Samsung

KNOX

White Paper : An Overview of Samsung KNOX 2.0

February 2014
Enterprise Mobility Solutions
Samsung Electronics Co., Ltd.

SAMSUNG

Contents

Acronyms

AES	Advanced Encryption Standard
BYOD	Bring Your Own Device
CAC	U.S. Common Access Card
DAR	Data-at-Rest
DISA	U.S. Defense Information Systems Agency
DIT	Data-in-Transit
DoD	U.S. Department of Defense
FIPS	Federal Information Processing Standard
IPC	Inter Process Communication
MAC	Mandatory Access Control
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
NSA	U.S National Security Agency
ODE	On Device Encryption
PKCS	Public Key Cryptography Standards
ROM	Read-Only Memory
SBU	Sensitive But Unclassified
SE for Android	Security Enhancements for Android
SE Linux	Security-Enhanced Linux
SRG	Security Requirements Guide
STIGs	Security Technical Implementation Guides
TIMA	TrustZone-based Integrity Measurement Architecture
VPN	Virtual Private Network

Introducing the Samsung KNOX

The Samsung KNOX is the next-generation secure Android platform introduced by Samsung in 2013. Targeted primarily at mid and high-tier devices, it leverages hardware security capabilities to offer multiple levels of protection for the operating system and applications.

Key features of Samsung KNOX include Trusted Boot, TrustZone-based Integrity and Security services, SE for Android enhancements, and the KNOX Container.

In addition, The KNOX platform features a new enterprise enrollment process that vastly improves the experience of both the employees and IT administrators for enrolling devices into the company's MDM system.

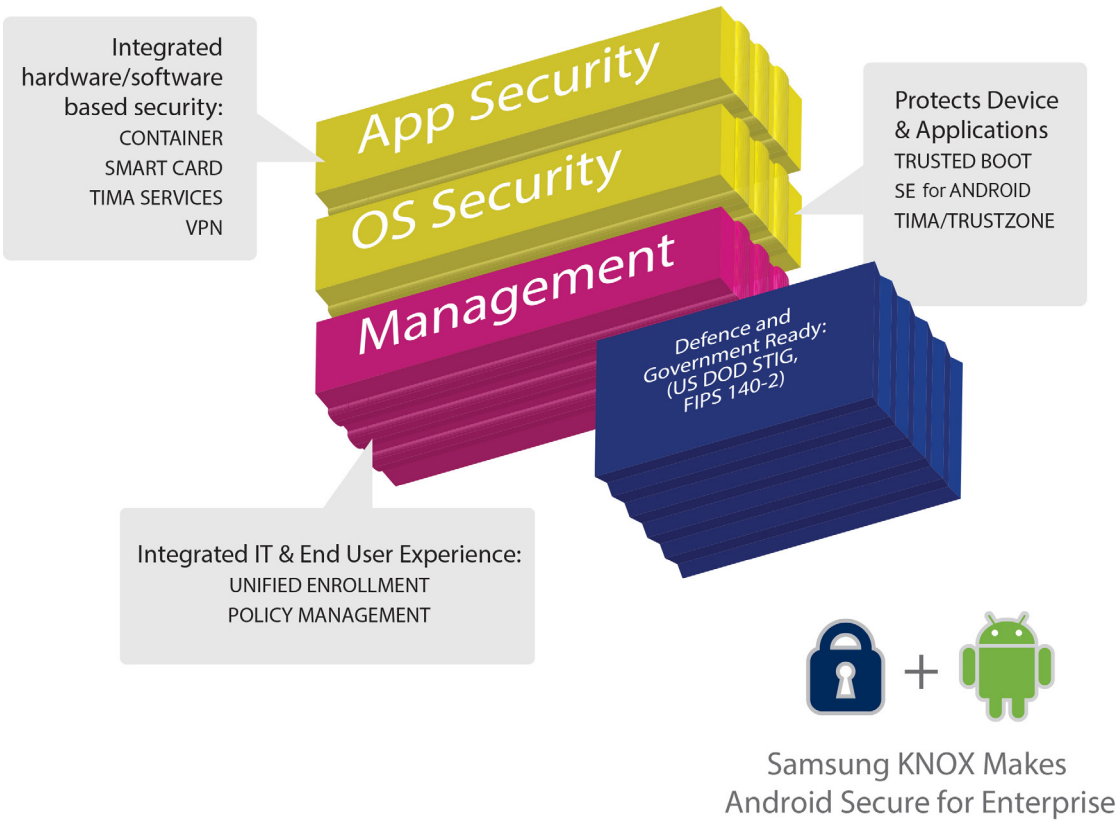


Figure 1 – Samsung KNOX Platform

The KNOX platform offers several new security and management features.

What's new in Samsung KNOX 2.0?

Samsung KNOX 2.0 includes a number of new features that address key enterprise needs. In response to requests for additional security features, the platform includes:

- SE for Android protection for third-party containers
- Enhanced TrustZone-based KeyStore
- Enhanced TrustZone-based Client Certificate Management
- TrustZone-based On Device Encryption

The user experience of enterprise enrollment of Android devices has generally lagged behind that of other mobile platforms. The KNOX platform now offers a unified enrollment option that MDM vendors can leverage to offer their employees a simple and intuitive experience.

Inaddition, several features of the original KNOX platform have been enhanced to offer additional security features to enterprises. These include:

- TrustZone-based Real-time kernel protection in additon to periodic kernel monitoring
- Major enhancements to the KNOX Container that eliminate wrapping, feature more management policies, and allow for more flexible data sharing
- A multi-vendor Virtual Private Network (VPN) framework that allows a variety of third-party clients including SSL VPN
- An open SmartCard framework that enables enterprises to choose from an array of SmartCard readers

Technology Overview

This section describes the technical aspects of three key features of Samsung KNOX:

1. Platform Security
2. Application Security
3. Mobile Device Management

1. Platform Security

Samsung KNOX addresses security using a comprehensive, three-prong strategy:

- Secure Boot and Trusted Boot
- Security Enhancements for Android (SE for Android)
- TrustZone-based Integrity Measurement Architecture (TIMA)

Trusted Boot, SE for Android, and TIMA are the cornerstones of KNOX security.

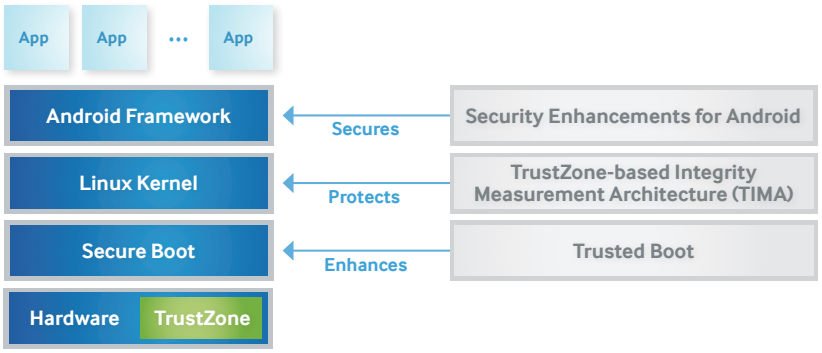


Figure 2 – Samsung KNOX Platform Security Overview

1. Platform Security

- **Secure Boot and Trusted Boot**
- Security Enhancements for Android
- TrustZone-based Integrity Measurement Architecture

The startup process for Android begins with the primary bootloader, which is loaded from ROM. This code performs basic system initialization and then loads another bootloader called a secondary bootloader from the file system into RAM and executes it. Multiple secondary bootloaders may be present, each for a specific task. The boot process is sequential in nature with each secondary bootloader completing its task and executing the next secondary bootloader, finally loading the Android bootloader known as aboot. This bootloader loads the Android operating system.

Secure Boot is a security mechanism that prevents unauthorized bootloaders and operating systems from loading during the startup process. Secure boot is implemented by each bootloader cryptographically verifying the next bootloader in the sequence using a certificate chain that has its root-of-trust resident in the hardware. The boot process is terminated if verification fails at any step.

Typically the bootloader verification process is only performed until aboot is loaded, which itself does not verify the Android operating system. This allows users to install and boot customized OS kernels and thereby run customized Android operating systems. As a result, there is no guarantee for enterprise users that their Android system is enforcing OS-level security protection, such as SE for Android, which is essential for protecting enterprise apps and data.

Samsung KNOX implements Trusted Boot to address this limitation of Secure Boot. With Trusted Boot, measurements of the bootloaders are recorded in secure memory during the boot process. At runtime, TrustZone applications use these measurements to make security-critical decisions, such as access to security keys, container activation, etc.

Additionally, if the aboot bootloader is unable to verify the Android kernel, a one-time programmable memory area (colloquially called a fuse) is permanently written to indicate the suspected tampering. Even if the boot code is restored to its original factory state, this evidence of tampering still remains and is used in preventing creation of KNOX container and protecting already created container and its data. However, the boot process is not halted, and the aboot bootloader continues to boot the Android operating system. This process ensures that normal operation of the device is not affected.

1. Platform Security

- Secure Boot and Trusted Boot
- **Security Enhancements for Android**
- TrustZone-based Integrity Measurement Architecture

Samsung KNOX utilizes SE for Android to enforce Mandatory Access Control (MAC) policies to isolate applications and data within the platform. While Google also introduced SE for Android in version 4.4 of the Android platform, Samsung's implementation offers significant enhancements in the level of protection offered to applications and system services. The Google SE for Android policy defines 40+ security domains, of which only 4 domains enforce policies while the others operate in the so-called permissive mode of SELinux. In contrast the KNOX SE for Android Policy defines over 100+ security domains that strictly enforce security policies.

The KNOX platform includes real-time kernel protection.

The KNOX platform introduces a new feature called SE for Android Management Service (SEAMS) that provides controlled access to the SELinux policy engine. SEAMS is used internally by the KNOX Container, and is also available to third party vendors to secure their own container solutions. For security considerations, the domains for third party containers are defined a priori by Samsung and activated on demand when the container application is first invoked.

1. Platform Security

The system protection offered by SE for Android relies on the assumption of OS kernel integrity. If the kernel itself is compromised (by a perhaps as yet unknown future vulnerability), SE for Android security mechanisms could potentially be disabled and rendered ineffective. Samsung's TrustZone-based Integrity Measurement Architecture (TIMA) was developed to close this vulnerability. TIMA leverages hardware features, specifically ARM® TrustZone to ensure that it itself cannot be pre-empted or disabled by malicious software running on the Android operating system.

TIMA Periodic Kernel Monitoring

TIMA PKM performs 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 SEAndroid data structures in OS kernel memory to prevent malicious attacks from corrupting them to disable SEAndroid.

TIMA Real-time Kernel Protection (RKP)

TIMA RKP performs periodic real-time monitoring of the system from within TrustZone to prevent tampering of the kernel at run time. It protects against malicious modifications and injections of kernel code, including those that coerce the kernel into corrupting its own data.

Attestation

Attestation offers verification of a mobile device's core system software i.e, the boot loaders and the kernel, at runtime based on the measurement data collected during trusted boot. Attestation can be requested at any time by the enterprise's Mobile Device Management (MDM) system. All security critical operations of attestation are performed in Trustzone.

When requested, the Attestation feature reads the previously stored measurement information and the fuse value (see Trusted Boot above) and combines these data to produce an Attestation "verdict". This verdict, which essentially an indicate for whether tampering has occured, is simply returned to the requesting MDM. The Attestation result is returned to the requesting MDM server with a signature based on the device's unique "Attestation Certificate" that is configured in the device during the manufacturing process. This ensures that the Attestation verdict cannot be altered during transfer.

Any further action is determined by the enterprise's MDM security policy. It might choose to detach from the device, erase the contents of the secure application container, ask for the location of the device, or any of many other possible security recovery procedures.

KNOX leverages TrustZone to offer enhanced security to applications.

2. Application Security

In addition to securing the platform, Samsung KNOX provides solutions to address the security needs of individual applications:

- TIMA-based Security Services
- KNOX Container
- Virtual Private Network Support
- SmartCard Framework

2. Application Security

- TIMA-based Security Services
- KNOX Container
- Virtual Private Network Support
- SmartCard Framework

TIMA Client Certificate Management (CCM)

TIMA CCM enables generation, installation, storage and retrieval of digital certificates, as well as other operations using those certificates such as encryption, decryption, signing, verification, etc. in a manner similar to the functions of a "smart card". The certificates and associated keys are encrypted with a device-unique hardware key that can only be decrypted by the hardware from within TrustZone, and all security critical operations are performed in Trustzone.

TIMA CCM also provides the ability for an application to generate a key pair and a corresponding certificate signing request (CSR) in order to obtain a digital certificate for the key. A default certificate, which can be verified through a Samsung root certificate is provided for applications that do not require their own certificates.

Programming interfaces for certificate storage and management are provided in the KNOX Premium SDK. Application developers are provided with industry standard PKCS #11 APIs for signing, encryption, and certificate operations therefore interact with the CCM as if it were a virtual smartcard. In Addition, Java APIs are also provided to developers to access CCM in Android. All operations are permitted only if the system integrity is verified through Trusted Boot.

TIMA KeyStore

TIMA KeyStore provides applications with services for generating and maintaining cryptographic keys. The keys are further encrypted with a device-unique hardware key that can only be decrypted by the hardware from within TrustZone. All cryptographic operations are performed only within TrustZone, and are disabled if system is compromised, as determined by Trusted Boot.

TIMA KeyStore is offered as an Android KeyStore provider. As a result, Application developers can continue to use the familiar Android KeyStore APIs.

TrustZone-based On Device Encryption

The KNOX platform further strengthens the full device encryption capability offered by the Android platform. In addition to successful, password authentication, the system integrity as determined by Trusted Boot is also verified before the data is decrypted.

This feature is available only if encryption is activated by the enterprise IT administrator via the MDM, and enables enterprises to ensure that all device data is protected in the event an untrusted operating system is installed on the device.

The KNOX Container runs unmodified Android applications.

2. Application Security

The Samsung KNOX Container provides a separate Android environment within the mobile device, complete with its own home screen, launcher, applications, and widgets.

Applications and data inside the container are isolated from applications outside the container, that is, applications outside the container cannot use Android inter-process communication or data-sharing methods to interact with applications inside the container. For example, the Gallery application outside the container will not display photos taken from the camera inside the container. Likewise, applications inside the container generally do not have the ability to interact with applications or access data outside the container.

The enterprise can manage the container like any other IT asset using an MDM solution. Samsung KNOX supports many of the leading MDM solutions on the market. Container management is affected by setting policies in the same fashion as those traditional MDM policies. Samsung KNOX Container includes a rich set of policies for authentication, data security, VPN, email, application blacklisting, whitelisting, etc.

The KNOX 2.0 platform features major enhancements to the Application Container from the original KNOX platform. The most significant enhancement is the elimination of application wrapping. This is achieved by leveraging technology introduced by Google in Android 4.2 to support multiple users on tablet devices. This enables enterprises to easily deploy custom applications without requiring Samsung to wrap the applications. It also reduces the barrier to entry for independent software developers wishing to develop applications for the KNOX container.

The new platform also introduces multiple container support, meeting the needs of professionals that use their own devices (BYOD) and have multiple employers.

The new container also allows enterprise IT administrators to control the flow of information between the container and the rest of the device. This allows enterprises to strike the right balance between security and user productivity. Users can also control the data sharing capability based on their personal preferences, within the limits specified by the enterprise IT administrator.

KNOX includes multi-vendor support for both IPsec and SSL VPNs.

Samsung KNOX offers comprehensive support for enterprise virtual private networks (VPN). This enables businesses to offer their employees an optimized, secure path to corporate resources from their BYOD or corporate-issued devices.

The original KNOX platform offered broad support for the IPsec protocol suite including features such as:

- Internet Key Exchange (IKE and IKEv2)
- Triple DES (56/168-bit), AES (128/256-bit) encryption
- Split tunneling mode
- Suite B Crytography

However, a large number of enterprises have deployed SSL VPNs to enable remote access to their workforce as they do not require the full connectivity to the enterprise network but rather a small set of resources such as web-based applications and file shares.

The KNOX platform adds support for leading SSL VPN vendors. As SSL implementations are proprietary, KNOX features a new generic VPN framework that allows 3rd party SSL vendors to provide their clients as plugins into this framework. Enterprise IT managers use KNOX management policies to download and configure the VPN clients of their choice.

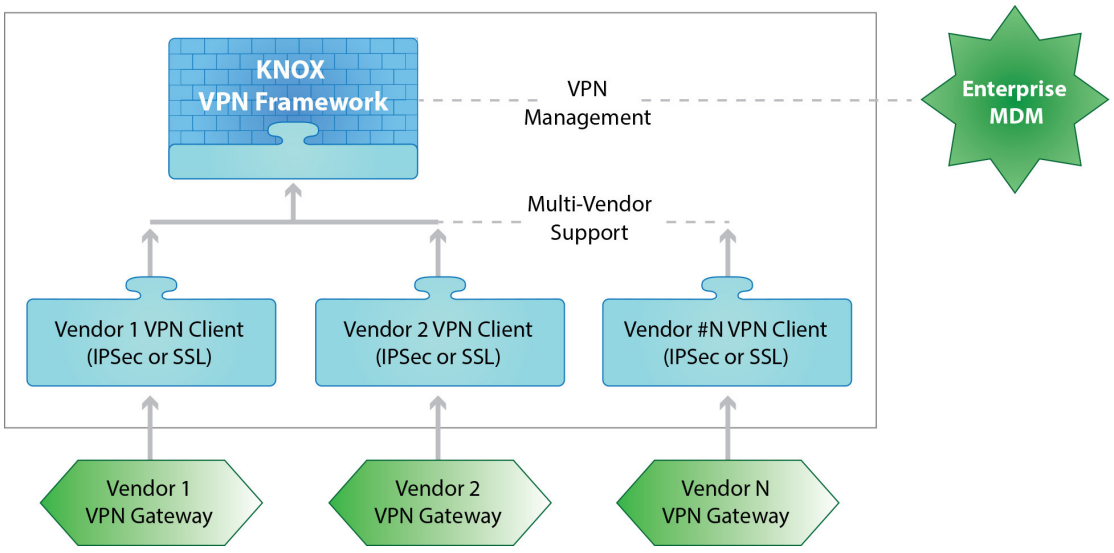


Figure 3 – Multi-Vendor Support in KNOX

The per-application VPN feature in the original KNOX platform has been extended to support SSL VPNs. This feature allows the enterprise to automatically enforce the use of VPN only on a specific set of applications. For example, the enterprise IT administrator can configure an employee's device to enforce VPN for only business applications. This ensures that the data from the user's personal applications do not use the VPN and overload the company's intranet. At the same time user privacy is preserved as their personal data does not transit the enterprise network.

The KNOX platform supports a variety of SmartCard readers.

The per-app VPN feature can also be applied to the KNOX container either for all or a subset of the applications in the container.

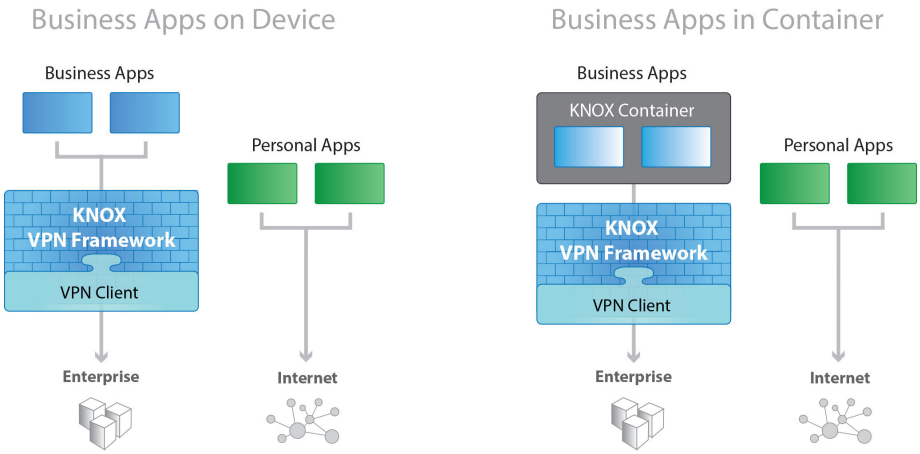


Figure 4 – Per Application VPN in KNOX

2. Application Security

- TIMA-based Security Services
- KNOX Container
- Virtual Private Network Support
- SmartCard Framework

The United States Department of Defense (US DoD) has mandated the use of Public Key Infrastructure (PKI) certificates for employees to digitally sign documents, encrypt and decrypt email messages, and establish secure online network connections. These certificates are stored on a smartcard called the Common Access Card (CAC).

The Samsung KNOX platform provides applications access to the hardware certificates on the CAC via standard based Public Key Cryptography Standards (PKCS) APIs. This enables the use of the CAC card by the browser, email application, and VPN client as well as other custom government applications.

There is growing interest among other enterprises to also use smartcards for the same purpose, especially those that require high levels of security and information protection.

The KNOX platform provides improved smartcard compatibility via a new software framework that allows third-party smart card and reader providers to plug in their solutions into the framework.

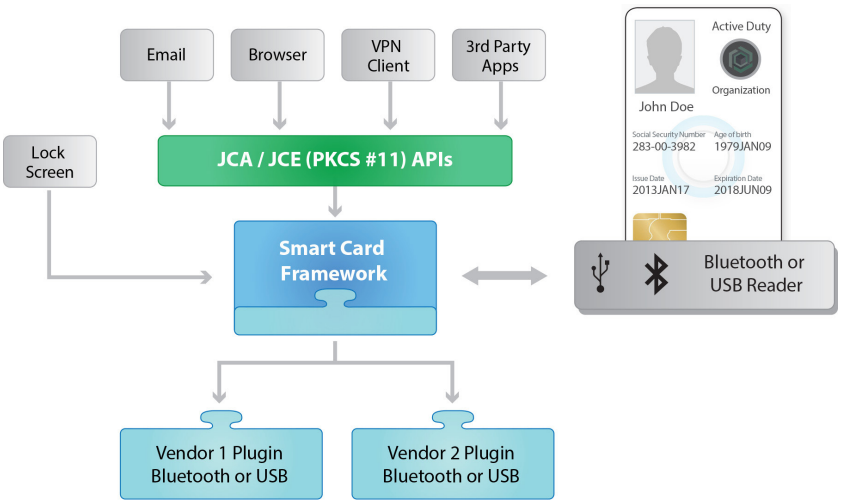


Figure 5 – Samsung KNOX Support for SmartCards

KNOX offers comprehensive management capabilities for the enterprise IT adminstrators.

3. Mobile Device Management

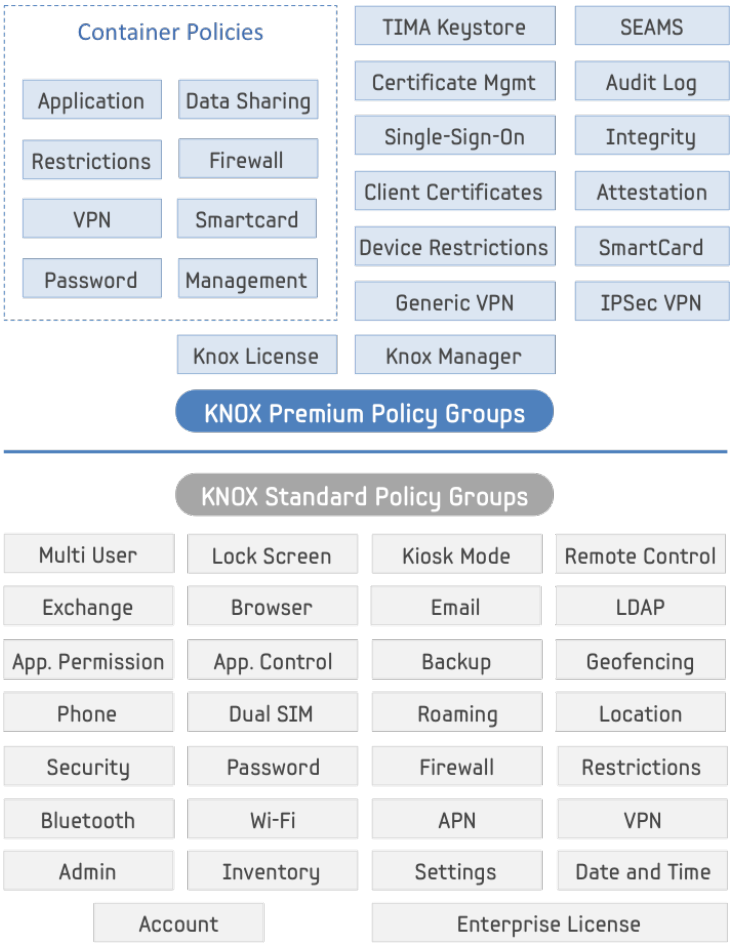
Enrolling mobile devices into the enterprise network and remote managemnet of these devices are key aspects of an enterprise mobility strategy. The KNOX 2.0 platform makes these easier by introducing more MDM supports.

- Enhanced Management Policies
- Unified Enrollment

3. Mobile Device Management

The KNOX 2.0 platform offers significant enhancements to the management policies offered in the original KNOX platform. The various policy groups are classified into two major categories: Standard and Premium.

The Standard Policy suite represents the continuous enhancements Samsung has developed over Google Android management capability since 2009. The SDK for these policy APIs is available to MDM vendors and other interested ISVs free of charge, and there is no runtime license fee associated with these APIs.



The Premium Policy suite is the collection of policy groups that offers advanced capabilities such as management and control of the KNOX container, security features such as the TIMA KeyStore and Client Certificate Manager, Per-application VPN, and so on. The SDK for these policies APIs is also available at no charge, but enterprises using these features are required to purchase a KNOX License that is verified on the device at runtime.

Samsung KNOX has simplified the enterprise enrollment process.

3. Mobile Device Management

- Enhanced Management Policies
- Unified Enrollment

Enrolling an Android device into a company's MDM system typically begins with the user downloading the agent application from the Google Play store and then configuring it for work. Enterprises are facing increasing help desk calls as more and more users are activating mobile devices for work and run into issues during this process. In addition the user is presented with prompts, privacy policies and license agreements at various stages resulting in a poor overall experience.

The KNOX platform provides a unified enrollment solution that is simple and intuitive, and eliminates many steps in the enrollment process.

The process begins with the employee navigating to a web page and clicking on an enrollment link. The link to the original web page may be provided to the employee via an e-mail or SMS, or via the company's internal or external website. Clicking on the enrollment link brings up a screen that prompts for the user's corporate email address. The device then displays all notices for the user to accept, which include privacy policies and agreements from Samsung, the MDM vendor and the enterprise. Upon accepting the terms, the user is directed to a screen to enter the password for the corporate account. If authentication is successful the enrollment is complete. Any agent application required by the MDM server is automatically downloaded and installed, without user intervention.

MDM vendors can take advantage of this feature and simplify the onboarding process for enterprise users and significantly improve the user experience and reduce support costs.

Samsung KNOX is ready for deployment in high security environments.

Certifications and Validations

4. Certifications & Validations

- FIPS 140-2 Certification
- DISA MOS SRG Compliance
- Common Criteria Certification

Issued by the National Institute of Standards and Technology (NIST), the Federal Information Processing Standard (FIPS) is a US security standard that helps ensure companies that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information and controlled unclassified information (CUI) can make informed purchasing decisions when choosing devices to use in their workplace.

Samsung KNOX meets the requirements for FIPS 140-2 Level 1 certification for both data-at-rest (DAR) and data-in-transit (DIT).

4. Certifications & Validations

- FIPS 140-2 Certification
- DISA MOS SRG Compliance
- Common Criteria Certification

The Defense Information Systems Agency (DISA) is an agency within the US DoD that publishes Security Requirements Guides (SRGs) as processes to improve the security of DoD information systems. SRGs guide the development of Security Technical Implementation Guides (STIGs) which document specific product policies and requirements as well as best practices for configuration. In 2012, DISA published the Mobile Operating System SRG to specify the security requirements that commercially available mobile devices should meet in order to be deployed within the DoD.

On May 2, 2013 DISA approved the STIG for Samsung KNOX drafted for the Mobile Operating System SRG.

4. Certifications & Validations

- FIPS 140-2 Certification
- DISA MOS SRG Compliance
- Common Criteria Certification

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.

Samsung is currently pursuing Common Criteria certification for the KNOX platform.

Summary

The Samsung KNOX platform introduced in 2013 addressed several key CIO concerns about security and management of Android devices:

- Trusted Boot, TIMA and SE for Android protect the operating system and platform services from malware attacks and hacking
- The KNOX container provides enhanced security to enterprise applications by preventing data leakage
- The per-application VPN feature enables enterprises to enforce secure VPN connectivity only for corporate apps.
- Remote attestation capability that allows enterprises to verify the authenticity and integrity of KNOX devices during and after enrollment
- The rich set of management policies enables enterprise IT administrators to comprehensively manage the device

The KNOX 2.0 platform further raises the bar on security, manageability and ease-of-use with several new features and enhancements:

- Real-time kernel protection against malicious kernel attacks
- Container runs unmodified Android applications and eliminates the need for application wrapping
- Enterprise-controllable data sharing between personal space and enterprise container
- Trustzone based handling of cryptography keys and client certificates
- A multi-vendor VPN framework that allows a variety of 3rd party clients including SSL VPN
- An open SmartCard framework that allows enterprises to choose from an array of smartcard readers

These and numerous other enhancements make the new KNOX platform the most secure and enterprise-ready Android platform whether employee owned (BYOD) or corporate issued.

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.samsung.com/knox

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