KNOX 2.0: The evolution of enterprise mobility

Samsung KNOX continuously evolves to address enterprise mobility challenges

WORK SECURED
Constantly evolving mobile security with Samsung KNOX : Experience a more secure work environment and enhanced business performance.

Support business objectives with leading-edge core platform security, an improved user experience and an expanding ecosystem

In 2013, Samsung introduced the new comprehensive mobile security platform, Samsung KNOX. Samsung KNOX is designed to satisfy enterprise security requirements without compromising corporate security or employee privacy. In doing so, KNOX offers security for both platforms and applications.

KNOX platform and application security features include:

- **Trusted Boot.** Trusted Boot is a procedure that prevents unauthorized operating systems and software from loading during startup.
- **TIMA.** TrustZone-based Integrity Measurement Architecture (TIMA) provides continuous integrity monitoring of the Linux kernel.
- **SE for Android.** Security Enhancement (SE) for Android provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements.
- **KNOX Container.** KNOX Container provides a totally secure area in the device for business functions. Apps and data inside the container (for example, email, calendars and contacts) are completely isolated from the rest of the device and can't be shared with it.

KNOX 2.0 key enhancements

KNOX 2.0 represents a portfolio of multiple products and services designed to meet the rapidly evolving enterprise mobility needs of customers.

New and evolved features for the KNOX 2.0 platform include:

- **Cutting-edge core platform security.** KNOX Workspace offers TrustZone-Protected Certificate Management and Key Store, Real-Time Protection for System Integrity, TrustZone-Protected ODE, Two-factor Biometric Authentication and the Enhanced Generic Framework of KNOX.
- **An improved user experience.** KNOX Workspace offers a more flexible approach for enterprise deployment. KNOX container provides use of almost all Android apps without requiring prior app wrapping process third-party container support and a simplified enrollment process.
- **An expanding ecosystem.** KNOX 2.0 includes two new cloud-based services: KNOX EMM, which offers cloud-based MDM and Identity and Access Management (IAM) (with Single Sign-On (SSO) and Directory services) along with a rich set of IT policies, and KNOX Marketplace, a one-stop shop for KNOX and enterprise cloud apps.

Deliver cutting-edge core platform security to your mobile business

Samsung KNOX Workspace offers cutting-edge core platform security that delivers a robust, hardware- and software-integrated security foundation for the mobile enterprise. KNOX Workspace features hardware security that delivers multiple protection layers for the operating system and applications. The industry-leading, innovative security in KNOX Workspace protects devices and applications through Trusted Boot, TrustZone-based Integrity Measurement Architecture (TIMA), and improvements on SE for Android and enhancements.

Enterprise-ready certifications

Whether business or personal information is at stake, Samsung KNOX offers comprehensive, enterprise-class security that keeps it safe and helps users maintain productivity, anywhere. Years of research and engineering have culminated in a sophisticated, secure mobile platform that is relied upon by some of the most strictly regulated private sector industries and highly secure government agencies. Samsung KNOX Workspace has extensive, internationally recognized security certifications to provide a mobile platform that you can trust to help your employees work securely, such as:

- **Common Criteria (CC) for Information Technology Security Evaluation** issued by the National Information Assurance Partnership.
- **Federal Information Processing Standard (FIPS) 140-2 Level 1 Certification** issued by the National Institute of Standards and Technology.
- **DISA Mobile Operating System Security Requirements Guide Compliance** issued by the Defense Information Systems Agency.
- **End User Devices (EUD) Security Guidance** issued by the Communications and Electronics Security Group (CESG).

Protect the enterprise with multi-layered security

KNOX Workspace offers key improvements for strengthened hardware and software security through a comprehensive strategy:

Trusted Boot and Secure Boot. Secure Boot is a security mechanism that prevents unauthorized bootloaders and operating systems from loading during the startup process. With Trusted Boot, measurements of the bootloaders are recorded in secure memory during the boot process. At runtime, TrustZone applications use these measurements to make security-critical decisions, such as access to security keys, container activation, and so on.

Enhancements for TIMA. TIMA was developed to protect against potential vulnerability of SE for Android security mechanisms. TIMA leverages hardware features, specifically TrustZone to ensure that it cannot be pre-empted or disabled by malicious software running on the Android operating system. Enhancements for TIMA strengthen both platform security and application security.

- **TIMA Real-time Kernel Protection.** Performs continuous, real-time monitoring of the system from within TrustZone to prevent tampering of the kernel and system partition; protects against malicious modifications and injections to the kernel code.
- **TrustZone-based KeyStore.** Protects encryption keys in TrustZone and does not release keys when device tampering has occurred; allows export of TIMA KeyStore APIs to third-party developers**.**
- **TrustZone-based Client Certificate Certificate Manager.** Provides secure storage for client certificates in TrustZone (for email, browser, Wi-Fi, and so on); enables client certificates for one or more enterprise (or MDM) instances with the storage of a client certificate manager private key in TrustZone; enables mobile devices to replace Smartcards and their readers.
- **TrustZone-based On Device Encryption.** Encrypts the data stored in the device through the TrustZone-protected encryption key, which can be disabled at the detection of system integrity compromise.

Deliver cutting-edge core platform security to your mobile business

Improvements on SE for Android. KNOX Workspace offers significant enhancements in the level of protection offered to applications and system services. KNOX Workspace utilizes SE for Android to enforce Mandatory Access Control (MAC) policies to isolate applications and data within the platform. With the KNOX Workspace improvements on SE for Android, KNOX Workspace supports third-party containers such as from Fixmo, Good and MobileIron to receive the same level of HW-based protection as the KNOX Workspace container receives. The KNOX Workspace SE for Android Policy defines more than 100 security domains that strictly enforce security policies.

Improve secure access with two-factor biometric authentication

Two-factor biometric authentication employs both password and fingerprint recognition to identify and authenticate the device user before allowing device usage. The new container supports a two-factor authentication process, with which, the user can complete a fingerprint scan to access the container and select either a PIN, password, or pattern as a second process to follow the fingerprint.

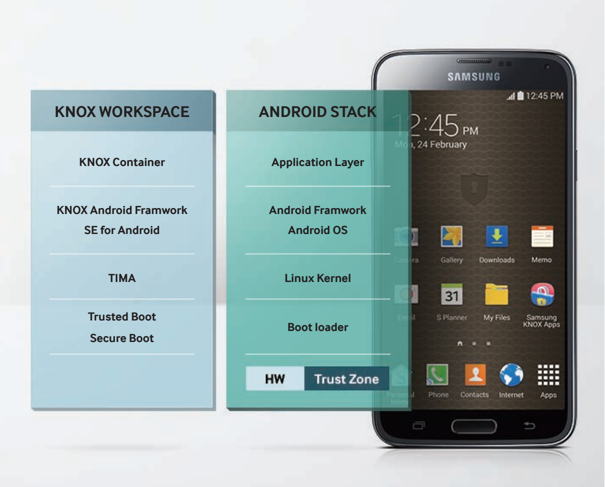

Figure 1. KNOX enhanced platform layers

Provide access to corporate resources with the enhanced generic KNOX Workspace framework

KNOX Workspace offers comprehensive support for enterprise virtual private networks (VPNs) that enables businesses to provide employees an optimized, secure path to corporate resources from their personal or corporate-issued devices. The enhanced generic KNOX Workspace framework supports leading SSL VPN solutions, and the per-application VPN feature has been extended to support SSL VPNs.

Deliver authentication and access with MS Workplace Join integration

KNOX Workspace supports Microsoft Workplace Join, introduced by Microsoft in Windows Server 2012 R2. Workplace Join enables employees to register their devices of choice with a company to allow access to corporate resources. With this support, IT organizations gain the robust authentication that enterprises demand and the assurance that employees who bring their own Samsung mobile devices can be strongly authenticated and allowed access to private corporate resources. KNOX Workspace is the first Android implementation to provide full support for Workplace Join, offering support on the latest Samsung mobile devices.

By controlling access to corporate resources, IT administrators can manage risk while helping users remain productive. As a seamless experience for end users, Workplace Join offers a second factor of device authentication through Active Directory.

Improve the user experience to increase business productivity

KNOX Workspace container improves the user experience, providing security for enterprise data by creating a secure zone in the employee's device for corporate applications, and encrypting enterprise data both at rest and in motion. KNOX Workspace container provides users with an isolated and secure environment within the mobile device, complete with its own home screen, launcher, applications and widgets for easier, more intuitive and safe operation. Applications and data inside the container are separated from applications outside the container.

With KNOX Workspace's enhanced container usability, businesses can receive support for various apps, and flexibly run and manage container policies of apps and data with the ability to instantly install up to two containers. This capability improves productivity, efficiency and the user experience.

Offer support for a variety of apps

Samsung KNOX Workspace provides use of a greater variety of apps, including KNOX Workspace apps and Google Play™ apps, without the need for prior app-wrapping process. Therefore, Android apps that support a multi-use framework (MUF) are available within the KNOX Workspace container. The apps' services and support include:

- **KNOX apps.**
- **Google Play apps.** The user's Google account can be supported for using GMS, including Google Maps™, Gmail™ and Google Docs.

Deliver flexible use of apps and data

KNOX Workspace container offers adjustable and flexible use of apps, data and the clipboard between the user's personal area and container. Flexible uses include:

Ability to move and copy apps from the personal area into the container. IT administrators have the authority to allow users to copy apps from the personal area into the container. Users can easily move apps with a Drag & Drop feature; however, this capability only works one-way. Copying apps from the container to the personal area is not allowed. The copying operation remains secure as KNOX Workspace screens the copied apps for malware.

Ability to move and copy data. Users can move data bi-directionally between the personal area and the container. Controlled by IT administrators, this capability offers convenient movement of data and multiple files in apps such as Music, Video, Gallery, My Files and Contacts with an easy user experience.

Users can display Calendar, Task List and Contact data from the container in the personal area through a two-way sharing capability that is controlled by IT administrators.

Improve the user experience to increase business productivity

Boost convenience and efficiency for an enriched user experience

KNOX Workspace offers solutions that are manageable, with comprehensive mobile device control in the cloud, including the ability to conveniently manage mobile devices and download business apps.

Offer better policy control through third-party container support

Third-party container support provides better policy control compared to the Native SE for Android, allowing the user or IT manager to choose a preferred container.

Simplify deployment and user management

Users can easily register and enroll their devices through the SEG cloud server and the UMC, minimizing the steps needed to create a KNOX Workspace container. The MDM server registers the company profile at SEG. UMC, a preloaded application in Samsung GALAXY devices, communicates with SEG to download and install the MDM application. After installation, the MDM application automatically authenticates user credentials communicating with the MDM server.

An example of simplified enrollment begins with an employee navigating to a web page and clicking an enrollment link that is provided to the employee through an e-mail or SMS, or through the company's internal or external website. Clicking the enrollment link displays a screen that requests the user's corporate email address. The employee's device then displays all notices for the user to accept, including privacy policies and agreements from Samsung, the MDM vendor and the enterprise. Upon accepting the terms, the employee is directed to a screen in which the password for the corporate account can be entered. If authentication is successful, the enrollment is complete. Any agent applications required by the MDM server are automatically downloaded and installed, without the need for user intervention.

Figure 2. KNOX Workspace

KNOX EMM

Leverage a cloud-based mobile security management solution for an expanding ecosystem

KNOX EMM is a cross-platform, cloud-based enterprise mobile security management solution that provides IT administrators with a centralized web console for managing employees' devices, containers and apps. Samsung KNOX EMM offers a complete set of cloud-based Mobile Device Management (MDM), Identity and Access Management (IAM) and security services.

Because it is a cloud-based enterprise mobility management solution that does not require an on-premises infrastructure, KNOX EMM helps solve common enterprise mobility adoption issues, such as integration of diverse devices. Devices can be managed through an Admin Portal with optional on-premises AD support, eliminating the need to regularly update the employee directory for on-premises MDM as a company grows. In addition, apps that are purchased in KNOX Marketplace are automatically synced with KNOX EMM. The enterprise can manage the KNOX container like any other IT asset using an MDM solution. KNOX supports many of the leading MDM solutions on the market. Container management is affected by setting policies in the same fashion as those traditional MDM policies. KNOX container provides IT administrators with policies that enable them to easily implement company guidelines, such as remote wipe, password reset, remote lock, device storage encryption, restriction on jail-broken or rooted devices, restricted use of camera, location reports and more. The new container also allows enterprise IT administrators to control the flow of information between the container and the rest of the device. This allows enterprises to strike the right balance between security and user productivity.

Through Identity and Access Management (IAM), Samsung KNOX EMM's provides employees with Single Sign-On (SSO) for easier, more convenient access to authorized business apps. KNOX EMM's SSO eliminates the need for an additional login with simplified single-click access to mobile and web apps. SSO optimizes security, manageability and accessibility. And, with IAM, IT managers can grant employees convenient, role-based app authorization, allowing them to enroll devices and activate KNOX SSO, thereby eliminating the need to log in.

Figure 3. KNOX EMM

KNOX Marketplace

Support your growing ecosystem with easy app purchasing and deployment through KNOX Marketplace

KNOX Marketplace is a convenient service through which customers can acquire and implement apps, including a broad range of leading cloud-based apps, all from a single website. KNOX Marketplace features consolidated billing, combining multiple products into a single invoice. The service also provides a competitive and flexible pricing model, and easy, centralized user and license configuration and management. IT Administrators pay only one bill for all users and one-time or recurring and usage-based payments. Also, a variety of billing methods (credit cards, WorldPay and direct deposit) in multiple currencies is available. For added convenience, an IT administrator can sync a list of users from KNOX EMM, so that apps purchased in KNOX Marketplace can be assigned to users in KNOX EMM.

For example, an IT administrator browses through services and applications in KNOX Marketplace and selects a product. Volume purchasing capability is integrated with the app product information display, enabling the IT administrator to purchase ten copies of the app. A list of employees that are synced with Active Directory through KNOX EMM is displayed. The IT administrator can assign the apps to the selected employees within his company. Immediately, the apps appear in the EMM WebApps in the KNOX container with the SSO enabled on the selected employees' devices.

Figure 4. KNOX Marketplace

Legal and additional information

About Samsung

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 TVs, smartphones, tablets, PCs, cameras, home appliances, printers, LTE systems, medical devices, semiconductors and LED solutions. We employ 286,000 people across 80 countries with annual sales of US$216.7 billion. To discover more, please visit www.samsung.com.

For more information

For more information about Samsung KNOX, visit www.samsungknox.com

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

www.samsung.com

2014-07