Beyond basic Android

Security with Samsung KNOX

Contents

Google and Samsung are committed to mobile enterprise security, each bringing its own considerable expertise to the challenge of protecting devices and data from ever-growing threats and attacks. Backed by years of research, Samsung KNOX offers unsurpassed levels of mobile security that make Samsung devices truly enterprise-ready right out of the box.

Google Android™ Lollipop and Android for Work: A starting foundation for mobile security

Coinciding with the release of Android Lollipop, Android for Work improves the basic security of the Android platform with new security features including:

- Verified Boot of the operating system during the boot process.
- Limited VPN functionality for secure connections to enterprise networks.
- Google Safe Browsing technology.

Google relies on device manufacturers such as Samsung to expand basic security and provide integrated security solutions for enterprises addressing issues, including:

- Regulatory compliance
- Liability
- Risk tolerance

As the leader in security and enterprise readiness, Samsung KNOX delivers the most comprehensive solution of all Android device manufacturers. KNOX mobile security provides unmatched protection against mobile threats from the moment you turn on the device.

Enterprise-ready security built in with Samsung KNOX

KNOX is the defense-grade mobile security platform built into all of Samsung's newest devices.

Cyber attacks exploit weaknesses in device software and architecture. KNOX minimizes the attack surface with the following:

- Security checks starting from the hardware level at power up.
- TrustZone-based Integrity Measurement Architecture (TIMA) Real-time Kernel Protection.
- TIMA Periodic Kernel Measurement.
- Reporting (Attestation) of tampering with the OS, apps, or device architecture.

KNOX is always on, always vigilant

KNOX establishes its first line of defense with Secure Boot and Trusted Boot architecture, coupled with chip-level security. These hardware, firmware, and software checks are followed by multiple checks to ensure that each part of the operating system hasn't been tampered with before corporate applications can run. If any of those checks fail, KNOX reports the threat to the Mobile Device Management (MDM) system.

Secure by design

KNOX fully leverages the hardware Trusted Execution Environment (TEE) of ARM® TrustZone® capabilities found in Samsung's flagship mobile devices. KNOX provides strong guarantees for the protection of enterprise data by building a hardware-rooted trusted environment. A trusted environment ensures that enterprise-critical operations, such as decryption of enterprise data, can occur only when the device is proven to be in an allowed state. For many pieces of device software, such as the kernel and TrustZone apps, the allowed state is represented by the cryptographic signature of each piece of software. A trusted environment is hardware-rooted if both the cryptographic keys and code used to compute these signatures are tied back to unmodifiable values stored in hardware.

Controlling the manufacturing process

Samsung manufactures and configures all its devices in its own factories, providing Samsung with complete control over the devices and software before they leave the factory. In addition to provisioning the software on the devices, Samsung provisions each device with the cryptographic keys, such as the Device-Unique Hardware Key (DUHK) and the Samsung Secure Boot Key (SSBK). The Secure Boot process uses the SSBK to verify whether each boot component it loads is approved. Data encrypted by the DUHK becomes bound to the device, because it cannot be decrypted on any other device.

Other device manufacturers that outsource hardware cannot guarantee the same end-to-end control of these critical security elements. The additional steps Samsung takes to protect the manufacturing process surpass what other device manufacturers and OEMs can provide to their customers.

Figure 1. Samsung KNOX makes Android secure for enterprises

Warranty Fuse

The KNOX warranty bit is a one-time programmable fuse that indicates whether the device has ever been booted into an unapproved state. If the Trusted Boot process detects that non-approved components are used, or if certain critical security features such as SELinux are disabled, it sets the fuse. Once the fuse is blown, the device can never run Samsung KNOX; access to the DUHK and DRK in the TrustZone Secure World is revoked, and the enterprise's data on the device cannot be recovered.

Boot-time defenses

One of the most fundamental requirements of mobile security is to ensure the authenticity and integrity of the software allowed to run on the device. This includes the operating system as well as all the modules that the OEM is required to provide on the device. KNOX employs Secure Boot and its own Trusted Boot layers to verify the authenticity and integrity of bootloader modules and the Android kernel during boot. It does this by verifying chunks of code against previously-generated cryptographic signatures stored in secure memory of the TEE.

Load-time defenses

Today's smartphones and tablets have a large amount of preloaded system software beyond the operating system kernel. The size of this system software makes it impractical to verify its integrity and authenticity at boot time, because it would introduce unacceptable start-up delay for the user.

KNOX uses an enhanced version of the stock implementation of DM-Verity included with Android Lollipop to ensure the integrity of system software not covered by the boot time checks. Samsung's implementation of DM-Verity differs from standard Lollipop in several important ways:

1. Modified to accommodate the real-world need for devices to accept firmware over-the-air (FOTA) software updates.

2. File-based checking instead of block-based to support carrier-specific and region-specific software builds.

3. Optional for non-enterprise consumer users of devices.

With Secure Boot, Trusted Boot, and DM-Verity, enterprises can be confident that the all device software is authentic and uncompromised.

Run-time defenses

More sophisticated attacks can compromise the system or intercept data at run time. These are the most difficult attacks to prevent, but KNOX gives users and enterprises confidence that malicious apps or code can't run on KNOX-protected devices. The combination of Periodic Kernel Measurement, Real-time Kernel Protection, and device Attestation protects devices beyond the basic levels provided by Android for Work through other OEMs. KNOX gives enterprise IT Admins the tools to track down and prevent attacks while they can be easily contained.

Periodic Kernel Measurement (PKM)

TIMA PKM performs continuous periodic monitoring of the kernel to detect if legitimate kernel code and data have been modified by malicious software. In addition, TIMA also monitors key Security Enhancements (SE) for Android data structures in operating-system kernel memory to detect malicious attacks that corrupt them and potentially disable SE for Android.

Real-time Kernel Protection (RKP)

TIMA RKP performs ongoing, real-time monitoring of the operating system from within TrustZone to prevent kernel tampering. RKP protects against malicious modifications and injections to kernel code, including those that coerce the kernel into corrupting its own data. RKP intercepts and inspects critical kernel events in the TrustZone, and if an event is determined to have unauthorized impact on the integrity of the OS kernel, RKP either stops the event or logs an attestation record that tampering is suspected.

Attestation

Attestation reads the data collected by Trusted Boot and fuse values and combines them to produce an Attestation verdict that can be requested on-demand by the enterprise's Mobile Device Management (MDM) system (typically before creating the KNOX Workspace). This verdict, a coarse indication that tampering is suspected, is returned to the requesting MDM. The Attestation verdict is cryptographically signed to ensure its integrity and authenticity.

RKP and PKM are essential to protect against future threats to Android and devices that haven't yet been uncovered or predicted. Flagging activities that we know are suspicious is the first step in identifying and preventing security breaches. These real-time checks, together with Attestation, give enterprises confidence that devices are continuously monitored for breaches, and that IT is alerted if corporate devices have been compromised.

Update-time defenses

Rollback Prevention blocks the device from loading an approved but old version of boot components during Trusted Boot. Old versions of software may contain known vulnerabilities that attackers can exploit. Rollback prevention checks the version of the bootloader and kernel during both Trusted Boot and updates, and blocks these processes from continuing if versions are unacceptably old. The lowest acceptable version of the bootloader is stored in secure hardware fuses at the time of manufacture, and the lowest acceptable version of the kernel is stored in the bootloader itself.

Table 1 - Summary of KNOX Defense Mechanisms

Feature	Description
Hardware	
Samsung Secure Boot Key	Verifies that all firmware is from Samsung before allowing the device to boot.
Device Root Key	Provides a unique key per device that is used to perform cryptographic operations (authentication and encryption) associated with that specific device.
Warranty Bit	Creates a one-time, writeable hardware "fuse" used to flag devices whose system software has been replaced, in part or in full, either intentionally or maliciously.
Rollback Prevention Fuses	Set at manufacturing time in the Samsung factory to prevent old firmware versions from overwriting newer ones.
Bootloader	
Secure Boot	Ensures the integrity of each component of the boot software until just before the Android kernel is launched. (Uses the Samsung Secure Boot Key). If anything else tries to run outside of the valid, trusted sequence, the boot process terminates.
Trusted Boot	Builds upon Secure Boot to ensure the end-to-end integrity and consistency of boot software—including the kernel—for the entire boot process. Any evidence of tampering is permanently logged.
Rollback Prevention	Uses rollback prevention fuses to ensure that an old (but valid) firmware image cannot overwrite more recent images.
TrustZone	
Periodic Kernel Measurement	Performs continuous periodic monitoring of the kernel to detect if kernel code or data has been modified by malicious software.
Real-time Kernel Protection	Maintains runtime integrity by monitoring critical events that occur in the Android kernel and enforces protection of the kernel code so that it cannot be moved, changed, or amended.
Attestation	Allows a device to attest to a remote server, such an MDM server, that it has loaded authorized images during boot time.
TIMA KeyStore	Provides applications with services for generating and maintaining cryptographic keys. The keys are further encrypted with the device-unique hardware key that can only be decrypted by the hardware inside TrustZone.
Client Certificate Management	Enables storage and retrieval of digital certificates for encryption, decryption, signing, verification, and other operations.
Fingerprint Authentication	Requires apps to use fingerprints as a primary or two-factor authentication with checks performed in the TrustZone.

Application-level security mechanisms

Once KNOX verifies device integrity, it begins testing application and data security for threats. Organizations must trust that data stored on devices cannot be breached or shared inappropriately, and that applications accessing company information can be used only for corporate purposes. KNOX also protects against data attacks with sophisticated, automatic VPN capabilities.

TIMA KeyStore

Samsung KNOX builds and improves upon the basic Android KeyStore foundation to provide enterprise class mobile application and data security with a hardware-based TIMA KeyStore. KNOX uses a TrustZone-based TIMA KeyStore for cryptographic key storage. Keys stored in the TIMA KeyStore can be accessed only if the measurements collected by Trusted Boot match the expected golden measurement values, and the warranty fuse has not been set. If the device fails these critical integrity checks, then applications cannot access enterprise data. The TIMA KeyStore protects sensitive data, including keys, by hardware-derived keys in TrustZone. Hardware-bound security ensures protected data can only be decrypted on the same device by TIMA KeyStore.

Automatic and per-app VPN settings

While Android for Work allows for some granular control for app-by-app VPN settings, KNOX extends this capability to a broader range of supported VPNS, using different VPNs for different apps, and even separating out the data used by corporate applications for easier accounting for BYOD and Corporately Owned, Personally Enabled (COPE) devices. Recognizing the increasing complexity of enterprise IT, Samsung has built sophisticated VPN support into KNOX to make integrating KNOX into IT environments easier to manage.

Table 2 - Application-level security features

Feature	Description
TIMA KeyStore	Improves upon the standard Android KeyStore by denying access to its contents when Trusted Boot or Warranty Bit reports that the device has potentially been compromised. Stored keys cannot be cloned for use on other devices.
TIMA Client Certificate Management (CCM)	Enables cryptographic keys to be sequestered in a secure area of the device, so that private key information is never exposed to the Android operating system.
Workspace	Offers a defense-grade, dual-persona container product designed to separate, isolate, encrypt, and protect work data from attackers. This work/play environment ensures work data and personal data are separated and that only the work container can be managed by the enterprise. Personal information such as photos and messages are not managed or controlled by the IT department. Once activated, the KNOX Workspace product is tightly integrated into the KNOX platform.
Sensitive Data Protection	Builds upon Workspace encryption, defining a sensitive class of data, which the device cannot decrypt without user intervention. TIMA KeyStore is used to manage cryptographic keys.
VPN Framework	Adds FIPS 140-2 certified cryptographic algorithms, or the option to use CCM to manage cryptographic keys, to establish secure VPN connections to corporate network resources. Integrates with Workspace to assure that applications route network traffic through approve channels.
SSO Framework	Enhances authentication of Workspace apps by providing a common framework. Backed by TIMA KeyStore and CCM.
On-Disk Encryption	Uses a derivative of the Device Root Key to strengthen Android's On-Disk Encryption feature, ensuring that copying raw data from one device to another is not possible.
Hardware Attestation	Uses a derivative of the Device Root Key, plus measurements collected from Trusted Boot, Warranty Bit, and RKP, to securely attest the state of the device to a remote server.
No Mandated Cloud Connection	Eliminates the requirement to connect an employee's device to a third-party cloud server (Google Cloud). KNOX license server can be deployed as an on-premises instance to avoid any cloud connection.

Independent security certifications

Samsung KNOX has been awarded multiple, internationally recognized security certifications from government authorities around the world. These certifications help set Samsung apart from other OEMs and help validate the security claims that Samsung makes for its devices.

Table 3 - Independent Security Certifications

Country	Certification	Issued by
USA/Canada	Federal Information Processing Standard 140-2 Certification – Level 1 certification for both data-at-rest (DAR) and data-in-transit.	National Institute of Standards and Technology (NIST)
USA	Security Technical Implementation Guides (STIGs), DISA Approved Product List	Defense Information Systems Agency (DISA)
USA	Common Criteria Certification for Mobile Device Fundamental Protection Profile (MDFPP)	National Information Assurance Partnership (NIAP)
USA	US Department of Defense Approved Products List	National Information Assurance Partnership (NIAP)
UK	End User Devices (EUD) Security Guidance	Communications and Electronics Security Group (CESG)
Finland	Finnish National Security Auditing Criteria (KATAKRI II)	Finnish Communications Regulatory Authority (FICORA)
Australia	Protection Profile for Mobile Device Fundamentals	Australian Signals Directorate (ASD)

Advanced security that fits your existing IT infrastructure

Enterprises large and small have diverse device management needs. KNOX provides enterprises with a comprehensive set of tools for configuring the secure KNOX Workspace to their needs, including more than 1500 MDM APIs.

KNOX provides tools for rapid enterprise deployment, such as per-application VPN controls, a smartcard framework, Single Sign-on (SSO) integration with Microsoft Active Directory, KNOX Mobile Enrollment (for bulk loading devices into an MDM) and Enterprise Billing for tracking employee data usage on BYOD and COPE devices.

Unlike Android for Work, KNOX allows access to a broader range of approved app stores in addition to Google Play. If you have your own in-house apps, KNOX allows enterprise apps to be securely side-loaded onto devices. Android for Work requires private, proprietary apps to be uploaded to private Google Play accounts. KNOX allows secure signing and loading of apps into your Workspace without accidentally risking exposure of private apps to the public. Additional features only available with Samsung KNOX are in the table on the following page.

Table 4 - Defense-grade security features

Enterprise Mobility Infrastructure	
Identity/Email Registration	KNOX allows you to avoid registering an email address with Google to manage user identity on a device.
Exchange/ActiveSync	KNOX supports use of Exchange/ActiveSync for messaging.
LDAP Support	KNOX has explicit built-in support for LDAP account configuration and credentials. KNOX also supports Microsoft Active Directory.
VPN	KNOX provides tailored support for a growing list of industry-leading VPN clients from Cisco, Juniper, F5, OpenVPN, StrongSwan and more. The VPN framework also allows easy adoption of additional VPN solutions.
Third-party Container Support	KNOX enables third-party container solutions to benefit from various KNOX security features.
Firewall Configuration	KNOX provides APIs to configure firewall policies.
User Experience	
Multiple Simultaneous Containers	KNOX supports multiple simultaneous containers/profiles, while Android alone can only accommodate one profile.
Kiosk and Container-Only Mode	KNOX kiosk and container-only mode allow clear work/personal boundaries.
Container UX	KNOX allows the user or enterprise to choose between three different user experiences, depending on the needs of the individual or organization: Classic (separate, isolated UX), Folder (pop-up UX), or Full Screen (continuous feed).
Mobile Device Management	
Onboarding/Enrollment	KNOX never requires devices to connect to Samsung servers to authenticate or register an identity for onboarding or enrollment.
Device Control	KNOX includes a fully integrated set of management tools that offers deep device control of security, usability, hardware, and application policies. KNOX also offers easy integration with third-party Mobile Device Management solutions.
My KNOX	Individual mobile professionals can use Samsung My KNOX to keep work and personal data separate.
Application Management	KNOX supports Google Play, Samsung App Store, KNOX marketplace, MDM solutions, and manual side-loading to deploy applications. All transactions are 100% anonymous in an enterprise-managed model. Android requires that you use Google Play for every app management transaction and prohibits side-loading.
Telephony	KNOX enables policies to block incoming/outgoing voice and SMS.
Password Policy	KNOX extends Android password policies with more granular control over precise requirements for character sets, repeated characters, refresh periods, and re-use.
User Privacy	KNOX Workspace limits the employer's visibility into and control of the Workspace, putting the non-Workspace data and apps beyond the reach of the employer.

Samsung has worked with MDM, VPN, and application vendors for nearly three years to ensure that KNOX can be deployed in the widest possible number of circumstances.

Comprehensive enterprise mobile security and productivity

When implementing your enterprise mobile strategy, centralizing on Android devices alone is not enough. While the security features in Android for Work have improved Android's position with competitors on other platforms, most enterprises find that their security and compliance requirements are not met.

Samsung KNOX augments Android for Work's security features to produce a tightly integrated and holistic security architecture. By enabling all of the security, compliance, and control features enterprises require, organizations can use Samsung KNOX to enable employee productivity while also protecting corporate assets.

Appendix: Feature comparison of Samsung KNOX and Android for Work

Capability	Samsung KNOX	Android for Work
Silent Install	Using the Samsung KNOX Workspace Mobile Device Management (MDM) APIs, IT admins can install and enable applications automatically. The simplified enrollment process supports the fully automated creation of an enterprise-grade Workspace and provisioning of apps and policies. **KNOX adds:** Samsung KNOX Mobile Enrollment allows IT Admins to stage and enroll hundreds or thousands of employees automatically by configuring device information in the cloud. Samsung also provides a web tool and an application to scan smartphone package bar codes (the device IMEI).	Using the EMM console, IT admins can install, remove, and update apps inside Android for Work.
Application Configuration	KNOX provides the following capabilities to IT admins: • Install and uninstall applications. • Restrict installation and uninstallation of applications. • Disable and enable applications. • Query the current state of an application. • Control application behavior. • Control notifications of applications. • Configure the email client. • Configure the SSL VPN Client for Cisco, F5, and Juniper.	Using the EMM console, IT admins can configure the settings for a particular application. When Android for Work is configured, app settings are pushed to the device.
Secure App Installation from Google Play	With more than 1500 MDM APIs, KNOX gives IT admins control over which apps can be run inside the Workspace, thus eliminating the problem of sideloading of untrusted apps. Additionally, administrators can deploy any app from the Google Play store to the Workspace, or allow users to install the Google Play app inside the Workspace. IT admin can also install applications from a private app store.	Google has introduced a new set of Google Play APIs for EMM providers to enable app management and distribution and control app deployment in Android for Work.
Separate Container for Work Apps	The KNOX Workspace provides an isolated environment and UI for enterprise use, consisting of a separate home screen, launcher, enterprise apps, and widgets. Data owned by apps in the KNOX Workspace is protected by extensive Data At Rest (DAR) protections. IT admins can use KNOX's extensive set of Workspace configuration APIs to provision and configure the Workspace and its DAR protections.	Android for Work provides a secure profile, or container, to Android devices running Android 4.0 and higher.
Data Loss Prevention	KNOX MDM policies can regulate sharing of information between the Workspace and personal apps. This includes sharing of calendar, contacts and notifications. Copy/paste clipboard data is blocked from the Workspace environment to the personal environment, and vice versa. **KNOX adds:** **Sensitive Data Protection.** Any sensitive data received when the Workspace is locked will still be protected by Sensitive Data Protection (SDP). This works by using a public key algorithm in which the private part of the key is maintained in an encrypted partition, and the public part is used to encrypt the new sensitive data. Once the Workspace is unlocked, the data is decrypted with the private key, and re-encrypted using the usual symmetric key, which is guarded by the Container Master Key (CMK). Currently, email subjects, bodies and attachments are marked sensitive. Additionally, the SDP Chamber provides a directory in which all files are automatically marked as sensitive and are protected by SDP.	EMM governance policies manage a user's ability to share into and outside of Android for Work. This includes the ability to block copy/paste or block screen capture for apps inside the managed profile. (Note that copy/paste can be disallowed from the managed profile to the personal profile, but not vice versa.)

Capability	Samsung KNOX	Android for Work
Container VPN	KNOX enables additional modes of granular VPN capabilities both for the Workspace and individual apps. The MDM-configurable KNOX VPN supports multiple concurrent VPN connections allowing for IPSec or SSL VPNs with configurable auto-reconnect and VPN tunnel chaining. The KNOX VPN subsystem also supports other forms of packet processing, including split billing and network access control. **KNOX adds:** Enterprise Billing provides enterprises a mechanism to separate enterprise data usage from personal data usage. This enables enterprises to compensate employees for costs related to work, particularly in BYOD cases, or to pay only work-related data in COPE cases. VPN features of KNOX include: • Administrator-configured System VPN. • Administrator-configured Per-App VPN. • Administrator-configured Workspace VPN. • Multiple concurrent VPN connections. • IPsec and SSL VPN support. • Administrator-configured FIPS and non-FIPS VPN mode. • Common Access Card (CAC)-based authentication. • Always on VPN connections with auto-reconnect. • VPN tunnel chaining.	Android for Work enables VPN capabilities within the managed profile.
Selective Wipe	IT admins can wipe internal and external SD cards and application data. The entire container can be locked when compromised and can be deleted with all its data.	Android for Work enables IT administrators to retire lost or stolen devices and remotely wipe all work data while leaving personal content intact on the device.
Protection Against Malicious App Downloads	The KNOX Workspace isolates enterprise apps and data from personal user apps. Untrustworthy personal user apps outside the Workspace cannot affect the Workspace. **KNOX adds:** Real-time Kernel Protection (RKP) provides three important security benefits: • Prevents running unauthorized privileged code (i.e., code that has the kernel privilege) on the system. • Prevents kernel data from being directly accessed by user processes. This includes preventing double mapping of physical memory that contains critical kernel data into userspace virtual memory. This is an important step to prevent kernel exploits that map kernel data regions into malicious processes where they could be modified by an attacker. • Monitors some critical kernel data structures to verify that they are not exploited by attacks. KNOX Warranty Fuse: The KNOX warranty bit is a one-time programmable fuse that signifies whether the device has ever been booted into an unapproved state. The warranty bit prevents a compromised device from running Samsung KNOX, accessing the Device-Unique Hardware Key (DUHK) and Device Root Key (DRK) in the TrustZone, and accessing any enterprise data. TIMA Attestation allows a device to attest facts about its state to a remote server, such as an MDM server. The attestation message contains measurements about the state of the device. This is evaluated by the MDM to prove the device is in a trusted state, or if there is evidence of tampering.	Android for Work protects business apps and data from issues arising from the user's personal activity outside the profile, such as sideloading web apps.

SAMSUNG Kn⬛x

About Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd. is a global leader in technology, opening new possibilities for people everywhere. Through relentless innovation and discovery, we are transforming the worlds of TVs, smartphones, tablets, PCs, cameras, home appliances, printers, LTE systems, medical devices, semiconductors, and LED solutions. We employ 286,000 people across 80 countries with annual sales of US $216.7 billion. To discover more, please visit www.samsung.com.

For more information

For more information about Samsung Enterprise Mobility and Samsung KNOX,
visit: www.samsung.com/enterprise and www.samsung.com/knox

SAMSUNG
BUSINESS