Meet evolving enterprise mobility challenges with Samsung KNOX™

Samsung Knox

SAMSUNG

Solve today's dynamic enterprise mobility demands with the right solution platform

Enterprise Mobility Trends

The growth of enterprise mobility, driven by the Bring Your Own Device (BYOD) trend, has recently fostered a rapid shift in the enterprise mobility marketplace. Mobile consumer device leaders are increasing their presence in the enterprise business world with robust, next-generation solutions, pushing out platforms that lag behind in innovation or fail to meet user demands. After failing to meet user demands, the previous standard in business mobile devices is being replaced by more innovative solutions.

The phenomenal growth of smartphone and tablet shipments and the shifting popularity of different mobile device brands make it clear why enterprises must continually revisit their mobility strategies and policies. Two or three years ago, no one could have known that, according to the market research firm IDG Enterprise[1], nearly 80 percent of the 236.4 million smartphones shipped in the second quarter of 2013 were Android™-based devices, or that Samsung alone would hold nearly 40 percent of the Android smartphone market share.

Mobile device vendors that fail to innovate and miss the mark on user demand, can quickly transition from market leaders to also-rans. These types of shifts can have a big impact on enterprises, especially given the widespread corporate adoption of BYOD policies.

Companies that support BYOD allow employees to use their personal mobile devices to access corporate resources and do work. If corporate mobility policies fail to reflect the changing profile of their employees' mobile devices, enterprise IT may quickly lose the ability to manage and control those devices effectively.

As earlier-generation mobile devices fall out of favor, and mobility technologies evolve, enterprises need to follow a well-thought-out process to optimize their mobility strategies. That process, which this document discusses, goes well beyond simply evaluating the functionality of any given mobile device. Also important are everything from employee preferences to partner ecosystems, along with the management and security requirements that typically top the list of concerns of CIOs and business executives alike.

Assess mobility needs and employee preferences

Any effort to initiate or fine-tune a mobility strategy should not begin with a focus on mobile devices. Rather, the first step should be an in-depth assessment of the current mobility practices and processes already in place within the organization. In other words, before companies can determine how they can best use current-generation mobile devices and technologies, they first need to understand how mobility intersects with their core business objectives, and how their employees currently use mobile devices.

In many cases, there will be a generational element that comes into play in such evaluations. Younger workers, who came of age in a world of pervasive social networking and mobility, may suggest new use cases that can make them and their employers more efficient and productive. Simply swapping out old devices for new ones and changing little else can be a missed opportunity to optimize an enterprise's mobility operations based on the new platforms' capabilities and on new use cases and processes.

A key piece of this macro assessment is learning which mobile devices employees prefer. Companies that have instituted BYOD programs can get a good sense of these preferences simply by determining what types of personal mobile devices employees are bringing into the work environment.

Even when companies follow the traditional model of purchasing, distributing and supporting corporate-owned mobile devices, they should take employee preferences into account before deciding to adopt any given platform. If IT and business managers fail to determine employee preferences, they may discover that the devices they select are either rejected or underutilized.

Once companies have gained a good understanding of their existing mobility profile and their employees' mobile practices and preferences, they can move on to additional stages of the evaluation process. Failure to perform this first critical step can severely undermine the ultimate success of any evolving mobility strategy.

Ensure that the mobile platform meets security and compatibility requirements

Having completed an overview of the mobile environment and deciding where to take, enterprises must next ensure they can manage and secure that environment and the corporate data within it. This step is usually high on enterprises' evaluation checklists.

According to IDG Enterprise survey[1], more than 1,600 IT and business managers and professionals found this to be the case. As illustrated in Figure 1, in that early 2013 survey, 88 percent of the respondents working at corporations with more than 1,000 employees said the ability to provide device security is an important factor when they evaluate mobile technology vendors. Among this group of respondents, 69 percent also cited the need for these vendors to help manage the proliferation of mobile devices.

Enterprises should begin this stage of their evaluation not with a focus on a particular device, but with an assessment of their organization's overall risk profile. Among the key questions, an enterprise must answer:

- What corporate information and resources are especially valuable and/or sensitive?
- How can the company best balance the benefits versus the risks of providing mobile users access to corporate data and resources?
- Which corporate data can be downloaded to mobile devices and which data needs to stay behind the corporate firewall?
- What types of security technologies and practices are available for mobile devices and their use cases?

Only after these and other risk-profile questions have been answered can organizations intelligently determine the level of security controls they require on mobile devices, in their mobile management systems and in their security policies.

Factors considered critical or very important when evaluating mobile technology vendors

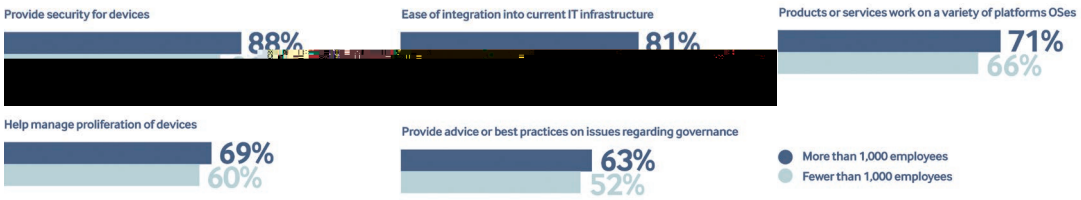

Figure 1. Evaluating mobile technology vendors

Meet the full range of enterprise mobility needs with Samsung

As it grew to become a leading mobile device provider worldwide, Samsung committed itself to meeting the wide range of requirements that enterprise customers bring to the table. That commitment extends beyond creating enterprise-grade smartphones, tablets and other mobile devices. It also encompasses the full scope of programs and partnerships that enterprise mobility initiatives entail.

Samsung offers a broad portfolio of device form factors, including smartphones and tablets. In addition to offering different screen sizes and formats, Samsung devices deliver an unmatched collection of features and functions. As a result, enterprises can find Samsung devices that match virtually any mobility use case.

When it comes to employee preferences, employees have already voted with their personal device purchases. As noted in the market figures cited earlier, Android-based devices dominate smartphone shipments of which Samsung takes nearly 40 percent.

Given these figures, companies with BYOD programs already have large numbers of Samsung devices active within their employee populations. Enterprises looking to update their mobile devices from earlier models that have fallen into disfavor should give appropriate weight to the mobile device choices their employees are making on their own.

Samsung offers a broad suite of security and management capabilities. For example, the company's devices support Exchange ActiveSync® (EAS), a protocol that helps mobile phone users be more productive by giving them secure access to their corporate email accounts, calendars, contacts and tasks. In 2013, Samsung introduced the new comprehensive mobile security platform, Samsung KNOX.

Key Enhancements of Samsung KNOX

Key Features	Description
Device & Data Security	Security Enhancements for Android (SE for Android) that enable KNOX to secure third-partycontainer solutions; also, ARM®TrustZone-based Integrity Measurement Architecture (TIMA), which safeguards certificates and encryption keys from hacking
Container Usability	Elimination of wrapping third-party apps that increases app availability for users; more flexible use of apps and data between containers and personal area; instant container creation (up to two containers), which uses less memory
Easy Enrollment	Easy registration and enrollment of third-party MDM downloads through SEG and Universal MDM Client that minimizes the process for creating a KNOX container
Cloud-based Mobile Device Control	Effective and efficient management of cross-platform mobile devices and content through a complete set of cloud-based MDM services, and a single source of purchasing and billing KNOX licenses and cloud-based business applications

Advance and secure the enterprise with an all-inclusive mobility platform

Samsung KNOX is a holistic enterprise platform that provides enhanced security and container solutions with cloud-based enterprise mobility management services as well as a marketplace, which provides KNOX products and software-as-a-service (SaaS) apps. With greater security and improved usability, based on constant innovation in mobile technology to meet rapidly changing mobility needs, Samsung KNOX provides an evolving platform for today's dynamic enterprise mobility requirements.

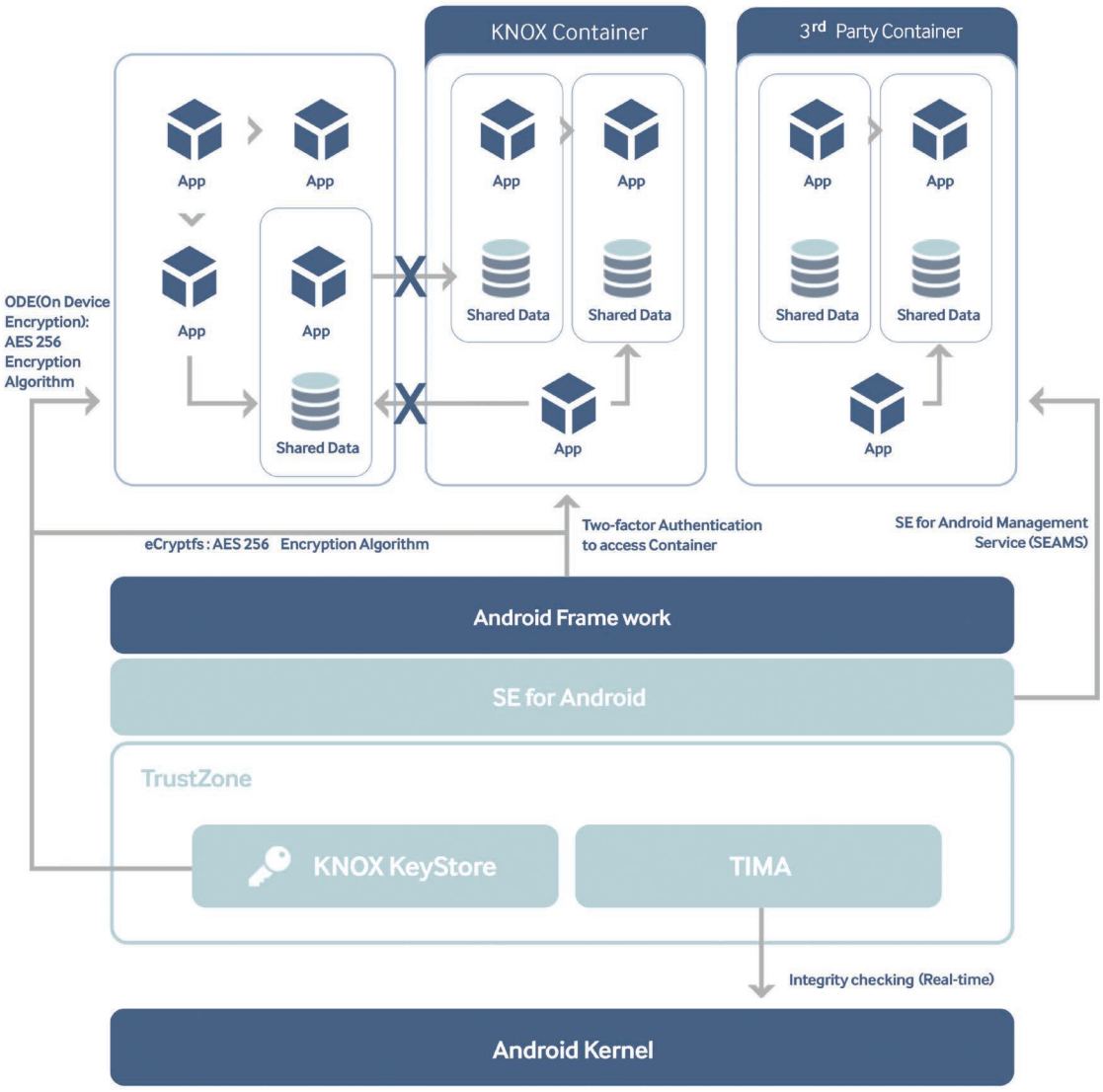

Figure 2. Samsung KNOX enhanced features diagram

Provide safe and flexible enterprise mobility with enhanced security technology

Samsung KNOX

- **Device & Data Security**
- Container Usability
- Easy Enrollment
- Cloud-based Mobile Device Control

Increase protection with heightened security

Samsung KNOX meets the needs of the most demanding enterprise business environments by offering comprehensive protection against malware attacks and hacking with its multi-layered security model and industry-leading device management capabilities.

- **Trusted Boot.** Trusted Boot is a primary component that forms the first line of defense against malicious attacks on devices equipped with Samsung KNOX. Trusted Boot ensures that only verified and authorized software can run on the device.
- **ARM®TrustZone-based Integrity Measurement Architecture (TIMA).** TIMA runs in the secure world and provides continuous integrity monitoring of the Linux® Kernel. When TIMA detects that the integrity of the Kernel or the boot loader is violated, it notifies the enterprise IT by way of the MDM, which can then take policy-driven action in response. One of the policy actions disables the Kernel and powers down the device.
- **Security Enhancements for Android (SE for Android).** With the SE for Android enhancement, Samsung KNOX supports platform security of third-party container solutions in addition to the KNOX container.

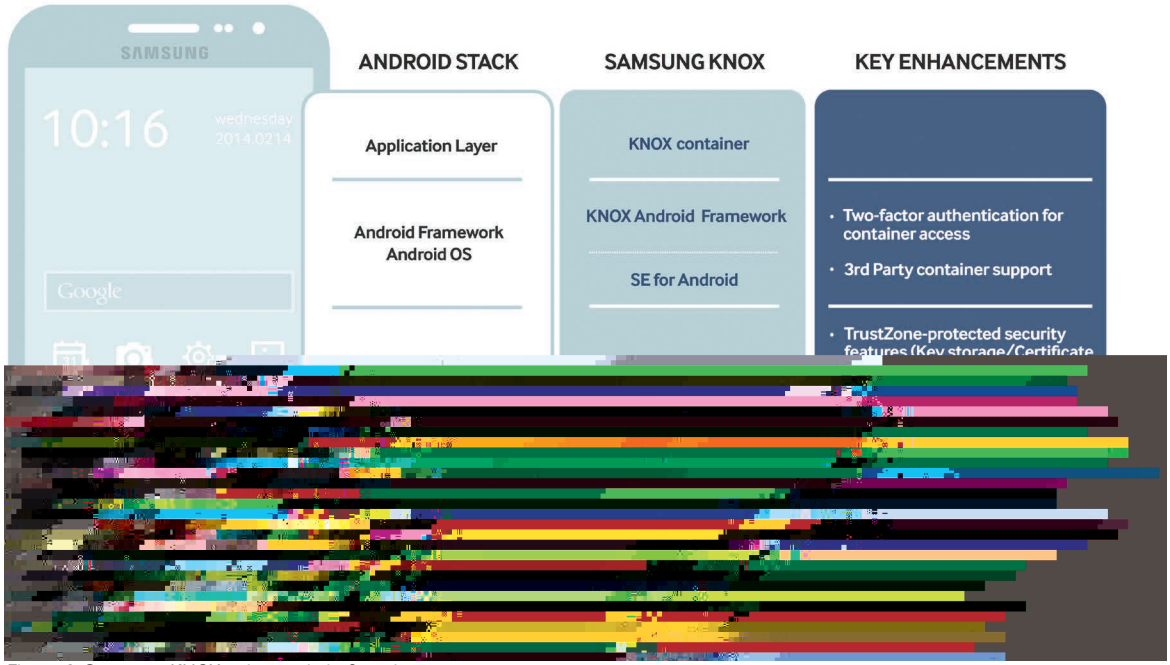

Figure 3. Samsung KNOX enhanced platform layers

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.

For more information about Samsung KNOX,
Visit https://www.samsung.com/KNOX

Copyright © 2014 Samsung Electronics Co. Ltd. All rights reserved. Samsung and KNOX are either trademarks or registered trademark of Samsung Electronics Co. Ltd. Specifications and designs are subject to change without notice. Non-metric weights and measurements are approximate. All data were deemed correct at time of creation. Samsung is not liable for errors or omissions. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

Android and Google Play are trademarks of Google Inc.

ARM and TrustZone are registered trademarks of ARM Ltd. or its subsidiaries.

iOS is a registered trademark of Cisco Systems Inc., registered in the U.S. and other countries, and licensed to Apple.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and ActiveSync are registered trademarks of Microsoft Corporation in the United States and/or other countries, or both.

1. 2013 Consumerization of IT in the Enterprise survey, IDG Eneterprise

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

www.samsung.com/KNOX