



Samsung Knox Native Solution 2026

Knox Native Solution for Classified Use

from...

Crypto-MicroSD as HW-Security Anchor



High effort and cost due to additional HW and manual handling

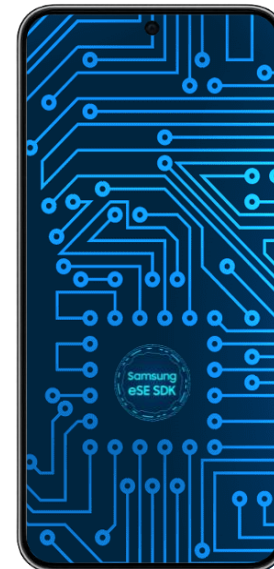


Slow certification process
Every solution partner needed to certify their solution from scratch



...to

embedded Secure Element (eSE) as HW-Anchor



Lower cost through automatic provisioning of cryptographic keys



Go-to-Market faster because Samsung runs the platform approval with BSI



No vendor-specific container view but consistent and native Customer Experience



Government keys protected in eSE, integrated into Knox platform



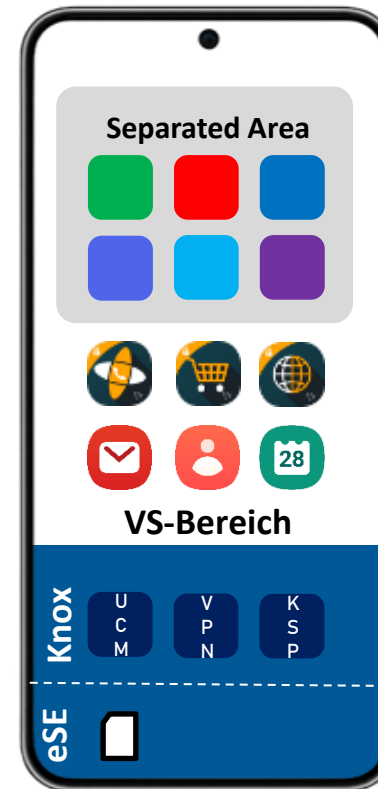
02 Update

Secure Domain Concept

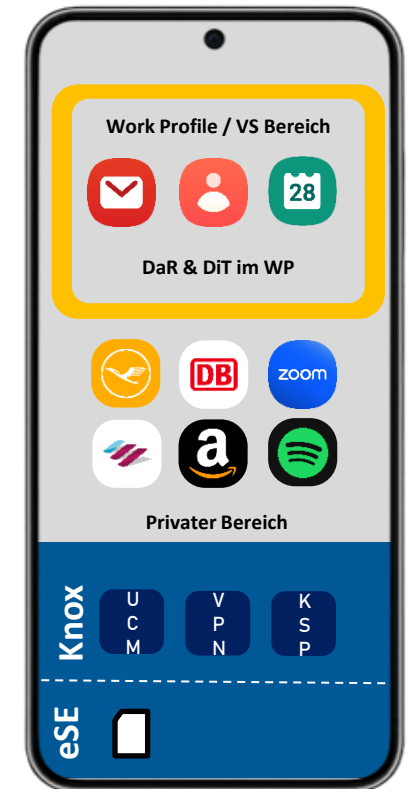
A **fully managed device** in which evaluated applications can be installed, with a separate area for other applications

- **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

Fully managed
separated apps



Work profile company
owned





03 Ecosystem



Knox Native Portfolio

Galaxy
Z Fold7



Galaxy
S25 5G EE



Galaxy
S25 Ultra 5G



Galaxy
S24 5G EE



Galaxy
S24 Ultra 5G EE



Galaxy XCover7
Pro EE



Galaxy Tab Active5
Pro EE



Galaxy Tab
Active5 EE



Galaxy Tab
S10 FE EE



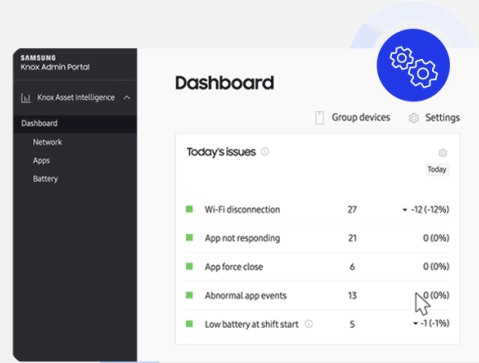
Tools available to deploy & manage Samsung Smartphones

SAMSUNG Knox Suite

Cloud based Plattform



Knox Mobile Enrollment



Knox Asset Intelligence



Knox E-FOTA



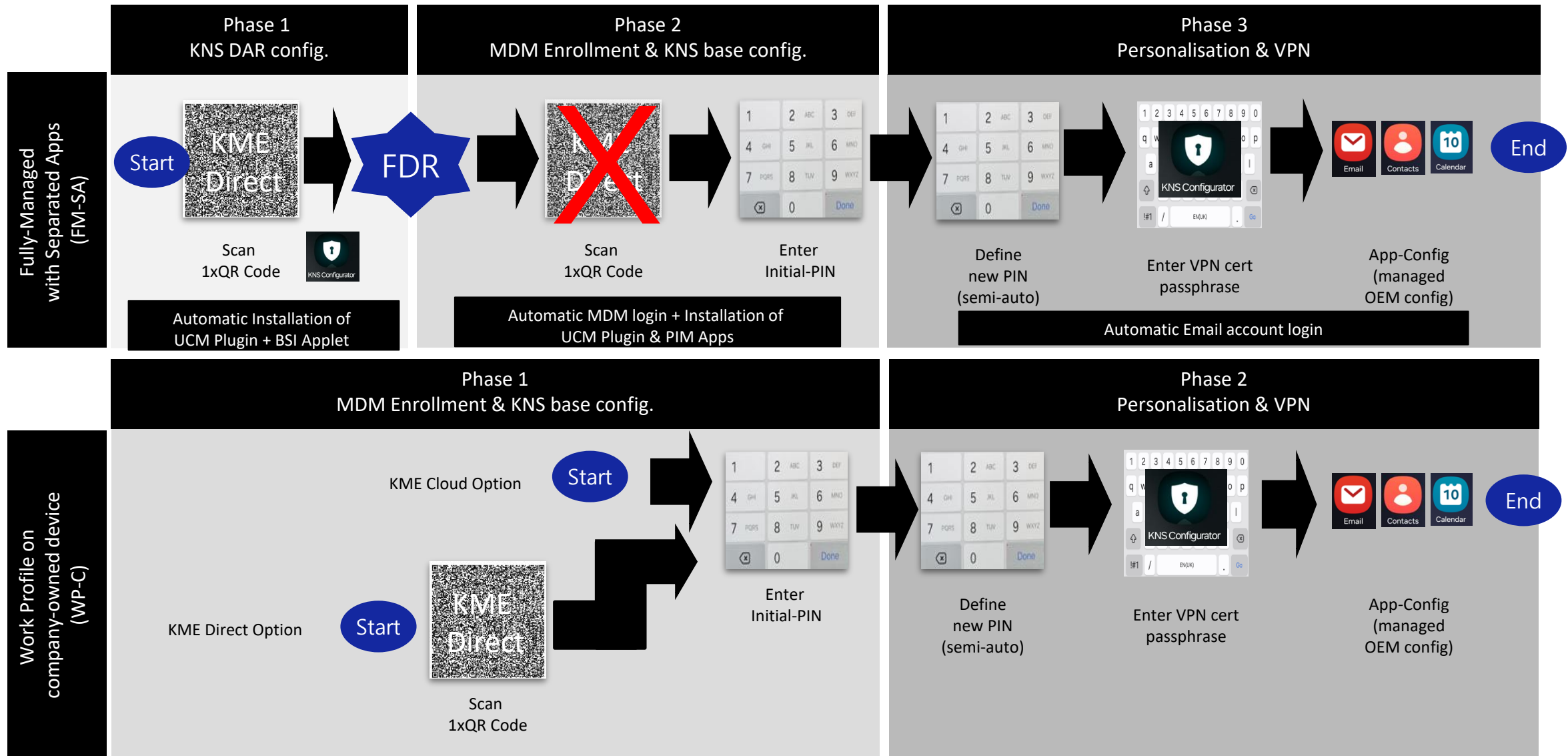
Knox Manage
or Samsung SDS EMM*

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



03 KNS Enrollment

Enrollment of KNS will be improved to reduce user interactions during the setup and improve the speed of the device installation.

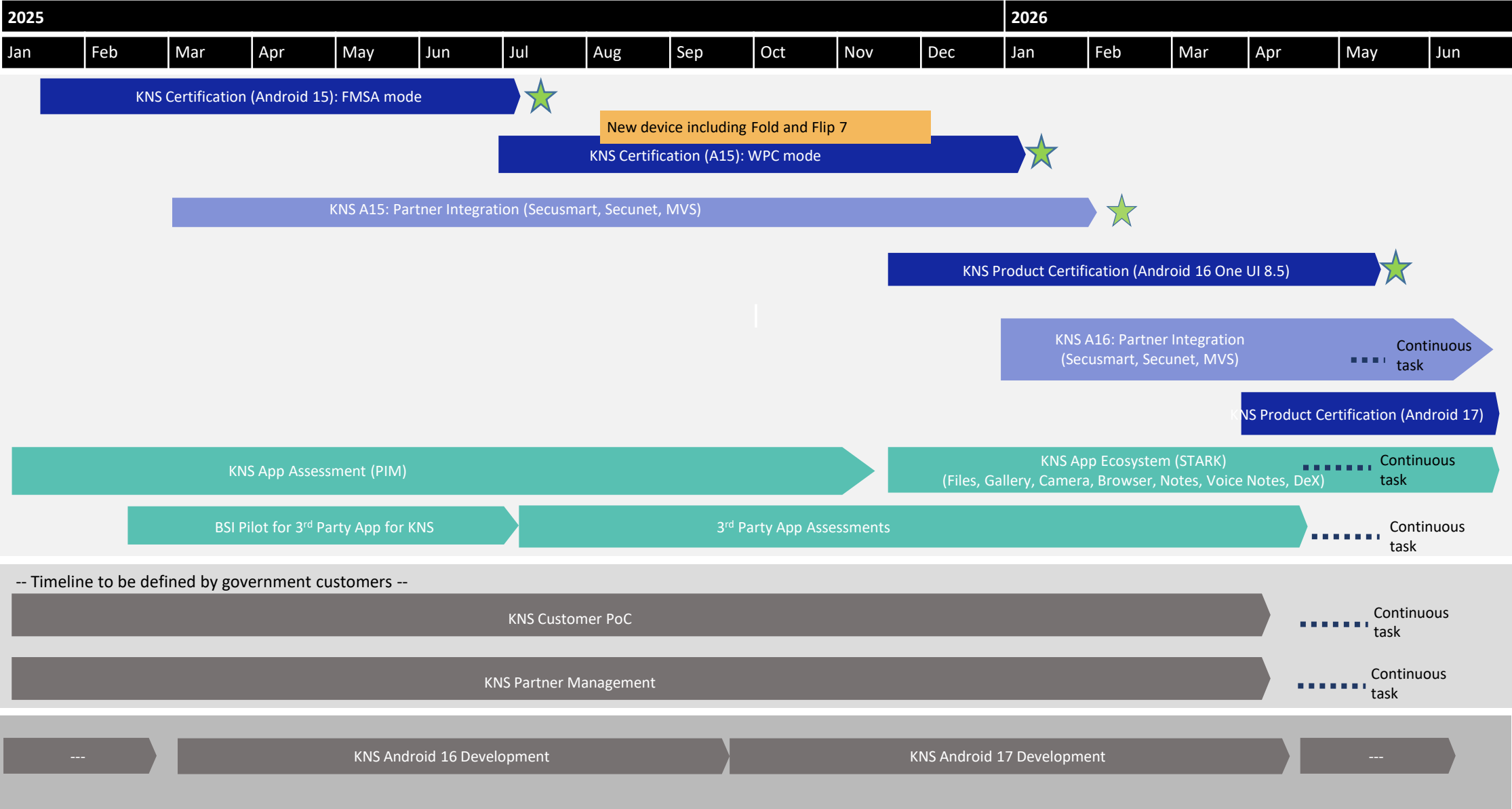




KNS Roadmap 2025/2026

Confidential

KNS Roadmap – Overall view



KNS Roadmap

Roadmap – technical implementation November 2025

- Support for RSA4K with Keystore for Samsung email app
- Key Agreement
- DNS traffic handling for VPN
- Support for PURPOSE_WRAP_KEY
- VPN/KSP feature enhancements
- Samsung KNS approved Apps enhancements
- New DeX support
- Improved KME Enrolment for FMSA Mode
- Keypair generation for UCM KeyChain

Roadmap - Candidate for Android 17

- ACME for trial with new flagship
- App Isolation features in Knox SDK
- URI transfer feature for Separated Apps (0 to 10)
- Copy paste and clipboard controls
- System apps hardening

Android 16 Roadmap (1)

Support RSA4K with Keystore for email app

- Android Keystore is the most reliable device method to support RSA4K
- Keys are protected by the TEE but stored outside of BSI Applet protection
- Android Keystore keys must be stored in CE protected space or with a security binding to the BSI Applet

DNS Traffic Handling for VPN

- Device sends traffic to a configured DNS server before the VPN is fully established
- Potentially leaks sensitive customer information outside the VPN
- Issue is in the Google tethering mainline module
- Fixed in the mainline release and now needs testing on B OS

Key Agreement

- Allow a remote application to securely exchange or agree a key
- Applet needs to support required algorithms
- UCM framework needs to implement the KeyAgreement JCE API
- Applet supports ALG_EC_SVDP_DH_PLAIN

Support for PURPOSE_WRAP_KEY

- PURPOSE_WRAP_KEY should only allow a key to be used to wrap and unwrap other keys as part of secure key imports
- Current bug in the implementation means this operation also requires the PURPOSE_ENCRYPT/PURPOSE_DECRYPT
- These purposes are too permissive for keys that should only be used for wrapping/unwrapping
- applet allows encrypt/decrypt if key has only 'PURPOSE_WRAP_KEY

Android 16 Roadmap (2)

VPN/KSP feature enhancements

- KSP will be updated to allow the admin to allow or block certain VPN ciphers for IKE/ESP connections
- KSP should support the use of "*" when setting the package allow or block list for the Knox VPN

Improved KME Enrolment for FMSA Mode

- Current enrolment requires two QR codes. One for DAR configuration and the other for normal enrolment
- KME will now allow just one QR code for KNS enrolment
- After the factory data reset, KME will detect the DAR configuration and automatically enrol the device based on the IMEI

New DeX support

- DeX is being integrated into Android's Desktop Windowing – known as New DeX
- APIs provided by Classic DeX are being deprecated and will no longer function as expected in Android 16
- DeX is still an important feature for KNS users and partners

Keypair generation for UCM KeyChain

- To allow partner SCEP client to make use of eSE to generate Keypair
- To make the keypair and certificate available to other applications (Keychain)
- Same keypair could be used with different CRL protocol

Android 17 Roadmap (1)

ACME for trial with new flagship

- Knox ZT framework implements the ACME protocol, but without eSE integration
- Add eSE device attestation to allow an IT admin to verify identity and trustworthiness of a device during certificate enrolment
- Applet to do the attestation will only be available in the next device chipsets

Secure domain enhancements (TBD)

- Implementation of an intent firewall to restrict inter-process communication
- Android supports good cross profile data flow controls but internal to the profile, the control is limited
- Solution helps to protect the DIU PIM data within the Secure Domain

URI transfer feature for Separated Apps

- In certain instances, users need to copy and paste information from work to personal side (Ex. Teams call)
- Samsung should provide the user with a dialog that explains the implications and allows user to proceed
- New KPE APIs are required to control this policy

Android 17 Roadmap (2)

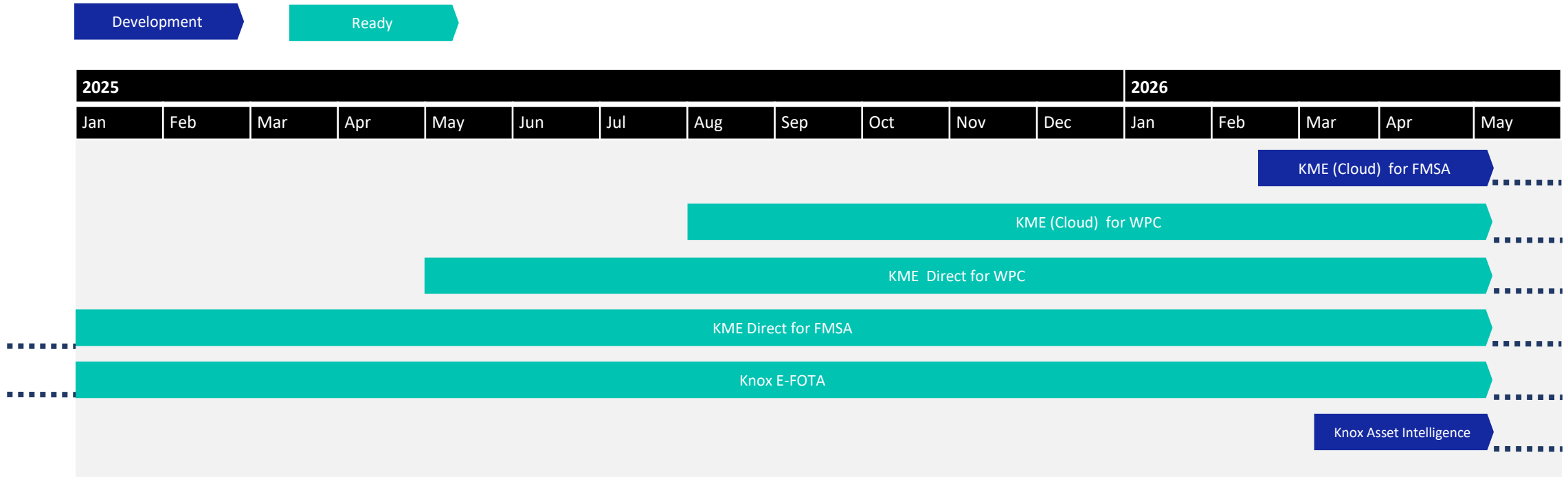
Copy paste and clipboard controls

- Create an allow-list of applications that may access the clipboard
- Allow only KNS Secure Domain applications to use the clipboard
- New KPE APIs to support controlling this policy

System apps hardening

- Make sure system apps have only the permissions they require
- Where possible, do not sign system apps with platform key

Knox Cloud Services – Availability for classified use



- KME Cloud needs to be updated for supporting FMSA mode, due to specific Rollout behaviour of the device.
- Minor changes for WPC
- Knox Asset Intelligence will be evaluated with Android 17, if official customer Request will be raised.

Добро дошли

Почетак





04 Partner Solution



SecuSUITE für Samsung Knox & Knox Native Roadmap

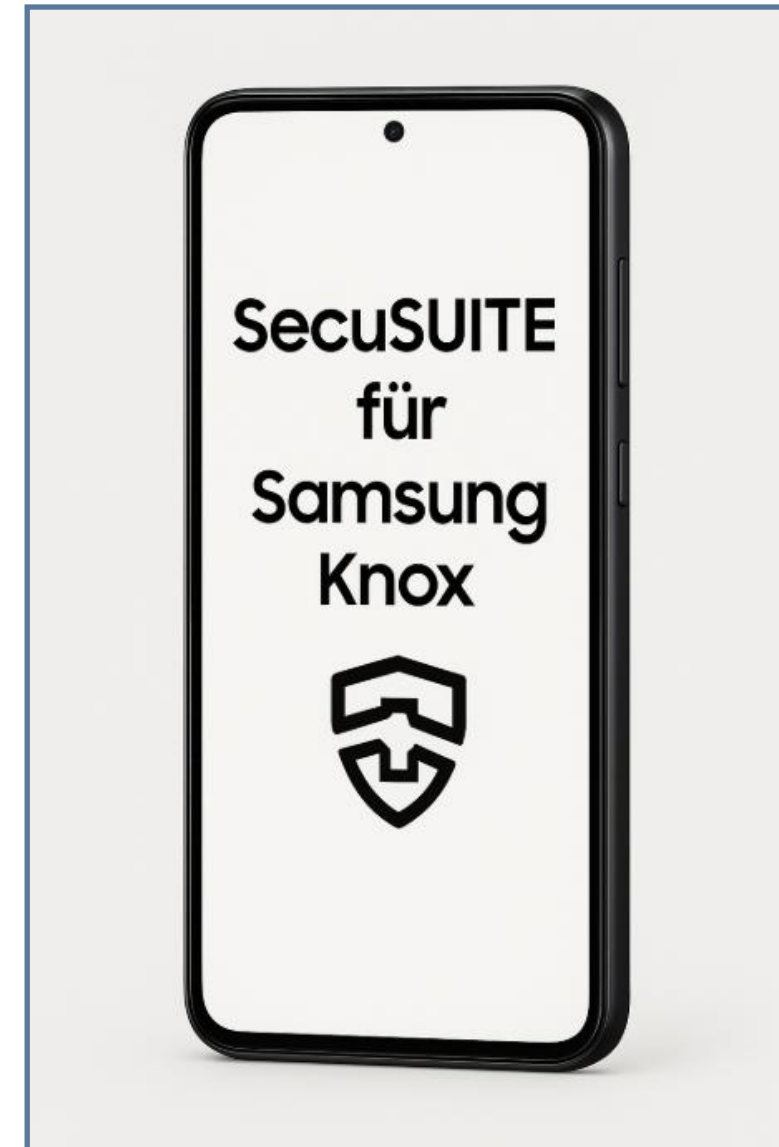
20.01.2026 Berlin

Oliver Krüger, Senior Director Technical Product

SS4SK in a Nutshell

SecuSUITE für Samsung Knox

- ist auf mehr als **100.000 Geräten** im Feld ausgerollt
- unterstützt **Samsung Geräte** - Smartphones, Foldables und Tablets
- geeignet für **Selbstentwickelte & Standards-Apps** ohne App-Anpassung
- unterstützt die Nutzung von **persönlichen** und **dienstlichen** Apps
- hat einen **eigenen Freigabeprozess** für dienstliche Apps
- unterstützt heute **25 native Apps** zur Verarbeitung von **VS-NfD**
- **Desktop-Modus** via DEX auf Tablets und Smartphones



SS4SK: Ihr VS-NfD Arbeitsplatz

Browser



SecuFOX

Voice



SecuVOICE

PIM



BB Hub

Office



SecuOFFICE

Utilities



Camera



Gallery



SecuDRIVE

Messenger & Video



Webex



Bw
Messenger

Virtual Desktop



Horizon



Citrix



Customer Apps



...

PDF Viewer



Acrobat
Reader



Foxit
PDF

Secusmart Produktportfolio für Samsung Knox

SecuSUITE für Samsung Knox

- SecuSUITE Core & optionale sichere Apps
- Integration von KNS ab der Version SS4SK 2.0.0
- Geräterücksetzung nicht erforderlich
- Sicherung von Apps mit SPL



- Im eSE laufen SSA & BSI Applet parallel

SecuSUITE Apps für Knox Native Solution

- Bereitstellung von SecuSUITE Core Apps BBHub, SecuOFFICE, SecuFOX, SecuDRIVE und SecuVOICE auf KNS
- Optionale SecuSUITE-Apps nutzen die App Shield-Technologie, um nativ auf KNS zu laufen (minimale SPL-Technologie angewendet)



- Im eSE läuft ausschließlich BSI Applet

In Aufbau: KNS VS-NfD Arbeitsplatz

Browser



SecuFOX

Voice



SecuVOICE

PIM



BB Hub

Office



SecuOFFICE

Utilities



Camera



Gallery



SecuDRIVE

Messenger & Video



Webex



Bw
Messenger

Virtual Desktop



Horizon



Citrix

Customer Apps



...

PDF Viewer



Acrobat
Reader



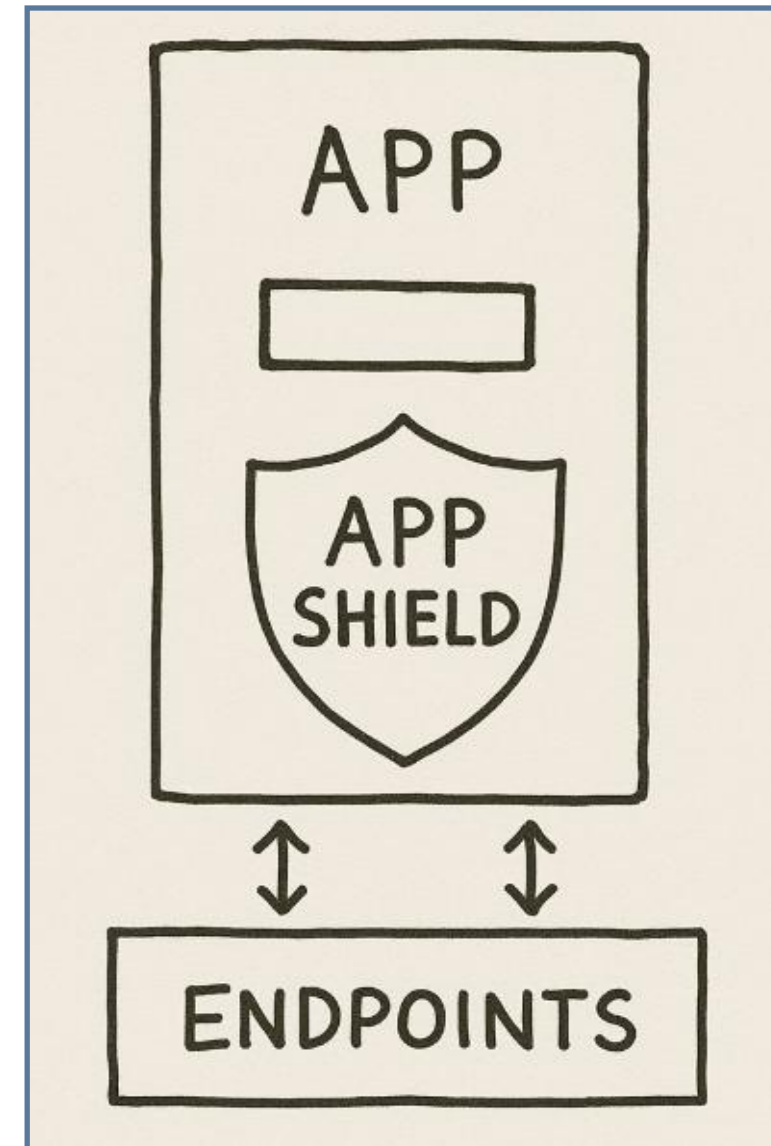
Foxit
PDF



Funktion des App Shields

Zulassung von Apps auf KNS:

- **Prüfprozess beim BSI:** Für die Zulassung müssen Apps einen Prüfprozess beim BSI durchlaufen
- **Sicherheitskriterien:** Der Prozess prüft, dass keine vertraulichen Daten abfließen, z.B. keine VS-Daten ins Systemlog geschrieben werden oder Websockets verwendet werden
- **App-Shield-Technologie:** Implementiert die Anforderungen des Prüfprozesses, sodass Apps als sichere KNS-Apps genutzt werden können
- **Evaluierte Technologie:** Grundlage des App Shields ist die Data-in-Use Protection des Security Policy Layers, dessen Zulassung im Rahmen von KNS schnell erfolgen kann



SecuSUITE Apps für Knox Native

SecuSUITE Core Apps:

- Für Pilotierung bereit: SecuSUITE Core Apps (BB Hub, SecuVOICE, SecuOFFICE, SecuDRIVE, SecuFOX) stehen bereit
- Freigabe von SecuFOX für KNS im Q1/26 erwartet
- Weitere SecuSUITE Core Apps werden im Q1/26 eingereicht

SecuSUITE Optional Apps:

- Basierend auf dem KNS Release für Android 16 werden die SecuSUITE Apps (Core und Optionale Sichere Apps) mit Hilfe der App Shield Technologie verfügbar gemacht



Ihre App für Knox Native?

Sprechen Sie uns an!

- **Secusmart** ist Ihr **erfahrener Partner** bei der Zulassung von Apps auf Mobilien Plattformen
- Wir unterstützen Sie bei der **Zulassung Ihrer eigenen App**:
 - Erstellung von Unterlagen für die Zulassung
 - Durchführung von Sicherheitsanalysen für den Zulassungsprozess
 - Technisches Enablement mit und ohne App Shield

