****

***Embargo to be lifted on February 25, 20:00PM CET***

**Samsung KNOX™ Keeps Evolving to Meet Changing Enterprise Needs**

*Newly evolved secure mobile platform provides enhanced security and new features to address BYOD and enterprise mobility challenges*

* Cutting-edge security enhancements make KNOX the most secure Android platform for the enterprise
* A better user experience with the option to choose a KNOX container or 3rd party container, simple enrollment process and Spilt-Billing feature
* Expanded partner ecosystem for more variety and flexibility; and new services like EMM and Marketplace to cater to SMBs

**BARCELONA, Spain – February 25, 2014 –** Samsung Electronics Co, Ltd., today announced KNOX 2.0, the evolution of KNOX, the company’s end-to-end secure mobile platform solution designed to provide advanced data and privacy protection for enterprise users. The new features better support IT departments looking for reassurance and convenience as they implement and manage their Bring Your Own Device (BYOD) strategies.

Since October 2013 when KNOX was first commercially available in the market, Samsung has sold over 25 million KNOX-enabled devices and has over 1 million active KNOX users today. On average, 210,000 KNOX-enabled devices are being activated per month which is about 7,000 devices each day.

“Thanks to the rapid adoption of KNOX over the past 5 months since its first commercial availability, we needed to evolve the Samsung KNOX platform to meet the changing needs of our customers and the enterprise as a whole,” said JK Shin, President and CEO, Head of IT & Mobile Communications Division at Samsung Electronics. “As a leading provider of Android devices, it is our mission to make Android platform even more secure to lead enterprise mobility market. With the new features of KNOX 2.0 we are able to provide our users with a truly enterprise-ready mobile solution. We will continue to work hard and listen to both our partners and customers to constantly improve the KNOX platform to meet these ever-changing needs.”

**Cutting-edge Core Platform Security**

KNOX 2.0 offers a series of core platform security improvements to better protect device integrity from kernel to apps for a more secure, integrated mobile experience. These upgraded features include:

* TrustZone-Protected Certificate Management: Device-wide feature that generates and maintains client certificates inside Trustzone with additional support for industry standards such as PKCS#11; allows mobile devices to play the role of the smart card and its readers.
* KNOX Key Store: Generates and maintains encryption keys inside the TrustZone protected environment; allows third parties to utilize encryption for security sensitive applications and makes sure that encrypted data is protected if the system is compromised
* Real-Time Protection for System Integrity: Real-time monitoring that both detects and prevents any unauthorized modifications to the kernel code, critical kernel data and system partition
* TrustZone-Protected ODE: Encrypts the data stored in the device through the TrustZone-protected encryption key, which can be disabled at the detection of system integrity compromise.
* Two-factor Biometric Authentication: Makes container access even more secure by requiring both password and fingerprint verification to authenticate
* Enhanced Generic Framework of KNOX: Supports Per-App VPN functions for SSL VPN solutions such as Juniper, F5 and Cisco while previously supporting them only for IPsec VPN.

**Improved User Experience**

KNOX 2.0 provides users with enhanced container features such as support for most of Android apps from the Google Play Store, meaning there is no need to go through the wrapping process for third party apps. KNOX 2.0 also supports SE Android policy configurations for third party containers, such as Good’s secure container, Fixmo’s SafeZone, MobileIron’s AppConnect so that these 3rd party containers will receive the same level of HW-based protection as the KNOX container receives. This evolution of KNOX allows for the choice of different types of containers for a more flexible approach to enterprise BYOD strategies. Besides, UMC and SEG make user enrollment process simpler than before since the user profile is pre-registered to SEG by MDM servers.

KNOX 2.0 supports a dual APN capability that can be used to charge the data traffic usage of enterprise applications from that of personal applications. By assigning a different APN to the data traffic of the enterprise container which runs only enterprise approved applications. From that to the personal data traffic, KNOX can allow a telecom carrier to separately bill customers for personal and enterprise uses. This capability removes one of the most critical industry-wide impediments to the adoption of the BYOD programs which allows employees to use their personal mobile devices for work.

**Expanding Ecosystem**

In addition to the core features of KNOX, Samsung also announced new cloud based services, KNOX EMM and KNOX Marketplace, broadening the KNOX customer base by catering specifically to SMBs.

Samsung is providing the following services with KNOX:

* EMM: Provides cloud-based Mobile Device Management and Identity and Access Management (SSO + Directory service) with a rich set of IT policies to implement company guidelines. KNOX EMM includes:
  + Over 326 IT policies
  + Single sign-on for web-based and mobile apps
  + Cloud directory service as well as on-premise active directory to manage credential information
  + Cloud-based enterprise services including productivity enhancement suites CRM and ERP
* Marketplace: A one stop shop for SMBs to find, buy and use KNOX and enterprise cloud apps in a unified environment and includes:
  + A comprehensive catalogue of business applications including KNOX and 140+ cloud apps
  + Customizable bundling for customers to buy multiple apps in a custom bundle
  + Consolidated billing to allow customers to combine multiple products into a single invoice

The key feature of KNOX EMM and Marketplace is that all the services purchased from the marketplace come with the zero-sign capability implemented by KNOX EMM. IT Admin can easily supervise employee access rights to the purchased services according to the credentials defined in the directory and employees can access these services from mobile devices and PCs without an explicit registration and sign-in process.

Samsung has also expanded its partner ecosystem. Some of our new partnerships include:

* KNOX now supports SE Android policy configurations for third party containers such as Good’s secure container, Fixmo’s SafeZone, MobileIron’s AppConnect which provide better policy control compared to the Native SE for Android, allowing users or IT managers to choose their preferred container.
* By partnering with Microsoft, KNOX allows users to join their devices with their company to access company resources and services with Microsoft Workplace Join.
* The new split-billing feature that separately calculates bills for personal and enterprise apps works by partnering with carriers like 3 Hong Kong Telecommunications.

New features of KNOX 2.0 will be commercially available in Q2 2014. Once available, previous generation KNOX users will be able to upgrade to KNOX 2.0 after upgrading to KitKat. KNOX 2.0 will also come pre-installed on the newly launched Samsung Galaxy S5.

**Note to Editors**

PKCS#11: Cryptographic Token Interface Standard

ODE (On Device Encryption): Encryption method used in Samsung devices to encrypt the file storage of device

VPN (Virtual Private Network): Networking method for secure communication between employee’s device and corporate network

APN (Access Point Name): The name of a gateway between a GPRS, 3G or 4G mobile network and another computer network, frequently the public Internet

MDM (Mobile Device Management): Solution for managing mobile devices according to company’s IT compliance policy

EMM (Enterprise Mobility Management): Solution for managing devices, applications, identities and accesses

SSO (Single Sign-On): Solution that make uses to log-in once and gain access to company resources

SSL (Secure Sockets Layer): a protocol for encrypting information over the Internet

SEG (Samsung Enterprise Gateway): Samsung cloud server that make registration and enrollment simple

UMC (Universal MDM Client): hidden application in the device that works with SEG

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