

# Samsung Knox

---

White Paper : An Overview of Samsung KNOX™

---



June 2013  
Enterprise Mobility Solutions  
Samsung Electronics Co., Ltd.

---

# Contents

Acronyms	1
Android and the Enterprise	2
Introducing Samsung KNOX™	2
Technology Overview	3
1. Platform Security	3
• Customizable Secure Boot	3
• TrustZone-based Integrity Measurement Architecture	4
• Security Enhancements for Android	4
2. Application Security	5
• Application Containers	5-6
• On-Device Data Encryption	7
• Virtual Private Network Support	8
3. Mobile Device Management	9
Samsung KNOX for Government and High Security Use	10
1. Boot Attestation	10
2. Smartcard - CAC Support	11
3. Certification & Validations	11
Summary	12
About Samsung Electronics Co., Ltd	13

---

## Acronyms

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

## Samsung KNOX is a new Android-based solution designed from the ground up with security in mind

### Android and the Enterprise

With over 75% of the smartphone market share as of 3Q 2012<sup>1</sup>, Android is currently the world's most popular smartphone platform.

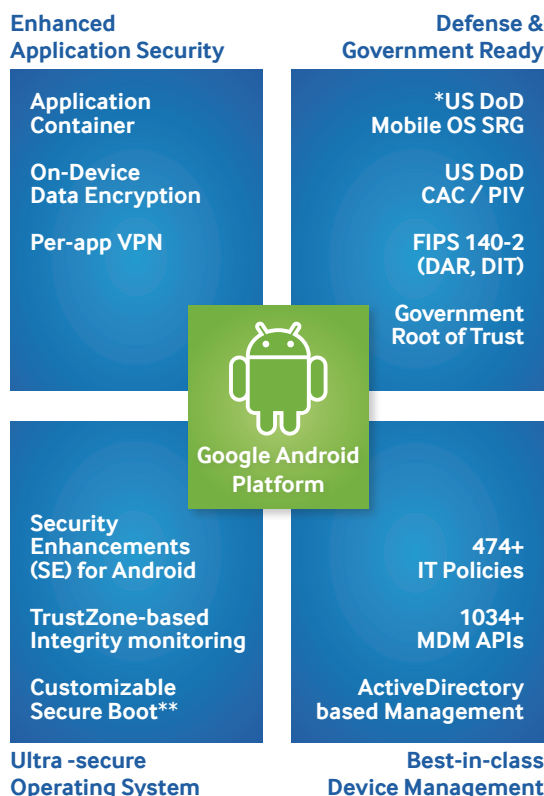
There are several factors behind Android's success: the open source aspect attracted early adopters and developers, while Google's services and the abundance of third party applications drove consumer adoption.

The success of Android among consumers and the developer community has, however, not translated to the enterprise. An April 2012 survey by Gartner found that fewer than 10% of enterprises planned on deploying Android devices in the next 12 months.<sup>2</sup> The principal reasons cited were a perceived lack of security and limited management capability.

As a global leader in Android smartphones, Samsung developed Samsung KNOX to provide a more compelling and secure enterprise experience.

- 1. IDC, "Worldwide Quarterly Mobile Phone Tracker," 2012
- 2. Gartner, "Magic Quadrant for Mobile Device Management Software," 2012

### Introducing Samsung KNOX™



\* in process  
\*\* Customizable Secure Boot availability varies depending on hardware specification.

Figure 1 – Samsung KNOX Makes Android Enterprise-Ready

Samsung KNOX is a new Android-based solution designed from the ground up with security in mind to address the perception of the current open source Android platform. Samsung KNOX retains full compatibility with Android and the Google ecosystem while integrating fundamental security and management enhancements. All of these advantages make Samsung KNOX the perfect choice for both regulated and general enterprise environments.

Samsung KNOX incorporates key technologies patented by the National Security Agency (NSA) and leverages hardware-level features to provide enhanced security to protect the operating system and applications. In addition, Samsung KNOX has been submitted to the US Government and Department of Defense (DoD) for compliance with initiatives, requirements and standards for mobile device security to enable its use in government and other highly regulated enterprise environments.

Finally, Samsung KNOX features one of the most comprehensive Mobile Device Management (MDM) capabilities available. Samsung KNOX, combined with its unique application container technology, enables enterprises to support both BYOD and Corporate-Liable models without compromising corporate security or employee privacy.

## Samsung KNOX addresses security at the operating system level in a comprehensive, three-prong strategy

### 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

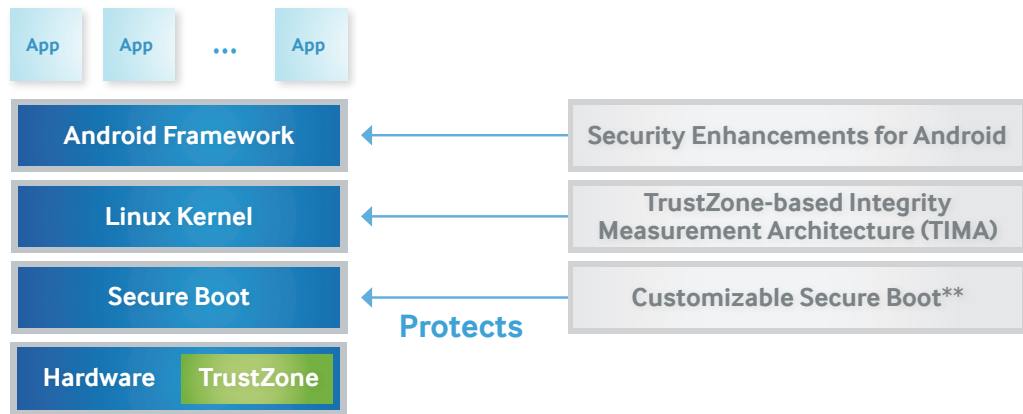


Figure 2 – Samsung KNOX System Security Overview

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

- Customizable Secure Boot\*\*
- TrustZone-based Integrity Measurement Architecture (TIMA)
- Security Enhancements for Android

Samsung KNOX also takes full advantage of all available hardware elements to enhance this security posture.

\*\* Customizable Secure Boot availability varies depending on hardware specification

#### 1. Platform Security

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

Secure Boot is a procedure that prevents “unauthorized” operating systems and software from loading during the startup process. Firmware images (that is, operating systems and other system components) that are cryptographically signed by known, trusted authorities are considered as “authorized” firmware. Secure Boot is the first line of defense against malicious attacks on KNOX-based mobile devices.

Secure Boot requires the device boot loader, kernel, and system software to be cryptographically signed by a key verified by the hardware. Secure Boot uses X.509 certificates and public keys which are embedded into the boot loader of the device. A secure hash of the certificates is fused into hardware Read-Only Memory (ROM) at the time of manufacture. The Secure Boot loader will only continue if the authorized secure signed binaries are present. Next, Secure Boot verifies the cryptographic signature of the Linux kernel and system image before handing control to the OS.

The use of industry standard X.509 certificates and hardware-protected keys provides a strong degree of robustness and confidence in the secure boot scheme. By default, the root of trust is a Samsung-issued certificate that enables verification of the stock Samsung Android image. The KNOX Enterprise root of trust is activated when the device is enrolled in an enterprise that has deployed a KNOX-compliant MDM system. This root of trust enables verification of the Samsung Android image with KNOX features activated. The KNOX Government root of trust is reserved for government deployments and is discussed in greater detail in the section entitled “Samsung KNOX for Government and High Security Use”.

---

## Platform security of Samsung KNOX is the first line of defense against malicious attacks

---

### 1. Platform Security

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

Samsung KNOX utilizes SE for Android (Security Enhancements for Android) to enforce Mandatory Access Control policies to isolate applications and data within the platform. SE for Android, however, relies on the assumption of OS kernel integrity. If the Linux kernel 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. Introduced in Samsung KNOX as a unique feature on Samsung mobile devices, TIMA uses ARM TrustZone hardware and provides continuous integrity monitoring of the Linux kernel. The ARM TrustZone hardware effectively partitions memory and CPU resources into a "secure" and "normal" world. TIMA runs in the secure-world and cannot be disabled, while the SE for Android Linux kernel runs in the "normal" world.

TIMA is used along with Customizable Secure Boot\*\* and SE for Android to form the first line of defense against malicious attacks on the kernel and core boot strap processes. When TIMA detects that the integrity of the kernel is violated, it notifies the enterprise IT via MDM which can then take policy-driven action in response.

\*\*Customizable Secure Boot availability varies depending on hardware specification

---

### 1. Platform Security

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

Security-Enhanced Linux (SE Linux) is a technology invented by the NSA in 2000 and has long been established as the standard for securing enterprise Linux assets. Samsung R&D teams have worked very closely with the NSA to port and integrate this technology into Android. This port of SE Linux to Android is commonly referred to as Security Enhancements for Android, or "SE for Android".

SE for Android provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements. It incorporates a strong, flexible Mandatory Access Control (MAC) architecture into the major kernel subsystems and isolates applications and data into different domains.

This architecture prevents a compromise in one domain from propagating to other domains or the underlying mobile operating system (OS). This additional security, on top of Linux, reduces threats of tampering and bypassing of application security mechanisms. It also minimizes the amount of damage that can be caused by malicious or flawed applications, as applications are provided the minimum amount of permission required for their task.

SE for Android includes a set of security policy configuration files designed to meet common, general-purpose security goals.

Out of the box, Samsung KNOX is provisioned with a set of security policy configuration files designed to strengthen the core Android platform and meet general enterprise needs. Samsung KNOX offers management APIs that allow the default SE for Android policy files to be replaced with stricter or enterprise-specific policy files. These new policy files can be pushed to the device.

## Samsung KNOX provides enterprises the ability to create and manage a secure container within their employees' personal mobile devices

### 2. Application Security

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

- Application Containers
- On-device Data Encryption
- Virtual Private Network Support

### 2. Application Security

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

- Application Containers
- On-device Data Encryption
- Virtual Private Network Support



Figure 3 – Samsung KNOX Container

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 (IPC) or data-sharing methods with applications inside the container.

Likewise, applications inside the container generally do not have the ability to interact with applications or access data outside the container. However, some applications inside the container can be granted read-only access to data outside the container via a policy configuration.

For example, photos taken from the camera inside the container won't be viewable from the Gallery outside the container in a user's personal area. Conversely, contacts and calendar events created outside the container are viewable inside the container.

## 2. Application Security

- Application Containers
- On-device Data Encryption
- Virtual Private Network Support

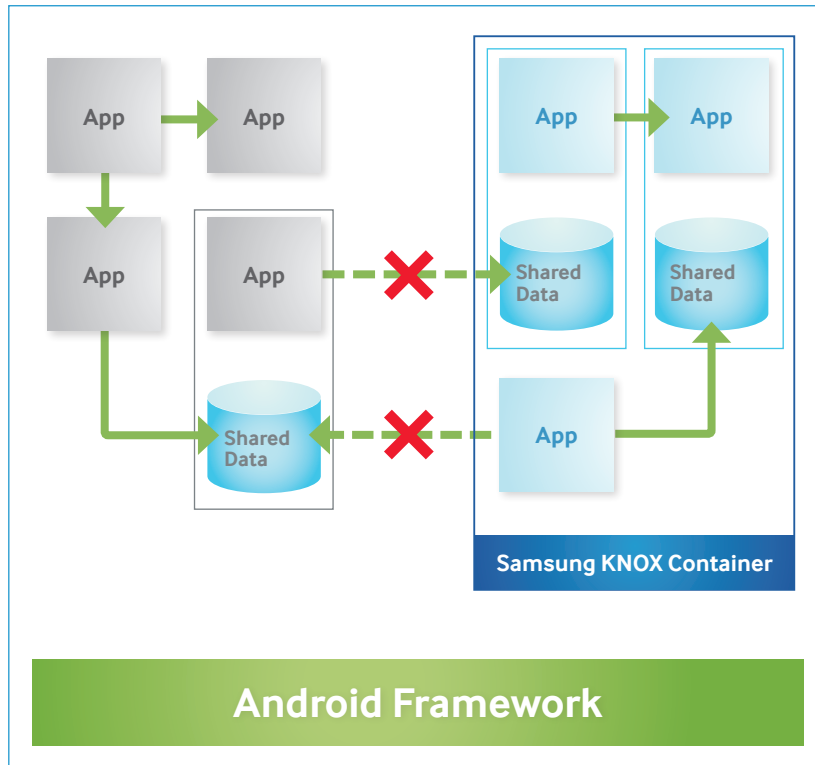


Figure 4 – Application Isolation in Samsung KNOX

This total isolation of applications and data within the container enables a powerful solution for the “data leakage” associated with the BYOD model. Data leakage occurs when a user sends sensitive or critical information outside of the corporate network via a personal email account, social network site, or public cloud storage system.

Samsung KNOX allows a “Work” container to be setup for corporate applications such as email, calendar, browser, storage clients, and so on, and the container will ensure that any data downloaded from the enterprise, such as email attachments and files, cannot be accessed by applications outside the container. All the data stored by applications inside the container are encrypted via strong encryption algorithms (AES-256). A password is required to gain access to applications inside the container.

Samsung KNOX Container is deeply integrated into the native Android platform – unlike other third party container solutions that are available via download from an app store. This deep integration enables a superior user experience that clearly separates the two environments to minimize user confusion, preserves the Android navigation paradigm in each environment for consistency, and provides a unified but privacy-aware view of notifications and active applications for efficiency.

Furthermore, the deep integration allows Samsung KNOX Container to execute at the system level and leverage additional security and isolation guarantees provided by Security Enhancements for Android.

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 traditional MDM. Samsung KNOX Container includes a rich set of policies for authentication, data security, VPN, email, application blacklisting, whitelisting, etc.



## Samsung devices offer the levels of security required by government and regulated industries

### 2. Application Security

- Application Containers
- **On-device Data Encryption**
- Virtual Private Network Support

The On-device Data Encryption (ODE) feature allows users and enterprise IT administrators to encrypt data on the entire device, as well as any configured Samsung KNOX Container. The ODE feature on Samsung devices uses a FIPS 140-2 certified Advanced Encryption Standard (AES) cipher algorithm with a 256-bit key (AES-256) and offers the levels of security required by government and regulated industries such as healthcare and finance. The key utilized for this encryption is developed from a user-created passphrase using well-known key-derivation algorithms such as Password-Based Key Derivation Function 2 (PBKDF2).

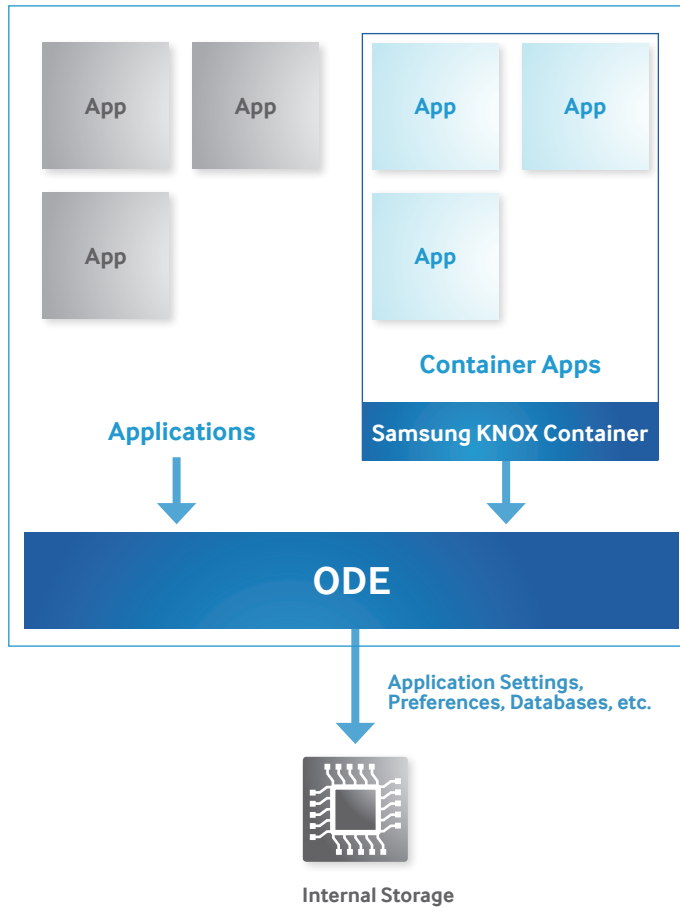


Figure 5 – On-Device Data Encryption in Samsung KNOX

The encryption feature spans internal storage (system partition and internal SD card) as well as any user-installed external SD card\*. Hardware acceleration is employed to speed up the encryption and decryption process and minimizes the impact of the overhead on the overall user experience.

Encryption can be activated directly by the user via the “Settings” user interface, or remotely by the enterprise IT administrator as a policy setting using Exchange ActiveSync or an MDM system.

The use of NIST-compliant algorithms for ODE in Samsung KNOX devices satisfies federal data-at-rest (DAR) requirements.

\*While data in KNOX container is encrypted through ODE, the data can not be stored in an external storage such as an external SD card.

## Samsung KNOX offers comprehensive support for an enterprise virtual private network (VPN) found in any mobile device

### 2. Application Security

- Application Containers
- On-device Data Encryption
- Virtual Private Network Support

Samsung KNOX offers a high level of comprehensive support for an enterprise virtual private network (VPN). This enables businesses to offer their employees an optimized, secure path to the enterprise intranet from their BYOD or corporate-issued device.

Samsung KNOX VPN implementation offers broad support for the IPSec protocol suite:

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

Samsung KNOX VPN is FIPS 140-2 certified, enabling its use in regulated environments like government, healthcare, finance and etc.

Another distinguishing feature of Samsung KNOX VPN feature is the ability for enterprise IT administrators to configure, provision, and manage the use of VPN on a per-application basis. This capability allows the enterprise to automatically enforce the use of VPN only on a specific set of corporate applications. This has the benefit of ensuring that enterprise data is communicated on a secure connection while keeping the user's personal data from overloading the company's Internet connection.

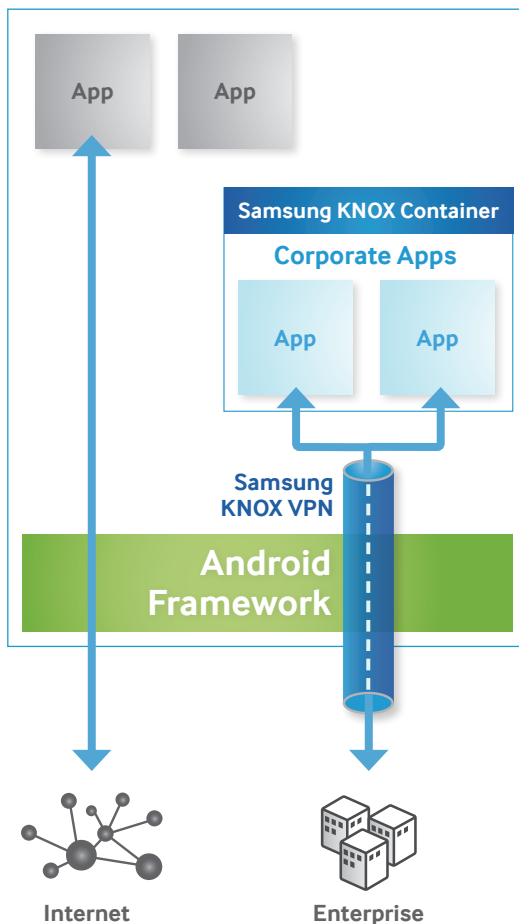


Figure 6 – Per-App VPN in Samsung KNOX

In addition, the per-app VPN feature allows personal-use applications to bypass the VPN and connect directly to the Internet, preserving user privacy.

The per-app VPN capability is also available for applications within Samsung KNOX Container.

Other features of Samsung KNOX VPN implementation include:

- Up to 5 simultaneous VPN connections
- RSA SecureID® support for Cisco VPN gateways
- Common Access Card (CAC) support for government use

## MDM enables a company’s IT department to monitor, control and administer all deployed mobile devices across multiple mobile service providers

### 3. Mobile Device Management

Mobile Device Management (MDM) enables the enterprise IT department to monitor, control, and administer all deployed mobile devices across multiple mobile service providers.

Samsung KNOX builds upon Samsung’s industry leading SAFE™ MDM capabilities by providing additional policies for security, enterprise integration, and enterprise applications such as asset tracking, remote control, and so on.

Enterprise need	KNOX MDM Policy Groups***		
Remote Management	WiFi	Security	Email Accounts
	Bluetooth	Password	Browser
Limit Features and Functions	Kiosk Mode	Application permissions	Firewall
Secure Access to Enterprise Resources	Application	VPN	Exchange Account
Geo-fencing	Location		
Real-time Device Status and Activity	Device Inventory		
Manage Voice and Data Usage	Roaming	Phone Restrictions	APN Settings
Real-time Mobile User Support	Remote Control		
Prevent Data Leakage	Email Forwarding	Container Management	Integrity Management
Enterprise Integration	Single Sign-on	Active Directory	

\*\*\* Availability of Samsung KNOX features may vary by MDM partners.

Figure 7 – KNOX MDM Policy Groups

Specific MDM enhancements include:

- Policies to comply with the US DoD Mobile OS Security Requirements Guide (MOS SRG)
- Support for Samsung KNOX Container
- Support for management via ActiveDirectory/Group Policy Manager
- VPN and Wi-Fi Provisioning
- Idle screen and lock screen configuration

Samsung KNOX meets the requirements for FIPS 140-2 Level 1 certification for both DAR and DIT

## Samsung KNOX for Government and High Security Use

---

For government and DoD installations, KNOX provides additional security features, including:

1. Boot Attestation
2. Smartcard - CAC Support
3. Certification & Validations

---

### 1. Boot Attestation

Samsung KNOX technology uses a Secure Boot protocol that requires the device boot loader, kernel, and system software to be cryptographically signed by a key whose root of trust is verified by the hardware. Commercially sold Samsung devices will have Samsung-issued root certificates.

Government deployments generally require that government agencies or approved system integrators be the custodian of the entire mobile device software. As mentioned previously, Samsung KNOX devices have a hardware-protected root certificate reserved for government agencies or their trusted partners to create their own chain of trust. To achieve this Samsung signs the government's (or system integrator's) Level-2 (CA) certificate with the aforementioned root certificate, and provides tools to perform a one-time change from the default Samsung root of trust to the KNOX Government root of trust.

The government (or its SI) can then develop and deploy its own software images that are signed by its Level-2 certificate which in turn is verified by the KNOX Government certificate in the hardware during boot time.

It should be noted that Samsung does not produce any binary that can boot devices with a certificate chain rooted at the Knox Government root certificate; only Government-designated entities, whose certificates are certified by the Knox Government root certificate, can produce such binaries.

## 2. Smartcard - CAC Support

The United States Department of Defense (US DoD) has mandated the use of Public Key Infrastructure (PKI) certificates for employees to “sign” documents digitally, encrypt and decrypt email messages, and establish secure online network connections.

In compliance with DoD regulations, Samsung KNOX allows the PKI certificates to be stored securely on the mobile device (software certificates) or be retrieved from a CAC (hardware certificates).

Samsung KNOX provides applications access to the hardware certificates on the CAC via standards-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.

In addition, Samsung KNOX allows the lock screen to be secured by the CAC card, providing an additional level of device security.

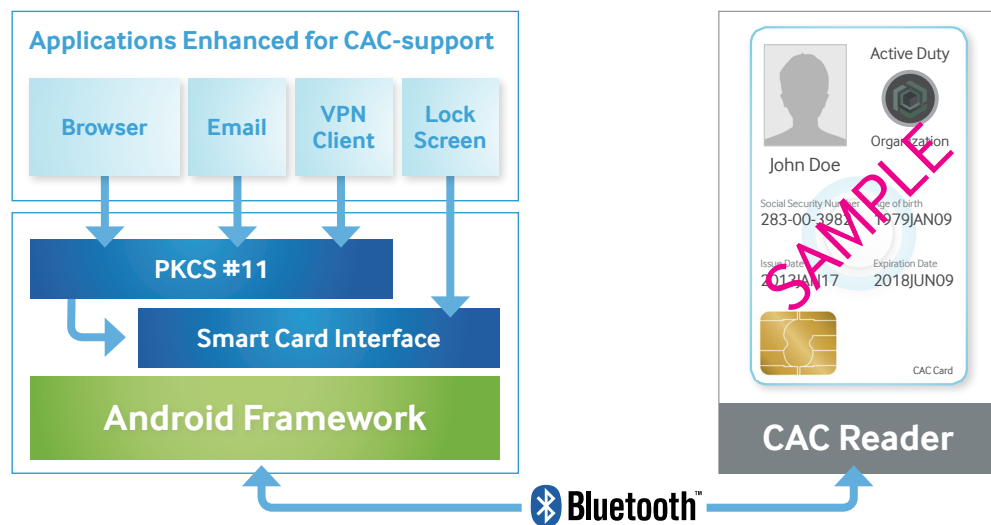


Figure 9 – Samsung KNOX Support for CAC

## 3. Certification & Validations

- FIPS 140-2 Certification
- DISA MOS SRG Compliance

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). The Samsung KNOX support for DIT covers the following:

- Web browser (HTTPS)
- Email (S/MIME)
- IPSec VPN

## 3. Certification & Validations

- FIPS 140-2 Certification
- DISA MOS SRG Compliance

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.

## Summary

---

Reasons cited by CIOs for the poor acceptance of Android in the enterprise stem primarily from concerns over the current state of security in the platform, as well as the lack of management policies. For example, attacks against mobile devices and especially Android devices have been increasing at an alarming rate:

- In their “2012 Q2 Threats Report”, McAfee, a leading security technology company, has discovered nearly 13,000 different types of mobile malware in 2012, up from 2,000 in 2011. They also announced that Android malware reports nearly doubled in Q3 2012 compared to Q2 2012.
- Trend Micro, in their “5 Predictions for 2013 and Beyond” report for small/medium businesses (SMBs), estimates that the number of malicious and high-risk Android applications will increase three-fold from about 350,000 in 2012 to more than 1 million in 2013.

Furthermore, as more and more employees are bringing their own devices to work (BYOD), IT administrators are concerned about the increased risk to corporate data and network resources:

- In a survey of 500 leading British CIOs by Virgin Media Business, 51% indicated their secure IT network was breached due to employees using personal services. In addition, smaller businesses experienced 25% less breaches of security compared to larger organizations.

With its multi-tiered security model and industry-leading device management capability, Samsung KNOX fully addresses the shortcomings of the open source Android platform for broad enterprise adoption.

- The enhanced security at the operating system level provided by Customizable Secure Boot\*\*, Security Enhancements for Android, and TIMA protect against malware attacks and hacking.

\*\*Customizable Secure Boot availability varies depending on hardware specification

- Samsung KNOX Container allows enterprises embracing the BYOD trend to create a secure zone in the employee’s device for corporate applications. Access to corporate data and network resources can be restricted to applications within the container.
- The rich set of MDM policies enables IT administrators to better manage their employees’ devices and offer improved support by being able to remotely configure various features including Wi-Fi, VPN and email.

## 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](http://www.samsung.com)

For more information about Samsung KNOX,  
Visit [www.samsung.com/knox](http://www.samsung.com/knox)

Copyright © 2013 Samsung Electronics Co. Ltd. All rights reserved. Samsung is a registered trademark 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. 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