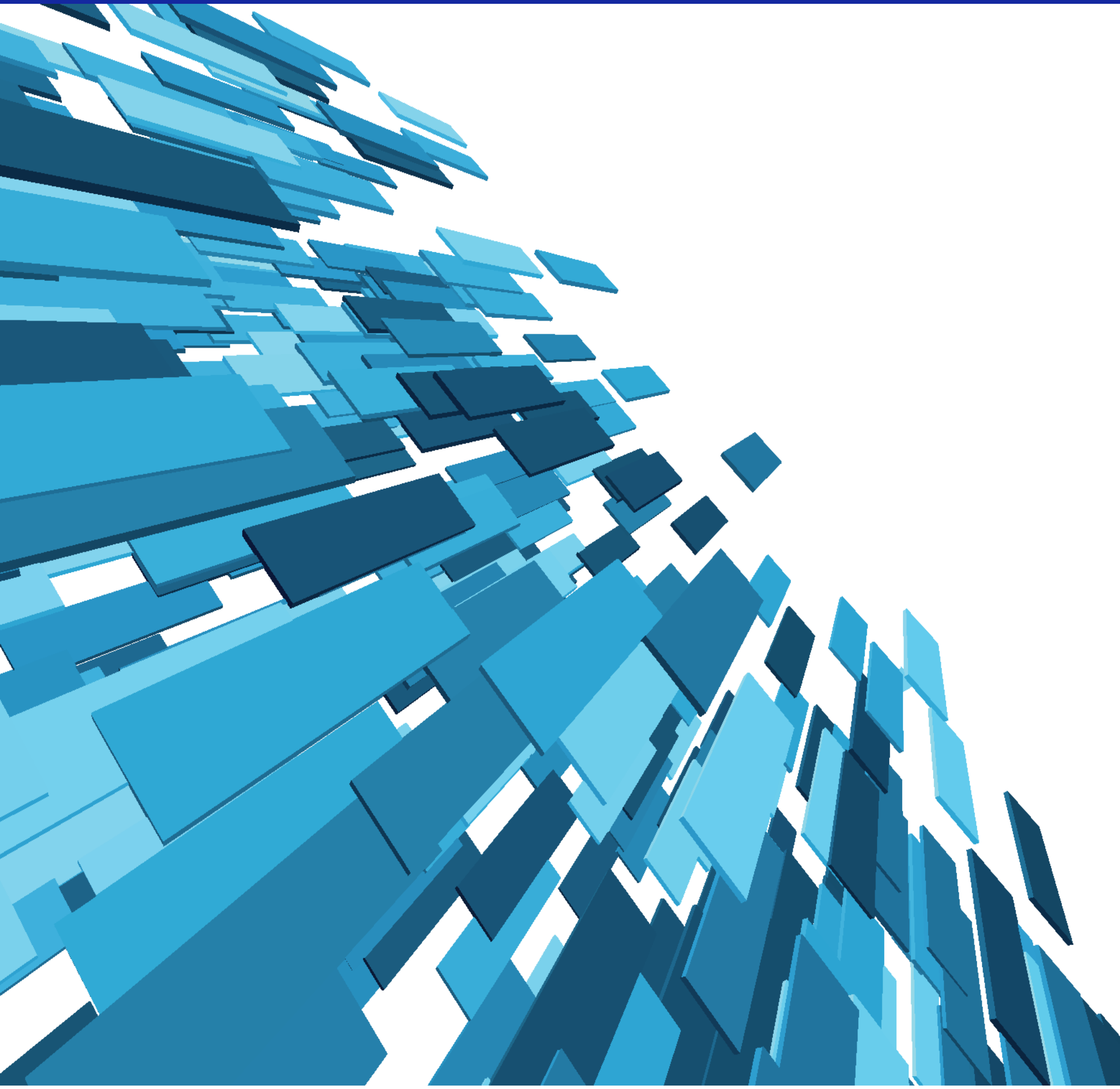
Whitepaper

The Samsung Knox™ Platform



August 2016
Samsung Electronics Co., Ltd.

Table of Contents

Samsung Knox^{TM} Platform

Knox is Samsung's defense-grade mobile security platform built into our devices. Simply turn on the device, and you're protected.

Knox provides strong guarantees for the protection of enterprise data by building a hardware-rooted *trusted environment*. A trusted environment ensures that enterprise-critical operations, such as decryption of enterprise data, can only occur when core system components are proven to be uncompromised. For many pieces of device software, such as the kernel and TrustZone apps, this is done by checking the cryptographic signature of each piece of software. A trusted environment is hardware-rooted if both the cryptographic keys and code used to compute these signatures are tied back to unmodifiable values stored in hardware.

Key features of Knox include Secure Boot, Trusted Boot, ARM® TrustZone®-based Integrity Measurement Architecture (TIMA), Security Enhancements for Android (SE for Android), and TrustZone-based Security Services.

The Knox Workspace container is designed to separate, isolate, encrypt, and protect work data from attackers. This enterprise-ready solution also provides management tools and utilities to meet security needs of enterprises large and small.

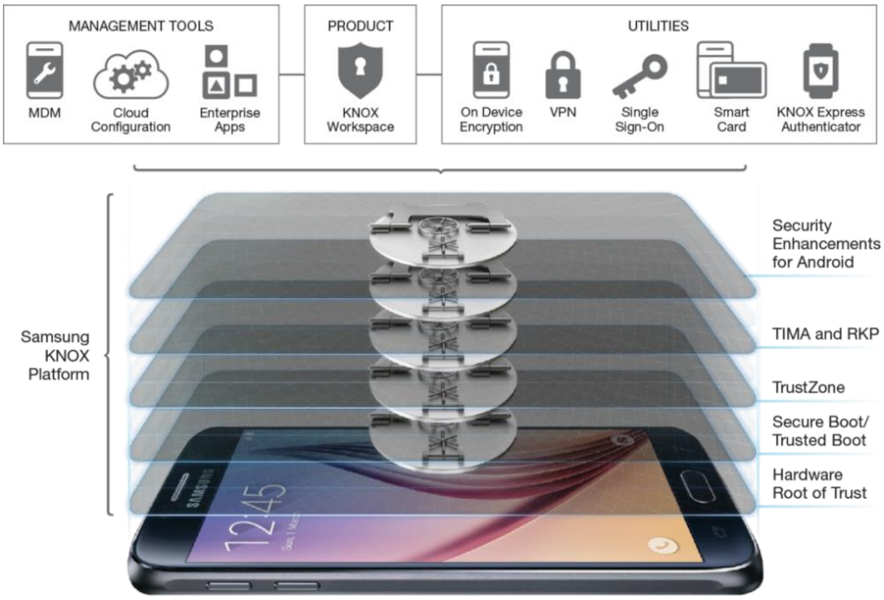


Figure 1 – Samsung Knox Platform, Workspace, Management Tools and Utilities

Technology Overview

This section describes the technical aspects of three key pillars of Samsung Knox platform including Platform Security, Application Security, and Mobile Device Management.

Platform Security

Samsung Knox addresses security using a comprehensive, hardware-rooted trusted environment including Hardware Root of Trust, Secure Boot and Trusted Boot, Security Enhancements for Android (SE for Android), TrustZone-based Integrity Measurement Architecture (TIMA), and TrustZone-based Security Services.

Hardware Root of Trust

Three hardware components are the foundation of Samsung Knox's trusted environment.

The Device Root Key (DRK) is a device-unique asymmetric key that is signed by Samsung through an X.509 certificate. This certificate attests that the DRK was produced by Samsung. The DRK is injected in the device during the manufacturing process in the Samsung factory, and is only accessible by specially privileged software modules within the TrustZone Secure World. Because the DRK is device-unique, it can be used to identify a device. For example, a certificate included with TIMA attestation data is signed by DRK (more precisely, through a key attested by the DRK), which proves that the attestation data originated from the TrustZone Secure World on a Samsung device. Knox also uses device-unique hardware keys and keys derived from the hardware keys, which are only accessible in the TrustZone Secure World. Such keys can be used to tie data to a device. Knox Workspace data, for example, is encrypted using such a key, and cannot be decrypted on any other devices.

The Samsung Secure Boot key is used to sign Samsung-approved executables of boot components. The public part of the Samsung Secure Boot key is stored in hardware at the time of manufacture in the Samsung factory. The Secure Boot process uses this public key to verify whether each boot component is approved.

Rollback prevention fuses are hardware fuses that encode the minimum acceptable version of Samsung-approved executables. Because old images may contain known vulnerabilities that can be exploited, this feature prevents approved-but-old versions of boot executables from being loaded.

Secure Boot and Trusted Boot

The startup process for Android begins with the primary bootloader, which is loaded from Read-only Memory (ROM). This code performs basic system initialization and then loads another bootloader, called a secondary bootloader, from the file system into Random-Access Memory (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 last bootloader (sometimes known as *aboot)*, which loads the Android kernel.

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 signature of the next bootloader in the sequence using a certificate chain that has its root-of-trust resident in hardware. The boot process is terminated if verification fails at any step.

Secure Boot is effective in preventing unauthorized bootloaders (and sometimes the kernel when it is also applied to the kernel binary). However, Secure Boot is unable to distinguish between different versions of authorized binaries, for example, a bootloader with a known vulnerability versus a later patched version, since both versions have valid signatures.

Samsung Knox implements Trusted Boot (in addition to Secure Boot) to address this limitation. 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 cryptographic keys from the TIMA KeyStore, container activation, and so on.

Additionally, if the final 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 Android kernel is restored to its original factory state, this evidence of tampering remains. However, the boot process is not halted, and the final bootloader continues to boot the Android kernel. This process ensures that normal operation of the device is not affected.

Security Enhancements for Android

Samsung Knox introduced Security Enhancements for Android (SE for Android) in 2012 to enforce Mandatory Access Control (MAC) policies. These Android enhancements, and the security policies we enforce, protect applications and data by strictly defining what each process is allowed to do, and which data it can access. Samsung remains the leader in SE for Android experience and continues to add features to protect sensitive data and actions without negatively impacting user productivity.

Samsung has also built an innovative global policy validation system that can detect when prohibited actions are attempted on Samsung devices. This data gives us unique visibility into how our devices are used and can alert us to new threats. Determining which usage patterns are benign or malicious helps us to refine our security policies for best security and performance.

The Security Enhancements for Android Management Service (SEAMS) provides Application Programming Interface (API)-level control of the SE for Android policy engine. The SEAMS APIs allow software protection to be tailored for each organization by allowing dynamic creation of security containers to isolate applications and their data.

TrustZone-based Integrity Measurement Architecture

The system protection offered by SE for Android relies on the assumption of Operating System (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 detect malicious attacks that corrupt them and potentially disable SE for Android.

Real-time Kernel Protection (RKP)

RKP performs ongoing, strategically-placed real-time monitoring of the operating system to prevent tampering with the kernel. RKP intercepts critical kernel events, which are then 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 alert that tampering is suspected. This alert information is included in remote attestation results sent to the MDM for IT Admins to determine any further actions required by the enterprises security policies. This protects against malicious modifications and injections to kernel code, including those that coerce the kernel into corrupting its own data. RKP checks are performed in an isolated environment that is inaccessible to the kernel, so potential kernel exploitations cannot be extended to compromise RKP. Depending on the device model, this isolated environment can be in the TrustZone Secure World or the hypervisor extensions.

Remote Attestation

Remote Attestation (sometimes simply called attestation) is based on Trusted Boot and used to verify the integrity of the platform. Remote attestation can be requested on-demand by the enterprise's Mobile Device Management (MDM) system, typically before creating the Knox Workspace.

When requested, attestation reads the Trusted Boot collected measurement data and returns them to the attestation requestor. To simplify the handling in MDM servers, the attestation agent on the device produces a verdict indicating the overall status of attestation. It compares these measurements to the factory values inside the TrustZone Secure World. Trusted Boot measurement data includes a hardware fuse value that indicates if the device booted into an unauthorized kernel in the past. Trusted Boot measurement data, along with the SE for Android enforcement setting, forms the basis of the produced attestation verdict. This verdict, essentially a coarse indication that tampering is suspected, is returned to the requesting MDM. In addition to the verdict, the attestation data includes all the trusted boot measurements, RKP and PKM logs that can indicate the presence of malicious software in the device, and other device information that can be used to bind the attestation result to the device.

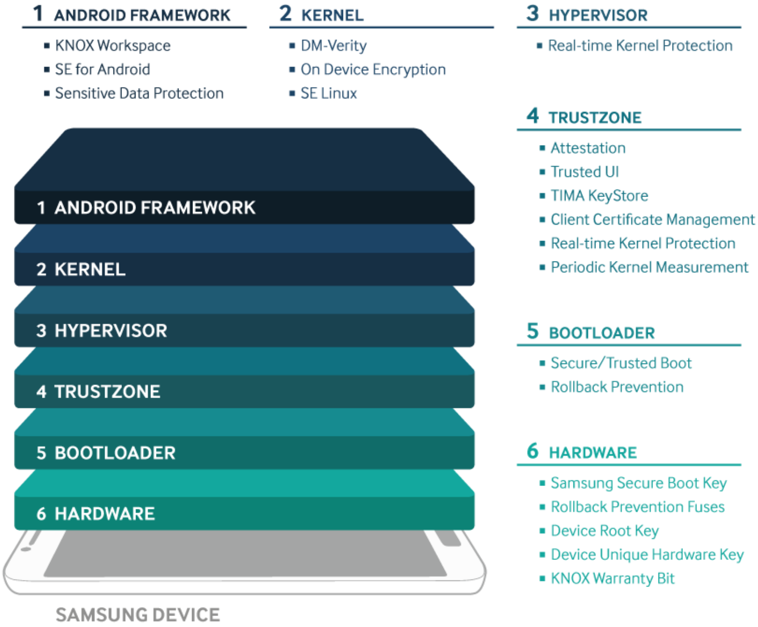


Figure 2 – Samsung Knox Platform Security Overview

TrustZone-based Security Services

TrustZone-based Client Certificate Management (CCM)

TIMA CCM is a TrustZone-based security service also built on the basis of Trusted Boot. A key feature of TIMA CCM is that if the Trusted Boot measurements do not match the authorized values, or if the Knox warranty bit is voided, the entire TIMA CCM functions shut down, ensuring the protection of enterprise data in case of device compromise. TIMA 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 CCM TrustZone code provides a PKCS #11 interface to the Android OS, effectively emulating a smart card interface on a mobile device. The certificates and associated keys are encrypted with a device-unique hardware key that can only be decrypted from code running within TrustZone.

All cryptographic components used by CCM are FIPS-140 2 compliant to meet US government requirements for Mobile Device Fundamentals Protection Profile (MDFPP).

TrustZone-based KeyStore

Similar to TIMA CCM, TIMA KeyStore is a TrustZone-based security service also built on the basis of Trusted Boot. 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.

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 the enterprise IT Admin activates encryption via the MDM. This ensures that all device data is protected in the unlikely event that the operating system is compromised.

Application Security

In addition to securing the platform, Samsung Knox provides solutions to address the security needs of individual applications including Knox Workspace, Virtual Private Network support, and Single Sign-on.

Knox Workspace

Samsung Knox Workspace is a defense-grade dual persona container product designed to separate, isolate, encrypt, and protect enterprise data from attackers. This work/play environment ensures work data and personal data are separated and that only the work container is managed by the enterprise. Personal information such as photos and messages are not managed or controlled by the IT department. Once activated, the Knox Workspace product is tightly integrated into the Knox platform.

Applications and data inside Workspace are isolated from applications outside Workspace, that is, applications outside Workspace cannot use Android inter-process communication or data-sharing methods with applications inside Workspace. For example, photos taken with the camera inside Workspace are not viewable in the Gallery outside Workspace. IT Admins can allow or prevent the ability to copy and paste between Workspace and the personal side of the device. When allowed by IT policy, some application data such as contacts and calendar data can also be shared across the Workspace boundary. The end user can choose whether to share contacts and calendar events between Workspace and personal space; however, IT policy ultimately controls this option. The enterprise can manage Workspace like any other IT asset using an MDM solution. This container management process is called Mobile Container Management (MCM). Samsung Knox supports many of the leading MDM solutions on the market. MCM is affected by setting policies in the same fashion as traditional MDM policies. Samsung Knox Workspace includes a rich set of policies for authentication, data security, VPN, e-mail, application blacklisting, whitelisting, and so on.

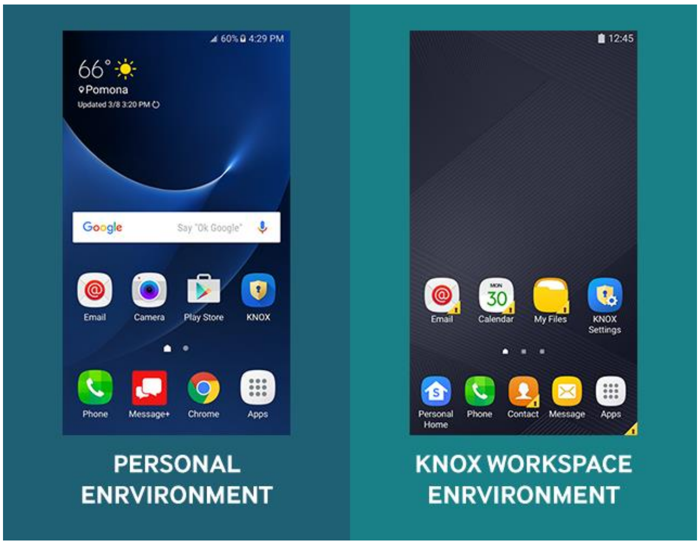


Figure 3 – Samsung Knox Personal Environment and Knox Workspace Environment

Google Play for Work

IT Admins can install Google Play for Work inside Knox Workspace for app management to silently install and uninstall apps and blacklist or whitelist apps. Enterprise employees can download apps in Knox Workspace that are approved by IT Admins.

Sensitive Data Protection

Knox defines two classes of data – protected and sensitive. All data written by apps in the secure Workspace is protected. Protected data is encrypted on disk when the device is powered off. In addition, the decryption key for protected data is tied to the device hardware. This makes protected data recoverable only on the same device. Furthermore, access controls are used to prevent applications outside the Knox Workspace from attempting to access protected data.

Even stronger protection is applied to sensitive data. Sensitive data remains encrypted as long as the Workspace is locked, even if the device is powered on. When a user unlocks Knox Workspace using their password, Sensitive Data Protection (SDP) allows sensitive data to be decrypted. When the user re-locks the Workspace, SDP keys are cleared. The SDP data decryption key is tied to both device hardware and to the user input. Therefore, the data is recoverable only on the same device and with user input.

SDP can be used in one of two ways. First, all emails received are considered sensitive, and are immediately protected by SDP encryption. Emails received when the Workspace is locked, are immediately encrypted, and can only be decrypted the next time Workspace is unlocked.

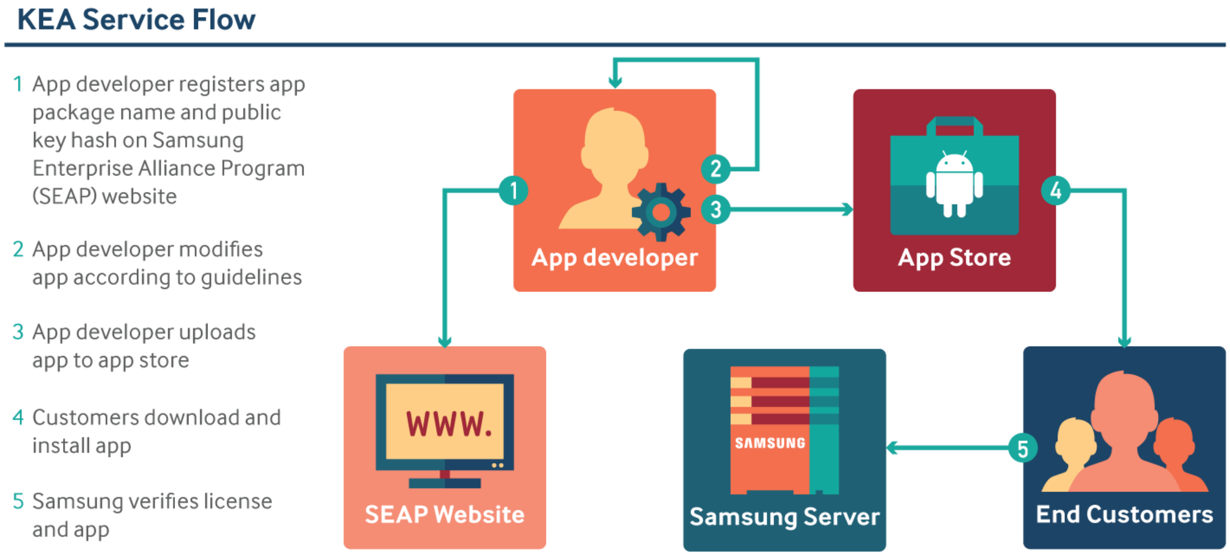
Knox Enabled App (KEA)

Knox Enabled App is a per-app invisible container designed for application developers and vendors to provide security services to Samsung device users. KEA allows service providers to deploy their applications and make maximum use of the Samsung Knox platform security without the need for Mobile Device Management (MDM). Since KEA is an invisible, unmanaged container, the user experience is the same as the original version of the application. Knox platform security extended to KEA provides end users data protection by encrypting app data. If a device is compromised, lost, or stolen, app data cannot be unencrypted.

The KEA workspace is implemented based on Knox Workspace and customized according to use case requirements. Knox Workspace is created and managed by an MDM, and suitable for the enterprise environment. For individual app vendors and developers, creating, managing and configuring the KEA workspace presents challenges without an MDM. However, with KEA, the device automatically creates and manages the KEA workspace when the KEA app is installed.

To operate as a KEA app, additional information (metadata) is required. When a KEA app is installed in KEA-capable devices, the device detects the metadata and authenticates the app through a Knox License Manager (KLM) Server. After authentication is completed, the KEA workspace is created, and the app is installed inside the workspace, including configuration of the SE for Android Management Service (SEAMS) container.

If the KEA app is installed in devices not capable of using KEA, including non-Samsung devices, the KEA metadata is ignored, and the app works as regular Android app, which eliminates the need for a separate version of the app.



KEA Service Flow

1 App developer registers app package name and public key hash on Samsung Enterprise Alliance Program (SEAP) website

2 App developer modifies app according to guidelines

3 App developer uploads app to app store

4 Customers download and install app

5 Samsung verifies license and app

Figure 4 – Service flow of Knox Enabled Apps

Virtual Private Network Support

The Knox 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.

Knox offers the following VPN features for IPsec and SSL:

- Per-app connections
- On-demand connections
- Always-on connections
- Device-wide connections
- VPN chaining (nested connections)
- Blocking routes to prevent data leakage if a mandatory VPN connection drops
- Pushing VPN profiles to multiple managed devices
- Traffic usage tracking
- HTTP Proxy over VPN

Single Sign-On

Single Sign-On (SSO) is a feature that provides common access control to 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 example, SSO allows access to the Workspace container (and participating apps that require credentials within the container) with one password.

Mobile Device Management

Enrolling mobile devices into the enterprise network and remote management of these devices are key aspects of an enterprise mobility strategy. Key device management features of the Knox platform include comprehensive management with over 1500 MDM APIs, Active Directory integration, Knox Mobile Enrollment, and Enterprise Billing.

Comprehensive Management Policies

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. Furthermore, no runtime license fee is associated with these APIs.

The Knox Premium Policy suite is the collection of policy groups offering advanced capabilities such as management and control of the Knox Workspace, security features such as the Trusted Boot-based TIMA 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. The Knox Audit Log meets MDFPP 2.0 audit requirements. IT Admins can select a set of events to audit and periodically push logs to the server.

Active Directory integration

Knox provides an option for the IT Admin to choose an Active Directory password as the unlock method for Knox containers. This has two important benefits. First, it allows IT Admins to use a one-password management policy for desktop and mobile devices. Second, the end user only needs to remember one password to access all services offered by the employer, thereby reducing employee password fatigue and improving productivity.

Knox Mobile Enrollment

The Knox platform provides a simplified enrollment solution for supported MDMs that is streamlined and intuitive and eliminates many steps and human error.

The enrollment process happens via either self-discovery using an email domain, or employees are provided 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.

Samsung Knox Mobile Enrollment allows IT Admins to enroll hundreds or thousands of employees at the same time. Samsung provides a web tool and an application to scan package bar codes (the device IMEI). This enrollment method is targeted for devices purchased for COPE enterprises and for supported carriers and resellers.

Another option for IT Admins includes using a master device to automatically enroll devices using NFC. The master device is configured by downloading an app from the Google Play^{TM} store.

Enterprise Billing

Enterprise Billing provides enterprises a mechanism to separate enterprise data usage from personal data usage. This enables enterprises to compensate their employees for costs generated because of work, particularly in BYOD cases, or to pay only for work-related data in COPE cases.

The Knox platform supports Enterprise Billing from Knox version 2.2 or above, and requires MDM support. Enterprises configure two Access Point Name (APN) gateways. One APN is for data associated with enterprise-approved apps, and a different APN is for all other personal data. Enterprises must first register with a network operator’s enterprise billing service. Once a new APN is provisioned for business use, Knox Workspace can be enabled for that dedicated APN. IT Admins can also select individual apps inside or outside Workspace to use data over the enterprise APN.

The enterprise APN can also be configured to allow or not allow roaming. When roaming is enabled, personal data is routed through the default APN, and enterprise data is routed through a dedicated enterprise APN. By default, roaming over the enterprise APN is disabled. When a user is roaming in a single Packet Data Protocol (PDP) network, all enterprise apps are automatically routed to the personal APN for work continuity.

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 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. DISA approved the STIG for Samsung Knox 2.x.
DISA Approved Product List	DISA has approved select Knox-enabled devices to the US DoD Approved Products List (APL). Note: Select Samsung Knox-enabled devices and tablets are certified under the National Information Assurance Partnership (NIAP) Common Criteria (CC) Mobile Device Fundamental Protection Profile (MDFPP).
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. The current CC certification targets the new Mobile Device Fundamentals Protection Profile (MDFPP) of the National Information Assurance Partnership (NIAP), which addresses the security requirements of mobile devices for use in enterprise. Samsung Knox is approved by the United States government as the first NIAP-validated consumer mobile devices to handle the full range of classified information.
ANSSI	Samsung Knox has obtained first-level security Certification Sécuritaire de Premier Niveau (CSPN) from the Agence nationale de la sécurité des systèmes d'information (ANSSI). The CSPN methodology and criteria is defined by ANSSI with evaluations run by ANSSI accredited testing labs.
ISCCC	Samsung Knox received the security solution certificate by the China Information Security Certification Center (ISCCC). Samsung worked closely with ISCCC to develop the certification process, including device requirements and security standards. By securing the critical ISCCC certification, Samsung has a stronger foothold to garner mobile device contracts with China's regulated industries, including government authorities, ministries, and finance.
CSfC	Fifteen Samsung devices have been listed in the NSA/CSS's Commercial Solutions for Classified Program (CSfC) for approved security components.
CESG Approved	The Communications and Electronic Security Group (CESG) approved Knox-enabled Android devices for United Kingdom government use.
FICORA	Samsung devices with Knox fulfill national security requirements as defined by the Finnish National Security Auditing Criteria (KATAKRI II).
ASD	Australian Signals Directorate: ASD endorsing the Protection Profile for Mobile Device Fundamentals as well as recognizing evaluations against this Protection Profile.

Note: For the most recent updates to Samsung Knox certifications, see the following link: https://www.samsungKnox.com/en/security-certifications

About Samsung Electronics Co. Ltd.

Samsung Electronics Co., Ltd. inspires the world and shapes the future with transformative ideas and technologies that redefine the worlds of TVs, smartphones, wearable devices, tablets, cameras, digital appliances, printers, medical equipment, network systems, and semiconductor and LED solutions. We are also leading in the Internet of Things space with the open platform SmartThings, our broad range of smart devices, and through proactive cross-industry collaboration. We employ 319,000 people across 84 countries with annual sales of US $196 billion. For more information, please visit www.samsung.com.

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

Author	Version	Date
Knox@samsung.com	V1.02	August 1, 2016
Knox@samsung.com	V1.01	July 5, 2015
Knox@samsung.com	V1.0	April 26, 2016