SAMSUNG

White Paper

Samsung Knox

Version 1.5 — July 8, 2021

Copyright

About this White Paper

This White Paper provides an overview of Samsung Knox, focusing on the unique advantages that differentiate it from other options in the mobile device security market.

This document is designed for C-level executives, security professionals, IT managers, IT admins, and others evaluating Samsung Knox as a solution. For additional information, go to samsungknox.com.

Revision History

Version	Knox Version	Date	Revisions
1.4	3.7.1	May 1, 2021	New info about Knox Vault and Separated Apps. Updates to Device Health Attestation, Universal Credential Management, and Knox Warranty Fuse.
1.3.1	3.5	May 7, 2020	Updates to Knox Certifications.
1.3	3.5	March 31, 2020	Replaced Feature Comparison with Feature Summary.
1.2	3.4	September 17, 2019	Updates to Device Health Attestation.
1.1	3.3	February 20, 2019	New info about DualDAR Encryption and Knox Verified Boot. Updates to Feature Comparison and Sensitive Data Protection.
1.0.1	3.2	November 1, 2018	Minor revisions.
1.0	3.2	September 12, 2018	First release.
1.5	3.2	July 8, 2021	Updates to Knox Vault

Table of Contents

Introduction

Samsung Knox

Samsung's Knox platform brings defense-grade security on the most popular consumer devices to all enterprises. The Knox Platform provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features commonplace in today's mobile device market. The Knox platform is the cornerstone of a strong mobile security strategy supporting a wide variety of Samsung devices.

Why use Samsung Knox?

The Knox platform helps you and your enterprise avoid the security gaps common on many mobile platforms. Knox received *strong* ratings in 25 of 28 categories in Gartner's December 2017 Mobile OSs and Device Security: A Comparison of Platforms and has received strong ratings for the last three years in a row.

The Knox Platform's security hardening supports every aspect of mobile device operation. The Knox Platform enables trust in your mobile endpoints with advanced features like the evolutionary Knox Vault to the patented Real-Time Kernel Protection (RKP). The Knox Platform ensures IT admins can securely bulk deploy the best mobile device hardware, and quickly integrate with existing business infrastructure and apps.

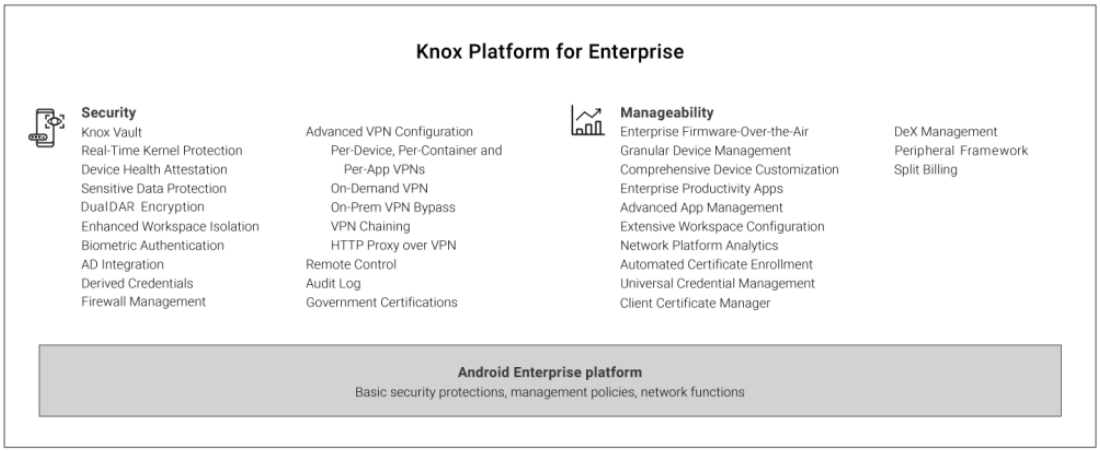
Key benefits for enterprises

- Easily meet your organization's security and compliance requirements by providing solid platform integrity, strong data protection, and fine-grained policy enforcement.
- Seamlessly activate and manage Knox Platform features through an Enterprise Mobility Management (EMM) system.
- Flexibly support infrastructure, deployment, and management requirements through centralized remote device control, advanced VPN management, allowing and blocking apps, and granular policies that control all aspects of Samsung devices.
- Effortlessly upgrade from Android Enterprise, leveraging a comprehensive set of Knox Platform benefits without affecting existing deployments.
- Securely deploy the innovative Samsung Desktop Experience (DeX) in new work environments, unifying mobile and desktop computing on one device.

The Knox Platform's cutting-edge security technology continues to be widely adopted and proven by numerous government, security, and financial agencies throughout the world. Samsung continually works with global government organizations and international regulatory bodies to meet a wide range of certification requirements designed to protect public safety and consumer privacy.

Knox Platform highlights

The Knox Platform provides a robust set of features to fill security and management gaps, resolve pain points identified by enterprises, and meet the strict requirements of highly regulated industries. Key strengths include the following:



For a quick overview of these features, see Feature Summary.

Security highlights

The following sections describe how the Knox Platform provides an industry-leading ecosystem of products and services to secure and ease mobile device management.

Hardware-backed security

The Knox Platform defends against security threats and protects enterprise data through layers of security built on top of a hardware-backed trusted environment.

- **Trusted environment** — A trusted environment separates security-critical code from the rest of the operating system. This strategic separation ensures only trusted processes that are isolated and protected from attacks and exploits can perform sensitive operations, such as user authentication and key encryption and decryption. Trusted environments perform integrity checks prior to executing any software. These checks detect malicious attempts to modify the trusted environment and the software running on the device.
- **Hardware-backed** — A trusted environment is hardware-backed if hardware protections isolate the environment from the rest of the running system. This isolation ensures that vulnerabilities in the main operating system don't directly affect the security of the trusted environment. The environment also ties integrity checks of the software running in the trusted environment to cryptographic signatures stored in the device hardware. Hardware-backed integrity checks prevent an attacker from exploiting software vulnerabilities to bypass protections and load unapproved software into the trusted environment.

The Knox Platform uses a hardware-backed trusted environment and the specific components depend on the device hardware. For example, ARM processors provide a Trusted Execution Environment (TEE) that leverages components such as the ARM TrustZone, ARM Hypervisor Mode, and Embedded Secure Elements. Knox features that use the trusted environment include Real-time Kernel Protection (RKP), Trusted Boot, Device Health Attestation, Certificate Management, Sensitive Data Protection (SDP), and Network Platform Analytics (NPA).

Futhermore, the Knox Vault introduced with the Samsung Galaxy S21 offers an isolated, tamper-proof, secure subsystem with its own processor and memory. Knox Vault operates completely independently from the primary processor running the Android OS, and guards against attacks that exploit shared resources, such as software side-channel attacks that can compromise other software executing on the same processor. This separation means Knox Vault protects sensitive data even if the primary processor itself is completely compromised.

App isolation

The Knox Platform uses app isolation to prevent rogue apps from intentionally or inadvertently accessing unauthorized data. The Knox Platform provides several forms of app isolation to create a protected app container space on Samsung devices. Each option is based on the same core isolation technology called Security Enhancements for Android (SE for Android.) SE for Android is an integration of SELinux and Android, expanded to cover Android components and design paradigms. The Knox Platform offers these options:

- **Android Enterprise on Samsung devices** — Android Enterprise provides app isolation through work profiles, which provide basic isolation of enterprise apps from personal apps. When using Android Enterprise on Samsung devices, Knox provides features like Real-time Kernel Protection (RKP), secure enterprise apps, and hardware-backed storage of certificates and keys, making Android Enterprise even better on Samsung devices.
- **Separated Apps** — For enterprises that need full control over a corporate-owned device, while still enabling authorized third-party business apps, Samsung exclusively offers Separated Apps to isolate third-party apps in a sandboxed folder.
- **SE for Android Management Service** (SEAMS) — With SEAMS, you can isolate a single app or small set of trusted apps, to lock down the apps in the same container. SEAMS containers have no special GUI. Apps in a SEAMS container appear with the rest of the apps on the device, but are differentiated with a shield badge to show that they're isolated and protected from apps not sharing their same container. You can create as many of these SEAMS containers as you want on-the-fly.

Data protection

Enterprises can protect personal and enterprise data on mobile devices using a rich set of Knox features:

- **User authentication** — Samsung Knox devices support not just password, PIN, and pattern authentication but also the latest biometric authentication such as ultrasonic fingerprint sensors. Options are available for both device lockscreen authentication as well as work profile authentication. Through the Knox Platform, you can enforce two-factor authentication or enterprise AD credentials for the work profile to ensure stronger data protection.
- **Encryption of device data** — Samsung Knox devices provide data encryption through Sensitive Data Protection, which binds to the hardware-backed Root of Trust and user authentication. This encryption ensures data is decrypted only on the device where the data is stored, and only by the device owner. DualDAR Encryption offers two instances of encryption to achieve an even higher level of reliability.
- **Encryption of network data** — Samsung Knox devices offer the widest selection of advanced VPN features, providing the ability to configure a separate VPN for individual apps to reinforce data isolation even further. Knox also offers always-on VPN, on-demand VPN, on-premise VPN bypass, HTTP proxy over VPN, multiple active tunnels, strict data leakage controls, and VPN chaining or cascading.
- **Device tracking, locking, and erasing** — Samsung Knox devices offer the ability to track, geofence, and automatically lock devices based on events and security policies. For example, a device that leaves a specified geographic perimeter is locked, wiped of data, or reset to factory defaults.

Manageability highlights

Device management and deployment

Enterprises with tens, hundreds, or thousands of employee mobile devices need to manage them easily, securely, and efficiently. Through EMM systems, IT admins can use a web console to centrally manage remote devices over-the-air. IT admins can control Samsung Knox devices comprehensively, managing device features with ease.

This management is possible through the Samsung Knox SDK, which offers over 1300 APIs for granular and flexible control over Samsung devices. This functionality is on top of the basic APIs offered through the Android SDK, providing an even more powerful superset of capabilities. An EMM app on an employee device receives IT admin commands from the EMM web console, and calls Knox APIs to deploy commands on Knox devices. This integration enables enterprise IT admins to deploy IT policies to manage and secure every aspect of Knox devices.

Device management services

To address a variety of business needs beyond security, the Samsung Knox portfolio is complemented by robust cloud services that ease mobile device deployment, customization, and management. These services include:

- **Knox Mobile Enrollment** — With this free service, enterprises can use a web console or REST API calls to automate device enrollment, either individually or in bulk. After an IT admin registers a device with this service, the device user simply turns it on and connects it to a Wi-Fi or 3G/4G/5G mobile network to enroll it with an EMM system. There is no manual enrollment of individual devices, and no need for IMEI management and verification – all onerous, time-consuming, and error-prone tasks.
- **Knox Configure** — Samsung phones, tablets, and wearables are fully customizable to work in numerous vertical markets such as hospitality, retail, and entertainment. Through a web console, Systems Integrators can create purpose-built devices that present a customized user interface, for example, an information kiosk, point-of-sales terminal, or in-flight entertainment system. The Systems Integrators can customize or restrict almost all aspects of device configuration and the user experience, including boot animations incorporating custom enterprise logos, display settings, wallpapers, network configurations, notifications, and software updates.

Learn more

This White Paper provides an overview of the Knox Platform's security features and how they can resolve common enterprise mobile deployment pain points. The document focuses on the unique abilities of the Knox Platform. For information about other features, see the Samsung Knox website.

Feature Summary

For those wanting a quick reference to the security, manageability, and advanced VPN features offered by Samsung Knox devices, review the summary below. For details about how Samsung Knox differentiates compared to other OEM devices, speak with your Samsung account manager or contact us if you do not have one.

Feature	Summary
Security	
Hardware-Backed Keystore	This feature is a hardware-dependent claim. All Samsung Knox devices have keystores backed by hardware protections.
Secure Lockdown on Tampering	Upon detecting critical security compromises, the system locks down sensitive areas, preventing unauthorized enterprise data access and leakage. When there is evidence of device tampering, Samsung prevents users from accessing the data in a work profile or on a fully managed device. To unlock the device again, one needs to factory reset the device, which wipes out the data inside.
Remote Device Health	Get visibility into which devices have security issues like unauthorized firmware, allowing you to take action right away. Knox checks the record of IMEI tampering and whether the warranty bit is blown.
Knox Vault	An isolated, tamper-proof, secure subsystem with its own processor and memory, Knox Vault stores sensitive data such as hardware-backed Android Keystore keys, the Samsung Attestation Key, biometric data, and blockchain credentials. It runs security-critical code that authenticates users with increasing timeouts between failures and controls access to keys depending on authentication.
Keystore Support of eSE & Other High-Security Storage	Numerous services require credentials for access. They include Wi-Fi, VPN, email, and websites. In order to safely store sensitive credentials, developers need to write new credential storage code for any new storage hardware. Knox provides a plug-and-play framework for credential management across a variety of hardware, eliminating the need to develop in-house credential management implementation logic.
Sensitive Data Protection (SDP)	SDP keeps data encrypted while a work profile or fully managed device is locked, even during runtime when other solutions decrypt data.
Real-Time Kernel Protection (RKP)	Drastically limits possible attacks on Samsung devices with best-in-class kernel attack prevention features: Kernel Text Protection (KTP): Protects against any attempt to forge or manipulate Kernel text (code and RO data). Page Table Protection (PTP): Protects against any attempt to forge or manipulate the Kernel and user page table. Kernel Data Protection (KDP): Protects against any attempt to forge or manipulate the Kernel namespace/credential/security ID/double map including kernel code, kernel data, and kernel control flow protections. Control Flow Protection (CFP): Prevents Return-Oriented Programming (ROP) and Jump-Oriented Programming (JOP) attacks that re-use existing kernel logic to piece together exploits from the kernel's own code.
DualDAR Encryption	With a single instance of encryption, potential flaws in the implementation can result in a single point of failure. KPE DualDAR provides two independent layers of encryption to achieve an even higher level of reliability by enabling redundancies in protecting Data-At-Rest. You can further strengthen data encryption by using a third-party cryptographic module to customize encryption. This dual encryption is required for classified deployments. Note that there is an additional license fee to use DualDAR.
ML Model Protection	Machine Learning and Neural models come with unique security challenges that are difficult to address without support from the mobile operating system platform. Knox ML Model Protection leverages the Knox platform to provide developers with the secure encryption, operation, and access control of ML models.
Enforced Two-Factor Authentication	Enables IT admins to force end-user two-factor authentication for logging in to a work profile or fully managed device. Two-factor authentication is done through a combination of biometrics (fingerprint, iris, face) and more traditional means (password, PIN, pattern).

Feature	Summary
Government-Grade Common Criteria Mode	Simplifies configuring devices into a compliant state for Common Criteria (national security) deployments.
Separated Apps	For enterprises that need full control over a corporate-owned device, while still enabling authorized third-party business apps, Samsung exclusively offers Separated Apps to isolate third-party apps in a sandboxed folder.
App Isolation Groups (SEAMS)	Unlike classic app containers with a GUI, you can manage "invisible" app isolation groups to protect a set of apps from any other set. Up to 300 groupings are possible.
Secure Certificate Enrollment Agents (SCEP, CMP, CMC_EST protocols)	Samsung provides a free set of certificate enrollment agents that follow the latest security protocols. There is no reason to enroll certificates insecurely, or implement your own protocols.
Manageability	
Audit Log	Provides comprehensive and detailed device audit logs, recording numerous extra types of events in the areas of system security, authentication, app management, data protection, network connectivity, and peripheral control. Satisfies government requirements for security audit trails.
Device Software Updates	Knox E-FOTA running on top of KPE enables IT to deploy a particular firmware version that is not necessarily the latest version. These selective firmware updates provide a stable environment for business apps and services. KPE allows firmware updates under certain conditions such as a particular time of the day, network (Wi-Fi or mobile), or battery power status. These features help optimize productivity and ensure a successful upgrade.
Remote Control	KPE enables IT to remotely control devices, by injecting finger, keyboard, and mouse events. This is in addition to remotely viewing devices.
Peripheral Framework	In addition to managing mobile devices, you can use the Samsung Knox SDK to manage peripherals like barcode readers that are connected to or integrated with devices. Through a peripheral framework, partners can easily automate the setup, monitoring, diagnostics, and control of different peripheral models.
Customization	Allows IT to customize various aspects of the device software and UI. In addition to more common capabilities, KPE provides these additional abilities: • Change the bootup logo • Change power behavior such as auto power on/off • Change homescreen layout • Remap hardware key such as PTT and Emergency • Configure Settings at a deep granularity • Extend battery life by allowing charging only up to 80%
Granular Roaming Controls	IT can control which mission-critical apps are allowed to use data during mobile roaming, which often incurs high call, text, and data rates. AE only allows IT admins to disable mobile data – it can't block calls or app update downloads while allowing other mobile data use. KPE Premium also enables separate roaming controls for each APN.
Admin Device Lock	Knox allows IT admins to remotely lock a device in a way that a user cannot unlock at all. In addition, Knox allows controlling the personal space and work profile separately. For example, the personal space can be open while the work profile is locked.
Data Sharing Policy	KPE provides data sync of Contacts, Calendar, and Notifications. Also, KPE provides a unified Calendar with both personal and work events.
Firewall Management	Industry-exclusive ability to set on-device firewall rules. KPE can also notify IT when employees attempt to visit blocked domains.
Granular Device Policies	Meet compliance or other deployment requirements with policies not supported on AE for SMS/MMS disclaimers, RCS/SMS/MMS logging, call restrictions, read and write restrictions on SD cards, granular Bluetooth profile restrictions, and even manage DeX deployment settings.
Advanced Workspace Configuration	Enables strict policy enforcement for Bluetooth, SD Card, USB, and other technologies inside the work profile, while allowing full use outside the work profile.

Feature	Summary
Unlock using Active Directory Credentials	No need to make employees remember separate credentials for Windows laptops and mobile devices. Device users can use their existing Active Directory credentials to unlock their devices.
Split Billing (Dual APNs)	Enables enterprises to pay only for the data usage of their approved business apps. Employees are responsible for fees for personal data usage.
Network Analytics	Allows IT to deploy network threat detection solutions without granting such tools complete access to all network traffic. For details about the insights provided, see Network Platform Analytics.
VPN	
VPN Granularity: Per-App, Per-Container, or Whole Device	KPE provides the most granular VPN controls. In addition to configuring a VPN for an app, work profile, or fully managed device, KPE can configure a single VPN for the entire device — that is, work profile as well as fully managed device.
Non-bypassable VPN	KPE has strict controls that block any traffic from bypassing a configured VPN, even in edge cases where a device is rebooting, a VPN client crashes, an app accesses the physical interface directly, or an app using a VPN is deleted and re-installed.
On-Demand VPN	KPE can activate a VPN only when a target app is launched. Such a feature allows customers to save on service fees from unused VPNs.
HTTP Proxy over VPN	KPE has a wide range of network protocols that can use HTTP Proxy. No auth, basic auth, NTLM v2 auth Both IPv4 and IPv6 are supported
VPN Chaining	Allows the use of two VPN tunnels to double-encrypt traffic, enhance anonymity, and prevent a single security bug in a VPN layer from compromising network encryption.

Core Platform Security

Root of Trust

Imagine every device on your network simultaneously infected with malware and combing through your confidential data. Attacks and exploits continue to mature in sophistication in an attempt to stay ahead of advancing mobile device safeguards. So what's the single solution that works on all devices at the same time? Building a robust Root of Trust stack that minimizes exposure, detects intrusions, and locks down sensitive information.

A Root of Trust is the cornerstone of any modern security protocol. It is a series of stringent checks and balances, beginning at the hardware level rather than the software level. This feature adds a level of security to devices, making them difficult to attack since hardware is less mutable than software.

A Root of Trust answers many complicated security questions, such as:

- How do you **know** if a compromised OS was booted at runtime?
- Can you **trust** that your certificates are stored securely?
- Has an exploit **modified** the kernel or other system software?

Samsung's approach to addressing this issue is to bottleneck all security-critical functionality through trustworthy components. These trustworthy components are thoroughly designed, reviewed, and maintained with the following considerations:

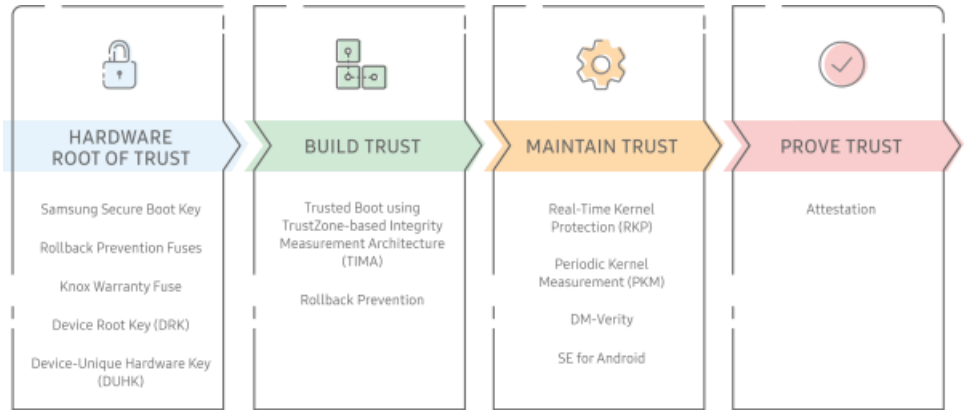
- **What are the assurances required?** High-security enterprise partners require near-total ability to control and audit the software interfacing with their systems. Device users must have the authority to deny permission to use their device features and data. Each user, partner, and integrated system has its own requirements, many of which are assured in large part through the Roots of Trust.
- **How can components contribute to more complex assurances?** A Trusted Boot process enables the trustworthy transfer of control from the bootloader to the Android framework. This trustworthy transfer of control plays a key role in the IT admin's ability to audit apps running on the device. Secure boot is a complex process built on top of many smaller components that validate software, configuration files, deployment processes, and update processes. Each of these smaller components contributes to the secure boot process, and a secure boot process itself contributes to the security of other processes.
- **How can we make these components, their assurances, and their usage more robust?** Each Trusted Application on a Samsung Knox device ultimately represents each Root of Trust. These Trusted Applications encompass functionality such as device identity, key management, and remote attestation of device health. Samsung Knox uses these same Trusted Applications to provide its own assurances.

Knox Platform trusted environment

The Knox Platform builds a unique, industry-leading trusted environment in four ways:

- **Establishes** a hardware-backed Root of Trust, on which other components rely.
- **Builds** trust during boot, through features like Trusted Boot.
- **Maintains** trust while the device is in use, through features like Real-Time Kernel Protection.
- **Proves** its trustworthiness on demand, through Device Health Attestation.

This process and its components are as follows:



How the Root of Trust works

1. Knox Platform security starts in the factory—before users even power on their device—when a Device-Unique Hardware Key (DUHK) is generated on the device using its hardware random number generator.
2. Next, the DUHK generates and encrypts the Device Root Key (DRK) and Samsung Attestation Key (SAK).
3. Upon device start up, Samsung uses the Samsung Secure Boot Key (SSBK) to check all software components. One of the components is the TrustZone Secure world, a chip partition reserved for secure code and data. Only specially privileged software modules running within the TrustZone Secure world can access these keys.
4. The software performs a check on each Knox Platform feature before allowing it to run. Since this chain of security checks begins with the very first hardware check, each feature is protected by hardware Root of Trust. No matter which link in the chain an attacker targets, one of the security checks detects it.

Secure hardware

The Knox Platform trusted environment leverages the following hardware components.

- **Bootloader ROM** — The Primary Bootloader (PBL) is the first piece of code to run during the boot process. The PBL is trusted to measure and verify the boot chain. To prevent tampering, the PBL is kept in the ROM of the secure hardware. The device hardware loads and runs the PBL from ROM at boot, and the PBL starts the Secure and Trusted Boot processes.
- **ARM TrustZone Secure world** — The Secure world is the environment in which highly sensitive software runs. The ARM TrustZone hardware ensures memory and components marked secure (for example, a fingerprint reader) can only be accessed in the Secure World. Most of the system, including the kernel, middleware, and apps, run in the Normal World. The Secure world software, on the other hand, is more privileged, and can access both Secure and Normal world resources.
- **Knox Vault** — The Knox Vault is an independent, tamper-proof, secure subsystem with its own processor, memory, and an interface to dedicated non-volatile storage. The Knox Vault stores sensitive data such as cryptographic keys and authentication data. Even if the main application processor that runs Android is compromised, the Knox Vault protects secrets and guards against hardware attacks such as probing and fault injection.

Hardware keys

- **Device-Unique Hardware Key (DUHK)** — Samsung incorporates the DUHK, a device-unique symmetric key, in the device hardware during the initial manufacturing of the device. The DUHK binds data—for example, device health attestation data— to a particular device and is accessible only by a hardware cryptography module and not directly exposed to any device software. However, software can request that the DUHK encrypt and decrypt data. This DUHK encrypted data is bound to the device, and thus can't be decrypted on any other device.
- **Device Root Key (DRK)** — The DRK is a device-unique, asymmetric RSA key pair that is signed by Samsung's root key through an X.509 certificate. This certificate proves that Samsung produced the DRK. The DRK is generated at manufacture in the Samsung factory and is stored on the device encrypted by the DUHK, thus binding it to the

device. The DRK is only accessible from within the TrustZone Secure world and is protected by the DUHK. The DRK is an important part of the Root of Trust, as it derives other signing keys. Because the DRK is device-unique, it can tie data to a device through cryptographic signatures. Signing keys are derived from the DRK and used to sign data.

- **Samsung Secure Boot Key (SSBK)** — The SSBK is an asymmetric key pair used to sign Samsung-approved boot executables.
    - The private part of the SSBK is used by Samsung to sign secondary and app bootloaders.
    - The public part of the SSBK is stored in the hardware's one-time programmable fuses at manufacture in the Samsung factory. The Secure Boot process uses this public key to verify whether each boot component it loads is approved.
- **Samsung Attestation Key (SAK)** — The SAK is also a device-unique, asymmetric key pair that is signed by Samsung's root key. This signed key pair proves that the SAK was produced by Samsung. The SAK is used to sign the Attestation blob that indicates if the device is in a trusted state. The signature proves that Attestation data originated from the TrustZone Secure world on a Samsung device. Unlike the DRK, the SAK is a set of ECDSA keys. ECDSA is a newer asymmetric algorithm, similar to RSA but smaller and faster for the same strength.

Hardware fuses

Samsung Knox security is built in layers, from low-level capabilities in the hardware to Android itself. One of the important low-level features are the hardware fuses, which provide a Root of Trust based in hardware. Samsung Root of Trust components are designed as one-time fuses, making a permanent record of data such as encryption keys, Rollback Prevention, and the Knox Warranty.

Rollback Prevention (RP) Fuses

These fuses encode the minimum acceptable version of Samsung-approved bootloaders. Old software may contain known vulnerabilities that may be exploited. Rollback prevention excludes approved, but out-of-date bootloaders from being loaded.

The RP fuse version number is set when system software is initially installed and when specific updates occur. Once the RP fuse version number is set, it is impossible to revert back to legacy software versions.

Knox Warranty Fuse

The purpose of the Knox Warranty Fuse is to provide a record of the integrity of the device. Samsung monitors the integrity of several different components, detecting if any particular component is in a non-approved configuration. For example, the Trusted Boot process sets the fuse when it detects the following:

- an unsigned kernel is loaded
- a critical security feature like SELinux is disabled

These types of checks are critical as non-approved components could lead to vulnerabilities such as privilege escalation or access to normally protected peripherals. Such non-approved components can even lead to vulnerabilities being persistent over reboots or even future updates, for example, returning to an approved component.

The Knox Warranty Fuse is designed to provide a tamper-resistant, persistent record of running in a non-approved state. Since the fuse can only be set one time, once it has been set to mark a non-approved configuration, the device is permanently marked as having had a non-approved configuration, regardless of any future actions. For the enterprise, this ensures that a previously compromised device cannot be brought back into a seemingly compliant state and used normally.

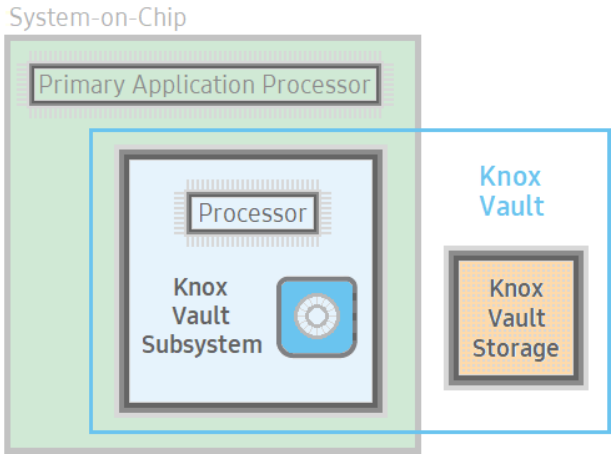
To use the Knox Warranty Fuse, Samsung has integrated the measurement into several checks on the device, both during boot and after, allowing processes such as the following to see the status of the device:

- Access to the core encryption keys of TrustZone. The Knox Warranty Fuse value is used in the decryption of the Device-Unique Hardware Key and all data protected by this key. This blocks access to any keys stored in TrustZone, such as keys stored by enterprise apps. This means any data stored on the device becomes inaccessible after the Knox Warranty Fuse has been set. This includes data encrypted by DualDAR Encryption and Sensitive Data Protection.
- Device is factory reset after the Knox Warranty bit has been set. In this case, a user may be able to use the device, but Knox functions such as creating a work profile are blocked. Similarly, functions that rely on Knox security, such as Samsung Pay, are also blocked. The Device Health Attestation reports that the device has been compromised at some point, and reports this status to requesting services such as an Attestation Key.

As a persistent record of the state of the device, the Knox Warranty Fuse is able to provide a unique capability to ensure that a Samsung device is trustworthy and has been maintained in a trustworthy state during its lifecycle.

Knox Vault

Samsung's Knox Vault is an evolution of the hardware-based security that Samsung has been building within Galaxy smartphones for years. Knox Vault extends upon the protection offered by our TrustZone, the Trusted Execution Environment (TEE) pioneered by Samsung to protect sensitive data such as passwords, biometrics, and cryptographic keys. Whereas the TrustZone runs a different OS alongside Android on the primary application processor, Knox Vault operates completely independently from the primary processor running the Android OS.



As a core component of the Knox security platform, Knox Vault is an isolated, tamper-proof, secure processor with its own core and memory, as well as an interface to dedicated, non-volatile secure storage. Knox Vault can:

- Store sensitive data such as hardware-backed Android Keystore keys, the Samsung Attestation Key (SAK), biometric data, and blockchain credentials.
- Run security-critical code that authenticates users with increasing timeouts between failures and controls access to keys depending on authentication.

Knox Vault is integrated into Samsung devices starting from the Galaxy S21, and is comprised of components that are Common Criteria evaluated to the requirements in BSI PP0084 at EAL4+ or higher. These components are tested by an independent lab against a wide array of hardware attacks and through a review of their software and firmware.

Protection from attacks

Knox Vault provides strong security guarantees against both software and hardware attacks. Because Knox Vault is independent from the primary processor that runs Android, code running on the Knox Vault Processor is resistant to attacks that exploit shared resources, such as software side-channel attacks that can compromise other software executing on the same processor. This separation means Knox Vault protects sensitive data even if the primary processor itself is completely compromised.

In addition to being resistant to software attacks, Knox Vault is also designed to be tamper-proof to thwart hardware attacks, which require that an attacker have physical possession of a device to extract secrets. Knox Vault is resistant to hardware attacks such as the following:

- Physical probing to disclose data
- Physical manipulation of the circuitry to deactivate security mechanisms
- Forced information leakage
- Hardware side-channel attacks such as differential power analysis to disclose data
- Fault injection to bypass security mechanisms.

For details about these attack types, see Protection from Hardware Attacks.

Knox Vault features

Among the many capabilities of Knox Vault, the following are key to the overall security of protected devices.

Weaver

Weaver is used for secure password authentication to Android. Running on the Knox Vault Processor, Weaver's data and secrets (passwords) are stored encrypted in the secure Knox Vault Storage. When Weaver receives the secret data to be stored, it also receives a key, and this key must be provided to read the secret data again from Weaver.

To prevent brute-force attempts to extract secrets, Weaver uses a binary exponential back-off algorithm. When attempting to read a secret, if the proper key is not provided, Weaver declines read operations for a time period decided by the back-off algorithm. A non-bypassable secure timer is used to track these time periods.

Credential storage

This feature stores data encrypted by the Knox Vault Processor in the Knox Vault Storage, using a secure channel to protect data transferred between the Knox Vault Processor and the Knox Vault Storage.

The following data is stored in the Knox Vault Storage:

- Cryptographic keys to protect biometric data
- Blockchain keystore credentials
- Samsung Attestation Key (SAK)

All data in Credential Storage is encrypted using a Knox Vault-unique key. This prevents the data from being decrypted in other devices.

Samsung Attestation Key

Samsung Knox Attestation is a Knox platform feature that is designed to detect if a device or its keys are compromised, and can be used to prevent access to security-sensitive Samsung systems like Knox services, Samsung Pay, and Samsung Pass.

Each device has a unique, asymmetric, elliptic-curve private Samsung Attestation Key (SAK) that is stored in Knox Vault. The SAK's digital certificate is signed by Samsung's Root-of-Trust and the key-certificate pair is injected into Knox Vault during the device's factory manufacturing process. SAK is used to attest keys and devices for Samsung security services like Knox services, Samsung Pay, Samsung Pass, and so on. The key generation processes ensure the keys are unique, based on strong random number generation.

StrongBox Keymaster support

The StrongBox Keymaster is a key management module supporting various cryptographic algorithms that can be used by applications to generate keys and perform cryptographic operations with them.

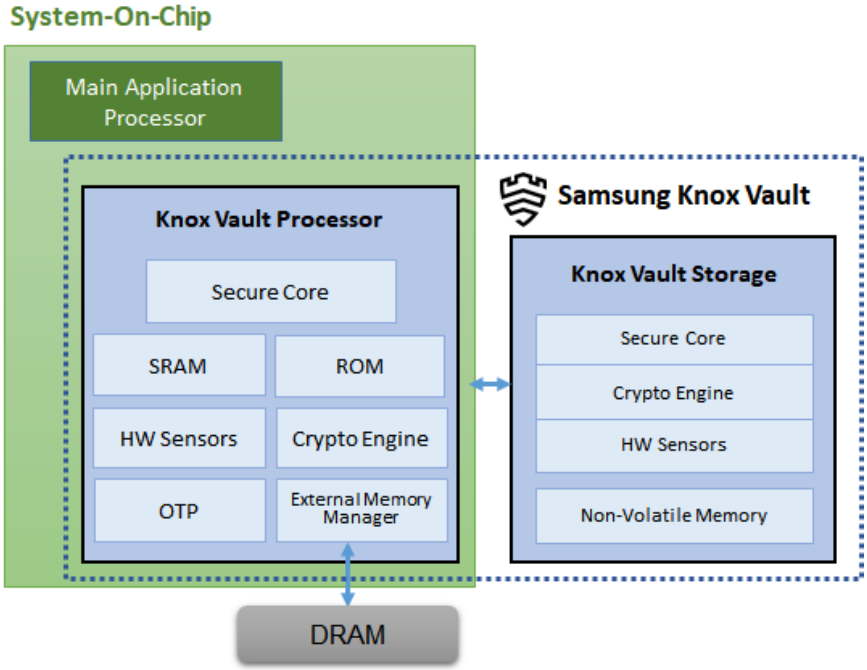
The Android framework provides a KeyStore API for applications to use the StrongBox Keymaster. All keys generated by the StrongBox Keymaster or imported into it are encrypted with the unique key of Knox Vault. Thus, these keys cannot be decrypted outside of the StrongBox Keymaster running on the Knox Vault Processor.

Knox Vault architecture

Knox Vault is made up of the following:

- Knox Vault Processor: implemented as part of the SoC
- Knox Vault Storage: an integrated circuit physically outside the SoC

Through a secure interface, the Knox Vault Processor communicates with the Knox Vault Storage.



Knox Vault Processor

The Knox Vault Processor is designed to operate separately from other SoC components. It has its own secure processing environment consisting of the Knox Vault Processor, SRAM, and ROM. It also provides enhanced security and data protection against various hardware-based attacks, by monitoring the hardware status and its environment using a series of security sensors or detectors including:

- High and Low Temperature detectors
- High and Low Supply Voltage detectors
- Supply Voltage Glitch detector
- Laser detector

The Knox Vault Processor also includes a dedicated random number generator, and its own Crypto Engine. The Knox Vault Processor can access system DRAM though the External Memory Manager. The Knox Vault Processor provides the main computing power for Knox Vault. To provide the strongest isolation, the Knox Vault Processor is separated from the primary processor on the SoC. This separation helps prevent side-channel attacks that depend on malicious software sharing the same execution core as the target software under attack.

Secure core

By executing the instructions and managing data on SRAM, the Knox Vault Processor also guarantees a physically isolated execution environment. The Knox Vault Processor ROM where the secure boot loader code is located is also separated and protected by the hardware protection mechanisms. When the Knox Vault Processor starts, the ROM code is loaded to SRAM. While the ROM code loads the Knox Vault Processor firmware, with the help of the modules running on the SOC main processor, the software stack of Knox Vault Processor has its own secure boot chain.

Hardware sensors

The hardware sensors check for abnormal hardware status from the security sensors and detectors. The monitoring and detection cannot be affected or bypassed by any application running on Knox Vault Processor.

Crypto engine

A hardware cryptographic module provides the following cryptographic functions:

- AES encryption/decryption
- DRBG random number generation
- SHA hashing
- HMAC keyed-hashing for message authentication code
- RSA and ECC key generation and services

Knox Vault unique key

The Knox Vault unique key is written into one-time-programmable fuses. This unique key is used for protecting keys imported into or generated in the Knox Vault Processor. Thus, a key generated in Knox Vault on one device cannot be used outside of that device.

External memory manager

The Knox Vault Processor can read or write to external memory using the External Memory Manager.

Knox Vault Storage

The Knox Vault Storage is a dedicated, secure, non-volatile memory device that stores sensitive data such as the following:

- Cryptographic keys such as Blockchain keys and Device keys
- Biometric data
- Hashed authentication credentials

Like the Knox Vault Processor, the Knox Vault Storage is designed to prevent various physical and side-channel attacks, using its own secure processor, SRAM, ROM, cryptographic module, and hardware monitor which detects physical tampering.

Secure core

The Secure Core is the Knox Vault Storage processor used to do the following:

- Execute the ROM code
- Provide cryptographic operations for public key algorithms (RSA, ECC) and SHA algorithm with software libraries
- Safely store data in dedicated SRAM and ROM

Crypto engine

The Crypto Engine supports symmetric encryption to verify authentication codes after receiving packets from the Knox Vault Processor and also to enhance performance.

Hardware sensors

As with the hardware sensors of the Knox Vault Processor, the hardware sensors of Knox Vault Storage also detect physical or side-channel attacks related to power, temperature, and electromagnetics. If the hardware sensors detect an attack, the Knox Vault Storage is automatically wiped.

Non-volatile memory

The Non-Volatile Memory is a bank of NOR (NOT OR) flash used to store data received from the Knox Vault Processor.

Knox Vault intercommunication

The Knox Vault Processor and Knox Vault Storage communicate securely over a dedicated I2C (Inter-Integrated Circuit) bus. All traffic on this bus is encrypted and transmitted with an authentication code. Additionally, all communications are protected against replay attacks.

Protection from Attacks

Knox Vault is tested to provide protection against the following classes of hardware probing attacks.

Physical probing

An attacker might physically probe secure hardware to disclose user data or other critical information, while the data is stored in memory or being processed. The attacker directly measures information using electric contact with the secure hardware internals, using techniques commonly employed in IC failure analysis and IC reverse engineering.

Physical manipulation

An attacker might physically modify the secure hardware to change user data, secure hardware software, or security services or mechanisms. The attacker might make modifications through techniques commonly employed in IC failure analysis and IC reverse engineering. To make these modifications, the attacker identifies hardware security mechanisms, layout characteristics, or software design, including how secure hardware treats user data. Changes of circuitry or data can be permanent or temporary.

Forced information leakage

An attacker might exploit information that is leaked from the secure hardware in order to disclose confidential user data, even if the information leakage is not inherent but caused by the attacker. For example, fault injection or physical manipulation might cause information leakage from signals which normally do not contain significant information about secrets.

Side-channel attack

An attacker might exploit information that is leaked from the secure hardware during its operation in order to disclose confidential user data. Direct contact with the secure hardware internals is not required. Information leakage might occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time. One example is the Differential Power Analysis (DPA). This leakage can be interpreted as a covert channel transmission, but is more closely related to the measurement of operating parameters. These operating parameters might be derived either from direct measurements or measurement of emanations. The attacker can associate the measurements with the specific operation being performed.

Fault injection

An attacker might cause a malfunction of the secure hardware software by applying environmental stress like light or a power glitch. This attack type could modify the hardware and software functions, or deactivate or affect security mechanisms of the secure hardware. Thus, the attacker could disclose or manipulate the user data existing in the secure hardware. For example, the modification of the security hardware function might affect the quality of random numbers provided by the random number generator, and then the software may get constant values or value with low entropy.

Common Criteria Certification

Common Criteria is a framework for evaluating security products in a standardized way that is recognized by 31 countries globally through the Common Criteria Recognition Agreement (CCRA).

Knox Vault components are evaluated and certified by a Common Criteria Testing Laboratory (CCTL), an independent third party. Depending on the processor configuration, Knox Vault is evaluated to the requirements specified in the Security IC Platform Protection Profile with Augmentation Packages at EAL4+ or EAL5+ assurance requirements, a measure of the depth of the review performed on the product. These evaluations cover testing of a wide array of hardware attacks in addition to a review of the software/firmware of Knox Vault.

Trusted Boot

Trusted Boot is a Knox Platform feature representative of Samsung's industry leading mobile device boot protection. Trusted Boot identifies and distinguishes unauthorized and out-of-date boot loaders before they compromise your mobile device.

If unauthorized boot components happen to load, an enterprise can trust that only validated and current components are loaded after Trusted Boot segregates authorized from unauthorized boot loaders.

Enterprises can check device integrity on demand through Knox Attestation, which reads Trusted Boot collected measurement data, along with an SE for Android enforcement setting, to form the basis of a device health verdict.

Secure lockdown on tampering

Bootloader measurements are recorded in secure TrustZone memory during device boot. At runtime, apps operating in the secure TrustZone can use these measurements to make security-critical decisions, such as whether or not to:

- Release cryptographic keys from the Knox Keystore.
- Launch the work profile app container.

If an unauthorized or out-of-date component version is detected, a tamper fuse is set. Once the fuse is set, sensitive work apps and data within the work container are permanently encrypted and inaccessible since the integrity of the device is no longer guaranteed or validated.

The device user can still boot the device and launch personal apps. This flexibility promotes a nice balance between consumer functions, such as smartphone calls and personal apps, and the requirement to protect enterprise data.

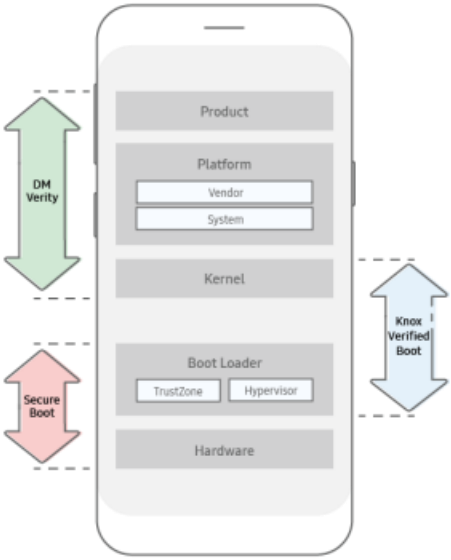
Building on Secure Boot

Before adopting Trusted Boot to work along with Secure Boot, Samsung devices were using Secure Boot to prevent unauthorized bootloaders and operating systems from loading during start-up. Secure Boot is implemented by each bootloader cryptographically verifying the signature of the next bootloader in sequence, using a certificate chain with its root-of-trust resident in hardware. If verification fails at any step, the boot process terminates.

While Secure Boot is effective at preventing unauthorized bootloaders, it is unable to distinguish between different authorized binary versions. For example, Secure Boot can't distinguish between a bootloader with a known vulnerability as opposed to a later patched version, since both versions have valid signatures. Trusted Boot however was introduced to verify the same bootloader, kernel and platform build.

Knox Verified Boot (KVB)

Knox Verified Boot (KVB) is a new solution that both extends and enhances Android Verified Boot (AVB). While AVB only checks the integrity of the kernel and platform components, KVB extends those checks to also cover the earlier bootloaders. This provides a more comprehensive guarantee the device is booting using properly signed components that are all from the same build. KVB performs the same type of validations as the existing Trusted Boot mechanism, but it is able to do so before the device kernel is booted, and thus provides the same data protection guarantees earlier.



With KVB, component checks are conducted in the bootloader, and validations are made before system services are even started.

KVB is supported on Samsung S10 and above devices running the Android P operating system or later.

Real-time Kernel Protection (RKP)

The Knox Platform's patented Real-time Kernel Protection (RKP) is the industry's strongest protection against kernel threats and exploits. RKP works seamlessly out-of-the-box, with no setup required. Simply powering on a Samsung Knox device provides world-class threat protection and attack mitigation. RKP supports the rest of the Knox security offerings to provide full security coverage without the typical gaps anticipated with mobile devices.

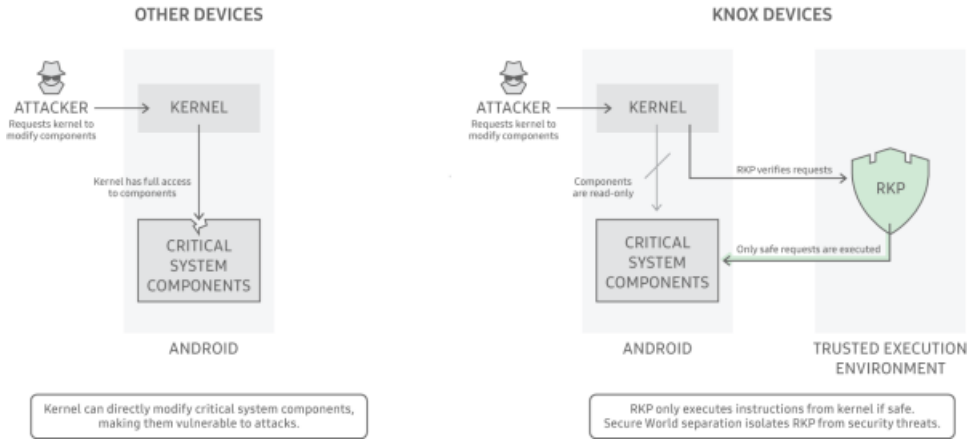
Why does kernel protection matter?

Kernel protection is central to device security and enterprise data protection. When attackers find software vulnerabilities, they often escalate privileges and compromise the core of the OS: the kernel.

A compromised kernel can leak sensitive data and even allow remote monitoring and control of the affected device. Other more commonplace protections like Secure Boot or hardware-backed keystores are of little value if the kernel itself is controlled at runtime. After a device boots and decrypts sensitive content, a kernel compromise can result in data leaks that directly impact an enterprise's data integrity.

RKP design and structure

As part of the Knox Platform's security offerings, RKP employs a security monitor within an isolated execution environment. Depending on the device model, either a dedicated hypervisor or the hardware-backed secure world provided by ARM TrustZone technology provides the isolated execution environment.



RKP's isolation from the kernel shrinks the Trusted Computing Base (TCB) and helps secure it from attacks designed to compromise the kernel. This unique ability enables RKP to detect and prevent the most common kernel attacks. RKP protections are grouped into three areas:

- **Kernel code** — RKP prevents modification of kernel code and logic.
- **Kernel data** — RKP prevents modification of critical kernel data structures.
- **Kernel control flow** — RKP prevents Return-Oriented Programming (ROP) and Jump-Oriented Programming (JOP) attacks that reuse existing kernel logic to piece together exploits from the kernel's own code.

How is kernel protection possible?

A kernel protection mechanism can't exist completely in the kernel only, since an attacker could circumvent it if the kernel itself has a flaw. The kernel is the lowest granular control level over the OS and, as such, usually can't be effectively monitored from any lower level in the system.

RKP uniquely employs a security monitor within an isolated execution environment. Running within an isolated execution environment would normally compromise a security mechanism's ability to see into the kernel and monitor activities at runtime. However, RKP succeeds by utilizing patented techniques to control device memory management and by intercepting and inspecting critical kernel actions before allowing them to execute. RKP is thus able to prevent a compromised kernel from bypassing other security protections. This prevention significantly reduces the severity of kernel attacks and limits the effectiveness of exploits that would typically cripple a mobile device.

Since RKP is always active and requires no management control, kernel protection is only possible if it meets strict usability and performance requirements. RKP's protections are activated out-of-the-box, with no performance impact to customers.

Periodic Kernel Measurement (PKM)

The *TrustZone-based Integrity Measurement Architecture* (TIMA) architecture provides a number of core features to protect against mobile device compromise. One of these central TIMA features is *Periodic Kernel Measurement* (PKM).

PKM periodically monitors the kernel to detect if legitimate kernel code and data were modified maliciously. PKM also monitors the key SE for Android data structures in OS kernel memory to prevent malicious attacks from corrupting and potentially disabling SE for Android. PKM protects the Linux kernel code and data pages from malicious exploits and helps prevent attacks attempting to disable SE for Android.

During a device firmware build, the SHA1 hash of every kernel code, and read-only data page, is calculated and gathered into a measurement file. These measurements are signed by Samsung to ensure data integrity and authenticity before its included in the firmware. When TIMA is initialized, PKM receives the kernel page measurements and verifies the signature to prove integrity and authenticity before storing the measurements in the secure world. During device operation, TIMA periodically recalculates the measurements of the running kernel and compares them to the signed measurements stored on the device. If any discrepancy is detected, a violation is reported to both system logs and the user.

When PKM runs, it reads the physical memory addresses used by SE for Android to determine whether:

- SE for Android is enabled
- SE for Android is in enforcing mode.

If malicious code manages to disable SE for Android, or switch it to permissive mode, PKM detects the state change and reports a violation to quickly assist an administrator in problem diagnoses.

Full security coverage

Each year, Samsung's research and development teams add the latest runtime protections to a growing list of unique capabilities found only within RKP. At a 2018 mobile security conference, RKP was touted as the best Android protection technology available and was credited with the lack of new public exploits in the past year for Samsung Knox devices.

Although RKP is only one piece of Samsung's holistic security solution, it successfully demonstrates the unique security guarantees possible when combining hardware, software, and advanced security research. Ensuring security claims are low maintenance, highly effective, and industry-leading is what provides enterprise customers the trust they need to deploy mobile devices in high-security environments.

Device Health Attestation

Mobile apps can be compromised if unauthorized actors are able to run them on untrustworthy hardware or firmware. Such unauthorized actors might include:

- a malicious user deliberately accessing a device they're not authorized to, for example, while the user is away
- a bad actor who manipulates the device, or its firmware in transit

Such an actor can easily gain full control over the device firmware, files, UI, and apps. Unfortunately, malicious actors can exploit these scenarios to:

- install apps
- steal passwords
- hijack identities

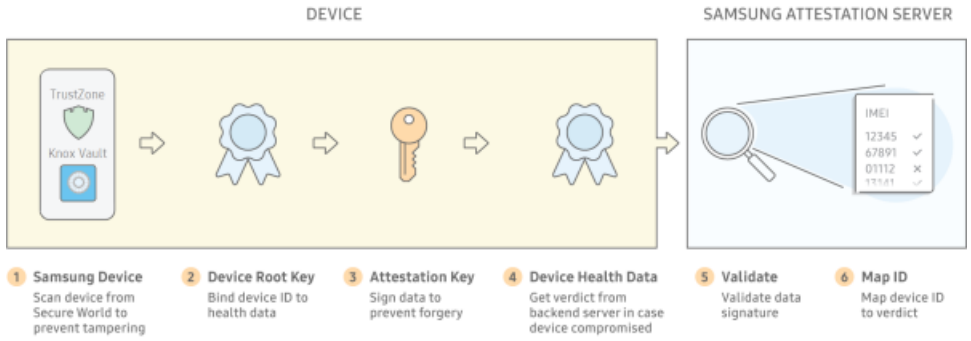
Enterprises with Bring Your Own Device programs are especially at risk, as employees may potentially use compromised Android devices in the workplace. Risks range from:

- the undetected exposure of confidential enterprise assets
- wider more insidious attacks on other enterprise resources and infrastructure

Knox Attestation provides a fail-safe way to detect if a device or its firmware is compromised, before allowing device users to use it in the workplace.

Reliable detection of compromised devices

Malware can potentially intercept and forge the results of a device health check, making a compromised device seem secure. Knox Attestation guards against this risk as follows:

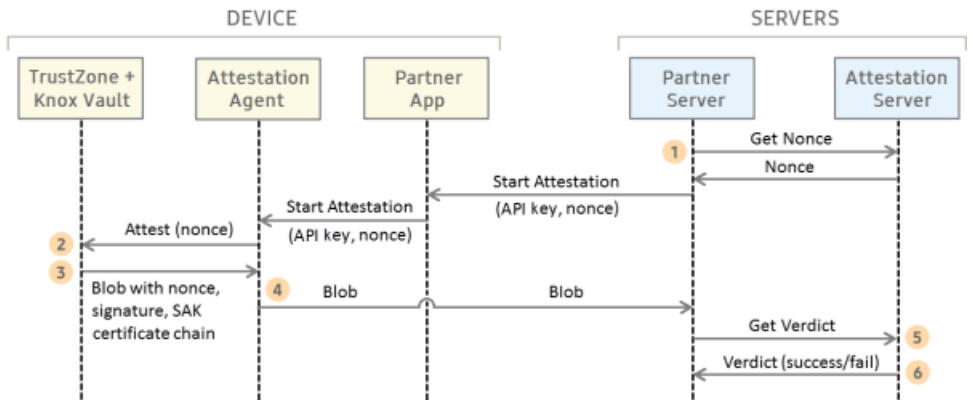


1. The Knox platform leverages its hardware-backed trusted environment to reliably detect and report compromised devices. Knox Attestation ensures the integrity of devices during deployment, bootup, and operation using the following:
    - Root of Trust: Starts in our factories, when devices are manufactured, with device-unique hardware keys providing a foundation of trust.
    - Trusted Boot: Detects unauthorized and out-of-date boot loaders before they compromise devices using bootloader measurements recorded in secure TrustZone memory.
    - Knox Vault: Stores sensitive data such as the Samsung Attestation Key in tamper-proof storage that resists both hardware and software attacks.
2. Samsung incorporates a Device-Unique Hardware Key in the device hardware during the initial manufacturing of the device. This key binds the device health attestation data to a particular device and is accessible only by a hardware cryptography module and not directly exposed to any device software.

3. Knox Attestation signs device health data to prove that it originated from the TrustZone Secure World on a Samsung Knox device. Each device uses a **Samsung Attestation Key**. When the device is manufactured, a unique RSA private/public key pair is generated. The public key is also signed by a special Samsung Root Key to generate a X.509 certificate. Both the Samsung Attestation Key and its certificate are secured in the device's TrustZone.
4. In case a device is already compromised when a health check is performed, the final test on device health is performed by a Samsung attestation server. To protect data-in-transit, Knox Attestation uses TLS encryption.
5. To validate device health data, the Samsung attestation server verifies the Samsung Attestation Key certificate, Attestation Key certificate, and signatures to ensure the integrity of the attestation result.
6. To protect from man-in-the-middle replay attacks, which replay the attestation result collected on a healthy device or the same device before it was compromised, the server verifies the random nonce value generated for each requested health check.

Highly secure or firewalled operations that don't want to access the web-based Samsung Attestation server can install an Attestation Validator tool onto a local server to parse the Attestation Result and keep device verdicts within the firewall.

How Knox Attestation works



Partners such as EMM vendors or ISVs use our Knox APIs to deploy attestation checks. They can enable device checks manually by an admin using a web console or automatically by a regularly scheduled process.

1. The web server that initiated the check does the following:
    - requests a nonce from the Samsung Attestation server. A nonce is a random number used in cryptographic communication to time-bound and identify each attestation result.
    - instructs the device to begin a check, passing the nonce as a check identifier.
2. The Keymaster Trusted Application (TA) in Secure World gathers this data:
    - the requesting app's package name, version code, and developer key
    - signed info about the device's current state and expected environment
    - hardware fuse readings indicating if untrusted firmware was ever loaded onto the device
3. The TA compiles this information into an Attestation Result and signs it with a key that can be verified using the Samsung Root Certificate.
4. The device communicates with the Samsung Attestation Server using TLS encryption to protect data-in-transit.
5. The Samsung Attestation Server validates the Attestation Result's signature to ensure that it was generated on Samsung hardware and by Samsung's TA.
6. The Samsung Attestation Server analyzes the Attestation Result to determine if the returned nonce matches the one sent out and whether the data within it can be trusted.

Managing compromised devices

On detecting a compromised device, the Knox platform fuses a one-time programmable Warranty bit that signifies whether or not the device has ever booted into an unapproved state. Once this bit is fused, the work profile no longer operates, preventing access to the secured enterprise apps and data.

The original requestor of the device check can take further action, for example,

- Report the verdict to the device user.
- Immediately prevent the device from accessing other enterprise systems.
- Uninstall any enterprise apps or assets already on the device.

Unique advantages of Knox Attestation

Knox Attestation provides these key differentiators:

- **Prevention of replay attacks**: Health measurements guaranteed per request through a nonce, a unique number randomly generated by the Samsung Attestation Server.
- **Prevention of device ID falsification**: Knox Attestation forms a chain of trust using the Samsung Root Key, Samsung Attestation Key, and Attestation Key. It signs attestation results using the Attestation Key, and appends the Attestation Key certificate and Samsung Attestation Key certificate.
- **Detection of systemless rooting**: Rooting methods like Magisk store system file modifications in the boot partition, which can go undetected by tamper detection methods other than Knox Attestation.
- **Correlation of results per device**: Health results that easily map to device identifiers like an IMEI. Unlike other solutions on the market, Knox Attestation enables IT admins to determine which attestation result correlates with which device, without having to painstakingly map IDs manually. With competitor solutions, results are returned for separate devices, but IT admins can't differentiate between devices, and consequently the results are not actionable. Knox Attestation returns a single device ID and enables IT admins to prevent or contain issues promptly.
- **Historical tamper record**: Knox Attestation guarantees not only the current health of the device, but also a record of whether the device ever ran a non-approved configuration in the past, through the Knox Warranty Fuse.

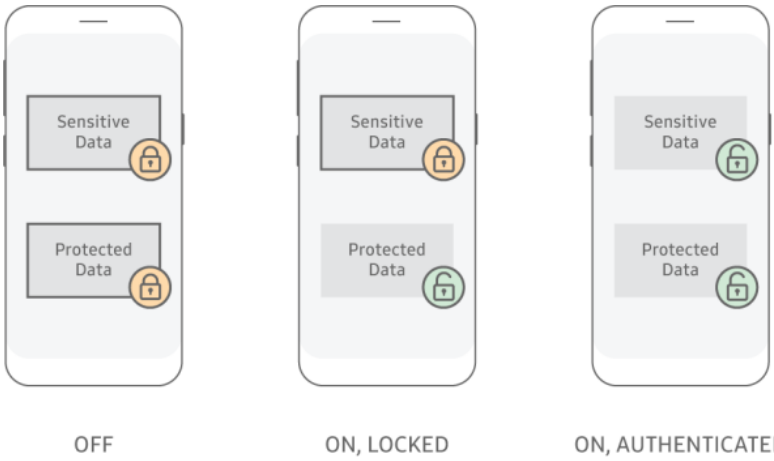
NOTE: The current release of Knox Attestation was enhanced with Knox version 3.4 and higher. Prior to that, Knox Attestation did not support the enhanced Samsung Attestation Key, detection of device ID falsification, or data-in-transit protection using TLS encryption (SSL encryption was used).

Sensitive Data Protection (SDP)

Protecting Data-At-Rest (DAR) on mobile devices is a major concern. While the industry standard is to encrypt all the data on a device, that data is decrypted and accessible after the device boots successfully. This access process means that once a device is lost or stolen, a sophisticated attack can extract data as long as the device is still running, even if the device is locked. Samsung created Sensitive Data Protection (SDP) to address this specific issue.

SDP meets the Mobile Device Fundamentals Protection Profile (MDFPP) requirements defined by the National Information Assurance Partnership (NIAP) for DAR, meaning that SDP is approved for use by the US government and military.

How SDP works



KPE protects user data on the device through Data-at-Rest encryption. Data remains encrypted on disk, and can only be decrypted when the device is powered on. Recovery of data decryption keys is tied to:

- device hardware, meaning data is recoverable only on the same device
- device boot-time integrity measurements
- a user credential dependent on configuration

Additionally, a mechanism is provided to optionally mark data as sensitive, which subsequently cannot be decrypted while the device is in the locked state. Here are the two protection modes that KPE provides for Data-at-Rest:

- **Protected**: All files stored on the device are treated as Protected by default. Protected data is stored on the device file system as encrypted data, and is only decrypted when an application accesses the data. This mechanism provides the data-at-rest protection while the device is powered off. Even if the device is in the lock state, applications can access protected data.
- **Sensitive**: Files can also be optionally marked as sensitive, using the Sensitive Data Protection (SDP) mechanism. SDP uses a key management scheme which ensures sensitive files can only be decrypted in the unlocked state, by purging keys from RAM when the device is locked. However, SDP also provides the ability for new files to be written and encrypted in the locked state using public key cryptography.

SDP encryption

Samsung Galaxy devices supporting Knox 3.3 and above are enabled to support Android's File Based Encryption (FBE) for Data-at-Rest. Data encryption is enforced across the device using:

- EXT4 encryption FBE mechanism
- FIPS compliant hardware crypto module (AES256-XTS)

Optionally, the external SD Card can be used with:

- dm-crypt (introduced with Android 11) or eCryptfs stacked file system
- FIPS compliant Kernel crypto module (AES256-CBC).

FBE keys are derived using a password entry, which is either the default hard-coded password or the device user's password used to unlock the device.

While in the unlocked state, SDP works as follows:

- Encrypts sensitive data using a per-file File Encryption Key (FEK). These keys are encrypted with the SDPK.sym (Sensitive Data Protection Key, symmetric), which is encrypted by the SdpMasterKey.
- Keeps the SdpMasterKey in memory only while the device is unlocked, to allow decryption of the SDPK.sym and SDPK.pri (private).
- Encrypts the SdpMasterKey using the key that is protected by both ephemeral keys derived from the device user's password and a key chaining to the Root Encryption Key (REK) using the Keystore.
- Clears the SdpMasterKey when it transitions to the locked state, and re-derives it when the user unlocks the device or work container.

While in the locked state, SDP handles apps writes of sensitive data differently:

- Rejects app attempts to open sensitive data files, as KPE no longer has the keys needed to retrieve sensitive data in memory and cannot re-derive them until the user unlocks the device or work container.
- Encrypts any new sensitive app data by using both a:
    - per-user sensitive data ECDH asymmetric key pair (SDPK.pri/pub)
    - per-file ECDH key pair [DataK.pri/pub] generated on behalf of the app
- Protects the private portion of the ECDH key pair (SPDK.pri) with the SdpMasterKey, the same Key Encryption Key (KEK) used to encrypt the sensitive data per-file FEKs.
- Clears the SdpMasterKey when it transitions to the locked state.

See also: File Based Encryption (FBE) and Full Disk Encryption (FDE).

SDP protection of apps

The native **Samsung Email** app automatically uses SDP to protect email bodies and attachments. For performance reasons, the email header (including the subject and sender) is not protected with SDP.

The **Knox Chamber** is a dedicated directory in the Knox container file system. All stored files within the Knox Chamber directory are automatically marked as sensitive and are handled by the SDP mechanism.

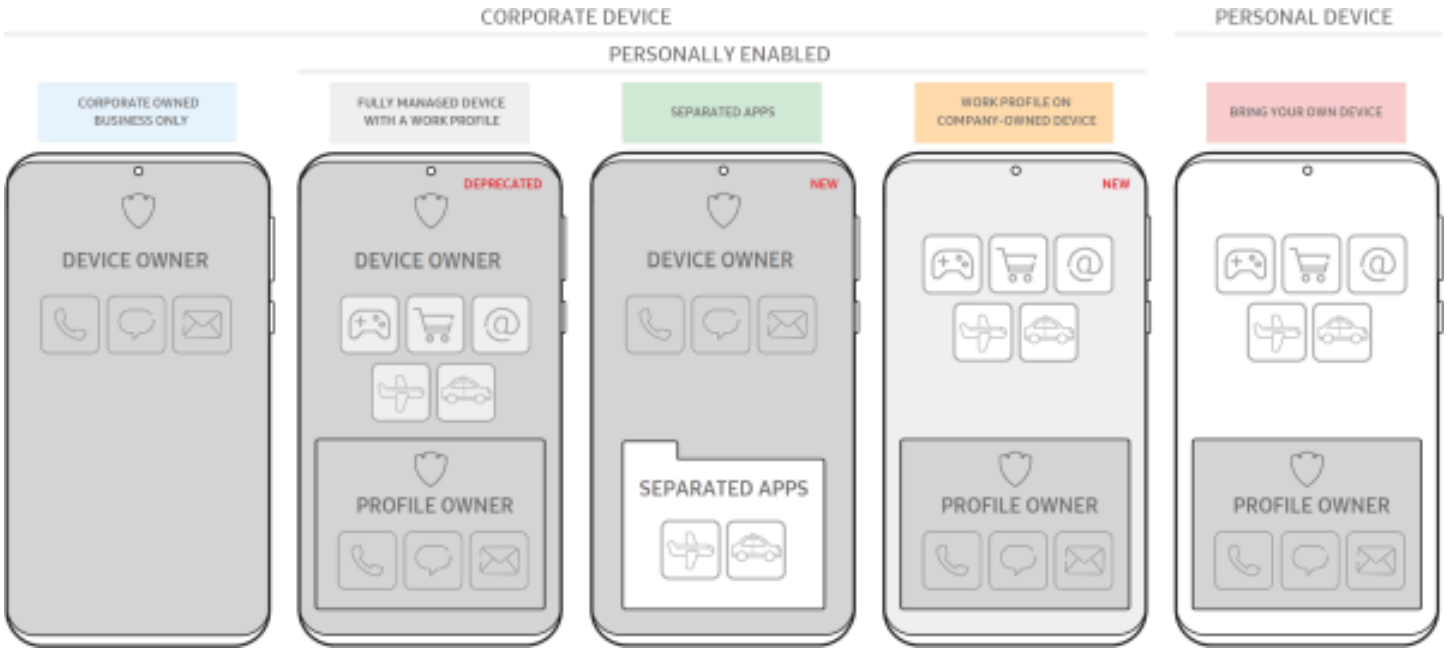
Unique advantages of Knox SDP

- **MDFPP-Compliant** — Knox SDP is certified as MDFPP-compliant. Without Knox SDP, the base Android system is not certified as satisfying MDFPP requirements, which mandates a form of SDP. MDFPP compliance is a requirement for many government agencies and the companies they work with. Samsung has more MDFPP-certified products than any other mobility solution provider.
- **Granular Control** — You can use Knox SDP to protect not just the whole device, a container, or individual files but also selected database columns.
- **Per-App Password** — You can further customize Knox SDP to decrypt a particular app's Sensitive Data only after an app user enters an app-specific password. In this case, the device or container unlock authentication alone does not decrypt app data. An app password is also needed for a higher layer of security.
- **App Protection** — Knox SDP is enabled by default to secure both Samsung Email as well as Knox Chamber.

App Security

Device users typically want their personal and work apps on the same device. This requirement presents a challenge for enterprises, which need to ensure that they fully protect their confidential corporate assets *and* don't run into any liability issues by accidentally interfering with a user's personal privacy.

With Android 11, Google continues to protect user privacy, extending these protections to company-owned devices. Specifically, Google has replaced the device management mode called fully managed device with a work profile with **work profile on company-owned device**.



Here is a summary of different device management modes and their use cases:

Corporate Owned Business Only (COBO)

- **Summary**: An enterprise owns the device, and doesn't allow personal apps on the device.
- **Control scope**: Through a UEM app, the enterprise serves as the device owner which has full control over the entire device.
- **Use case**: Enterprises use this model if they need strict control over the entire device and can't compromise corporate assets by allowing users to install their own apps.

Fully managed device with a work profile (FMDWP)

Deprecated in Android 11.

- **Summary**: An enterprise owns the device, allows users to install personal apps, and secures work apps in a work profile.
- **Control scope**: The enterprise uses one UEM app to serve as device owner which has control over the entire device, and a second UEM app to serve as profile owner which has control over the work profile.
- **Use case**: Enterprises used this model to give users freedom over the apps they installed, were able to fully view and manage personal as well as work apps.

Separated Apps

Exclusive to Samsung Knox devices, and set up only through the Knox Service Plugin (KSP).

- **Summary**: An enterprise owns the device, and allows users to install authorized third-party business apps (for example, airline, hotel, or ride-sharing apps) in a securely separated folder.
- **Control scope**: Through a UEM app, the enterprise serves as the device owner which has full control over the entire device. Through KSP, the enterprise can set up a Separated Apps folder and identify the apps allowed to be installed inside the folder.
- **Use case**: Enterprises use this model if they need strict control over the entire device, but want to enable staff productivity using a separate, lightly managed app folder.

For more detail about using this mode, see Separated Apps.

Work profile on company-owned device (WP-C)

New in Android 11.

- **Summary**: An enterprise owns the device, secures work apps in a work profile, and allows users to install personal apps.
- **Control scope**: The enterprise uses one UEM app to serve as profile owner with control over the work profile. If the enterprise deploys the work profile from the setup wizard using the provisioning tools added in Android 10, the device is recognized as **company-owned** and a wider range of asset management and device security policies is made available than that granted to personally-owned devices. Enterprises can still apply policies at the device level as long as they don't infringe on personal privacy; for details, see Android policies in the personal side and Knox policies in the personal side.
- **Use case**: Enterprises use this model if they want to give users freedom over the apps they use on company devices without infringing on their user privacy.

For more detail about using this mode, see Google's EMM migration guidelines (which requires a partner login) or Work profile on company owned devices.

Bring Your Own Device (BYOD)

- **Summary**: An employee owns the device, and installs work apps on their device to enable productivity.
- **Control scope**: The enterprise uses one UEM app to serve as profile owner with control over work apps in the work profile.
- **Use case**: Smaller enterprises might use this model to save on the capital costs associated with buying devices.

NOTE - Google deprecated the legacy device admin (DA) management mode in Android 10. By November 2, 2020, Google requires app updates to target API level 29 or Android 10. From this date onwards, app updates start throwing exceptions if they call the four deprecated DA policies. For more info, see Device admin deprecation.

NOTE— Knox Workspace containers were deprecated with Knox 3.4.1 on Android 10, which debuted with the Note 10. However, older devices like the S10 that are upgraded to Knox 3.4.1 or higher still support the Knox Workspace containers until EOL. To take advantage of all the latest Android Enterprise and Knox features, we strongly recommend that you use work profiles instead of Knox Workspace containers.

Knox-enhanced work profiles

The Android Enterprise work profile provides enterprises with a solution to securely isolate work apps and data on one device. The Knox Platform for Enterprise provides more granular management policies for work profiles on Samsung devices.

Data transfer

With the isolation of work and personal data, a device user has access to two separate spaces. To increase productivity in certain situations, it is often necessary to share data between spaces. For example, while using a phone app in the personal space, it may be necessary to call a work contact saved in the secure work space. With the work profile, IT admins have granular management policies to manage the import and export of data to and from the work profile. This data can include apps, files, clipboard data, call logs, contacts, calendar events, bookmarks, notifications, shortcuts, and SMS.

Container-only control

For liability and productivity purposes, IT admins can't apply effective policies on a device with both personal and work data. The work profile provides IT admins the ability to configure and control critical functionality for the container only. An IT admin can enable or disable the following exclusively for the container:

- Bluetooth
- NFC
- USB access
- External storage

Container configuration

With the isolation of work and personal data, the device user has access to two separate spaces. This dual access presents some challenges to quickly identifying and accessing work data.

To enhance usability, the work profile provides an IT admin the ability to add work shortcuts to personal spaces so device users can quickly access work data. The work profile also provides an IT admin with the ability to set custom resources like work badges on app icons, helping users quickly identify company work apps.

Password policy

An IT admin must ensure only authorized people have access to work data inside a container. The work profile supports advanced authentication mechanisms to meet all enterprise needs.

An IT admin can enforce and configure:

- Complex passwords or code schemes
- Two-factor authentication
- Active Directory authentication

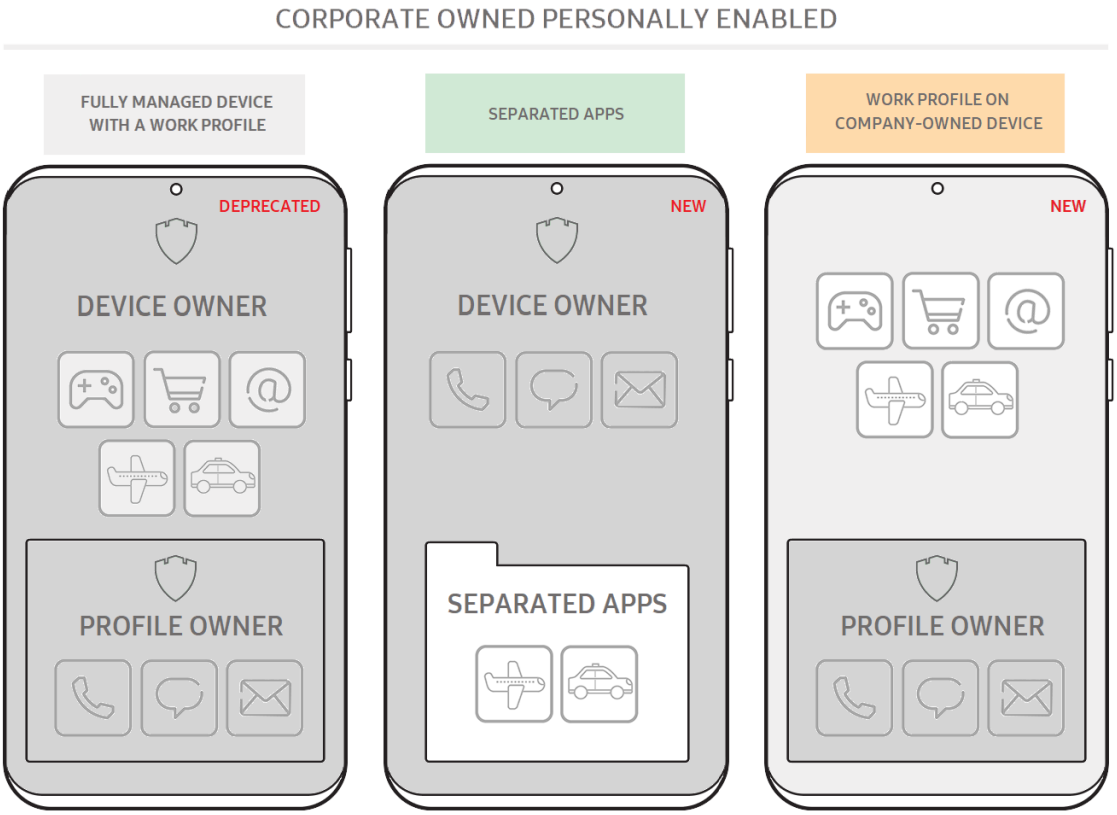
Additionally, an IT admin can lock the container to restrict access. This restriction is necessary when a device is out of compliance, lost, or stolen.

Separated Apps

Enterprises that provide corporate-owned personally enabled devices typically need to separate official work apps from third-party business apps installed by employees, for example,

- Airline apps (United, Delta, and so on)
- Hotel apps (Marriott, Hilton, and so on)
- Ride-sharing apps (Uber, Lyft, and so on)

An IT admin might not be comfortable with a third-party app that needs access to contacts, email addresses, or phone numbers. There may be concerns that sensitive work data may end up on third-party servers. The third-party apps are needed for productivity, but are not fully trusted and vetted by the IT admin. In this scenario, the enterprise is wholly responsible for their corporate assets and needs full control of their devices.

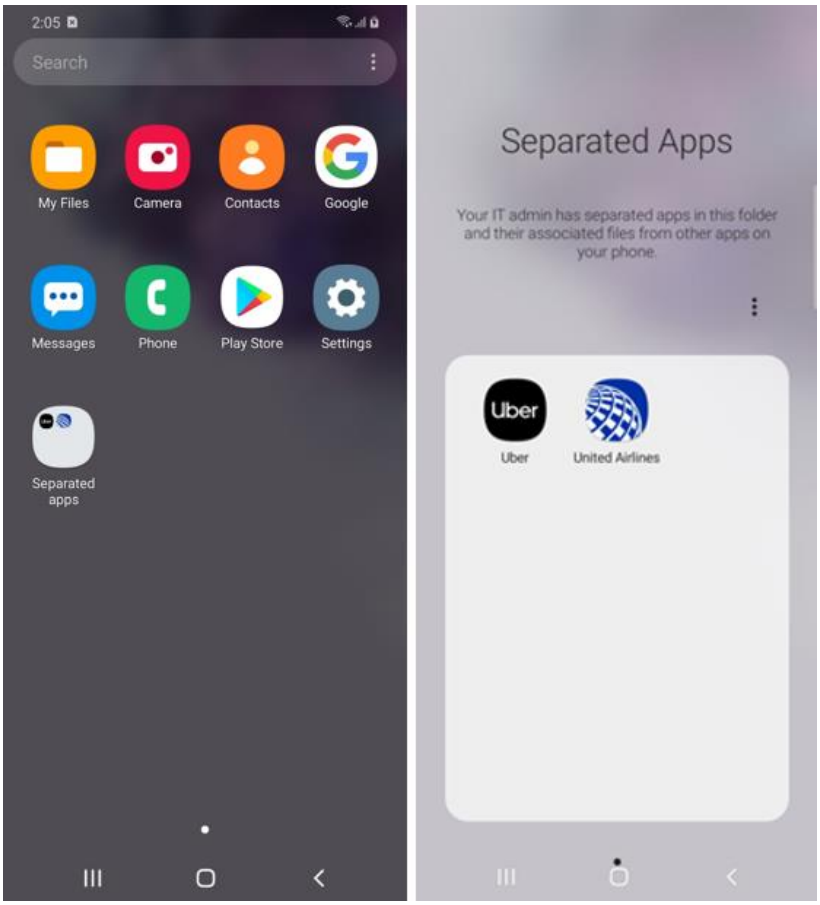


Android 11 replaced the fully managed device with work profile with a new work profile on company-owned devices. The goal is to protect the privacy of personal activities on company devices, and provide IT admins with adequate control over the personal side of the device. For enterprises that still need full control over a device while enabling authorized third-party business apps, Samsung exclusively offers an additional option called **Separated Apps**.

Separated Apps isolates third-party apps in sandboxed folder. The third-party apps cannot intercommunicate with work apps or access confidential work data. Keep in mind that Separated Apps does not provide the same privacy guarantees as the new work profile on company-owned devices. As such, it is not intended for personal apps and data.

How it works

Separated Apps are in installed in a securely separate folder:



An enterprise IT admin uses:

- a UEM system to install work apps on the fully managed device, for full access and control
- the Knox Service Plugin to enable Separated Apps and identify the apps to install in the folder

By default, the following apps are available inside the Separated Apps folder, but don't have launch icons. They can however be launched by other apps. For example, if you open an attached image in an email app, the Gallery displays the image.

- Google Chrome
- Microsoft Office (depends on model)
- Samsung Calendar
- Samsung Camera
- Samsung Contacts
- Samsung Gallery
- Samsung MyFiles
- Samsung Video

The device user can:

- set up an app shortcut from the device level, to launch an app inside the Separated Apps folder
- configure the following Settings inside the Separated Apps folder: apps, notifications, data usage, certificates, and keyboard and input.

Network Security

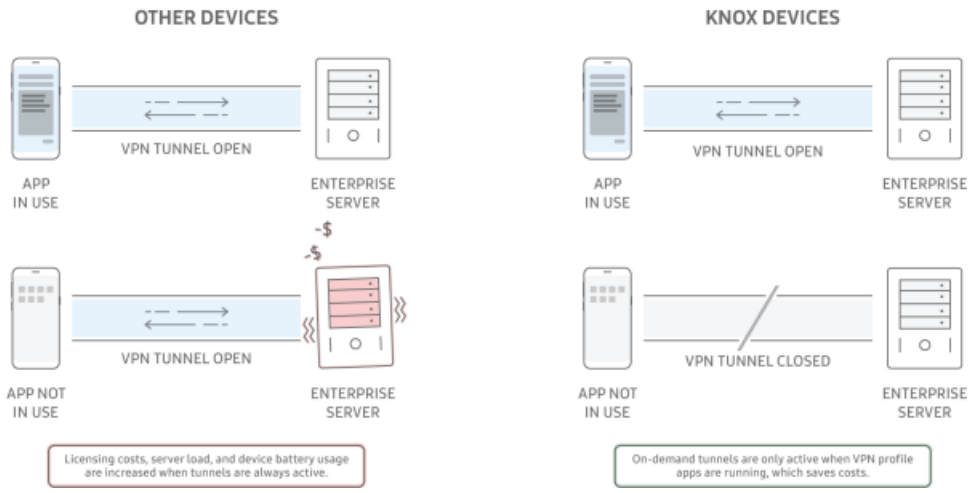
Virtual Private Networks (VPN)

Standard Android comes with basic VPN abilities that are adequate for most consumers. But many enterprises need better security and more flexible VPN controls for larger deployments. The Knox VPN framework includes the most advanced enterprise-focused feature set, which ensures that VPN connections are efficient, reliable, secure, and compliant with industry regulations and best practices. The Knox Platform VPN framework allows the integration of third-party VPN clients in addition to the built-in VPN client.

Unique advantages of Knox VPN framework

The Knox Platform VPN framework supports all common VPN types, protocols, and configuration options. When deploying VPN solutions, enterprise IT admins must ensure VPN deployments work smoothly, don't waste server resources, limit the VPN solution licensing costs, and enforce strict security policies that prevent data leakage.

The following is an example showing how Knox on-demand VPNs save cost:



The Knox Platform provides the following differentiating VPN features and advantages:

- The flexibility to use a VPN tunnel for the entire device (work profile as well as fully managed device) or a single app only.
- The cost saving benefit of using VPN tunnels on-demand, only when apps in a VPN profile are running.
- The convenience to bypass VPN tunnels when a device is on-premise in a local corporate network.
- The strict coverage of corner cases to prevent data leakage outside of VPN tunnels, even during a device boot.
- The ability to connect multiple tunnels simultaneously.
- The extra security of chaining VPNs (also known as cascading or nesting VPNs) for greater anonymity, for example, in classified deployments.
- The power of configuring web proxies over VPN:
    - Web proxy configurations are tunnel-specific.
    - Web proxy support for NTLM authentication, basic authentication, PAC, and PAC with authentication.
- The ability to configure SSL/IPSEC VPN profiles on multiple devices.
- The advantage of extending VPN tunnels from a mobile device to a tethered laptop, in situations where a laptop does not have network connectivity.

The following Knox VPN features are also available, but are dependent on the VPN client:

- **QoS or traffic tracking and shaping.** The Knox VPN framework can inform the VPN client when any installed apps generate any traffic.
- **Automatic reconnection of VPN tunnels when the server side disconnects.** Server-side disconnections are more difficult to detect and handle than device-side disconnections, which are usually related to detectable conditions like loss of connectivity or the presence of new network connections, such as a new Wi-Fi connection.

Robust handling of enterprise requirements

Regardless of the features you choose, the VPN should act predictably even when the unexpected occurs. The following are some common scenarios where Knox Platform enhancements ensure proper VPN behavior:

- VPN tunnels handle system events such as power saving mode entry or exit, package addition or removal, connectivity changes, and admin app changes.
- VPN profiles can specify which non-present apps must (not) use a VPN tunnel if they are ever installed.
- Even the free, built-in VPN client supports all the advanced VPN features listed in the previous list items.
- Robust blocking rules prevent data from leaking to the outside of the tunnel. Common gaps in coverage that Knox Platform VPNs correctly handle include:
    - A VPN client crash or other client app issues
    - A tunnel that has not yet been established, for example, during boot
    - A VPN client that is unable to connect to a VPN server
    - A proxy port that is blocking
- Handle captive portal prior to VPN tunnel establishment.

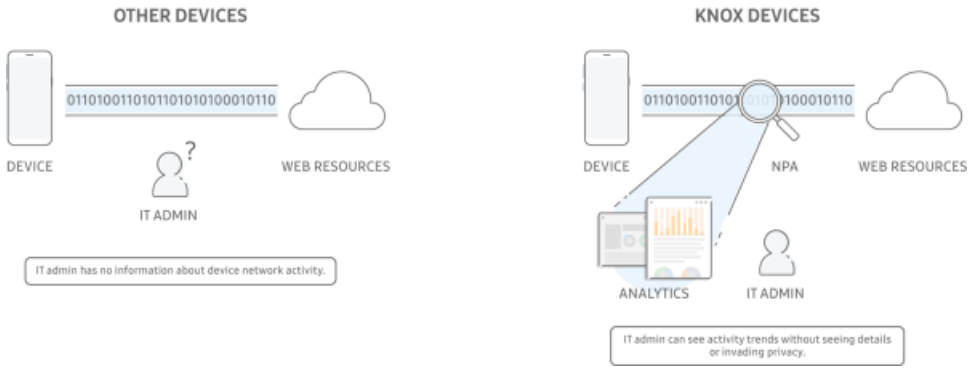
High-security built-in VPN client

The built-in Android VPN client (also called StrongSwan) is available on all Samsung devices, and is also integrated with the Knox Platform VPN framework, enabling the extra properties available within the Knox platform. The built-in VPN client, even without the Knox VPN framework, is differentiated from what Android offers, providing these advanced VPN features:

- FIPS 140-2 certified device cryptography components
- CPA certification at the Foundation grade, based on its successful Common Criteria evaluation against the Protection Profile for IPsec VPN Clients v1.4
- Security characteristics of IPSec VPN client version 2.5, as set by the NCSC
- Internet Key Exchange (IKE and IKEv2) and Suite-B algorithms:
    - IPsec IETF RFCs – IKEv1
    - IKEv1 – Main and aggressive IKE exchange modes with pre-shared key, certificates, Hybrid RSA, and EAP-MD5 authentications
    - IKEv2 with PSK and certificate-based authentication
    - IKEv2 – Pre-shared key, certificates, EAP-MD5 EAP-MSCHAPv2 authentication methods, and mobile extensions
    - IKEv1 Suite B Cryptography supported with PSK and ECDS signature-based authentications
    - IKEv2 Suite B Cryptography supported with ECDSA signatures

Network Platform Analytics (NPA)

Endpoint devices, such as mobile devices, are hard to monitor for security issues. Third-party apps can't inspect OS behaviors and networking patterns, something that is possible on desktop platforms. These limitations, combined with the prevalent use of endpoint encryption create an information "black hole". This information black hole makes it more difficult to detect misconfigurations, troubling network usage patterns, the misuse of enterprise resources, or other signs of issues that impact an enterprise's bottom line.



The NPA framework enables insights into mobile software and network use, misconfiguration, and network-based threats. Powerful analytics solutions use the NPA framework to increase endpoint visibility without violating the confidentiality of data moving across enterprise devices and networks.

Combined with a compatible analytics solution, NPA simplifies many device administration tasks:

- Detect **more** IT problems — "I don't know what I can't see!"
- Detect problems **faster** — "Notify me automatically of suspicious patterns."
- Investigate more **easily** — "Walk me through the chain of events."
- See root cause **attribution** — "Am I being attacked? Is this a bug? Is something misconfigured?"
- Provide **visibility** required to **trust** mobile devices — "Show me how my network is being used."
- Enable quicker **remediation** — "Lock down the device, user, or app causing this issue!"

NPA design

The NPA framework provides real-time information about the network packets leaving a device and the context surrounding the flow of data. An NPA-compatible Network Analyzer then analyzes the available data to provide valuable insights. Is your new beta app sending sensitive data to an unexpected server in a foreign country? Analyzing endpoint flow data gives us insights into network traffic, such as:

- The destination of every network flow, using either IPv4 or IPv6 addresses
- The domain name originator associated with the destination IP address
- The start and stop time for the network flow
- The number of bytes transferred in and out during the network session
- The name of the process or app initiating the data flow
- The cryptographic signature of the app initiating the data flow, and of its parent process
- Whether or not traffic originated from a tethered device (for example, a mobile hotspot) or from within the device

NPA maintains enterprise data confidentiality as it only inspects the header data and the context surrounding network traffic patterns. NPA and NPA-compatible network analyzers don't have access to actual data packets. This feature is a strong differentiator compared to solutions that unnecessarily collect and redirect all endpoint network traffic, usually by means of a web proxy or VPN.

Unique advantages of Knox NPA

The Knox platform NPA provides the only mobile platform for granular endpoint networking insights. Some unique advantages are:

- NPA is unaffected by endpoint network encryption.
- NPA can uniquely attribute network patterns to the specific software responsible.
- NPA can differentiate between traffic originating from a well-known Android app and a fake app impersonating the app.
- NPA does not expose your entire network traffic to the analytics solution.

NPA-compatible solutions

Samsung's release partner for NPA is Cisco. Cisco's network security products can now interface with Knox NPA to provide endpoint visibility of Knox devices. Admins can get this visibility even when a VPN is encrypting endpoint traffic. These insights are exposed to admins using the Cisco StealthWatch console and remediation steps performed using Cisco ICE.

Other Knox partners are preparing NPA-based solutions to help solve other common problems associated with mobile device deployments.

Certificate Management

Universal Credential Management (UCM)

Digital credentials are critical mobile security building blocks, leveraging trusted authorities to validate identity and secure private channels across public deployments. Your mobile device credentials provide seamless access to secured Wi-Fi, VPN, email, and websites. Credentials include certificates providing identity and private keys to decrypt sensitive data. These credentials must be securely stored to prevent malicious parties from exploiting your identity and accessing confidential data.

Secure elements

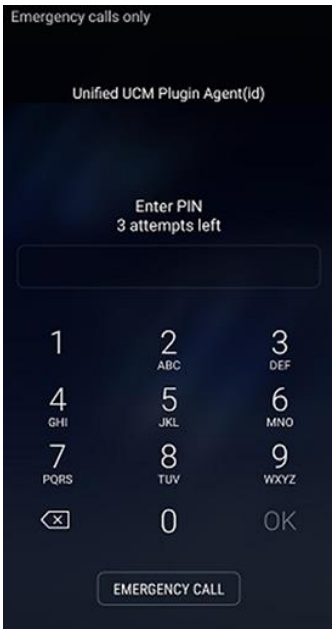
While Android apps are able to store digital credentials securely on Samsung Android devices using the hardware-backed Keystore, some use cases require the user credentials and secrets stored in a secure element, which can come in form factors such as the following:

- **Embedded Secure Element** (eSE) — Supports the storing and accessing of credentials, allowing secure storage on the device without additional hardware.
- **Micro SD card**
- **Universal Integrated Circuit Card** (UICC)
- **Smart card** — Smart cards' resiliency makes them ideal for storing credentials if the threat model calls for trust to be shifted outside the device.

NOTE: The Samsung eSE is not available with the following countries and carriers: USA-Verizon, Korea-All, Japan-All, Canada-Telus.

Certain customers, especially in government and related industries, have internal regulations requiring the use of approved secure elements for storing credentials and secrets. The secure element is provisioned with an applet that provides certain cryptographic functions.

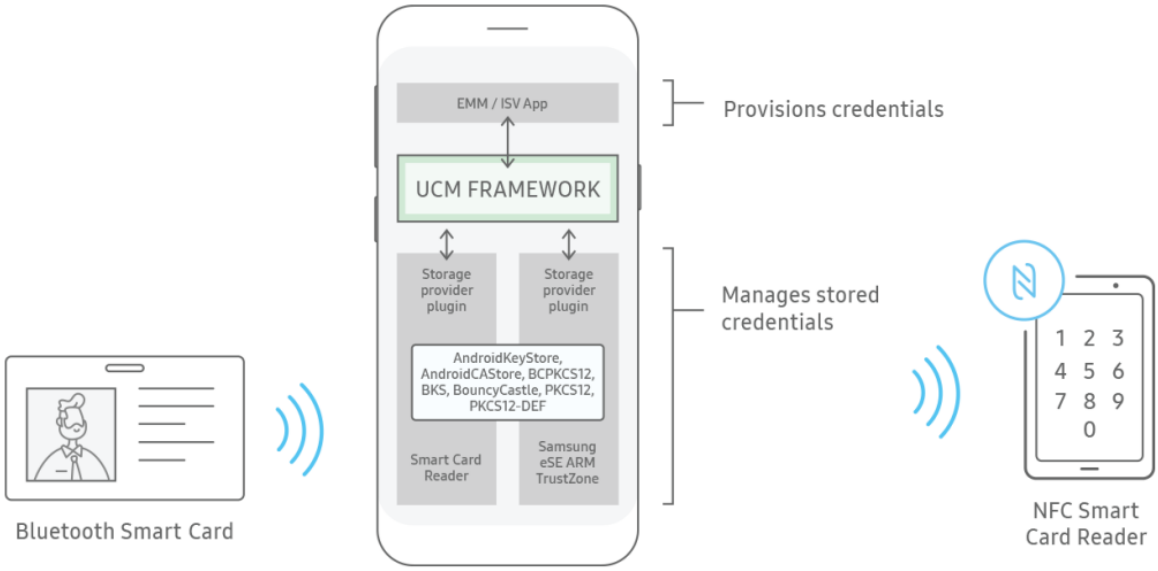
Use cases



The UCM framework implements a service layer that allows vendors to make their solution available to specialized apps on the device including:

- **Device lock** (keyguard) — The user inserts a PIN to authenticate themselves to the applet running in the secure element. If the PIN authentication is successful, the UCM framework retrieves a password from credential storage, which is used as the device password to unlock the device.
- **Data at Rest** (DAR) encryption — The applet provides another layer of protection for the device encryption keys. UCM allows for the device encryption key to be wrapped by the applet. The wrapped device encryption is unwrapped when the user provides the correct PIN on device boot.

UCM framework



The Universal Credential Management (UCM) framework enables Android apps to access all credential storage devices through the same standard programming interface—the Java Cryptography Extensions (JCE) API via either:

- a specific provider to carry out supported crypto operations
- the Android Keychain API for key and certificate operations

The vendor providing the secure element solution (including the applet) implements a UCM plugin, which registers their solution as a Keystore provider. Apps can simply refer to the vendor's provider when calling Keystore API.

A significant benefit of the UCM framework is that it uniquely enables storage vendors to develop a plugin that provides access to their storage space and cryptographic operations, without forcing app developers to change their code or forcing IT admins or end users to update their apps. The plugin essentially acts as the link between the UCM framework and a specific storage device.

The UCM framework consolidates and standardizes credential services to provide a streamlined interface for:

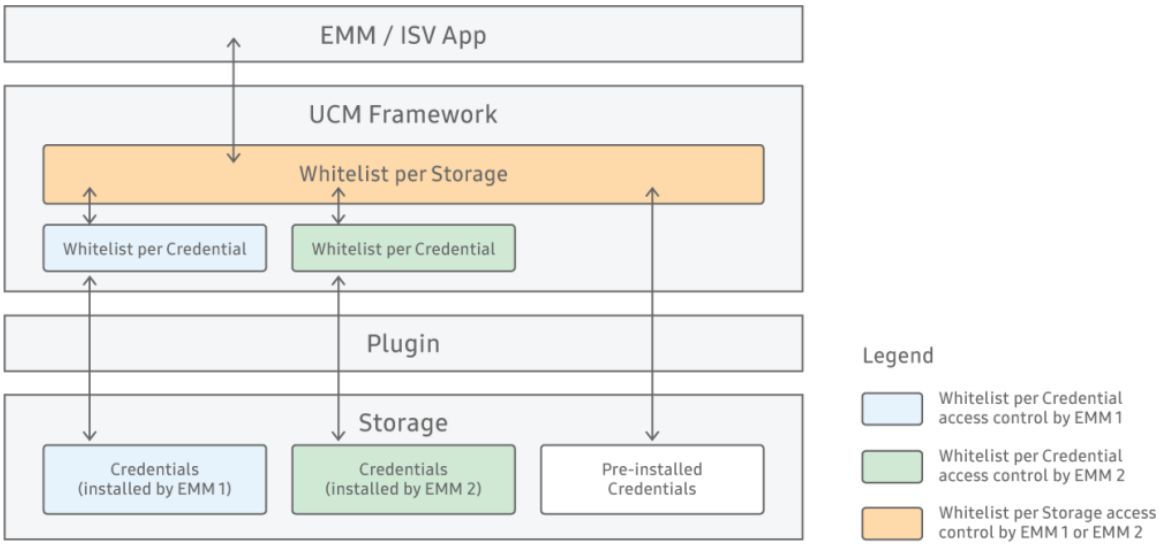
- **EMM or ISV apps** — These apps configure, provision, and consume credentials, managing credential storage access permissions, and activating advanced UCM permissions. The apps can enforce the installation, removal, or per-app access control of a credential.
- **Storage provider plugin** — These apps are provided by storage vendors to link the UCM framework to their storage solution, to manage stored credentials.
- **Secure storage** — This feature currently includes the Samsung eSE and Smart Card readers described in "Certificate Management" on page . You can easily support other storage options through additional vendor plugins.

The Knox SDK provides credential storage vendors a set of UCM APIs to make current and future storage options available on Samsung devices, hiding the implementation details of their solution so that mobile app developers can transparently access stored credentials through standard APIs, such as the Android Keychain. Similarly, developers can use the Java Cryptography Extension APIs to offload cryptographic operations to a capable Smart Card. This abstraction, made possible by the UCM framework, eliminates the need for complex vendor-specific code within mobile apps, meaning enterprise customers have a wide range of existing apps available to them and can easily develop in-house apps without worrying about the underlying storage implementation.

UCM allowlist

The UCM framework uses two types of allowlists, which uniquely manage access controls for credential storage and offer fully customizable access permissions:

- **App allowlist** — Enforces which apps can access each secure storage type. Every secure storage device maps to its respective UCM plugin, that a secure storage solution provider creates and maintains.
- **Credential allowlist** — Enforces each app's access to credentials, providing app-specific access permissions. By enforcing access control, admins can prevent credential usage by malicious or untrusted apps.



Client Certificate Manager (CCM)

Samsung builds upon the Android Keystore by providing a tamper-proof, detection-based lock-down of cryptographic keys and certificates. This solution supports a variety of high-security use cases important to enterprises, as described in the following sections.

Granular certificate and key access control

The Knox Platform supports an app allowlist for certificates, allowing the certificate installer to define which apps are allowed to perform cryptographic operations based on their certificates. This certificate allowlist process offers better control and flexibility than simply allowing app-only or device-wide access rights to certificates.

Silent installation

Knox 3.2.1 allows IT admins to install certificates while the device is still locked. This means certificates can be silently installed into a keystore without any interaction from the device-user.

Signing with device-specific certificates

A special certificate called the **Device Default Certificate** (DDC) resides within each device. What makes this certificate special is that it is tied to that device's hardware, is signed by the Device Root Key (DRK), and can never leave the device.

Any objects signed by the same DDC are guaranteed to have come from the same Samsung device. There is no way to spoof the identity of a device by reusing a DDC and its key pair on a different device.

Device integrity assurance

Objects signed with this certificate were signed while the device was in good health, meaning when the device was uncompromised. If a device fails its integrity checks—by failing the signature check of the kernel or OS or disabling SE for Android—the following happens:

- A tamper fuse is set; *and*
- The DDC is rendered permanently unusable.

This lockdown helps attest to the health of the device where the data was signed. After all, you can't trust a signature if the device doing the signing is compromised. The Knox Platform provides a CSR agent that benefits from this device health attestation claim. A CSR produced and signed by the CSR agent carries implicit device health security claims.

Keystore integration with other features

A keystore is only as useful as the use cases it supports. In addition to manual cryptographic actions—such as sign, verify, encrypt, and decrypt—the Knox Platform provides built-in logic to support sensitive certificate-based actions enterprises often need to secure their solutions such as the following:

- **Certificate Signing Requests** (CSRs) — The ability to complete CSRs with a trusted agent, tied to the Knox Platform's hardware-based Root of Trust, simplifies the secure handling of mobile endpoint requests for digital identity certificates. Instead of sending key pairs and certificates from servers, keys can instead be securely generated on-device and bound to hardware. The public certificate is then included in an appropriate CSR request. Using the CSR agent to validate CSR contents and sign the request avoids trusting sensitive actions to third-party code running in less trusted areas of the device.
- **Certificate Enrollment Protocols** (CEPs) — Similar to CSR, CEP provides built-in agents for logic that enterprises rely on, saving time and enhancing security claims. For more information, see Certificate Enrollment Protocols.

In addition to the DDC, you can generate or install your own certificate and key pairs and specify they are accessible only if the device is in good health. This additional process locks down the keystore in the event of a device integrity failure.

Certificate Enrollment Protocols (CEP)

The Certificate Enrollment Protocols (CEP) provision and support digital certificates for apps within Samsung devices. This feature is of great assistance to MDMs and third-party vendors. Why? Because the CEP helps complete certificate enrollment without device user intervention, further solidifying the claim that Samsung Knox devices provide both world-class security as well as industry-leading manageability.

Enterprises can use CEP to:

- Enroll, renew, or delete certificates
- Check your deployment's certificate enrollment or renewal status

The CEP service is very robust, and supports the following enrollment protocols and standards:

- Simple Certificate Enrollment Protocol (SCEP)
- Certificate Management Protocol (CMP)
- Certificate Management over Cryptographic Message Syntax, Enrollment Over Secure Transport (CMC-EST)

SCEP, CMP, and CMC are frequently used certificate enrollment protocols for provisioning digital certificates. For more information on these protocols, see Internet Engineering Task Force (IETF).

CEP asymmetric key acquisition

Apps use CEP to acquire the public part of an asymmetric key. Asymmetric keys have a public part and a private part. The private part never leaves the Keystore, but the public part is freely distributed. The key owner can use the Keystore to apply the private part of the asymmetric key to an encrypted message to decrypt it.

CEP operational environment

CEP functions within the scope of either the work container or personal space, depending on where it is installed. If the deployment objective is to provision and manage certificates for apps inside the work container only, then you must refer to your chosen MDM's documentation for instructions.

If the objective is to provision and manage certificates for apps in the personal space, then you can install the CEP services in the personal space to provision and manage certificates.

MDM agents can call the CEP services in either the personal space or work container. MDM agents don't have access to a service created outside their scope.

Device Management

Device Software Update Management

Frequent software updates are often necessary to resolve bugs, patch security vulnerabilities, and enhance device capabilities. But IT admins must understand and validate software changes prior to mass deployment. Samsung released the mobile industry's first firmware update management system on Android to enable IT to test and validate software updates and to control roll-out scope and timing.

Why manage device software updates?

In enterprises with fragmented platforms and firmware versions, mobile device deployment and support becomes a time-consuming and tedious task. Proprietary enterprise apps and application services behave inconsistently on different firmware versions, so features require testing and troubleshooting on a widening array of device platforms.

Controlling the rollout of software updates allows IT admins to:

- Homogenize the firmware versions and capabilities of deployed device models.
- Carry out interoperability or compatibility testing with in-house or proprietary servers, apps, and endpoint settings.
- Ensure that known issues are patched before deployment of major firmware version updates.
- Perform field tests of new firmware and software on a subset of devices before mass deployment.
- Force the use of firmware versions that have been validated to meet industry certification or regulation requirements.

Strict control over device firmware updates

Samsung developed Enterprise Firmware Over-the-Air (E-FOTA) to enable enterprises to save time and support costs, and manage the mobile infrastructure as efficiently as possible.

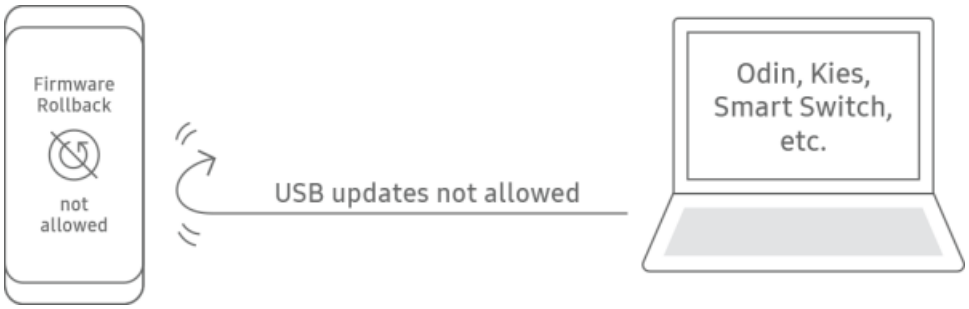
With E-FOTA, enterprises can control device software updates as follows:

- **Select the highest firmware version allowed on devices** — This option ensures that device users can't independently update to an unsupported firmware version, preventing issues that could negatively impact employee productivity, support costs, and data security.
- **Force the download of a specific firmware version onto select devices** — Enterprises can download new firmware to a few test devices to run interoperability or compatibility tests. This mandatory download is done with proprietary systems and apps to find any corner cases that might result in operational or performance issues.

- **Mass deploy a new firmware version** — Mass deployment prevents software version fragmentation so IT teams don't need to support multiple legacy firmware versions for each deployed device model.
- **Schedule updates during non-peak work times** — This option ensures updates don't interfere with employee productivity.

Knox control over user updates

A wide range of EMM partners support Samsung's firmware management features, integrating firmware management with other asset management activities. IT admins can use these tools to test and deploy software updates in a consistent and low-risk way. Through EMM solutions, enterprises can restrict users from loading unauthorized firmware, through their devices or USB-connected computers.



Through the Knox Platform, enterprises can:

- **Disable automatic firmware updates** – IT admins can prevent users from going to their Android Settings to enable or disable automatic firmware updates.
- **Disable all OTA updates** – IT admins can prevent users from going to their Android Settings to enable or disable software updates in general. This restriction includes updates for firmware, security patches, bug fixes, and apps.
- **Disable USB-connected updates** – IT admins can prevent users from booting into Download Mode and installing a manual software update. This restriction includes updates through the Odin, Kies, and Smart Switch update tools.

Granular Device Management

The Knox Platform's granular device management features are specifically curated, from partner feedback and industry data, to solve some of the most common frustrations enterprises face when mass deploying devices. These unique policies provide device flexibility and customization beyond any other device provider. The policies help organizations manage operations more effectively, secure confidential assets, and reduce administrative overhead. They also solve particular issues regarding industry regulation and compliance. For example, Rich Communication Services (RCS) logging is required by law in the financial industry. Samsung is the only vendor to provide this critical auditing feature.

Custom boot banner

Samsung Knox is the only mobile platform that allows an enterprise to natively change the device boot logo. In many industries, such as government or defense, this change is mandatory for compliance. Through the Knox Platform, enterprise IT admins and developers can customize the following:

- Samsung boot up display
- Splash screen animation, when the device is turned on or off
- Lockscreen image, which can provide an enterprise logo or contact info for lost phones

Enterprises can use these capabilities to mitigate problems such as the following:

- **Phone is lost and found** — Owner information is available by simply powering on the device. There is no need to attempt to unlock the device or call the carrier. The device can be returned to the enterprise quickly.
- **Multiple phones** — Displaying an enterprise logo on bootup lets users know that the device belongs to and is secured by the enterprise. This logo clearly distinguishes it from other devices in the user's possession.

Split billing (Dual APN)

Split billing separates enterprise and personal data usage.

- In Bring Your Own Device (BYOD) deployments, enterprise billing allows employees to be properly compensated for data costs generated from work-related app usage.
- In Corporately Owned, Personally Enabled (COPE) deployments, enterprise billing allows employers to pay for data usage incurred only for work purposes.

Split billing also works with dual SIM devices, by mapping some apps to using the data plan from one SIM, and other apps to the other SIM's data plan.

Remote admin lock of device

This feature allows an IT admin to remotely lock out a device, for example, when the device is out of compliance. Once the device is locked, only an IT admin can unlock it and not a device user. This functionality solves two problems:

- Prevents unauthorized users from accessing the device if it gets lost or stolen.
- Prevents users with valid login credentials from using the device, for example, if the credentials are stolen or the user is no longer allowed to use the device.

With stock Android, an IT admin can lock a device only if it is currently unlocked. If the device is already locked, an admin can't lock it to prevent future unauthorized logins.

Enterprise roaming

Roaming mobile connections can incur unexpected data costs. Multiplied across an enterprise's mobile workforce, these costs can become exorbitant. Rather than just simply disabling all mobile roaming, the Knox Platform provides more granular controls for enterprises, letting them control which mission-critical apps are allowed to use data during mobile roaming. Enterprises could enable roaming data for:

- All apps in the work container
- A single app within the work container
- A single app in the personal space

They can also set up Split Billing, with separate roaming policies for the APNs set up for personal and enterprise billing.

Granular policies

Call restrictions

Enterprises can apply granular settings to the caller app, allowing only:

- Emergency calling
- Calling to certain numbers
- A limited number of calls per day

RCS logging

The Knox Platform allows an enterprise to log RCS messages. For many industries, such as financial services, the ability to audit sent and received messages is required by law.

RCS messaging is a new messaging protocol that replaces SMS as the default messaging platform for carriers. It adds much needed features such as group messages and allows users to send more file types. Currently, enterprises that can't capture RCS messages must turn RCS off and lose the benefits of this new protocol. Knox RCS logging capabilities mean deployments can use powerful RCS abilities while staying compliant.

SMS management

Knox provides many advanced SMS policies. Policies frequently used by organizations include:

- Adding an automatic company disclaimer to the bottom of every outgoing text
- Restricting the number of texts per day
- Auditing and recording all incoming and outgoing SMS messages

SD card restrictions

Most vendors don't provide sophisticated options to manage an SD card. Typically, enterprises must choose between one of two options: allow full read and write access to the SD card or completely block it.

The Knox Platform addresses this industry pain point by giving enterprises independent control over read and write access. Knox can:

- Allow read access but block write access
- Allow write access but block read access

This level of control means you can provide one-way data access to sensitive data to effectively meet your security requirements.

Bluetooth restrictions

To mitigate attacks perpetrated through Bluetooth connections, Knox provides these controls:

- **Completely disable Bluetooth** — Turn off Bluetooth and Bluetooth background scanning.
- **Block specific Bluetooth profile types** — Restrict the types of Bluetooth devices that the user can connect to the device, for example:
    - Allow Bluetooth headphones
    - Block Bluetooth file transfers, which could leak private data

USB class restrictions

Knox can restrict or allow different types of USB-connected devices, more specifically, the USB device classes defined through usb.org. This feature includes access to the following USB device classes:

- Audio, Video, Audio/Video
- Mass Storage
- Content Security
- Smart Card
- Printer
- Hub, Type-C Bridge, Wireless Controller
- Human Interface Device (HID)
- Communications, CDC Control, CDC Data
- Personal Healthcare
- Billboard
- Diagnostic

For example, you could block all USB devices except Smart Card readers.

Keyboard Input Methods (IME)

The Keyboard Input Method (IME) framework has received a major security upgrade with Knox 3.2.1.

In Knox 3.2.1, the personal and work container keyboards are completely separate to ensure that important work data is not compromised. In an Android Enterprise Work Profile, the same IME is used for both the personal and profile side. An shared IME may potentially leak sensitive data through an exploit buried in the IME.

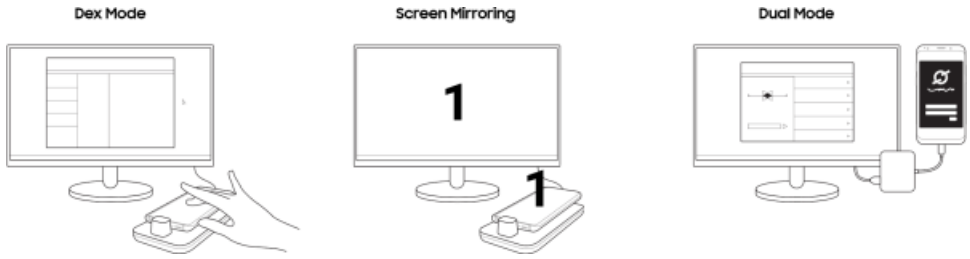
For example, let's say a device user downloads a malicious IME from Google Play for use on the personal side.

- **Android Enterprise:** this IME is shared with the Work profile and sensitive data may leak.
- **Samsung Knox**: The IME is isolated from the work containerand can't access sensitive information.

In previous versions of Knox, IT admins were required to add 3rd party IMEs to an allowlist for added security. Now that personal and work container IMEs are kept separate, users are able to use third party keyboards without prior explicit allowance from IT admins.

Samsung DeX Management

Samsung DeX is a unique product that lets you use your phone as if it were a laptop or desktop computer. You simply connect your phone to a monitor, and optionally use a mouse, keyboard, or S-Pen to launch apps, move objects, type text, write text, or draw images.



DeX supports three different modes:

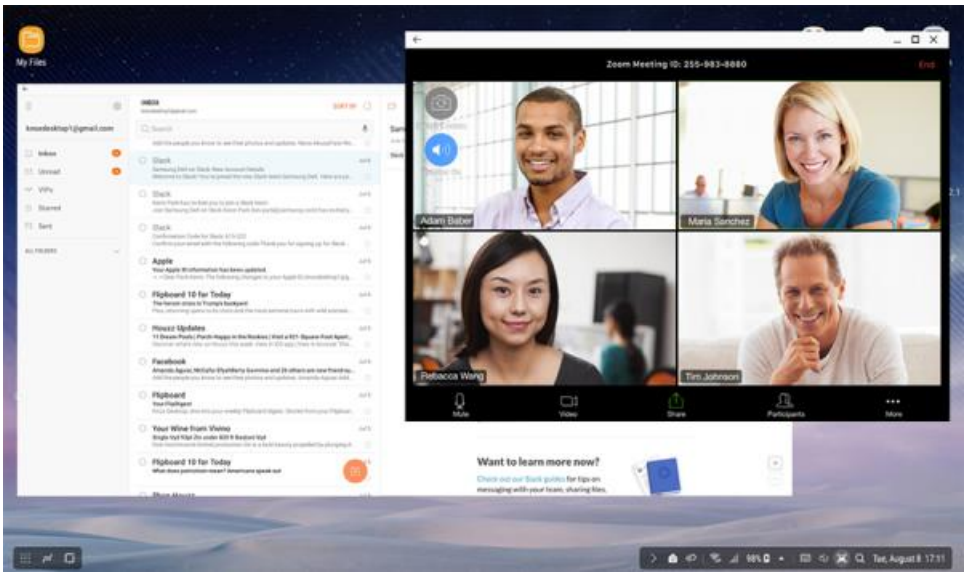
- **DeX Mode** — The phone's screen appears on the connected monitor. You can connect a keyboard and mouse to enter text and move the cursor on the monitor. Use this mode to read or write documents, participate in video conferences, compose more complex emails, edit images, or develop slide presentations.
- **Screen Mirroring** — The phone's screen is duplicated on the monitor. Use this mode to view images or videos.
- **Dual Mode** — You can use both the phone screen and the monitor at the same time.

You can connect your phone to a monitor and peripherals using one of the following options:

- Samsung DeX docking station
- Samsung DeX docking pad
- USB-C to HDMI adapter

Why use Samsung DeX?

Instead of having to carry both a laptop and phone, you now need only a phone. Through a single portable device, you can quickly write documents, edit spreadsheets, and create presentations on a conventional large screen. There is no need to purchase or carry along a separate laptop. The DeX mode untethers employees from their laptops, and offers enterprises many capital cost savings opportunities.



Using Knox to customize DeX

Enterprises can use the Samsung Knox platform to secure the way Samsung DeX works, allowing them to benefit from the Knox Platform's defense-grade security features without sacrificing the innovation and productivity that comes with DeX.

Using a large screen in DeX mode means that sensitive information may be visible to passersby. As such, you can use the Knox platform to improve security in DeX mode. You can deploy security policies such as:

- Setting a screen timeout while in DeX mode
- Allowing only Ethernet connections, no Wi-Fi or cellular data
- Disabling specific apps in DeX mode, for example, apps displaying confidential data
- Disabling DeX mode

You can also use the Knox Platform to customize the DeX interface. Available customizations include:

- Uploading a company logo to the DeX loading screen
- Adding or removing shortcuts from the DeX launcher

Unique advantages of Samsung DeX

- **Mobile desktop experience** — Enables phone use, on the go, in a desktop environment. A separate laptop is unnecessary. You can access the apps and files necessary directly using your phone.
- **Defense-grade security on a desktop** — Protects users and enterprises with industry-leading security while preserving the productivity enhancements of a desktop environment.
- **Universal app compatibility** — Compatible with the native Samsung and Android apps that are pre-installed on devices. Popular apps such as Microsoft Office apps and Adobe Photoshop Express are also optimized for use with DeX to take advantage of larger, multi-app displays.
- **Customizable** — Mobile app developers can enhance and control their apps while in use with DeX, using DeX APIs from the Knox SDK.

Firewall Management

Most mobile device platforms use built-in firewalls, but don't provide granular control over firewall settings and activity. With the Knox Platform, you can deploy firewall configurations specifically catered to your enterprise security needs.

Why manage and customize device firewalls?

Default firewalls may not provide your organization with the security and data protection it needs. In fact, some firewalls may not even let you see the rules they are enforcing. However, when configuring firewalls with the Samsung Knox Platform, you can know exactly what policies are deployed and take additional measures to secure your enterprise systems.

With the Samsung Knox Platform, you can:

- Restrict and redirect Internet access to specific IP addresses and domains
- Set firewall policies on a per-app or device basis
- Produce logs reporting the blocked domains that users accessed

Granular control of Internet access

You can limit the permissible network connections to only trusted addresses, by setting the appropriate Internet access restrictions. The Knox Platform offers a variety of restriction methods, all of which can be used together:

- **IP address filters** — Allow, deny, and redirect access to specific IP addresses. Configure a filter to apply to transmitted data, received data, or both. Allow or deny both IPv4 and IPv6 formatted addresses.
- **Domain name filters** — Allow or deny access to an entire domain or sub-domain.
- **Per-app and device-wide modes** — Give specific apps—for example, ones that handle confidential data—stronger firewalls, and all other apps on a device a more lenient firewall configuration.

Log unsafe URL access

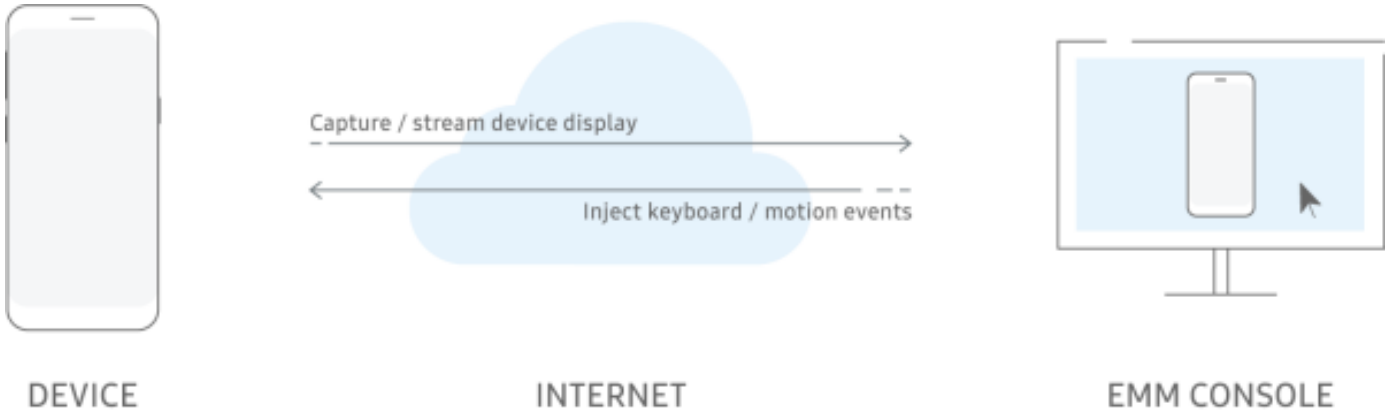
The Knox Platform provides visibility into denied attempts to access blocked domains. The improved visibility helps you to remain aware of potential security breaches or insecure browsing practices within your organization.

The Knox Platform logs reports with the following information:

- **App name** — The package name of the app attempting to access a blocked domain.
- **Blocked domain URL** — The URL of the domain name blocked by your firewall.
- **Timestamp** — The time the incident occurred, to assist with troubleshooting incidents.

Remote Control

With the increasing complexity of problems that IT admins must solve, Knox Remote Control provides IT admins a powerful way to quickly and remotely fix issues. Not only can IT admins have real-time access to what the remote device screen is displaying, but also control it by injecting actions such as finger, keyboard, and mouse events. Although other mobile platforms also offer remote viewing of remote device displays, only Knox provides built-in remote control of devices without requiring third-party solutions.



Here is an example use case: An enterprise employee is on a business trip. On encountering a problem with the company-issued mobile phone, the employee contacts an enterprise IT admin. The IT admin uses an EMM console to remotely view the device screen to observe the issue first hand, then remotely controls the device, through finger, mouse, or keyboard actions. The IT admin directly accesses the environment to remotely debug the issue on the device. The employee is now quickly productive, without the frustrating downtime associated with relaying instructions verbally or through email.

The continuous polling of the device screens doesn't impact device performance as devices send only screen changes.

Unique advantages of Knox Remote Control

The Knox Platform provides built-in remote control without requiring third-party solutions. For enterprises, this control:

- **Saves time** by enabling IT admins to troubleshoot remote mobile device issues in real-time.
- **Reduces employee down-time** and **optimizes employee productivity** through quick problem resolution.
- **Enables monitoring** of devices for corporate policy violations along with corrective actions on the devices.

Audit Log

Organizations that need to troubleshoot serious security breaches rely on audit logs for a forensic analysis of the activities leading up to actual and potential breaches. In regulated industries, these audit trails are a mandated requirement to comply with security audits.

With the Knox platform, an enterprise IT admin can use an EMM console to enable audit logging on all corporate devices. IT admins can proactively pull audit logs from time to time, to detect and defend against malware or viruses at the earliest onset. In the event of a possible intrusion, IT admins can parse the logged events for unauthorized activities.

Unique advantages of Knox Audit Log

The Knox platform provides comprehensive audit logging, above and beyond that provided in a standard Android audit log. These added capabilities provides enterprises with these benefits:

- Empowers IT admins with deeper, more valuable insights.
- Offers comprehensive help in detecting and defending against malware and viruses.
- Adheres to mandated requirements in regulated industries.
- Complies with the Mobile Device Fundamentals Protection Profile (MDFPP) 2.0 requirements to collect events.

Knox provides these additional insights:

System security

- Integrity verification failed
- Device Admin activation state

Authentication

- Minimum password complexity
    - Forbidden strings
    - Maximum character occurrences
    - Required pattern
    - Maximum numeric sequence
    - Maximum character sequence
    - Minimum character change length
    - Maximum failed passwords before disable
- Locked state
- Certificates
    - Removed certificate from untrusted DB
    - Added certificate to untrusted DB
    - Succeeded disabling system certificates

App management

- Install/uninstall
    - App signature allowlist
    - App package name allowlist
    - Installed apps
    - Removed apps

Data protection

- Requested full wipe of device
- Encryption state
    - Requested encryption of internal storage (Secure Startup)
    - Requested encryption of external storage
    - Encryption of storage card succeeded/failed
    - Failed to encrypt/decrypt/access file
- VPN protection state

Networks & peripherals

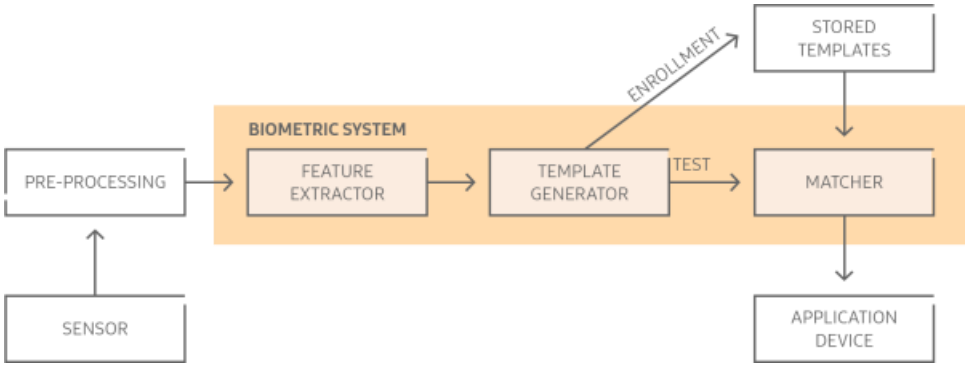
- NFC
    - Enabled/disabled
- Bluetooth
    - Enabled/disabled
    - Enabled/disabled discoverable state
    - Enabled/disabled limited discoverable state
    - Enabled/disabled Samsung Beam
- Wi-Fi
    - Enabled/disabled
- Cellular
    - Enabled/disabled
- Camera
    - Enabled/disabled
- Microphone
    - Enabled/disabled
- Location/GPS
    - Started/stopped
    - Enabled/disabled location provider

User Authentication

Biometric authentication

Traditional user authentication relies on things you know or have, like a password or ID card. These are susceptible to human mistakes, phishing, and duplication. Biometric authentication validates a personal trait, for example: fingerprints, irises, or facial features. Biometrics can lower the false acceptance rate (FAR). Users can use biometrics to unlock devices and app containers. Through Samsung Pass, users can also use biometrics to log into apps and websites.

Unique advantages of Knox Biometrics



The Knox Platform provides the following in addition to standard Android capabilities:

- **Secure storage** — On Samsung devices, the authentication software doesn't share or distribute the biometric measurements of any user. The measurements are stored in a format that can't be used to reproduce the original biometric, and can only be accessed and decoded within the specific part of the TrustZone that has access to the biometric hardware. Biometrics are used only on the correct device and by the correct user. This functionality means there is a lower chance of someone spoofing biometrics credentials to access a device.
- **Enforced two-factor authentication** (2FA) — The Knox Platform provides IT admins the option to enforce two-factor authentication with biometrics for the work container. For example, a user can be required to authenticate with an iris scan in addition to a standard device unlock method (password, PIN, pattern). While Android provides some combinations of two-factor authentication, the Knox Platform allows you to take your security one step further with biometric integration.
- **Samsung Pass integration** — Apps can use Samsung Pass APIs to enforce biometric authentication in place of a traditional login and password. This authentication method can save an organization a large amount of password management overhead, while further increasing device security. Samsung Pass features the ability to:
  - Support Fast IDentification Online (FIDO) authentication
  - Register and deregister a user's biometrics
  - Respond to remote wipe requests
  - Manage authentication transactions
  - Work in the Secure World of the TrustZone
- **Enterprise credentials override** — As required by enterprise policy, Knox devices allow you to enforce the use of enterprise AD credentials to unlock a device or work container. This setting overrides any biometrics set by the user, and forces them to use their enterprise credentials.

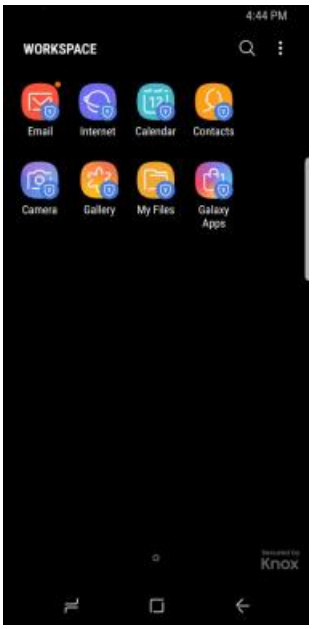
App and Data Protection

NOTE— SSO, AD Container, Shared devices, and Cloud SDK have been deprecated in the Knox 3.4.1 release. Although the features might still work, they will no longer be tested and will stop working in an upcoming Knox release. We strongly recommend that you use an equivalent feature in Android or stop using the feature altogether.

Enterprise Productivity Apps

Mobile apps have changed the way we work by providing new channels of communication, innovating customer engagement, and empowering organizations with critical data in real-time. Samsung Knox devices include a set of productivity apps for both personal and business use.

Business-critical apps include Samsung Email, Internet browser, Calendar, and Contacts. Enterprise IT admins can secure these apps within the work profile, along with other apps used by the enterprise.



The Knox Platform secures enterprise apps and protects confidential app data through these methods:

- **App installations and updates** — Apps are pre-installed within the mobile device's secure work profile and users can update these apps independent of firmware updates through Google Play.
- **App isolation** — Apps are sandboxed within the work profile, which uses SE for Android to prevent personal apps from interfering with the business apps that are in the work profile.
- **App permissions** — Knox provides App Permission Monitoring to help users prevent malware from using powerful permissions to gain unauthorized access to the device and work profile.
- **Data At Rest** — Through Knox's Sensitive Data Protection (SDP), the files and data used by an app can remain encrypted until device users authenticate at device unlock or work profile login. Individual apps can further deploy an app-specific password as another line of defense.
- **Data In Transit** — App data sent through the public Internet can be secured using Knox's advanced VPN features.
- **DeX integration** — Not only are all Samsung native apps optimized to work within DeX, enterprises can secure apps while they're displayed in DeX.

Samsung Email

The Samsung Email app is uniquely designed for customers requiring the secure synchronization of their mobile device's Email calendar, tasks, and memo functions. The Email app can use MS Exchange ActiveSync (EAS) for Single Sign On using company credentials.

In contrast with third-party security solutions, the Samsung Email app uses Sensitive Data Protection (SDP) by default, to automatically:

- Protect email text and attachments
- Secure incoming emails and notifications in real time

The Samsung Email app provides these key benefits:

- Productivity
    - Single Sign On (SSO) with EAS
    - EAS synchronization of contacts, calendar, tasks, and note data
    - Federated LDAP query support
- Security
    - EAS certification for account
    - EAS certification for S/MIME messages
    - EAS certification revocation checks
    - EAS certification history support
    - Card certification support
- Management
    - LDAP account management
    - EAS account management

Samsung Internet Browser

The Samsung Internet Browser provides enterprises with the following security features:

- **Biometric Authentication** — IT admins can enforce biometric authentication for website logins, web payments, and accessing Secret Mode.
- **Secret Mode Password** — IT admins can enforce password access to Secret Mode, which can contain confidential bookmarks and saved pages.
- **Protected Browsing** — IT admins can enable warnings to alert users if they try to view known malicious sites, which might try to steal confidential data such as passwords or credit card information.
- **Content Blockers** — IT admins can allow the use of third-party plugins to filter out content such as:
    - ads, which can come with cookies, malware, or viruses
    - invisible trackers, which can monitor online activity

Enterprises can take advantage of the following additional capabilities to secure mobile browsing:

- Set up an HTTP proxy
- Enable TLS encryption of browser traffic
- Filter URLs or domains
- Block pop-ups through extensions
- Disable or enable JavaScript
- Disable or enable the auto-fill of forms
- Disable or enable cookies, saved sign-in data
- Delete or preserve personal data

Samsung Contacts

Contacts are the lifeline of any collaborative business environment and empower mobile workers to stay connected. Enterprises need to strike a fine balance between providing employees with easy access to contacts and protecting private contact information from exploitation.

The Samsung Contacts app provides enterprises with the ability to disable or enable the following features:

- Synchronization of contact data with an MS Exchange or ActiveSync server
- Synchronization of contact data inside and outside the work profile
- Copying of contact info to a SIM card
- Accessing contact info at the end of a phone call

Advanced App Management

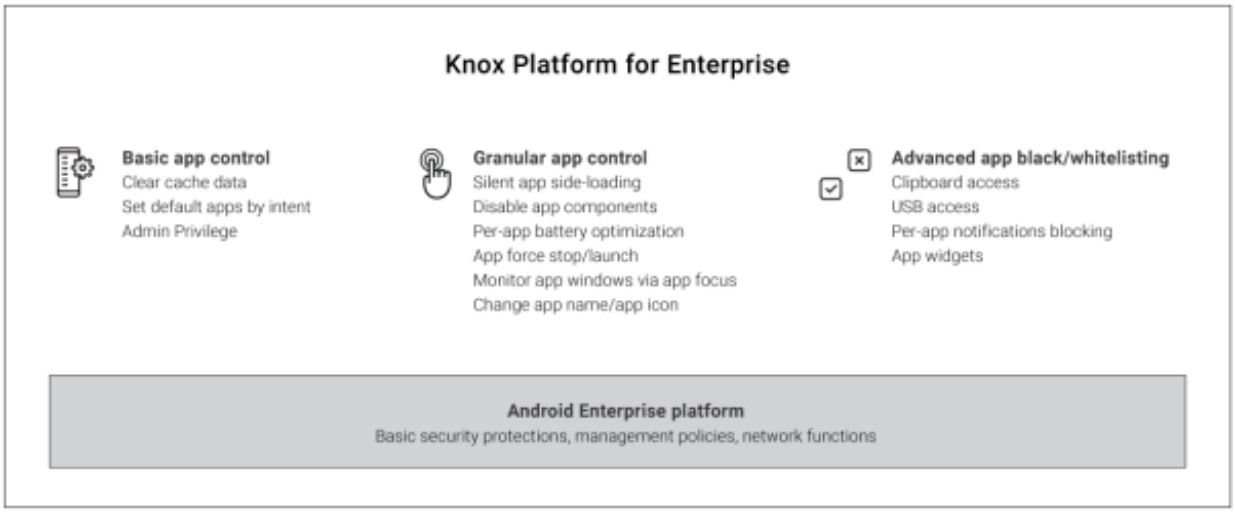
Enterprises need a strong Mobile Application Management (MAM) strategy to deploy apps effectively, manage app licenses, secure apps, optimize app usage, and handle app data safely. The Knox platform provides comprehensive app management capabilities that allow IT admins to control all aspects of apps installed on a device. These capabilities can also be extended inside the work profile to provide a safe haven for sensitive apps and data.

Enterprises use EMM solutions to centrally configure and remotely manage apps. Knox provides a full complement of management functions, providing IT admins with the ability to:

- Install, uninstall, update, enable, disable, start, stop, or wipe data for an app
- Allow or block the following:
  - apps that can be installed
  - apps that can auto-update
  - apps that can use the Clipboard
  - apps that can be started and stopped by users
  - apps that can access the USB port
  - app accounts, permissions, and notifications
- Disable or enable other apps like Google Play, Google Chrome, Voice Dialer, and YouTube
- Get info like the app code size, cache size, data size, total size, notification mode, and restrictions
- Get statistics like app launch count, component state, app focus state, CPU usage, data size, memory usage, and network stats

Unique advantages of Knox App Management

What sets the Knox platform apart from other mobile platforms are the advanced app management features not found in other solutions, providing additional advantages that enable enterprises to be fully efficient and productive.



App control

- **Clear cache data** — Remove cache memory for an individual or list of apps to help optimize space and have complete control over your data.
- **Set default apps by intent** — Set an app as the primary app for a given task. For example, ensure your solution only uses a certain Internet browser or force your SMS service to comply with your strict company policies.
- **Admin privilege** — An admin can prevent the activation of another admin's app, unless the app is part of the allowed apps.

Advanced app blocking and allowances

- **Clipboard access** — Prevent access to the native Android clipboard within an app. If an app tries to use the clipboard, the content is deleted.
- **USB access** — Prevent user permission for one or more USB devices to be used by an app.
- **Per-app notifications blocking** — Prevent status bar notifications for an app and choose to block either text, sound, or both.
- **App widgets** — Allow only approved widget packages into your Work container, and view them in launcher mode on a Samsung device.

Granular app control

- **Silent app side loading** — Silently install any app without user interaction or permission.
- **Disable app components** — Enable or disable a specific package component such as the activity, receiver, service, or provider class.
- **Battery optimization** — Allowlist apps from Google's Doze mode, app standby or power saving mode.
- **App force stop and launch** — Force stop any app including background processes and system apps.
- **App focus** — Monitor any app and receive a notification if a user leaves the window of an allowed app.
- **Change app name or app icon** — Change an app's package name and icon.

DualDAR Encryption

Protecting Data-At-Rest (DAR) on mobile devices is a major concern for security conscious enterprises. The Samsung Knox Sensitive Data Protection (SDP) already addresses this issue, by decrypting data only after user authentication, providing per-file and per-data decryption keys, offering per-app password checks, and meeting MDFPP requirements for US government and military use.

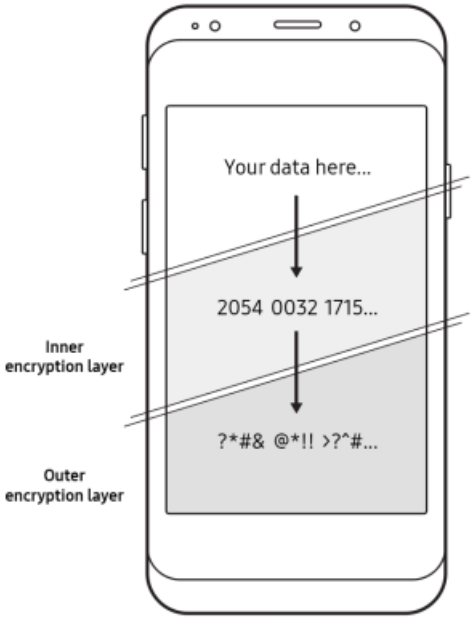
Knox DualDAR adds two separate layers of encryption, further meeting the requirements of classified deployments. Knox DualDAR secures all work profiledata on devices with two distinct levels of encryption. The solution also protects data by restricting apps from writing or saving data to the unencrypted space on the device. As the name implies, Knox DualDAR is based on two layers of data encryption. To fully understand how DualDAR works, we need to examine how the two layers of encryption within DualDAR work.

The DualDAR solution provides the following two separate layers of encryption and key generation. All data placed inside the work profileis dually encrypted by both layers. Currently, DualDAR only secures data placed inside the designated work profile.

- **Outer layer**: The outer layer of the DualDAR solution is built on top of Android's FBE and enhanced by Samsung to meet MDFPP requirements. This layer is implemented through the SoC dedicated to flash storage encryption. In this context, the SoC could be Qualcomm Integrated Crypto Engine (ICE) or Exynos Flash Memory Protector (FMP). Data encryption at this layer is AES 256 XTS and file encryption keys are encrypted using AES-GCM 256.
- **Inner layer**: The inner layer of encryption is based on a framework that allows an independent third party to install a separate cryptographic module. If no third party module is installed, an separate inner layer of encryption is secured by a FIPS 140-2 certified cryptographic module included with the Samsung Knox framework.

DualDAR is supported on the Galaxy S10, N10, S20, and subsequent flagship models, and is compatible with Android FBE.

How DualDAR encryption works



DualDAR's inner and outer security layers are independent and protect all information stored in the work profile when the device is in a powered off or unauthenticated state. Samsung Knox DualDAR leverages Android File Based Encryption (FBE) architecture.

On a FBE-enabled device, every device has the following two storage locations available to an app.

- **Credential Encrypted (CE) storage**: Default storage location and only available after a user has unlocked the device.
- **Device Encrypted (DE) storage**: Storage location available both during Direct Boot mode and after the user has unlocked the device.

From an app point of view, the DualDAR work profile functions as CE storage. The Knox framework prevents apps from writing data to non-DualDAR protected DE storage. In some cases an app is aware of both CE and DE storage, and needs to write unclassified content to DE storage. In such cases, IT admins can allow that app to write to DE storage. This strict allowlist process ensures that no app can write sensitive or classified content to DE storage without explicit IT admin approval.

When the work container is configured for DualDAR, the secured data is available as follows.

1. On a device that supports and is configured for DualDAR, access to app data inside the container is only available when the container is unlocked, that is when the user is actively using the container.
2. When the container—or device as a whole—is locked, the container encryption keys are evicted from memory.
3. In a data lock state, the Samsung device remains powered on but the user is locked out of both the work container and device. All sensitive data is protected in Credential Encrypted (CE) storage within the work profile. CE storage is not available until the user provides both their device and work profilecredentials.

Unique advantages of Knox DualDAR

DualDAR encryption has the following significant advantages over traditional single layer encryption methods.

- **Mitigate risks of implementation flaws**: DualDAR reduces the likelihood of unauthorized data access by mitigating the risks that arise from vulnerabilities in a single encryption layer. While one of the many methods available for unauthorized data access may crack through a single layer of encryption, the chances are very low that such vulnerabilities are available on both layers of encryption.
- **Mitigate risks of password configuration flaws**: Both layers of encryption on a DualDAR configured device use separate and distinct authentication methods to allow access. This separation of authentication methods reduces the likelihood that a single misplaced or misconfigured password is exploited on both layers of data encryption at the same time. Two layers of encryption and two methods of authentication ensure that encrypted data remains protected even in the event of breach on one layer.
- **Provide access using strict security evaluation criteria**: DualDAR meets the standards laid out in the FIPS 140 certification requirements. Both the inner and outer layers use FIPS 140 certified cryptographic modules. GCM is used to encrypt the key while data is encrypted using XTS or CBC.
- **Ease of deployment**: DualDAR leverages the in-built Android FBE framework and builds additional layers of security on top of this framework. This solution is available on devices that use a work container in PO mode as well as fully managed devices that include a PO mode. For more information on configuring this solution for your supported device, see the DualDAR architecture page.
- **Customize the second layer of encryption**: DualDAR allows IT admins to implement third party encryption solutions at the inner layer of encryption. This freedom of implementation means IT admins can use and configure any third party cryptographic modules, including solutions that meet FIPS 140 certification criteria.
- **Flexible deployment methods**: IT admins can implement and configure DualDAR on all kinds of devices, including BYOD and company-issued devices. Whether the device uses a work container in PO mode or is a fully managed device that includes a PO mode, DualDAR is compatible with both models. This flexibility means IT admins can use this superior data security solution on a wide variety of devices within their enterprise.

For more information on DualDAR and its unique design, see the DualDAR architecture page.

Appendix

Knox Certifications

The Knox Platform has successfully met the rigorous security requirements set by governments and major enterprises around the world, providing organizations with a trusted mobile security solution. The certifications acquired by the Knox Platform allow its mobile devices to be deployed in highly sensitive industries such as the military.

Samsung Knox continuously adds to its growing list of certifications for industries and agencies around the world. For more information on certifications and to review the latest list, see Knox certifications.

Unlike other mobile platforms, the Knox Platform is certified to have met the following countries' security requirements.

	USA	UK		Germany		France	Spain	Finland	Netherlands
	MDFPP	EUD	CPA	Endorsement	VS-NfD	CSPN	CCN	TRAFICOM	NCSA
Samsung	✓	✓	✓	✓	✓ pre-approved	✓	✓	✓	✓

Methodology

Certifications are granted by independent boards that use a specific set of hardware and software, for example, one certificate might be granted for the Galaxy S8 running Knox 3.0. These certifications must be renewed with each device and OS iteration to remain valid. Samsung remains dedicated to maintaining industry compliance and continues to grow and maintain our numerous certifications.

Security principles

Many of these certifications have a set of security principals that a device must uphold. Here are some examples of the security principles validated during certification.

- **Data-in-transit protection** — Does the device sufficiently protect data-in-transit?
  Yes - achieved with Advanced VPNs, Certificate Management, and Common Criteria mode.
- **Data-at-rest protection** — Does the device provide data that is encrypted by default? Is that data encrypted when the device is locked?
  Yes - achieved with Android Enterprise work profile, Sensitive Data Protection.
- **Authentication** — Does the device provide secure authentication methods?
  Yes - achieved with the Knox Vault, Client Certificate Manager, and authentication methods that include biometrics.
- **Secure boot** — Does the device have mechanisms to ensure the boot up process is free from modification?
  Yes - achieved with a hardware-backed Root of Trust and Trusted Boot.
- **Platform integrity** — Does the device ensure the integrity of the platform? Can it query the integrity of the platform?
  Yes - achieved with the Real-Time Kernel Protection, Device Health Attestation, and Secure lockdown on tampering.
- **App sandboxing** — Does the device provide app sandboxing?
  Yes - achieved with the Android Enterprise work profile, Separated Apps, and SEAMS.
- **App blocking** — Does the device allow apps to be added to an allowlist or a blocklist?
  Yes - achieved with Advanced App Management.
- **Security policy enforcement** — Does the device allow the enforcement of security policies? Can they take precedence over user activities?
  Yes - achieved with a full complement of EMM policies built on a Knox SDK offering over 1500 APIs.
- **External interface protection** — Does the device allow control over external peripherals such as Bluetooth, USB, and NFC?
  Yes - achieved with Granular Device Management.
- **Device update policy** — Can the device provide deliberate OS updates that match an organizations evolving needs?
  Yes - achieved with Device Software Update Management.
- **Event collection for enterprise analysis** — Does the device allow the collection, and subsequent audit, of business data?
  Yes - achieved with Audit Logs.
- **Incident response** — Can the device be managed if it is lost, stolen or damaged?
  Yes - achieved with custom lockscreen info, remote data wipe, auto-wipe after a number of unsuccessful log-in attempts, and remote factory reset.

What does this mean to you? You can rest easy knowing that Samsung Knox's holistic security platform is compliant with the highest security requirements and standards. Samsung Knox devices are built from the ground up to secure your organization's apps and data, providing robust integration with existing IT infrastructure and ensuring there are no functional or security gaps in your deployment.

Common Criteria Mode

Knox supports advanced device configurations tailored to the defense industry. A single Knox setting can apply many of the settings needed to put the device into a compliant state. This setting, called Common Criteria Mode or CC Mode, helps simplify the task of correctly configuring a device for deployments that must meet defense-grade security requirements. The Common Criteria for Information Technology Security Evaluation, commonly referred to as Common Criteria, is an internationally-recognized standard for defining security objectives of information technology products and for evaluating vendor compliance with these objectives. A number of Governments use Common Criteria as the basis for their own certification schemes.

Select Samsung Galaxy devices with the Knox Platform embedded received Common Criteria (CC) certification. The current CC certification targets the new Mobile Device Fundamentals Protection Profile (MDFPP) of the National Information Assurance Partnership (NIAP), which addresses the security requirements of mobile devices for use in enterprise. Samsung Knox is approved by the United States Government as the first NIAP-validated consumer mobile devices to handle the full range of classified information.

An IT admin can enable the device to be placed into the Common Criteria configuration. When enabled, the device:

- Blocks bootloader download mode, the manual method for software updates
- Mandates additional key zeroization on key deletion
- Prevents non-authenticated Bluetooth connections
- Requires that FOTA updates have a 2048-bit RSA-PSS signature
- Uses many other security settings

While other optional configuration steps are still recommended on top of Common Criteria Mode, the value is clear: simplifying the correct configuration of endpoints for high-security deployments saves time and prevents mistakes that can lead to misconfigurations and added security risks.

More information

Refer to the following Knowledge Base Articles for details about:

- Common Criteria Mode, supported Samsung devices, and test APKs
- Common Criteria evaluation, by Android version