


Samsung Knox

White Paper: An Overview of the Samsung KNOX™ 2.0 Platform



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

Contents

Acronyms	1
Introducing Samsung KNOX™ 2.0 Workspace	2
What's New in the KNOX 2.0 Platform	3
Technology Overview	3
1. Platform Security	4
• Secure Boot and Trusted Boot	4
• Security Enhancements for Android	4
• TrustZone-based Integrity Measurement Architecture	5
2. Application Security	6
• Trust-Zone-based Security Services	6
• KNOX Container	7
• Virtual Private Network Support	9
• SmartCard Framework	10
• Single Sign-On	11
3. Mobile Device Management	11
• Comprehensive Management Policies	11
• Simplified Enrollment	13
4. Certifications	14
• FIPS 140-2 Certification	14
• DISA Compliance	14
• DISA Approved Product List	14
• Common Criteria Certification	14
• CESG Approved	14
Summary	15
About Samsung Electronics Co., Ltd.	16

Acronyms

AES	Advanced Encryption Standard
BYOD	Bring Your Own Device
CAC	U.S. Common Access Card
CESG	Communications and Electronic Security Group
COPE	Corporate-Owned Personally Enabled
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
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
SSO	Single Sign-On
STIGs	Security Technical Implementation Guides
TIMA	TrustZone-based Integrity Measurement Architecture
VPN	Virtual Private Network

Introducing Samsung KNOX™ 2.0 Workspace

Samsung KNOX 2.0 is the next-generation of the secured Android™ platform introduced by Samsung in 2013 as Samsung KNOX. 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 KNOX Workspace include Trusted Boot, ARM® TrustZone®-based Integrity and Security services, SE for Android enhancements (KNOX platform), and the KNOX 2.0 container.

In addition, KNOX 2.0 features a new enterprise enrollment process that vastly improves both the employee and IT administrator experience for enrolling devices into the company's MDM system.

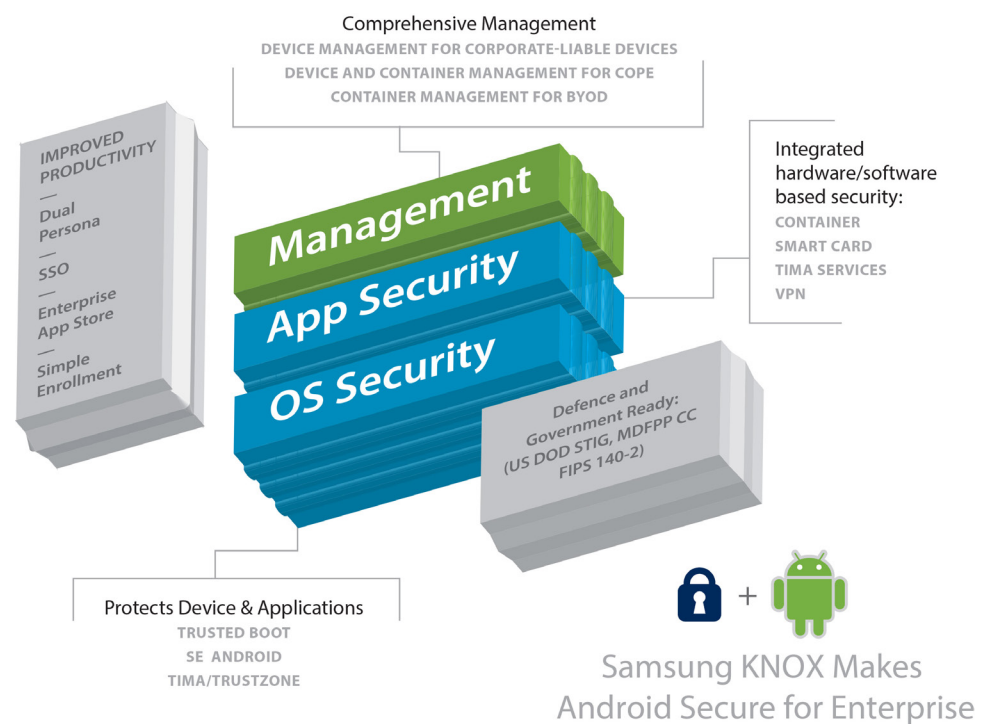


Figure 1 – Samsung KNOX 2.0 Platform

The KNOX 2.0 platform offers several new security and management features.

What's New in the KNOX 2.0 Platform

The KNOX 2.0 platform 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 that enterprise may have already deployed
- TrustZone-based KeyStore to provide hardware-based protection for encryption keys
- TrustZone-based Client Certificate Management for hardware-protected certificate management
- TrustZone-based On-Device Encryption to verify system integrity at boot time before data decryption occurs

The user experience for enterprise enrollment of Android devices has generally lagged behind that of other mobile platforms. The KNOX 2.0 platform now offers a unified enrollment option that MDM vendors can leverage to offer their customers a simple and intuitive experience.

In addition, several features of the original KNOX 1.0 platform have been enhanced to offer additional security features to enterprises. These enhancements include:

- Real-time kernel protection in addition to periodic kernel monitoring
- Major enhancements to the KNOX container that eliminates wrapping, features more management policies, and allows for more flexible data sharing
- A multi-vendor Virtual Private Network (VPN) framework with a variety of third-party clients including SSL VPN are available
- 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 2.0 platform:

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.

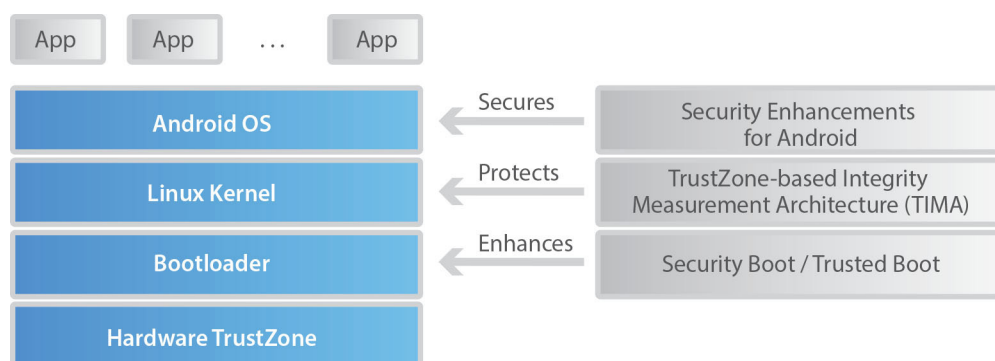


Figure 2 – Samsung KNOX 2.0 Platform Security Overview

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 in the sequence, finally loading the Android bootloader known as *aboot*, which 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 versions of Android OS kernels. 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 2.0 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 verifying the release of security keys, container activation, and so on.

Additionally, if the *aboot* bootloader is unable to verify the Android kernel, a one-time programmable memory area (colloquially called a *fuse*) is written to indicate suspected tampering. Even if the boot code is restored to its original factory state, this evidence of tampering remains. 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 2.0 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 provides significant enhancements in the level of protection offered to applications and system services. The Google SE for Android policy defines 48 security domains, of which only four domains enforce policies while the others operate in the so-called permissive mode of SELinux. In contrast, KNOX SE for Android Policy defines over 100 security domains that strictly enforce security policies.

The KNOX 2.0 platform includes real-time kernel protection.

The KNOX 2.0 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 2.0 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. SEAMS also provides enterprises the ability to replace individual SELinux policy files. This feature is governed by a special KNOX license and intended only for very specialized environments.

1. Platform Security

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

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 TrustZone, to ensure that it cannot be preempted or disabled by malicious software.

TIMA 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 SE for Android data structures in OS kernel memory to prevent malicious attacks from corrupting them and potentially disabling SE for Android.

TIMA Real-time Kernel Protection (RKP)

TIMA RKP performs ongoing, strategically-placed real-time monitoring of the operating system from within TrustZone to prevent tampering of the kernel. RKP intercepts critical events happening inside the kernel, which are inspected in TrustZone. If an event is determined to have impact on the integrity of the OS kernel, RKP either stops the event, or logs an attestation verdict that tampering is suspected, which is sent to the MDM. This protects against malicious modifications and injections to kernel code, including those that coerce the kernel into corrupting its own data.

Remote Attestation

Attestation has many similarities to Trusted Boot and essentially uses the same fundamental data sources and procedures. The primary difference is that Attestation can be requested on-demand by the enterprise's Mobile Device Management (MDM) system.

When requested, Attestation reads the previously-stored measurement information and the fuse value (see Trusted Boot above), then combines the data in a proprietary way to produce an Attestation verdict. This verdict, essentially a coarse indication that tampering is suspected, is returned to the requesting MDM. The cryptographic signature is based on the device's unique Attestation Certificate, and embedded in the device during the manufacturing process. This process ensures that the Attestation verdict cannot be altered during transfer.

Any further action is determined by the enterprise's MDM security policy. The security policy 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 2.0 leverages TrustZone to offer enhanced security to applications.

2. Application Security

In addition to securing the platform, Samsung KNOX 2.0 provides solutions to address the security needs of individual applications:

- TrustZone-based Security Services
 - KNOX 2.0 container
 - Virtual Private Network Support
 - SmartCard Framework
 - Single Sign-On
-

2. Application Security

- **TrustZone-based Security Services**

- KNOX container
- Virtual Private Network Support
- SmartCard Framework
- Single Sign-On

TrustZone-based Client Certificate Management (CCM)

TrustZone-based CCM enables storage and retrieval of digital certificates, as well as other operations using those certificates such as encryption, decryption, signing, verification, and so on, 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.

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 and encryption, and therefore interact with the CCM as if it were a virtual SmartCard. Both types of operations are permitted only if Trusted Boot can guarantee system integrity.

TrustZone-based KeyStore

The 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 the system is compromised, as determined by Trusted Boot.

Application developers should continue to use the familiar Android KeyStore APIs and specify that the KeyStore is used to provide the service.

TrustZone-based On-Device Encryption

The KNOX 2.0 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 the enterprise IT administrator activates encryption via the MDM. TrustZone-based On-Device Encryption also enables enterprises to ensure that all device data is protected in the unlikely event that the operating system is compromised.

The KNOX 2.0 container runs unmodified Android applications.

2. Application Security

- TrustZone-based Security Services
- **KNOX container**
- Virtual Private Network Support
- SmartCard Framework
- Single Sign-On

The Samsung KNOX 2.0 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 with applications inside the container. For example, photos taken with the camera inside the container are not viewable in the Gallery outside the container. The same restriction applies to copying and pasting. Note that the contacts and calendar apps represent an exception, since container contacts and the calendar can be made visible inside the KNOX container and in the personal work space. The end user can choose whether to share contacts and calendar notes between the container and personal space, however, IT policy ultimately controls this option.

The enterprise can manage the container like any other IT asset using an MDM solution; this container management process is called Mobile Container Management (MCM). Samsung KNOX 2.0 supports many of the leading MDM solutions on the market. MCM is affected by setting policies in the same fashion as traditional MDM policies. The Samsung KNOX 2.0 container includes a rich set of policies for authentication, data security, VPN, e-mail, application blacklisting, whitelisting, and so on.

The KNOX 2.0 platform features major enhancements to the KNOX container in the KNOX 1.0 platform. The most significant enhancement is 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 enhancement enables enterprises to easily deploy custom applications without requiring Samsung to wrap the application. It also further reduces the barrier to entry for independent software developers wishing to develop and deploy applications for the KNOX 2.0 container.

The new container also adds a two-factor authentication process. The user can create a finger print to access the container and select either a PIN, password, or pattern as a second process to follow the finger print.



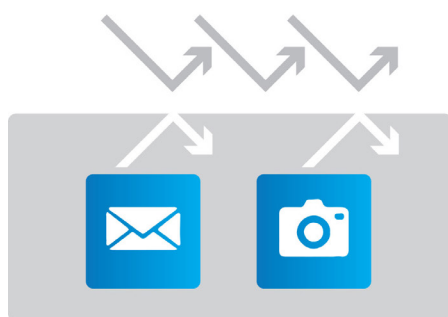
Figure 3 – Samsung KNOX 2.0 Container

The KNOX 2.0 container allows enterprises to balance security and user productivity.

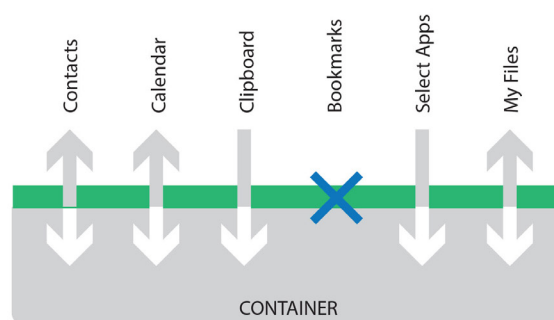
The KNOX 2.0 platform also introduces support for multiple containers, thus meeting the needs of professionals that use their own devices for corporate use (BYOD) and have multiple employers, such as doctors or consultants.

The new KNOX 2.0 container also allows enterprise IT administrators to control the flow of information between the container and the rest of the device. This feature enables enterprises to strike the right balance between security and user productivity. Users can also control the device's data sharing capability based on their personal preferences, according to the limits specified by enterprise IT administrators.

1. APP ISOLATION: NO DATA IS LEAKED



2. MDM POLICIES: IT CONTROLS, SELECTS & SHARES DATA



3. MULTI-CONTAINER SUPPORT



4. NO APP WRAPPING: MANY MORE BUSINESS APPS AVAILABLE



Figure 4 – Samsung KNOX 2.0 Container

KNOX offers stronger VPN support for both IPSec and SSL VPNs.

2. Application Security

- TrustZone-based Security Services
- KNOX container
- **Virtual Private Network Support**
- SmartCard Framework
- Single Sign-On

The KNOX 2.0 platform offers additional comprehensive support for enterprise Virtual Private Networks (VPN). This support enables businesses to offer their employees an optimized, secure path to corporate resources from their BYOD or Corporate-Owned Personally Enabled (COPE) devices.

The KNOX 1.0 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 Cryptography

However, a large number of enterprises have deployed Secure Socket Link (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 2.0 platform adds support for leading SSL VPN vendors. As SSL implementations are proprietary, KNOX 2.0 features a new generic VPN framework which enables third-party SSL vendors to provide their clients as plug-ins into the VPN framework. Enterprise IT administrators use KNOX MDM policies to download and configure a specific SSL client.

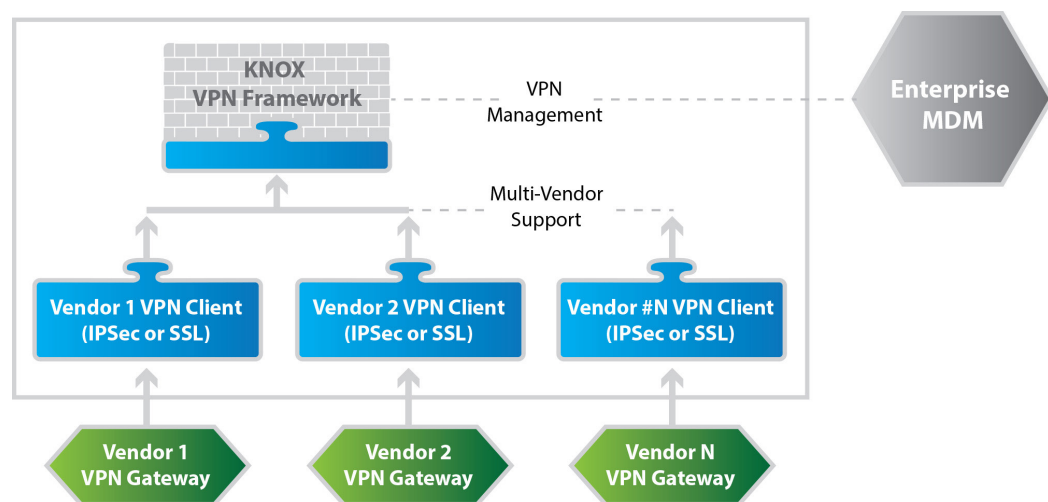


Figure 5 – Multi-Vendor Support in KNOX

The per-application VPN feature in the KNOX 1.0 platform has been extended to support SSL VPNs. This feature enables 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 feature 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 because personal data does not use the enterprise network.

The KNOX 2.0 platform gives comprehensive support across SmartCard readers.

The per-app VPN feature can also be applied to the KNOX 2.0 container either for all or a subset of the applications in the container.

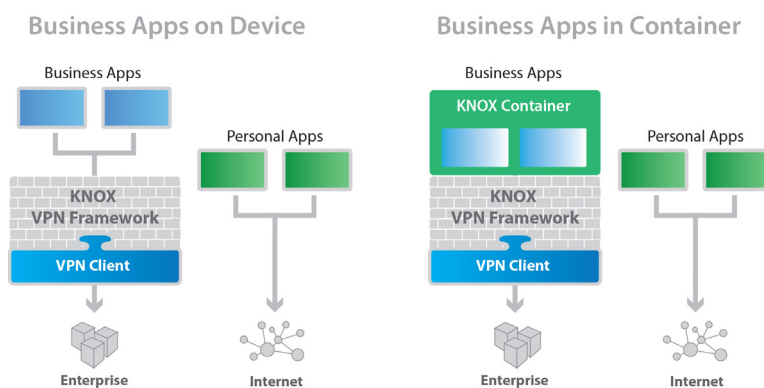


Figure 6 – Per Application VPN in KNOX 2.0

2. Application Security

- TrustZone-based Security Services
- KNOX container
- Virtual Private Network Support
- **SmartCard Framework**
- Single Sign-On

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 e-mail messages, and establish secure online network connections. These certificates are typically stored on a SmartCard called the Common Access Card (CAC).

The Samsung KNOX 2.0 platform provides applications access to the hardware certificates on the CAC via standards-based Public Key Cryptography Standards (PKCS) APIs. This access process enables the use of the CAC card by the browser, e-mail application, and VPN client, as well as other custom government applications.

Other enterprises have growing interest to use SmartCards for the same purpose, especially those that require high levels of security and information protection.

The KNOX 2.0 platform provides improved SmartCard compatibility via a new software framework that allows third-party SmartCard and reader providers to install their solutions into the framework.

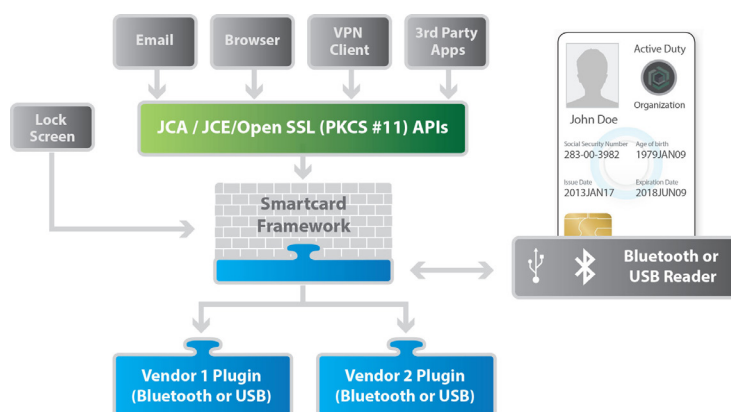


Figure 7 – Samsung KNOX 2.0 Support for SmartCards

Single Sign-On (SSO) increases security and reduces IT costs.

2. Application Security

- TrustZone-based Security Services
- KNOX container
- Virtual Private Network Support
- SmartCard Framework
- **Single Sign-On**

Single Sign-On (SSO) is access control of several related, but independent software systems. The user logs in once and has access to all systems without being prompted to log in again for each application. For example, SSO allows access to the container and apps within the container with one password.

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes. It combines this with techniques to ensure that users do not have to actively enter their credentials more than once.

Advantages of using SSO include:

- Reduces the number of user names and password combinations a user must remember
- Reduces time spent re-entering passwords for the same user
- Reduces IT costs with less help desk calls about passwords
- Increases security because tokens and certificates are transmitted over the internet for authentication as opposed to plain text passwords.

3. Mobile Device Management

Enrolling mobile devices into the enterprise network and remote management of these devices are key aspects of an enterprise mobility strategy. The KNOX 2.0 platform addresses both of these requirements:

- Comprehensive management with over 530 policies
- Simplified enrollment for a faster and intuitive user experience

3. Mobile Device Management

- **Comprehensive Management Policies**
- Simplified Enrollment

The KNOX 2.0 platform offers significant enhancements to the management policies offered in the KNOX 1.0 platform. The various policy groups are classified into two major categories: Standard and Premium.

The Standard Policy suite represents continuous enhancements Samsung 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. Further, no runtime license fee is associated with these APIs.

KNOX 2.0 offers comprehensive management capabilities for the enterprise IT administrator.

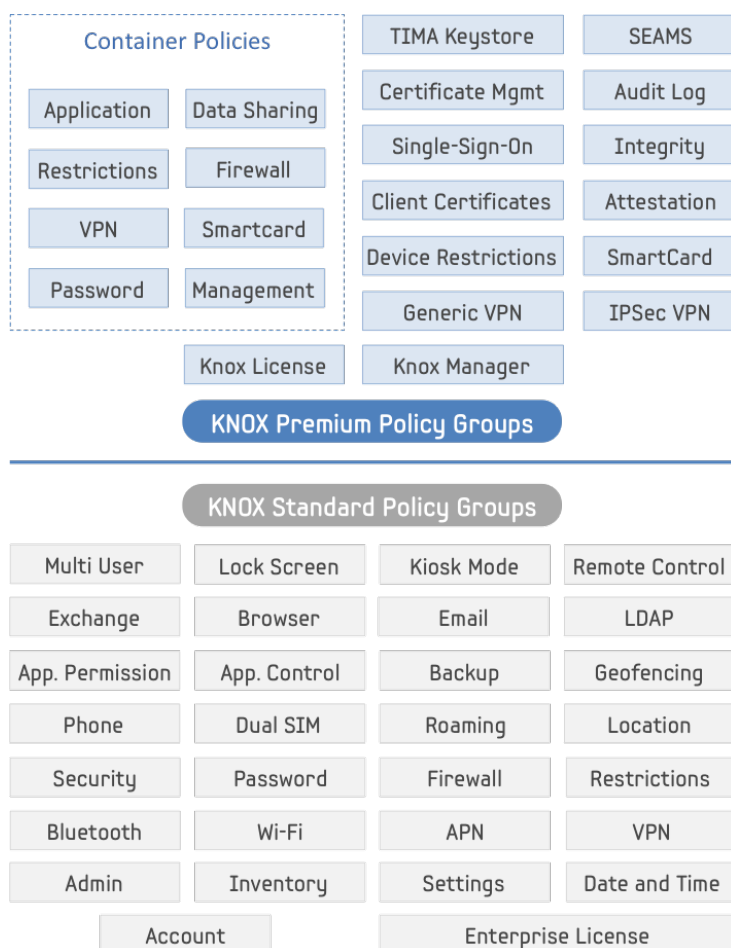


Figure 8 – Samsung KNOX 2.0 Management Policies

The KNOX 2.0 Premium Policy suite is the collection of policy groups offering advanced capabilities such as management and control of the KNOX container, security features such as the KeyStore and Client Certificate Manager, Per-application VPN, and so on. The SDK for these policy APIs is also available at no charge, however, 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

- Comprehensive Management Policies
- Simplified Enrollment

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

The KNOX 2.0 platform provides a simplified enrollment solution that is simple and intuitive and eliminates many steps and human error.

The simplified enrollment process provides the employee with an enrollment link sent by e-mail, text message, or through the company's internal or external website. Once the link is clicked, users are prompted to enter their corporate e-mail address. This action triggers the display of all required privacy policies and agreements. After accepting the terms, users enter a corporate account password for authentication from the enterprise. Any agent application required is automatically downloaded and installed.

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

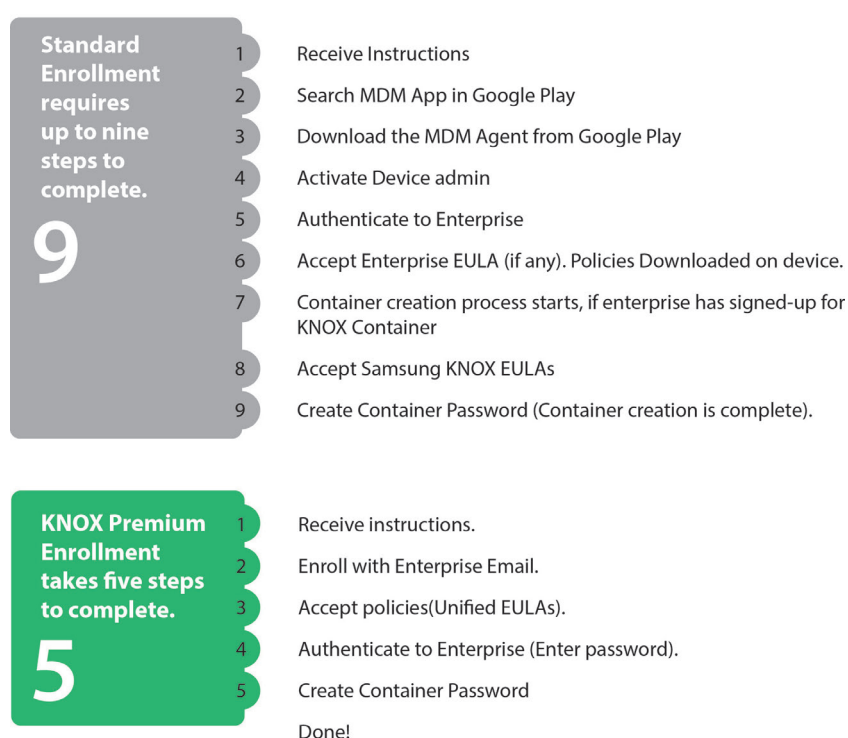


Figure 9 – KNOX 2.0 Container Simplified Enrollment

Samsung KNOX is ready for deployment in high security environments.

Certifications

4. Certifications

- FIPS 140-2 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 2.0 meets the requirements for FIPS 140-2 Level 1 certification for both data-at-rest (DAR) and data-in-transit (DIT).

- DISA Approved STIG

The Defense Information Systems Agency (DISA) is an agency within the US DoD that publishes Security Technical Implementation Guides (STIGs) which document security policies, requirements, and implementation details for compliance with DoD policy.

On April 17, 2014 DISA approved the STIG for Samsung KNOX 1.0.

- DISA Approved Product List

On May 14, 2014 DISA added five Knox-enabled devices to the US DoD Approved Products List (APL).

NOTE: The five Samsung devices added to DISA's APL are the only Android 4.4 OS devices on the list as of May 14, 2014. They are also the only devices certified under Common Criteria (CC) by Mobile Device Fundamental Protection Profile (MDFPP). These five new devices represent a twenty percent increase of mobile products available for purchase in the DoD.

- 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.

Select Galaxy devices with KNOX embedded received Common Criteria (CC) certification on February 27, 2014. The current CC certification targets the new Mobile Device Fundamentals Protection Profile (MDFPP) of the National Information Assurance Partnership (NIAP), published in October 2013, which addresses the security requirements of mobile devices for use in enterprise.

- CESG Approved

The Communications and Electronic Security Group (CESG) approved KNOX-enabled Android devices for United Kingdom government use on May 14, 2014.

Summary

The Samsung KNOX platform addressed several 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 2.0 container provides enhanced security to enterprise applications by preventing data leakage
- The per-application VPN features enables enterprises to enforce secure VPN connectivity only for corporate apps.
- The rich set of MDM policies enables enterprise IT administrators to comprehensively manage the device

The new 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
- Hardware-backed storage for cryptography keys and client certificates
- Remote attestation capability that allows enterprises to verify the authenticity and integrity of KNOX devices during and after enrollment
- The KNOX 2.0 container runs unmodified Android applications and eliminates the need for application wrapping
- Enterprise-controllable data sharing between personal space and enterprise container
- A multi-vendor VPN framework that allows a variety of third-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 2.0 platform the most secure and enterprise-ready Android platform, whether devices are employee-owned (BYOD) or corporate-issued (COPE).

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

Copyright © 2014 Samsung Electronics Co. Ltd. All rights reserved. Samsung is a registered trade-mark of Samsung Electronics Co. Ltd. Specifications and designs are subject to change without notice. Non-metric weights and measurements are approximate. All data were deemed correct at time of creation. Samsung is not liable for errors or omissions. Android and Google Play are trademarks of Google Inc. ARM and TrustZone are registered trademarks of ARM Ltd. or its subsidiaries. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

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