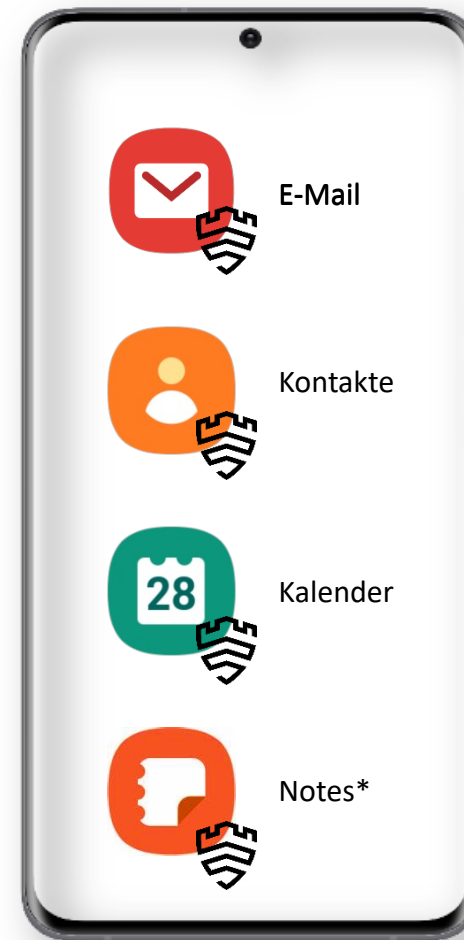


# What means Native?

# Secure Use of Native Apps



Next Security Level



\*Verfügbar mit Android 14

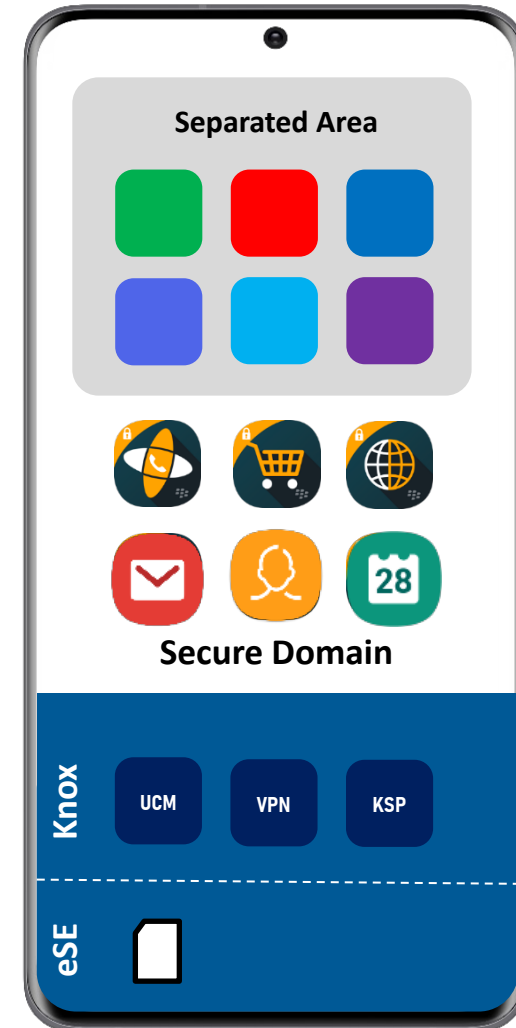


## Secure Domain

---

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



# embedded Secure Element (eSE)

---

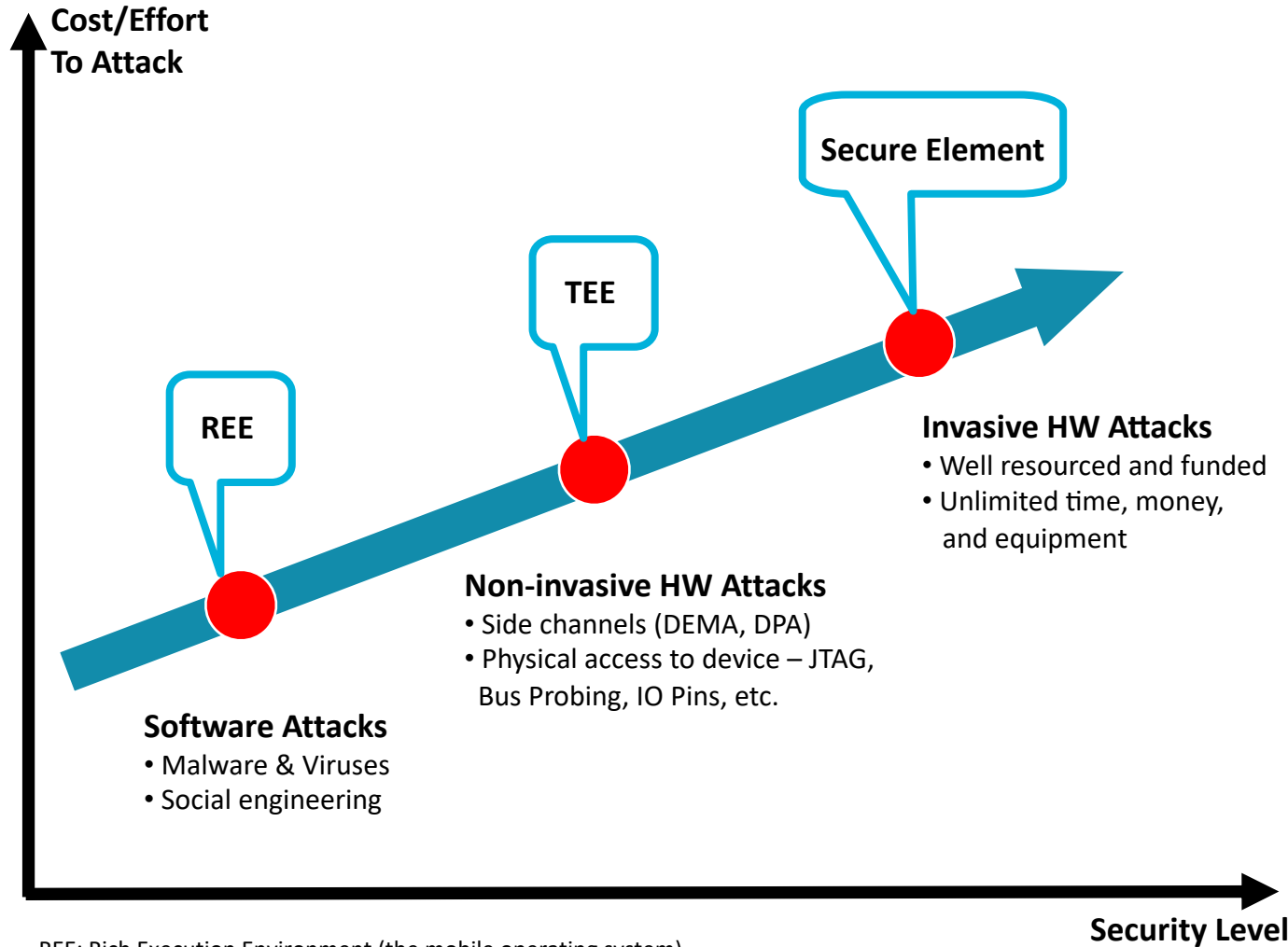
## Features

- An independent physical chip
- Complete subsystem with its own CPU, memory, firmware, etc.
- Similar to smart card chips on credit or SIM cards
- Designed for security-sensitive services
- Multiple apps can coexist, and may be loaded in the field
- Can interact with
  - the environment via NFC or UWB (depending on device)
  - apps inside the device

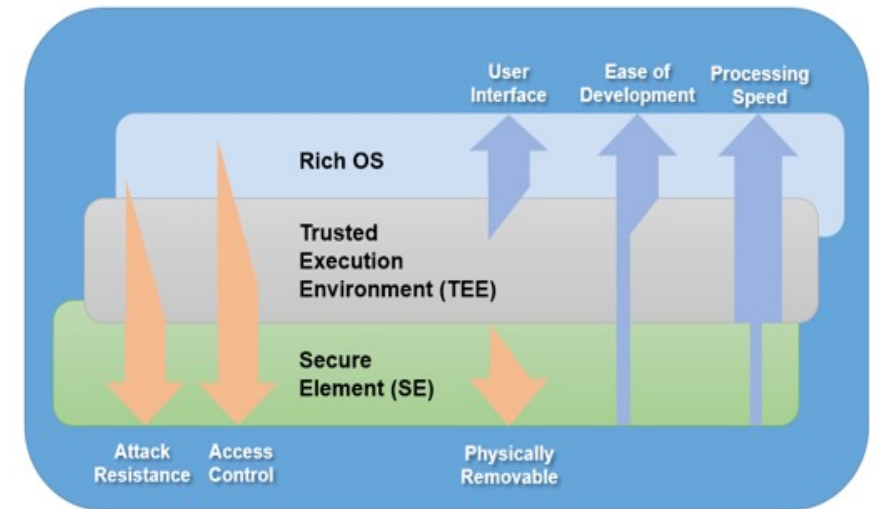
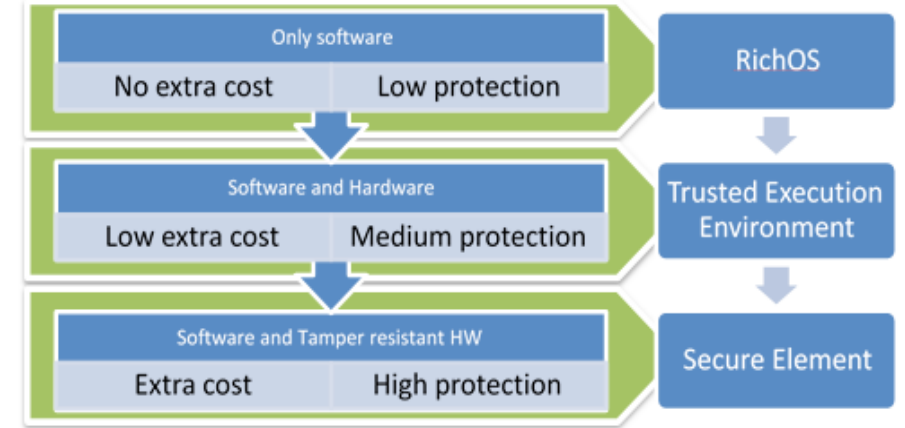
## Security Aspects

- Secure space to store and process confidential data
- Isolated secure execution environment
- Tamper-resistant HW/SW design
- Cryptographic hardware engines
- Certified security according Common Criteria
- HW Security Anchor according to BSI-VS-AP-0022







# Complexity is the worst enemy of security



REE: Rich Execution Environment (the mobile operating system)  
 TEE: Trusted Execution Environment (e.g. ARM Trustzone)



# Certifications

Component	Certifications
Applications	Smart eID Applet
Crypto-plugin	CSP (Cryptographic Service Provider) PP (EAL4+) PP 0104  
Platform (Javacard OS)	Java Card System PP (EAL4+) PP 0099  
Chip (H/W)	Security IC Platform Protection Profile (EAL6+) PP 0084  

BSI Mobile Security Anchor

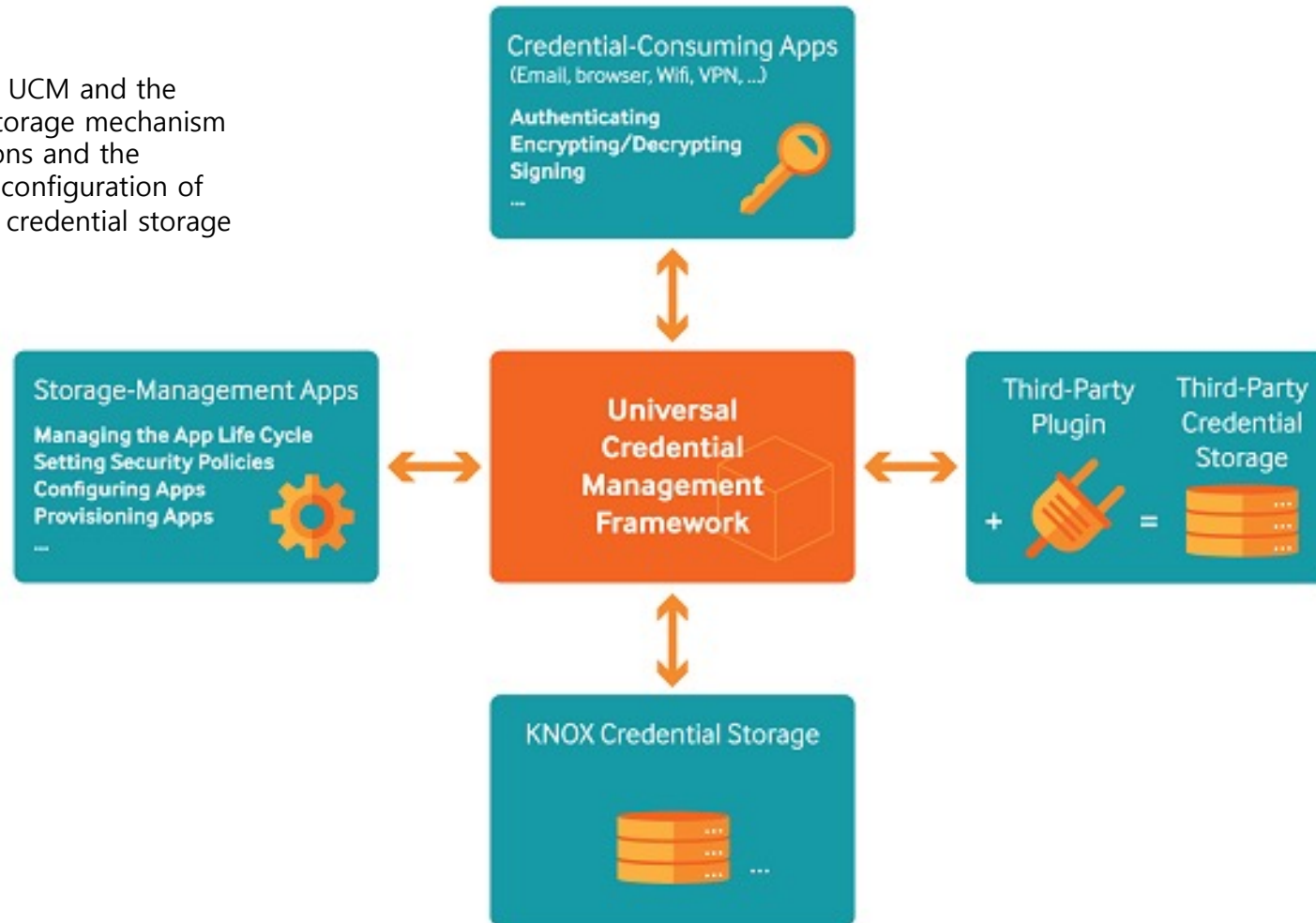
Access Card Emulation

...

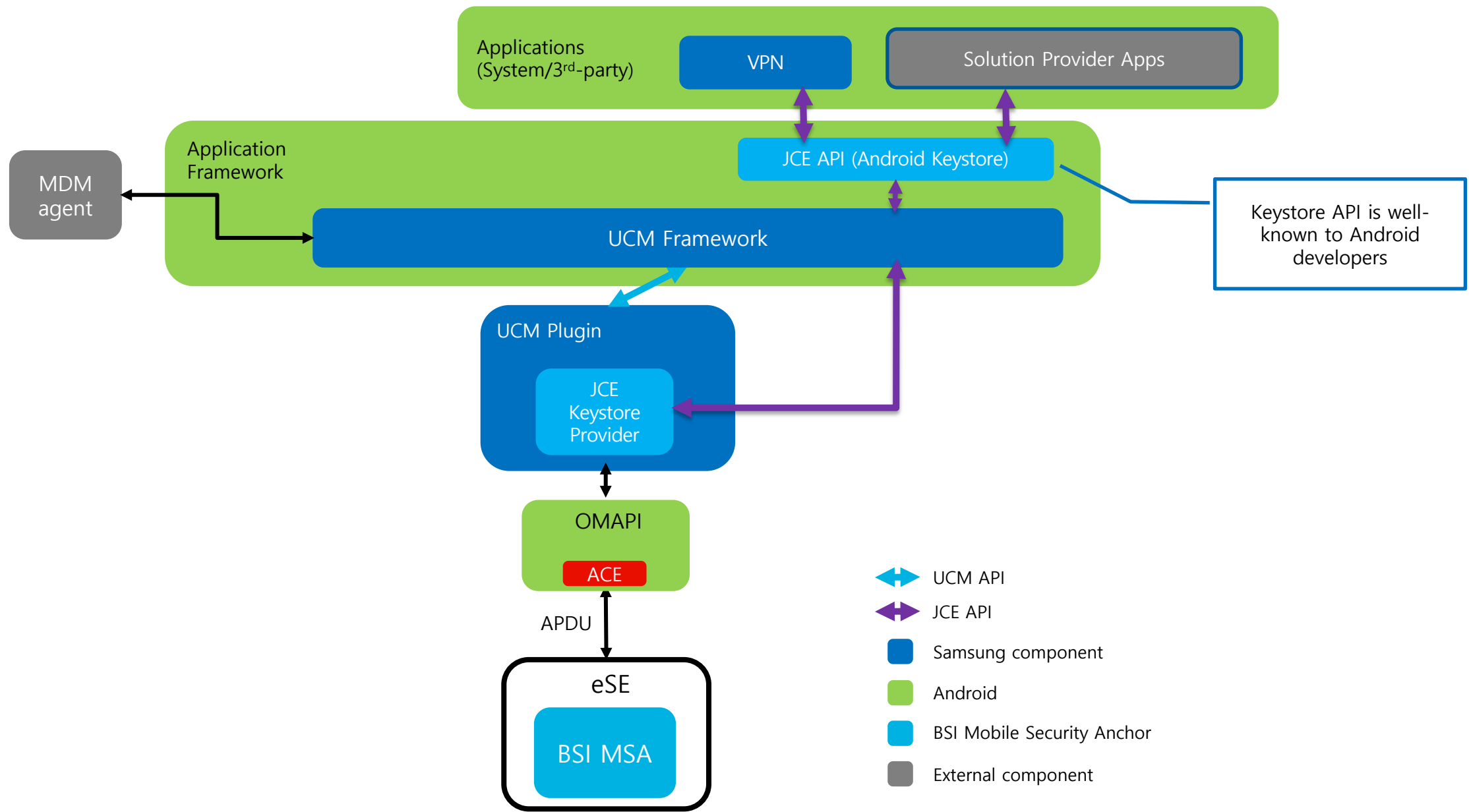








# Universal Credential Management (UCM) = Android integration for eSE

Interface to configure UCM and the Plugin, to make the storage mechanism available to Applications and the System. This includes configuration of Access Control to the credential storage mechanism.



# Native Keystore API: Easy to use



-  UCM API
-  JCE API
-  Samsung component
-  Android
-  BSI Mobile Security Anchor
-  External component

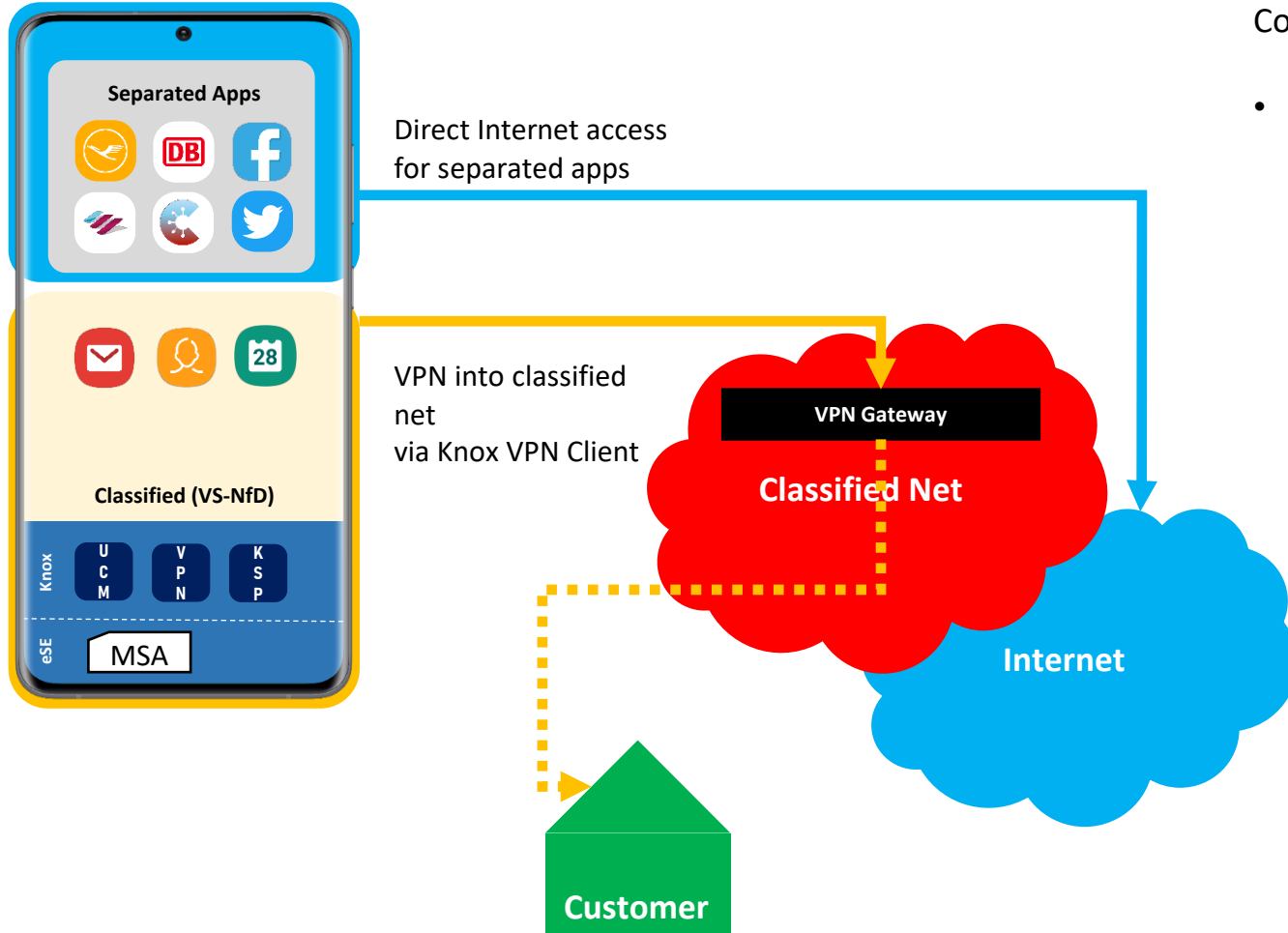
# BSI MSA Cryptographic Functions

Interface	Algorithm
Key Import	AES128
	AES256
	RSA2048
	RSA3072
	secp256r1
	secp384r1
	secp521r1
KeyGeneration	AES128
	AES256
KeyPairGeneration	RSA2048
	RSA3072
	secp256r1
	secp384r1
	secp521r1

Interface	Algorithm
Cipher	AES CBC No Padding
	AES CBC ISO9797M2 Padding
	AES GCM
	RSA PKCS1
	RSA OAEP with SHA256
	RSA SHA 256 PKCS1
Signature	RSA SHA256 PKCS1 PSS
	ECDSA SHA256
	ECDSA SHA384
	ECDSA SHA512
Secure Random	Physical TRNG

Support for Brainpool curves is added with Android 14

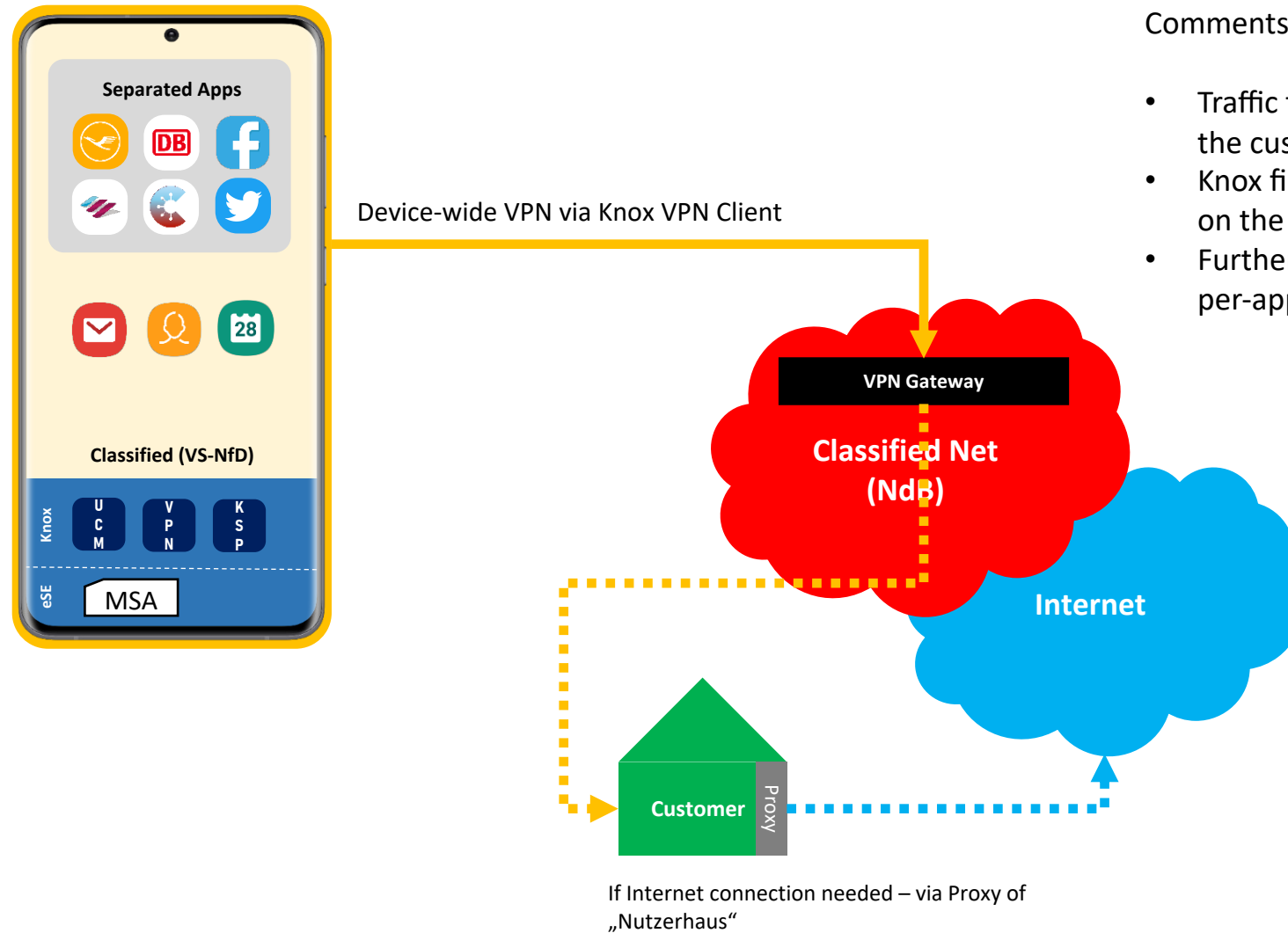
# VPN options with Separated Apps – KNS Default



Comments:

- Knox firewall rules may be configured per app on the device by the customer

## VPN options with Separated Apps – Alternative Option



# Security – ease of use



## Features

- MSA unlock by PIN according to BSI requirements
  - Unlocks also DAR encryption key in MSA
- PIN is also used to unlock the device – only one PIN required
- Optional Biometric unlock (fingerprint) for device lock-screen
  - Same look and feel as standard Android
- KNS features integrated into EMM through Knox Service Plugin (KSP)
  - MSA PIN policy
  - App access to UCM Keystore
- Easy roll-out process into managed environment (QR codes)

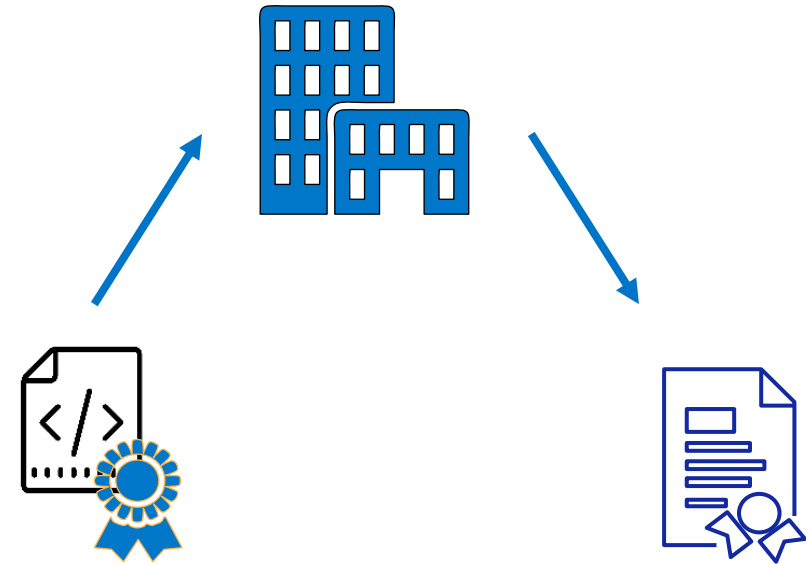
## Security Aspects

- Certificate enrollment over SCEP (RFC 8894)
- EAP-TLS support for VPN

## Key personalization into MSA

### ● Aspects to consider:

- Trust establishment device/user and PKI
- E2e protection method for key transport
- Transport path, systems, and networks involved
- Message flows
- Deep integration into customer environment
- Device API for integration (MDM or app)



### ● Import of PKCS#12 container

- Keys and certificates generated in PKI
- Container protected by passphrase
- Lowest integration effort
- Supported by UCM and Keystore API
- Passphrase transport out of band

### ● Key generation in eSE + CSR

- Keys generated inside MSA
- Certificate management protocol SCEP supported in Knox ZT framework
- Most widely supported certificate management protocol
- MSA signs CSR
- Optional authorization password (transport out of band)

# Knox Native Portfolio

Galaxy Z Fold5



Galaxy Z Flip5



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



\*Verfügbar mit Android 14



New Flagship

---

## Samsung S24 Enterprise Edition



7 Jahre SMR

7 OS Upgrades

Knox Suite

3 Y Warranty

AI on Device

Live Translate

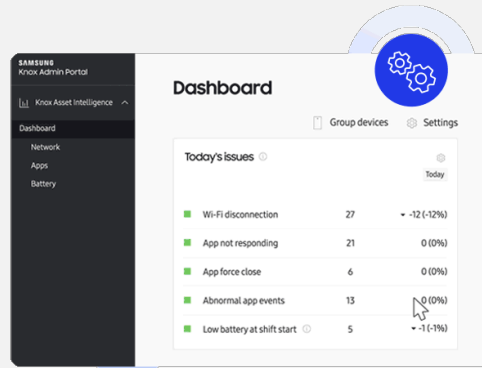
# Tools available to deploy & manage Knox Native Solution

## 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.

# Thank you



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