SAMSUNG Knox

White Paper: An Overview of the Samsung Knox™ Platform

December 2016

Samsung Research America
Samsung Electronics Co., Ltd.

SAMSUNG

Contents

Acronyms

AES	Advanced Encryption Standard
AOSP	Android Open Source Project
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
KEA	Knox Enabled App
MAC	Mandatory Access Control
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology
ODE	On-Device Encryption
OS	Operating System
PKCS	Public Key Cryptography Standards
RAM	Random-Access Memory
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

Samsung Knox™ Platform

Knox is Samsung's defense-grade mobile security platform built into our newest devices. Just 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 not be compromised. 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 provides management tools and utilities to meet security needs of enterprises large and small.

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

SAMSUNG

Technology Overview

This section describes the technical aspects of three key pillars of Samsung Knox platform:

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

Platform Security

Samsung Knox addresses security using a comprehensive, hardware-rooted trusted environment:

- Hardware Root of Trust
- Secure Boot and Trusted Boot
- Security Enhancements for Android (SE for Android)
- TrustZone-based Integrity Measurement Architecture (TIMA)
- 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 at manufacture time 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. For example, Knox Workspace data is encrypted by such a key, and it 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 manufacture time in the Samsung factory. The Secure Boot process uses this public key to verify whether each boot component it loads is approved.

Rollback prevention fuses are hardware fuses that encode the minimum acceptable version of Samsung-approved executables. These fuses are set at manufacture time in the Samsung factory. 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 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 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. In addition, when some carriers decide to allow custom kernels to run on their devices, Secure Boot is not effective in preventing non-Samsung kernels from running on these devices. This exposes an attack surface that poses a potential threat to enterprise applications and data.

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 *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.

Security Enhancements for Android

Samsung Knox introduced Security Enhancements for Android (SE for Android) in 2012 to enforce Mandatory Access Control (MAC) policies. These enhancements protect applications and data by strictly defining what each process is allowed to do, and which data it can access. Samsung's innovative collaborations with the authors of SELinux resulted in the gold standard for Android security. In version 4.4 of Android Open Source Project (AOSP), Google introduced a subset of the SE for Android enhancements Samsung pioneered (i.e., the SELinux portion). Samsung continues to lead Google, and all others, in continuing to implement new extensions of SE for Android. Our improvements allow us to protect areas of the Android framework to which access was previously unrestricted. Our policy protects software created by Samsung, AOSP, and other third-party partners. The increased

enforcement granularity from our AOSP enhancements, and Samsung's industry-leading granular access policies that define over 200 unique security domains, are designed together to enforce the tightest restrictions with the lowest rates of over- or under-privileging.

Samsung also built an innovative global policy validation system that can detect when prohibited actions are attempted. This gives us unique visibility into how our devices are used and can alert us to new threats. This system can be used to refine our policy and very accurately grant only the minimum permissions needed.

The Knox platform now includes the SE for Android Management Service (SEAMS) that provides Application Programming Interface (API)-level control of the security policy engine. SEAMS is primarily used internally by the Knox Workspace container, but is also available to third-party vendors to secure their own container solutions. The SEAMS APIs allow software permissions to be tailored for each organization. Leveraging our controls to define and protect security containers allows customers to dynamically isolate applications and data. Our containers use new SE for Android Multi-Level Security (MLS) protections designed to offer far more protection than any other existing Android isolation mechanism.

Our enhancements to Android, along with our robust policy, security tools, data collection, and policy management show that Samsung Knox devices are designed to provide the best protections of any mobile device manufacturer. These protections form a foundation for protecting users from malicious or accidental security breaches.

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 of 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.

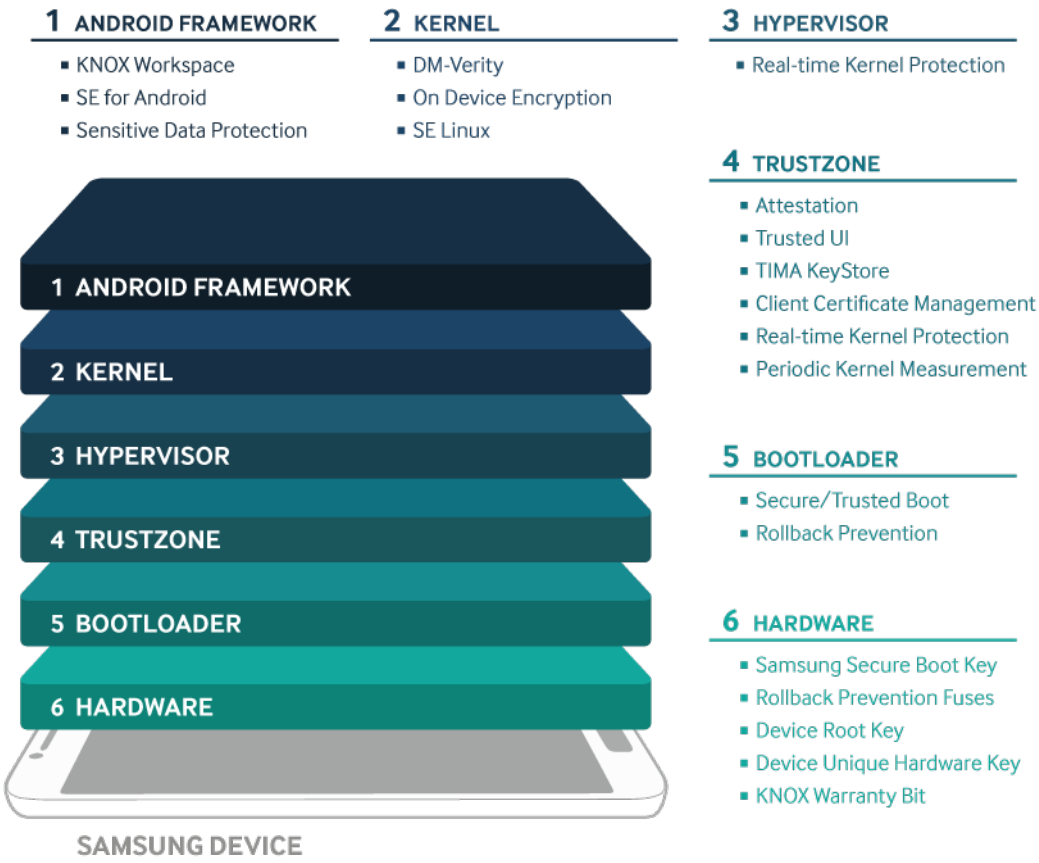

Figure 2 – Samsung Knox Platform Security Overview

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.

The remote server requesting attestation provides a random nonce to prevent replay attacks. The nonce, the attestation verdict, and the rest of the attestation data are returned to the server, signed with the attestation certificate. The attestation certificate is signed by the Device Root Key (DRK), a device-unique asymmetric key that is signed by a Samsung root key through an X.509 certificate. This chain of certificates ensures that the attestation verdict cannot be altered in transit.

Depending on the attestation verdict and the data, 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.

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.

TIMA CCM 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. TIMA CCM supports the standard Android Key Chain API, and apps can use CCM by calling APIs that configure Android to use an alternate Key Chain Provider.

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.

TIMA KeyStore supports the Android Key Store API. Application developers can continue to use the familiar Android KeyStore APIs and specify that the TIMA KeyStore is used to provide the service.

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:

- Knox Workspace
- Virtual Private Network Support
- SmartCard Framework
- 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.

Workspace provides this separate environment within the mobile device, complete with its own home screen, launcher, applications, and widgets.

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. The same restriction applies to copying and pasting. When allowed by IT policy, some application data such as contacts and calendar data can be shared across the Workspace boundary. The end user can choose whether to share contacts and calendar notes 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.

The Knox 2.X platform features the elimination of application wrapping, which was used by Knox 1.0 and many other competing solutions. This is achieved by leveraging technology

introduced by Google in Android 4.2 to support multiple users on devices. It reduces the barrier to entry for independent software developers wishing to develop and deploy applications for Knox Workspace.

At the time of container creation, IT admins can choose the UI style of the container (folder or launcher style), and can also prevent end users from changing the style.

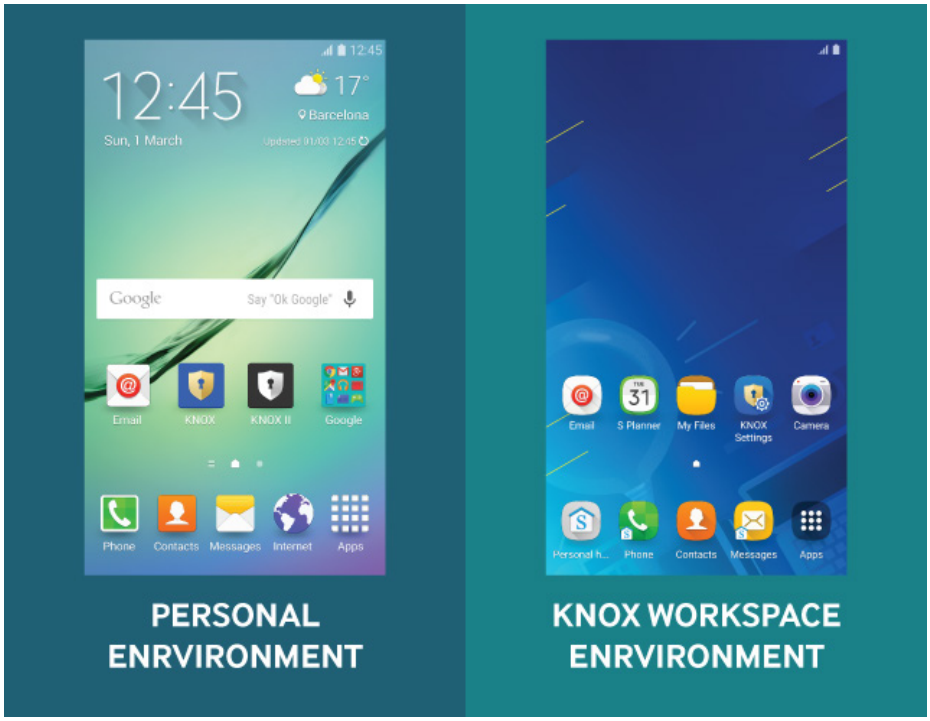

Figure 3 – Samsung Knox Personal Environment and Knox Workspace Environment

My Knox

Samsung My Knox is a free security solution that provides greater separation between enterprise and personal data. In My Knox, you can create a container that only authorized personnel can access. All files and data are encrypted within the container. My Knox is a virtual Android environment within the mobile device complete with its own home screen, launcher, apps, and widgets.

My Knox is not managed by an IT admin or an MDM, but separates work and the personal side of the phone. You can back up data stored on your device to the cloud and restore it to your device when needed.

Knox Workspace can also be configured for container-only mode. In this mode, the entire device experience is restricted to the Workspace. This mode is suitable for industries such as health care, finance, and others who provide devices for employees that seek to restrict access to business applications.

Workspace also has a two-factor authentication process. The user can configure Workspace to accept a fingerprint as the primary authentication factor for the container with a PIN, password

or pattern as a second factor.

The Knox platform also supports two containers, thus meeting the needs of professionals that use their own devices for corporate use Bring Your Own Device (BYOD) and have multiple employers, such as doctors or consultants.

IT admins can also enable Bluetooth® and Near Field Communication (NFC) inside Workspace. NFC enables a device to act as a SmartCard-based credential for use cases such as physical access and access to IT accounts. Bluetooth can be used to communicate with connected devices, and supports Bluetooth profiles that enable use cases beyond music and calls inside the Knox Workspace. Examples include printing, file sharing, and external card readers. External SD cards can also be enabled with security restrictions.

Apps inside Workspace can also connect with USB accessories such as a USB printer. For security purposes, IT admins must explicitly allow USB between container apps and external storage. The MDM default for mass storage is set to OFF, and is controlled by enterprise IT admin policy.

For Samsung Note users, S-Pen Air Command is also supported inside Workspace for writing memos, adding app shortcuts (personal apps only), screen capture, and writing notes on a screen capture (depending on IT policy).

Knox caller ID for incoming calls when in Personal mode can also be configured by IT admins to display caller ID information derived from personal contacts and Knox Workspace contacts.

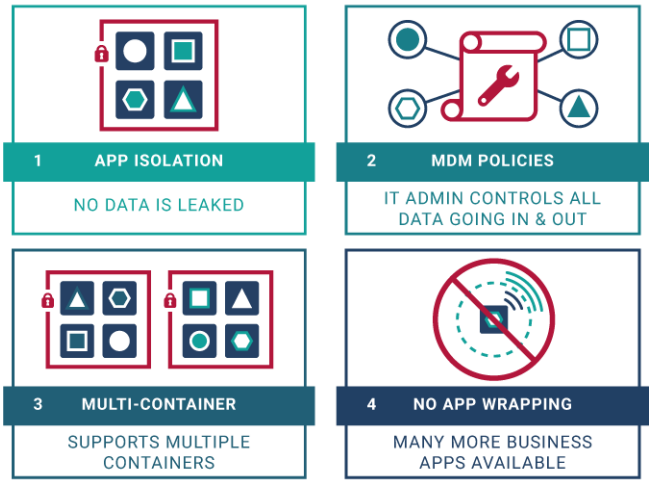

Figure 4 – Samsung Knox Workspace

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.

Google Voice for apps inside the Knox container allows users to use voice recognition for input

in addition to the touchscreen keyboard.

Sensitive Data Protection and Knox Chamber

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.

The second way to use SDP is through the Knox Chamber. The Chamber is a designated directory on the file system and a user-accessible folder inside Workspace. Any data placed into the Chamber is automatically marked as sensitive and protected by SDP.

Third-party app data can also be encrypted when a device is locked and decrypted when a device is unlocked to prevent data leakage if a device is lost, stolen, or re-used. Keys required for data decryption when unlocking a device are based on the user password.

Knox Quick Access

On Samsung Galaxy S6 devices, based on proximity of a registered and connected Gear device, Knox Quick Access extends the unlock period of the Knox Workspace, thereby reducing the frequency with which the end user must enter password credentials.

Shared device

Many enterprises such as hospitals, banks, and airlines use shared devices for employees. Knox supports the use of shared devices so IT admins can manage device and security policies, and install apps with an MDM. Each employee can login separately with an Active Directory ID and password, which is also integrated with SSO. For security and privacy, all user data is deleted when each employee logs out of the shared device.

Knox Active Protection (KAP)

End users can activate or deactivate Knox Active Protection (KAP) via the Smart Manager app on devices not managed by an MDM. KAP uses both Real-time Kernel Protection (RKP) and DM Verity, a feature that provides integrity checking for system code and data. On MDM-managed devices, KAP is always enabled.

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.

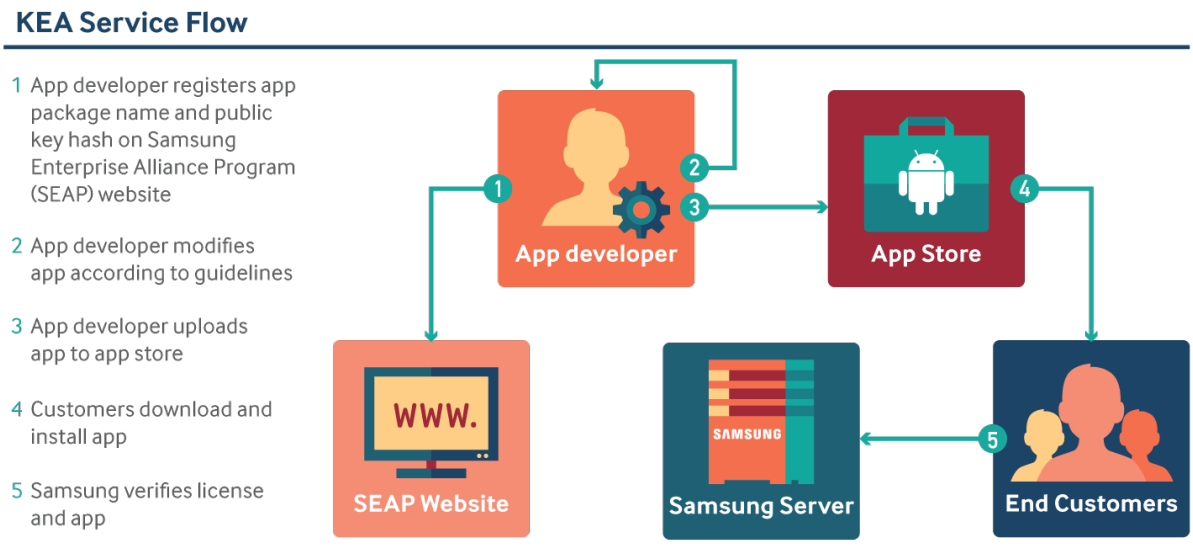

Figure 5 – Service flow of Knox Enabled Apps

Android for Work on a Samsung device

Android for Work Managed Profiles on a Samsung device benefit from key Knox security modules that protect the device and sensitive work data at all times. Knox enables Android for Work protection with the following Knox features:

- RKP actively prevents kernel code modification
- PKM periodically checks kernel code integrity
- DM-Verity verifies the integrity of applications and data stored on the critical system partition
- Trusted Boot measures each software component during boot-time and securely stores the cryptographic hash of the next component in TrustZone memory before loading it.
- Sensitive Data Protection APIs are available for apps in Managed Profiles. The native email app enables SDP once it's installed inside Managed Profiles.
- TIMA and CCM provides the TrustZone-based KeyStore as the default for storing certificates such as VPN and email app certificates.
- Access to Managed Profiles depends on the integrity of the device. If the integrity check fails at the time of creating Android for Work, it is not allowed. If an integrity check fails after Android for Work is installed, the device is not allowed to boot.

Android for Work on a Samsung device does not require a Knox license activation fee. Knox security enhancements for existing Android for Work Managed Profiles are updated seamlessly with Over-the-Air (OTA) updates.

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

Knox supports the ability to configure VPN connections to enforce redirection of web traffic through an HTTP proxy server, allowing enterprises greater visibility into network traffic and device usage patterns of employees. The Knox VPN framework supports VPN configurations using a static proxy server IP and port, and web proxy authentication.

The Knox platform offers broad feature support for the IPSec protocol suite including:

- Internet Key Exchange (IKE and IKEv2)
- IPsec IETF RFCs – IKEv1
- IKEv1 – Main and aggressive IKE exchange modes with pre-shared key, certificates, Hybrid RSA, and EAP-MD5 authentications
- I IKEv2 with PSK and certificate-based authentication
- IKEv2 – Pre-shared key, certificates, EAP-MD5 EAP-MSCHAPv2 authentication methods, and mobile extensions
- Triple DES (56/168-bit), AES (128/256-bit) encryption with MD5 or SHA
- IKEv1 Suite B Cryptography supported with PSK and ECDS signature-based authentications
- IKEv2 Suite B Cryptography supported with ECDSA signatures

Because a large number of enterprises have deployed Secure Socket Link (SSL) VPNs , the Knox platform provides support for leading SSL VPN vendors. As SSL implementations are proprietary, Knox features a generic VPN framework which enables third-party SSL vendors to provide their clients as plug-ins. Enterprise IT admins use Knox MDM policies to install and configure a specific SSL VPN client.

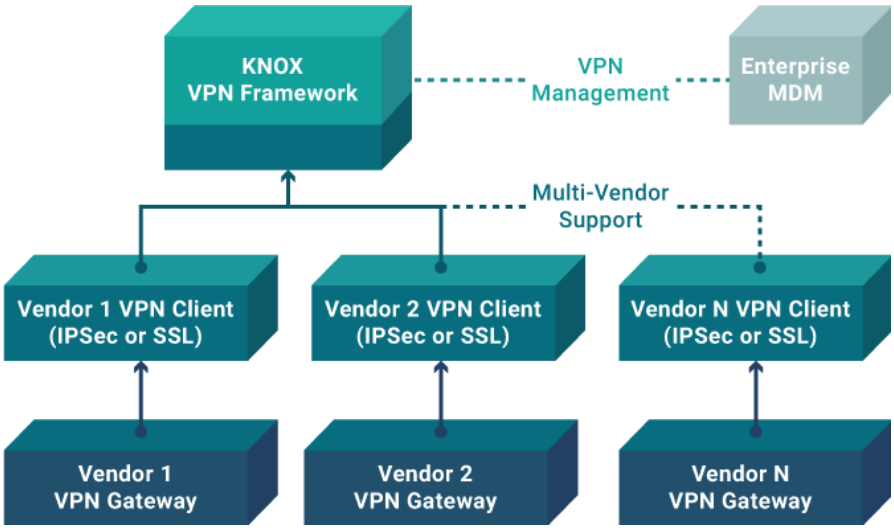

Figure 6 – Multi-Vendor Support in Knox

The per-application VPN feature in the Knox Workspace container enables the enterprise to automatically enforce the use of VPN only on a specific set of applications. For example, an IT admin can configure an employee's device to enforce VPN for only business applications. Such a configuration 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 enter the enterprise network.

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

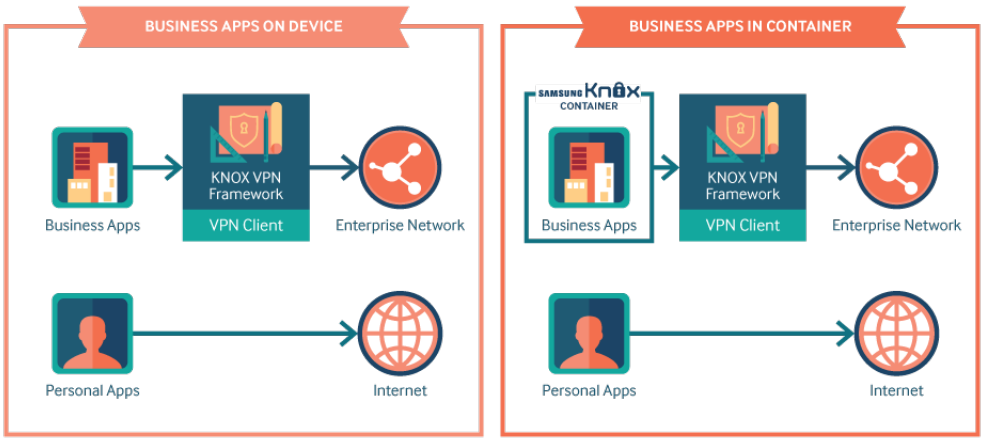

Figure 7 – Per Application VPN in Knox

SAMSUNG

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

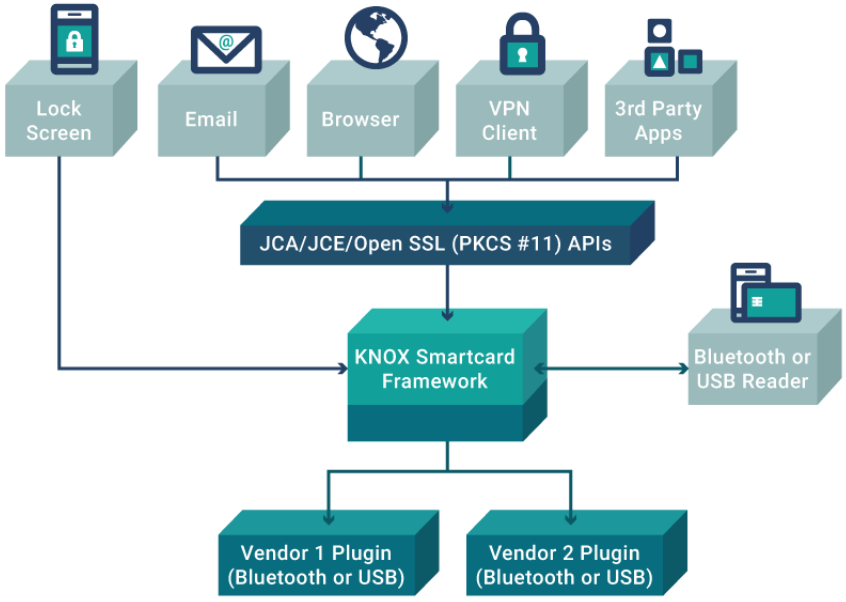

Figure 8 – Samsung Knox support for Smartcards

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.

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. SSO reduces the number of user names and passwords a user must remember, and reduces IT costs with fewer help desk calls about login credentials.

Knox Identity and Access Management (IAM) provides a comprehensive and flexible SSO solution to support enterprise applications on Samsung mobile devices. This framework was created to reduce the complexity for enterprise applications to support SSO on mobile devices. There are many Identity Providers with different SSO solutions and with various support protocols such as SAML, OAuth, OpenID, etc. They each distribute their Software Development Kits (SDKs) to mobile app developers, however, developers must customize multiple versions of their apps to support different SSO solutions.

The Knox generic SSO framework is a bridge between the Identity Providers and software developers that allows a single version of an app to work with any SSO solution. The Knox SSO solution provides a unified API for SSO token retrieval and management, called getToken. Samsung partners with leading Identity Partners including Microsoft (Azure Active Directory), CA Technologies, and Centrify. Identity Providers plug their Android Application Package (APK) authenticators into the Knox generic SSO framework and each authenticator works as a proxy to process SSO authentication requests and responses, thereby eliminating the need for developers to create multiple versions of their apps.

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 for a faster and intuitive user experience, including bulk enrollment to assist IT admins to quickly enroll many employees at once
- Enterprise Billing to separate work and personal data costs

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. Further, 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.

Some of the events include:

- Administrative actions such as creating containers, password setting policies for devices and containers, app installations and removal
- Certificate failure and key generation
- Adding and removing accounts
- Attempts to exchange files over Wi-Fi

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.

At the heart of this feature is the proven industry-standard Kerberos protocol. Active Directory is the most widely-deployed enterprise grade directory service that has built-in support for Kerberos. Knox provides a set of Workspace creation parameters to configure Workspace to use the Active Directory password as the unlock method. Additionally, IT admins can also configure Single Sign-on for services inside Workspace, along with the unlock method.

Active Directory passwords can be changed by the user on the mobile device from the settings menu inside the Knox Workspace container. When SSO is configured, the password change does not require entering the password a second time.

Knox Mobile 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 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 Playstore. Each device is enrolled to an MDM profile selected by the IT admin.

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.

Knox Mobile Enrollment supports multiple MDM configurations per account. With complex device environments, and multiple MDM profiles or configurations, Knox Mobile Enrollment gives IT admins the ability to prepare hundreds of devices and get them connected to the right MDM with ease. End users only need to turn on the device and connect to the network. Knox Mobile Enrollment takes care of activation without users needing to do a thing.

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 only pay 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.

Enterprise billing configured with a dedicated APN:

- Supports dual-APN Enterprise Billing for carriers using IPv6 networks.
- Separates data usage over the mobile internet for 2G/3G/4G connections
- Routes all data traffic from Knox Workspace over the enterprise APN
- Provides the capability to select individual apps inside or outside Knox 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.

If enterprise apps use a VPN connection to the network, the VPN profile can be configured to route data through the enterprise APN.

Dual SIM devices can also be enabled for Knox Enterprise Billing. The primary, or first SIM slot, is automatically selected to configure an APN and activate Enterprise Billing on the device.

To avoid personal use of a SIM card, IT admins can lock the SIM card with a unique PIN combination. This ensures that the SIM can only be used for enterprise billing on the authorized device. In addition, dedicated enterprise APNs are restricted, and APN settings are not visible or editable on the device.

Users can check personal and enterprise data usage on a Knox device in the Settings menu. To view data usage, employees can go to Settings > Data Usage > Mobile Tab (personal) or Enterprise Tab (work).

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.

Certifications

CSfC	Fifteen Samsung devices have been listed in the NSA/CSS's Commercial Solutions for Classified Program (CSfC) for approved security components.
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.
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

SAMSUNG

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

Version	Date
An Overview of the Samsung Knox Platform V2.1	Dec. 8, 2016
An Overview of the Samsung Knox Platform V2.0	Nov. 17, 2016
An Overview of the Samsung Knox Platform V1.15	August 1, 2016

SAMSUNG