Whitepaper:

Android for Work

on Samsung KNOX™ devices

March 2016
Samsung Research America
Samsung Electronics Co., Ltd.

SAMSUNG

Executive Summary

Android for Work on a Samsung KNOX device

Android for Work Managed Profiles, introduced in 2014, is an enterprise program to provide separation of work apps and data from personal apps and data for enterprises using Bring Your Own Device (BYOD) or Corporate-Owned Personally Enabled (COPE) devices. Business data in Managed Profiles allows IT Admins to apply policies to prevent data leakage, prevent installation of apps from unknown sources, and apply app policies. For more information, see the following link: https://www.android.com/work/

Samsung KNOX, introduced in 2013, is Samsung's defense-grade mobile security platform built into our newest devices. Just turn on the device, and you're protected.

The platform security of KNOX is now available for Android for Work, making Managed Profiles secure for enterprises that have strict security requirements such as financial industries, government agencies, and healthcare organizations.

The KNOX platform offers:

- Boot-time protection with Trusted Boot
- The KNOX Warranty Bit that does not allow Android for Work to run if the device is compromised
- The TIMA KeyStore that does not allow access to cryptographic keys if the device is compromised, and TIMA Client Certificate Management (CCM) that ensures keys are never exposed to the Android operating system
- Real-time Kernel Protection (RKP) completely prevents running unauthorized code on the system
- TIMA Attestation allows IT Admins to collect measurements from Trusted Boot to ensure a device is in a trusted state

In addition to the KNOX platform, Samsung explicitly added three default features available for Android for Work including:

- Sensitive Data Protection (SDP) is enabled by default for apps inside Managed Profiles. There is no license requirement, but the SDP Application Program Interface (APIs) must be integrated to use this feature.
- The TIMA KeyStore is used by default
- The integrity of the device must be in an approved state or Android for Work cannot be used

For detailed information on KNOX, see the whitepaper *Samsung KNOX Security Solution* on the KNOX website: https://www.samsungknox.com/en/support/knox-premium/white-papers

The icon legend below, used throughout this whitepaper, identifies security features in other Android OEMs, KNOX platform security, and how Android for Work benefits from KNOX on a Samsung device.

Icon Legend

Other
Android OEMS

Samsung
KNOX Platform

Benefits for Android for Work
on a Samsung device

SAMSUNG

Contents

Android for Work on Samsung devices

This whitepaper explains how Samsung KNOX™ provides platform security to Android for Work on Samsung devices, and is intended for audiences with a technical knowledge of KNOX. For detailed information about KNOX, see the whitepaper *Samsung KNOX Security Solution* on the KNOX website: https://www.samsungknox.com/en/support/knox-premium/white-papers

Android for Work Managed Profiles, used by enterprises to manage work data and applications on Android devices, allows IT Admins to control the work profiles which are separated from personal apps and data. 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, ordering from unknown websites, and other potentially insecure activity.

On a Samsung device, Android for Work benefits from the security platform of Samsung KNOX. All Samsung flagship devices are secured by KNOX out-of-the-box. The features described in this whitepaper are now available on the Samsung Galaxy S7.

Samsung KNOX aims to be the most comprehensively secure and manageable mobile device solution for enterprises large and small. Based on the Android OS, Samsung KNOX is designed around the philosophy that the foundations of device security should be rooted in fixed hardware mechanisms. KNOX bases this foundation on the principles of trusted computing, a set of methods for making devices that can prove to enterprises they are running the correct security software, and can raise alerts in the event that tampering is detected.

Figure 1 – KNOX Principles of Trusted Computing

Enterprises such as financial institutions, government agencies and healthcare can benefit by using Android for Work on a Samsung device. The platform security of Samsung KNOX integrates with Android for Work providing the hallmark of KNOX security—root of trust.

Andrew Regenscheid of the National Institute of Standards and Technology's (NIST) Computer Security Division and Cryptographic Technology Group outlined the following requirements in *Roots of Trust in Mobile Devices*:

- Boot firmware protections
- Secure measurement of firmware
- Secure storage
- Device authentication
- Application and data isolation[1]

Regenscheid also states, "Organizations need assurance that devices comply with their security practices. [The] current practice is to configure devices and distribute them to users. Strong roots of trust can transform the industry [by shifting] the emphasis from **configuring** compliance to **measuring** compliance."[2]

Android for Work on Samsung KNOX devices meets these stringent requirements. Samsung KNOX devices integrate with Android for Work and provide the following platform security measures:

- Trusted Boot
- DM-Verity
- KNOX Warranty Bit
- Real-time Kernel Protection (RKP)
- TIMA Attestation
- Trusted-Boot-based KeyStore (TIMA KeyStore)
- Trusted-Boot-based Client Certificate Management (CCM)
- Sensitive Data Protection (SDP)

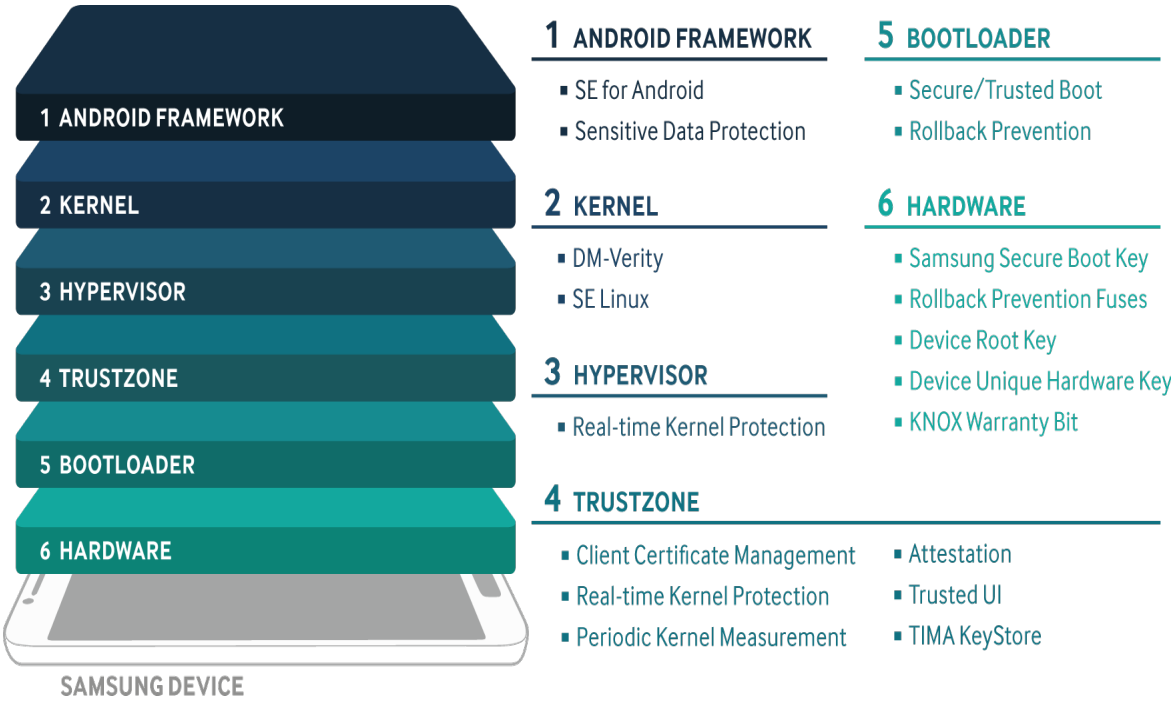

Figure 2 – Samsung KNOX Platform Security

The following pages explain the platform security extended to Android for Work on a Samsung KNOX device.

Boot-time protection

The Samsung KNOX platform provides security modules that are always enabled and protecting Samsung devices.

Trusted Boot

Samsung KNOX adopts Trusted Boot in addition to Secure Boot. In the Trusted Boot process, each software component in the chain measures and securely stores the cryptographic hash of the next component in TrustZone Secure World memory before loading it. Storing these measurements allows a third-party to identify the exact versions of software loaded on the device through the process of attestation. For example, this can be used to verify that only the latest patched versions of software are run, complementing the Rollback Prevention feature that ensures patched software is not downgraded to a vulnerable version.

If signature verification fails, KNOX either records the tampering by blowing a one-time fuse, called the KNOX Warranty Bit, or by preventing further booting, depending on the configuration.

Access to Android for Work's Managed Profiles depends on the integrity of the device. If the integrity check fails, Android for Work creation is not allowed. If an Android for Work profile already exists, the device is not allowed to boot.

Android for Work on other OEMs protect business apps and data from issues arising from the user's personal activity outside the profile, such as sideloading web apps, ordering from unknown websites and other potentially insecure activity.

Load-time protection

DM-Verity

To prevent unauthorized modifications to the system partition, KNOX integrates a customized implementation of DM-Verity, a Linux/Android kernel module that performs integrity checks on all data blocks contained in a block device (such as a partition). In stock Android, DM-Verity uses a hash tree to perform integrity checks of individual data blocks. The root of the hash tree is signed by an RSA key. Whenever a data block is read into memory, DM-Verity computes the hash of the block, and then uses it, along with the other hashes on the path to the root to compute the root hash. If this computed root hash matches the signed version, the block is considered good. Otherwise, unauthorized modification of the block is detected, and the access to the data block is restricted.

KNOX's implementation of DM-Verity differs from stock Android in supporting file-based firmware over-the-air (FOTA) software updates. This approach is easier to support with the existing infrastructure than the stock block-based approach.

Controlled manufacturing

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 cryptographic keys, such as the Device-unique Hardware Key (DUHK) and the Device Root Key (DRK). Data encrypted by the DUHK becomes bound to the device, because it cannot be decrypted on any other device.

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.

KNOX Warranty Bit

The KNOX Warranty Bit is a one-time programmable fuse that signifies 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 Security Enhancements for Android (SE for Android) are disabled, it sets the fuse. Thereafter, the device can never run Android for Work, device access to the DUHK and the DRK in the TrustZone Secure World is revoked, and enterprise data on the device cannot be recovered.

Run-time protection

Real-time Kernel Protection (RKP)

RKP achieves three important security features:

- First, RKP completely prevents running unauthorized privileged code (i.e., code that has the kernel privilege) on the system, which is accomplished by preventing modification of the kernel code, injection of unauthorized code into the kernel, or execution of the user space code in the privileged mode.

- Second, RKP prevents kernel data from being directly accessed by user processes. This includes preventing double mapping of physical memory that contains critical kernel data into user space 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.

- Third, RKP monitors some critical kernel data structures to verify that they are not exploited by attacks. In particular, RKP protects the data that defines the credentials assigned to running user processes to prevent attackers from escalating this credential by modifying this data.

TIMA Attestation

TIMA Attestation allows a device to attest facts about its state to a remote server, such as an MDM server. The attestation message contains state measurements that can be evaluated by a server, which can then decide whether to trust the device or not.

This message contains:

- Measurements collected by Trusted Boot to prove that only approved system software was loaded during boot.
- Security violation logs from Periodic Kernel Measurement (PKM) and RKP since the last reboot.
- Status of the KNOX Warranty violation Bit.
- Whether SE for Android is running in enforcing mode.
- Device-identifying information such as the IMEI and Wi-Fi MAC address.
- A locally-computed verdict whether the device believes it is in a trustworthy state.

Application-level security

Trusted Boot-based KeyStore (TIMA KeyStore)

The TIMA KeyStore provides applications with services for generating and maintaining cryptographic keys. The TIMA KeyStore is only enabled if the Trusted Boot measurements match the known good values in the file tima_measurement_info, and if the KNOX warranty bit is not set. Thus, cryptographic operations with keys in the KeyStore can only occur if the system was booted into an approved state. Keys stored in the TIMA KeyStore are further encrypted with the Device-Unique Hardware Key (DUHK), and can only be decrypted from within TrustZone Secure World on the same device. All cryptographic operations on the keys are performed within TrustZone Secure World.

The TIMA KeyStore is used by default for Android for Work Managed Profiles.

The TIMA KeyStore improves upon the standard Android Keystore by denying access to its contents when Trusted Boot or the Warranty Bit reports that the device has potentially been compromised. Stored keys cannot be cloned for use on other devices.

Trusted Boot-based Client Certificate Management (TIMA CCM)

TIMA CCM enables storage and retrieval of digital certificates, as well as encryption, decryption, signing, and verification in a manner similar to the functions of a SmartCard. The certificates and associated keys are encrypted with a device-unique hardware key that can only be decrypted from code running within TrustZone.

TrustZone-based CCM also provides the ability to generate a Certificate Signing Request (CSR) and the associated public/private key pairs in order to obtain a digital certificate. A default certificate is provided for applications that do not require their own certificate.

Similar to the TIMA KeyStore, TIMA CCM operations are permitted only if the device was booted into an approved state.

TIMA 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.

Sensitive Data Protection

Any sensitive data received when the Android for Work apps are locked is still 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 Android for Work is unlocked, the data is decrypted with the private key, and re-encrypted using the usual symmetric key, which is guarded by the sensitive data master key. Currently, email subjects, bodies and attachments are marked sensitive.

SDP for Android for Work does not require a license, but the SDP Application Program Interface (APIs) must be integrated to use this feature.

Sensitive Data Protection is used by default with Android for Work Managed Profiles.

Conclusion

Android for Work on Samsung devices now benefits from the platform security of KNOX. Apps and sensitive enterprise data are protected by Samsung's hardware root of trust, the recommendation of Regenscheid to transform security by measuring compliance. Enterprises such as financial industries, governments, and healthcare require rigorous security compliance that can be measured and proven at all times. TIMA attestation is available to prove the integrity of the device and never allows end users to access enterprise apps if a device is not in an allowed state of security.

Governments and related organizations around the world have some of the most stringent information and technology security requirements. Samsung Electronics works closely with these organizations on a continuous basis to ensure that our products and solutions meet and exceed these requirements. For a list of certifications for Samsung KNOX and Samsung KNOX Workspace, see the following link: https://www.samsungknox.com/en/security-certifications

For in-depth information on Samsung KNOX, read the *Samsung KNOX Security Solution* whitepaper on the Samsung KNOX website:
https://www.samsungknox.com/en/support/knox-premium/white-papers

Endnotes

[1]Andrew Regenscheid, *Roots of Trust in Mobile Devices*, Presented to the Information Security and Privacy Advisory Board of the National Institute of Standards and Technology, February, 2012.

[2] Ibid

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 televisions, smartphones, personal computers, printers, cameras, home appliances, LTE systems, medical devices, semiconductors and LED solutions. We employ 236,000 people across 79 countries with annual sales exceeding KRW 201 trillion. To discover more, please visit www.samsung.com

For more information about Samsung KNOX, visit www.samsungknox.com

Samsung Electronics Co., Ltd.
416, Maetan 3-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 443-772, Korea

Version	Date
Android for Work on Samsung devices_V1.02	March 21, 2016
Android for Work on Samsung devices_V1.01	March 9, 2016
Android for Work on Samsung devices_V1.0	March 1, 2016