Making Everything Easier!™

Samsung Special Edition

Samsung KNOX™

FOR DUMMIES®

A Wiley Brand

Learn to:

- Detect device rooting
- Protect corporate apps and data

Brought to you by

The SAMSUNG KNOX Team

and

Lawrence C. Miller, CISSP

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 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 KNOX™ FOR DUMMIES®

A Wiley Brand

Samsung Special Edition

by the Samsung KNOX Team
&
Lawrence C. Miller

FOR DUMMIES®
A Wiley Brand

Samsung KNOX™ For Dummies®, Samsung Special Edition
Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-24725-8 (pbk); ISBN 978-1-119-24726-5 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Special Acknowledgments

This Samsung Special Edition would not have been possible without the outstanding support and collaboration from the KNOX Team with special thanks to Janis Guthrie, known throughout the world as the Goddess of Tech Writers.

Introduction

As smartphones become more powerful and popular trends such as bring your own device (BYOD) and corporate-owned personally enabled (COPE) become more ubiquitous in the digital workplace, mobile threats have become more powerful and ubiquitous, too. Security and privacy concerns are now — or should be — top of mind for everyone.

In 2012, Samsung engineers began developing Samsung KNOX, the defense-grade mobile security platform built into Samsung's flagship mobile devices. Today, there are more than 144 million KNOX-enabled Samsung devices around the world. These devices are literally born (well, manufactured) with built-in, mobile security. Enterprises large and small, in industries like finance, government, healthcare, retail and many others, can now empower their mobile workforces with the confidence that only Samsung KNOX-enabled devices can deliver.

About This Book

This book explains the story behind KNOX (Chapter 1), the KNOX platform (Chapter 2), and KNOX products (Chapter 3), and wraps up by giving an overview of a few Samsung KNOX capabilities (Chapter 4).

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I'll assume a few things nonetheless:

- You want to learn more about mobile device security — specifically, Samsung KNOX mobile device security.
- You work for an organization that is struggling to manage the proliferation of smartphones in the workplace and the associated security and privacy risks.

- You may have heard about Samsung KNOX, but you need more information because you're evaluating mobile security solutions for your organization — or because one of your executives has just slid this book to you in a meeting!

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

This icon points out information that you should commit to your nonvolatile memory or your noggin.

You won't find a map of the human genome or the blueprints for the next-generation Samsung Galaxy smartphone here (or maybe you will . . . hmm), but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon!

Thank you for reading, hope you enjoy the book, please take care of your writers! Seriously, this icon points out helpful suggestions and useful nuggets of information.

This icon points out the stuff your mother warned you about. Okay, probably not. But you should take heed nonetheless — you may just save yourself some time and frustration!

Beyond the Book

There's only so much I can cover in 24 short pages, so if you find yourself at the end of this book thinking, "Gosh, this was an amazing book, where can I learn more?," just go to `www.samsung.com/business`.

Chapter 1

The Samsung KNOX Story

In This Chapter

- Recognizing the mobile threat and the need for KNOX security
- Taking a look at smartphone components and security functions

In this chapter, I survey the mobile threat landscape to show you why Samsung created KNOX security, built on the tenets of Trusted Computing.

Why KNOX Exists

In 2008, the first Android smartphone was introduced, and in just a few short years, Android has become the dominant operating system (OS) for smartphones. In 2014, approximately 75 percent of the more than 1.2 billion smartphones sold worldwide were Android smartphones, of which nearly 25 percent were Samsung smartphones.

The Android OS is open-source software that was originally designed primarily for end-users rather than for enterprise adoption. Developers can directly modify the Android OS source code, which makes it very powerful and popular for building advanced functionality and custom apps but also makes the OS vulnerable to attacks.

Open-source software is nonproprietary software that can be freely used, modified, and distributed by anyone (subject to licensing under the Open Source Initiative).

The 2013 Juniper Networks Mobile Threat Center *Third Annual Mobile Threats Report* found that mobile malware threats were growing at an alarming rate of 614 percent (276,259 total malicious apps). Aspect Security's *2013 Global Application Security*

Risk Report found that 98 percent of apps presented at least one security risk, while the average app registered 22.4 risks. Not surprisingly, due to their market dominance and open-source nature, Android smartphones and apps are the target of the vast majority of mobile security threats and attacks.

The original Android approach to security was to simply isolate apps from each other. However, this approach alone isn't enough for enterprise security needs. End-users could still do irreversible harm to the device by "rooting" the phone or by downloading unauthorized apps, software, and firmware.

Device rooting is the practice of intentionally exploiting privileged software or OS functions to install custom firmware and circumvent vendor restrictions (such as licensing). Rooting compromises many of the security protections built into the device and typically voids the device manufacturer's warranty.

Samsung introduced KNOX in 2013, recognizing the perfect storm that was developing due to

- The rapidly evolving mobile threat landscape
- The rising popularity of bring your own device (BYOD) and corporate-owned personally enabled (COPE) mobility trends in the enterprise
- The ineffectiveness of the traditional IT security model, which was originally designed to protect enterprise networks and based on perimeter-based security, instead of mobile devices with anytime, anywhere access to corporate apps and data

The Samsung KNOX security solution (the brand including the KNOX platform and KNOX security products and services) is designed to be the most comprehensively secure and manageable mobile device solution for enterprises large and small.

Trusted Computing: The Foundation of KNOX

The foundation of KNOX is hardware-based device security that is built on the principles of *Trusted Computing*.

In other words, KNOX ensures that the device is running the correct security software and hasn't been tampered with or disabled — either by an attacker (through an attack vector) or by the owner (through device rooting), and provides the following important security functions:

- **Platform integrity:** Ensures that no one has made changes to the device and that the device is operating in an allowed state (see Chapter 2).
- **Application and data security:** Provides a secure storage vault for security certificates (for example, your email application may have a digital certificate to prove an email message is a legitimate message from you) and encryption keys (used, for example, to protect the confidentiality and integrity of data).
- **Remote and wireless access security:** Provides hardware-based security for remote access (such as a virtual private network, or VPN) and wireless connections (such as a secure Wi-Fi network).

Chapter 2

The KNOX Platform

In This Chapter

- Starting with a secure device platform
- Providing secure assembly
- Ensuring authenticity and integrity during the boot process
- Loading software and applications securely
- Preventing attacks and malware at run-time
- Keeping smartphone devices up to date

KNOX uses Trusted Computing principles throughout the life cycle of KNOX-enabled Samsung devices — from the time of design, throughout the manufacturing process, to boot-time, load-time, and run-time — to ensure enterprise devices, apps, and data are always safe and secure.

In this chapter, you learn about the foundational elements of the KNOX platform that make Samsung smartphones the most secure Android devices available, from inception to the moment you turn the device on — and beyond.

Secure by Design

The KNOX platform was conceived and created using a design philosophy that incorporates Trusted Computing principles:

- **Build trust.** Establish security protections at the hardware level ("Hardware Root of Trust") and ensure security from

the moment the device is turned on. A Hardware Root of Trust is important for several reasons:

- Security is literally "built in" to the hardware as opposed to being an add-on software component.
- Hardware-based security usually means an attacker cannot compromise the device even with physical access.

- **Maintain trust.** Actively monitor key aspects of the device in real-time and perform periodic checks to ensure the ongoing "health" (integrity) of the device (like immunizations).
- **Prove trust.** KNOX-enabled devices provide the MDM with an *attestation,* a cryptographically verifiable collection of device state measurements to prove trust (you've got to show your immunization record to the daycare center so you don't get the other "kids" — programs and services — sick).

KNOX security starts at the processor level. KNOX uses a processor architecture known as *ARM TrustZone* to provide built-in, system-wide strong authentication for users, apps, and data through partitions called *worlds.*

In TrustZone, there are two worlds:

- **Secure World:** This world is reserved for highly sensitive operations such as those involving cryptographic keys (this is where KNOX comes in!).
- **Normal World:** Virtually all smartphone software as we know it, including the OS kernel, middleware, and apps, runs in this world. Software in the Normal World can never directly access data used by Secure World software — it must ask for access.

KNOX uses Secure World capabilities to protect confidential enterprise data and to monitor the OS kernel running in the Normal World. The combination of TrustZone hardware and software provides a Trusted Execution Environment (TEE). The TEE is important because it ensures that sensitive data and code are stored, processed, and protected in a separate trusted environment for maximum security — like a safe deposit box within a secure bank vault.

KNOX: Security from the hardware up

Samsung KNOX safely and securely enables enterprise mobility strategies by providing multiple layers of protection for mobile devices built on the KNOX platform.

The foundational layer of the Samsung KNOX platform is the Hardware Root of Trust. This layer of security is literally built into the device at the factory, providing a strong base on which to build additional security layers. This foundation is supported by the following key elements:

- **Device Unique Hardware Key (DUHK):** The DUHK (discussed in the section "Controlling the Manufacturing Process") is a cryptographic key that is unique to each Samsung device. The DUHK encrypts and decrypts data and encrypts other cryptographic keys on the device.
- **Samsung Secure Boot Key (SSBK):** The SSBK (discussed in the section "Controlling the Manufacturing Process") verifies that boot components on the device are approved.
- **Device Root Key (DRK):** The DRK is another type of cryptographic key that is unique to each Samsung device. The DRK identifies the device and proves that it is an authentic device manufactured by Samsung.
- **KNOX Tamper-Evident Fuse:** The KNOX Tamper-Evident Fuse (explained in the section "On Your Mark! Boot-time

(continued)

(continued)

Defenses") verifies that the device has never run unapproved components or had key security features disabled.

- **Rollback Prevention (RP) Fuses:** RP fuses are hardware fuses that encode the minimum acceptable version of Samsung-approved programs for a particular device. These fuses are set when the device is manufactured and prevent older, potentially vulnerable versions of boot programs from being loaded on the device.

The next layer of security consists of Secure Boot and Trusted Boot (explained in the section "On Your Mark! Boot-time Defenses"). Secure Boot and Trusted Boot run sequentially as soon as a user turns on the device. Secure Boot starts each bootloader and ensures that the bootloaders are authentic versions before it loads the Android OS kernel. Trusted Boot takes "snapshots" (called *measurements*) of all the bootloaders and OS kernels while they're running to ensure they remain secure and to validate their integrity.

The third layer of security, "TrustZone" (discussed in the section "Secure by Design"), creates a "Secure World" and "Normal World" partition in the device's processor architecture.

The fourth layer consists of the TrustZone-based Integrity Measurement Architecture (TIMA) and Real-time Kernel Protection (RKP), both explained in the section "Go! Run-time Defenses." RKP continuously monitors and protects devices while they are running.

Finally, "Security Enhancements for Android" protects apps and uses policies to restrict access to safe connections only. In addition, it offers utilities and tools including mobile device management (MDM), KNOX Workspace, Active Directory (AD), virtual private network (VPN), and single sign-on (SSO), among others — all described in Chapters 3 and 4.

Thus, KNOX provides a multi-tiered platform that layers in protection for mobile devices from the hardware level all the way up to the applications running on the device.

A "trusted environment" ensures that enterprise operations, such as decrypting sensitive data, can occur only when the device has been booted into an *allowed* state. The TEE helps make this trusted environment possible.

In trusted computing, an *allowed* state is the normal, unaltered condition of the device's hardware and software security functions. If the security functions have been tampered with in any way, the device is no longer in an *allowed state*. It's

like a tamper-evident seal on a bottle of aspirin or shrink wrap on your favorite DVD movie — it gives you confidence that no one messed with your medicine or replaced your DVD with a defective copy.

Controlling the Manufacturing Process

Samsung manufactures and configures all its devices in its own factories. This means that Samsung has complete control over the devices and software leaving the factory, which ensures both the quality and security of every Samsung device throughout the manufacturing process.

In addition to developing and installing secure device software, Samsung manufactures each device with special cryptographic keys, which are crucial components in the Hardware Root of Trust, and ensure the ongoing integrity of Samsung devices even *after* they leave the factory. Two of these keys are

- **Device-Unique Hardware Key (DUHK):** This is the fingerprint of the device — no two devices have the same DUHK. The DUHK is built in to the device and provides an additional level of security: Secure World data can only be decrypted on that specific device.
- **Samsung Secure Boot Key (SSBK):** Another hardware feature uses tamper-evident fuses to verify that the phone's OS and software load safely every time the device is powered on.

The additional steps that Samsung takes to protect the manufacturing process ensure a Trusted Computing environment for every Samsung KNOX device. Other device vendors that outsource manufacturing can't guarantee the same end-to-end control of these critical security elements.

When a user presses the On button of a device, several critical processes must run sequentially before the device is ready to be used. These processes include booting, loading, and running. In the following sections, I explain how

KNOX protects devices at boot-time, load-time, run-time, and beyond.

On Your Mark! Boot-Time Defenses

One of the most important jobs of mobile security is to ensure the software that is running on the device is authentic and safe. This software, of course, includes the operating system, but also any software or apps that are installed by the manufacturer, enterprise, or user. When a phone is turned on, Secure Boot checks for safety and authenticity, but can sometimes be tricked by an older version of a bootloader.

To overcome this limitation, KNOX uses Trusted Boot. Trusted Boot takes measurements ("snapshots") to prove whether the bootloaders are valid and running as expected. Trusted Boot further protects the boot process by blowing a tamper-evident fuse if it detects an unauthorized modification ("In case of emergency, break glass") so that your data stays encrypted and safe.

The KNOX *Tamper-Evident Fuse* (sometimes referred to as the "Warranty Bit") is a one-time programmable fuse that indicates whether the device has ever been booted in a *non-allowed* state. If Trusted Boot detects that unapproved components are used, or if certain critical security features such as SE for Android are disabled, it "blows the fuse." This means that a "bit" is set to indicate the device is no longer trusted or in an "allowed" state. ***Remember:*** KNOX wants to ensure your device starts and stays in an allowed state. Once the fuse is blown, the device can never successfully go through the KNOX boot process. Access to the DUHK and Device Root Key (DRK) in the TrustZone Secure World is revoked and enterprise data on the device using the TIMA key store (discussed in the next section) cannot be accessed or recovered.

What's in a smartphone?

Just like a desktop computer, at the heart of every smartphone there are one or more processors, where the OS and apps run.

Processors

A processor runs in one of two *modes* of execution (the privilege level for a piece of software running on the processor):

- **User mode:** When a user-installed app runs on the processor, it runs in *user mode.* In user mode, the app is not allowed to directly access hardware devices (such as a camera or GPS) or resources (such as memory) controlled by other apps.
- **Privileged mode:** Critical OS software runs in *privileged mode.* In privileged mode, the system's software is allowed to directly access hardware devices, as well as all data held by the user's applications.

Operating systems

Operating systems use both user and privileged modes for various functions. The portion of the OS running in privileged mode is called the *kernel.* Thus, gaining control of the OS kernel is often an objective for an attacker. With privileged mode access, an attacker could tamper with and steal potentially sensitive data from any app on the device.

Middleware

In most operating systems, when apps want to communicate with each other, they ask the kernel to set up the lines of communication for them. To facilitate this communication, the Android OS uses another layer of software, known as *middleware.* Android middleware runs in user mode and sits between the kernel and the apps. This middleware adds yet another layer of protection to Android devices — preventing apps from directly accessing the OS kernel (and its privileged mode of execution).

What does all of this mean? The security features built into KNOX and Android work together seamlessly from the hardware layer to the application layer, providing users with the most secure experience (see the sidebar "KNOX: Security from the hardware up," earlier in this chapter).

Get Set! Load-Time Defenses

The kernel isn't the only attractive target for malware and malicious users. Mobile devices have a lot of preloaded system software beyond the kernel (think about all the apps

your phone already has on it!). Unfortunately, it's impractical to verify the integrity and authenticity of all that software at boot-time, because it would (seemingly) take forever to the user — like booting up a computer every time you want to use your phone!

KNOX checks all this extra system software using an enhanced version of the basic "DM-Verity" software included with the Google Android Lollipop OS release. KNOX verifies the integrity of system software not covered by the boot-time checks (discussed in the previous section) and if a malicious process or user is detected, it blocks any attempt to access the modified software and data.

DM-Verity is a Linux kernel driver for verifying the integrity of a partition at run-time.

Go! Run-Time Defenses

More sophisticated attacks can compromise the device or intercept data at run-time (when you actually launch an app or access data). To protect devices against run-time attacks, KNOX uses the TrustZone-based Integrity Measurement Architecture (TIMA), a proprietary security technology developed by Samsung. More sophisticated attacks can compromise the device or intercept data at run-time (when you actually launch an app or access data). To protect devices against run-time attacks, KNOX uses TrustZone-based Integrity Measurement Architecture (TIMA) components, including the following:

- **Periodic Kernel Measurement (PKM):** PKM performs continuous periodic monitoring of the kernel to detect if legitimate kernel code and data have been modified by malicious software. PKM is analogous to a scheduled scan in traditional antivirus or antimalware software for desktop computers.
- **Real-Time Kernel Protection (RKP):** RKP performs ongoing, real-time monitoring of the OS from within TrustZone to prevent kernel tampering. RKP is analogous to real-time, on-demand antivirus or antimalware software scanning that is triggered when a USB thumb drive, for example, is connected to a desktop computer.

RKP and PKM are essential in protecting Android devices against unknown future threats. Flagging suspicious activities is the first step in identifying and preventing security breaches. These real-time checks give enterprises confidence that devices are continuously monitored for breaches, and that IT is alerted if corporate devices have been compromised.

Update Protection

Rollback prevention is a feature of KNOX that blocks the device from loading a valid but older version of boot components. Older versions of software may contain vulnerabilities that attackers can exploit. KNOX rollback prevention checks the version of the bootloader and kernel during both boot and updates, and blocks these processes from continuing if versions are unacceptably old. KNOX further secures this process by using hardware features installed at the factory.

The KNOX security platform is built in to flagship Samsung mobile devices and protects the device right out of the box, throughout the entire device life cycle.

Chapter 3

KNOX Data Protection Products

In This Chapter

- Securing enterprises, government, and regulated industries with KNOX Workspace
- Empowering individual users with My KNOX

Beyond the KNOX platform (discussed in Chapter 2), which provides built-in hardware-based protection — at no cost — from the moment you turn the device on, Samsung offers optional products to address your unique security requirements. Two of these products are KNOX Workspace and My KNOX, which I explain in this chapter.

KNOX Workspace

Samsung KNOX Workspace is a defense-grade dual persona container product designed to separate, isolate, encrypt, and protect enterprise data on a device from attackers. This work/play environment ensures that 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, KNOX Workspace is tightly integrated into the KNOX platform.

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

Apps and data inside KNOX Workspace are isolated from apps outside KNOX Workspace — apps outside KNOX Workspace cannot use Android inter-process communication or data-sharing methods with apps inside KNOX Workspace. For example, photos taken with the camera inside KNOX Workspace are not viewable in the Gallery outside KNOX Workspace. The same restriction applies to copying and pasting. When allowed by IT policy, some app data such as contacts and calendar data can be shared across the KNOX Workspace boundary. The end-user can choose whether to share contacts and calendar notes between KNOX Workspace and his or her personal space on the device; however, IT policy ultimately controls this option.

The enterprise can manage KNOX Workspace like any other IT asset using a mobile device management (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, virtual private network (VPN), email, application blacklisting, whitelisting, and so on.

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

KNOX Workspace also has a two-factor authentication process that can be configured with MDM. The user can configure the KNOX Workspace to accept a fingerprint as the primary authentication factor for the container with a PIN, password, or pattern as a second factor.

Two-factor authentication uses two of the following methods to establish identity: something you know (such as a password or PIN), something you have (such as a token), or something you are (such as a fingerprint).

The KNOX platform also supports multiple containers, thus meeting the needs of professionals who have multiple employers, such as doctors or consultants.

KNOX is continuously being updated with popular features and new additions, including the following:

- **Bluetooth:** Bluetooth support enables users to communicate with other connected devices, and do more than just listen to music and make calls inside the KNOX Workspace. Examples include printing, file sharing, and external card readers. IT administrators can enable security restrictions on external SD cards.
- **Near field communication (NFC):** NFC enables a device to act as a SmartCard-based credential for use cases such as physical access and access to IT accounts.

Finally, IT administrators can configure KNOX caller ID to display caller ID information derived from personal contacts and KNOX Workspace contacts for incoming calls when the user is using the device in personal mode.

My KNOX

My KNOX is a personal, encrypted workspace that allows you to securely separate your work/play apps and data while taking full advantage of the KNOX security platform built in to your device. You can think of this as your personal version of KNOX Workspace without all the IT people messing with your device.

My KNOX is a free product that can be downloaded from Google Play and managed via the My KNOX User website at `http://my.samsungknox.com`.

Key features of My KNOX include the following:

- Support for most email and PIM (Personal Information Manager) account types, such as Gmail and Hotmail, and email communication protocols including EAS (Exchange ActiveSync), POP3 (Post Office Protocol Version 3), and IMAP (Internet Message Access Protocol)
- A separate workspace on the device for email and app connectivity
- A simple end-user website for device management, including remote wipe, lock, and find-my-device tools

Securely mobilizing a major Canadian healthcare provider

The customer

Saint Elizabeth Health Care has been an active participant in the development of community health since 1908. Today, Saint Elizabeth provides a full range of integrated care solutions for client, community, and health system needs across Canada, employing more than 8,000 people and visiting more than 18,000 clients every day.

The challenge

Outfit the mobile workforce with a powerful, secure mobility solution that includes KNOX Workspace to improve in-home care.

"As our staff are delivering world-class care, Samsung's mobile devices are bringing innovation and efficiency to their everyday offices — which can often be a kitchen table, parked vehicle, or patient's home at any given time."

—Shirlee Sharkey,
CEO, Saint Elizabeth

The benefits

- Protects workers' personal information in a separate container from patient data and applications
- Requires health workers to input a password and one additional identifier to ensure only authorized personnel are accessing patient data
- Allows IT staff to centrally manage security and remotely troubleshoot any issues through MDM integration

Chapter 4

Ten (Or So) Essential Capabilities for Enterprise Readiness

Here are ten (or so) key capabilities of KNOX-enabled Samsung mobile devices for enterprises:

- **Protect enterprise Data-at-Rest by default:** Samsung KNOX does not depend on users to secure their own BYOD devices in case of loss or theft. KNOX defines two classes of data — protected and sensitive. All data written by apps in the secure Workspace is considered protected and is encrypted on disk when the device is powered off. Decryption is tied to the device hardware meaning protected data can only be recovered on the same device.

  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. Sensitive Data Protection (SDP) allows sensitive data to be decrypted only when a user unlocks his KNOX Workspace with his password and the decryption key is tied to the hardware. When the user re-locks the Workspace, SDP keys are cleared, and access can only be regained using the same device hardware.

- **On-device encryption:** The KNOX platform further strengthens the full-device encryption capability offered by the Android platform by allowing the IT Manager to tie the encryption key to a secret maintained in trusted hardware. TrustZone-based on-device encryption (ODE) also enables enterprises to ensure that all device data is protected in the unlikely event that the operating system is compromised.

- **Container isolation:** KNOX enables complete isolation of work-related and personal apps and data. This dual persona capability ensures that apps installed by individual users do not compromise the security of corporate apps and data. Container isolation also keeps IT administrators from accessing individual users' private data (such as photos, contacts, and text messages).
- **Virtual private network (VPN):** KNOX offers comprehensive support for enterprise VPNs, enabling individuals to connect to corporate resources from their KNOX-enabled smartphones over an optimized, secure path. The KNOX platform supports both IPSec and Secure Sockets Layer (SSL) VPNs.
- **SmartCard framework:** Public key infrastructure (PKI) certificates enable documents to be digitally signed, email messages to be encrypted and decrypted, and secure network connections to be established. PKI certificates are typically stored on a SmartCard, known as a Common Access Card (CAC). Samsung KNOX provides apps with access to the hardware certificates on the CAC and provides improved SmartCard compatibility via a software framework that allows third-party SmartCard and reader providers to install their solutions into the framework.
- **Single sign-on (SSO):** SSO allows a user to log in once and have access to all the SSO-enabled apps on the device without being prompted to log in again. For example, SSO allows access to the KNOX Workspace container (and participating apps that require credentials within the container) with one password.
- **Active Directory integration:** KNOX provides an option to choose an Active Directory password as the unlock method for KNOX containers. This has two important benefits:
    - It allows IT administrators to use a one-password management policy for desktop and mobile devices.
    - The end-user needs to remember only one password to access all services offered by the employer.

  Active Directory is the most widely deployed enterprise-grade directory service that has built-in support for Kerberos.
- **Mobile device management (MDM):** KNOX provides hundreds of MDM security policies for fine-grained control of devices, designed to lower cost and improve usability and manageability for small or medium enterprises.

Samsung Enterprise Alliance Program (SEAP) is a program for developers and partners who need tools and resources to help build and distribute the highest quality applications on Samsung mobile devices.

http://seap.samsung.com

Development Phase

Create and troubleshoot your solution to get ready for market.

- Samsung B2B SDKs
- Technical Resources
- Developer Forum
- Technical Blog

Distribution Phase

Promote your solution with sales and marketing resources.

- Production License Keys
- Device Loans
- Technical Support
- Marketing/Sales Resources

Safely enable "bring your own device" in your enterprise and empower your mobile workforce!

Samsung is committed to mobile enterprise security and protecting devices and data from increasingly sophisticated malware threats and attacks. Backed by years of research, Samsung KNOX offers unsurpassed levels of mobile security that make Samsung devices truly enterprise-ready right out of the box.

- ***Discover what's in a smartphone* — *and how KNOX secures each critical component of a smartphone***
- ***Learn why KNOX exists* — *and how KNOX delivers a multi-layered mobile security solution***
- ***Understand how the KNOX platform secures Samsung devices* — *and how add-on KNOX services can further enhance enterprise mobile security capabilities***

Open the book and find:

- **Why cybercriminals target smartphones and how to stop them with KNOX**
- **How the Hardware Root of Trust guarantees mobile device security from design to manufacture to powering on and beyond**
- **How to protect corporate apps and data and keep personal apps and data private**
- **What mobile security features are essential for enterprise readiness**

Go to Dummies.com® for more

Lawrence C Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 60 other *For Dummies* books.

FOR DUMMIES® A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-24725-8
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.