Samsung KNOX™ 2

UK Government EUD Guidance Whitepaper

December 2014

Copyright Notice

Document Information

This document was last modified on December 24th, 2014.

Document History

Date	Changes
November 4th 2014	First Draft
November 5th 2014	Updated Acronyms and references
November 7th 2014	Updated following review comments from HQ
December 24th 2014	Updated following final release of EUD Guidance for KNOXv2.x

Contact Information

Samsung Electronics Co., Ltd
416, Maetan-3dong,
Yeongtong-gu Suwon-City
Gyeonggi-do, 443-742
Korea

Samsung Enterprise Mobility Solutions – Santa Clara
Samsung Telecommunications America, Ltd
3920 Freedom Circle; Suite 101
Santa Clara, CA 95054
United States of America

Contents

List of Tables

Acronyms

API	Application Programming Interface
APN	Access Point Name
CESG	Communication & Electronics Security Group
COPE	Corporately Owned Personally Enabled
CPA	Commercial Product Assurance
DEK	Data Encryption Key
DH	Diffie-Hellman
EUD	End User Devices
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
KNOX	The Samsung enterprise security solution
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MDM	Mobile Device Management
NAT	Network Address Translation
NFC	Near Field Communication
ODE	On Device Encryption
OFFICIAL	UK Government Security Classification
OTA	Over The Air
PKM	Periodic Kernel Measurement
RAM	Random Access Memory
RKP	Real-time Kernel Protection
ROM	Read Only Memory

SD Card	Secure Digital Card
SEAMS	SE for Android Management Service
SSL	Secure Sockets Layer
SSO	Single Sign On
TIMA	TrustZone based Integrity Measurement Architecture
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

1 Introduction

Samsung KNOX 2 is the next-generation of the secured Android platform introduced by Samsung in 2013 as Samsung KNOX. Targeted primarily at mid and high-tier devices, it leverages hardware security capabilities to offer multiple levels of protection for the operating system and applications.

Key features of KNOX Workspace include Trusted Boot, ARM TrustZone -based Integrity and Security services, SE for Android enhancements (KNOX platform), and the KNOX 2 container.

In addition, KNOX 2 features a new enterprise enrolment process that vastly improves both the employee and IT administrator experience for enrolling devices into the company’s MDM system.

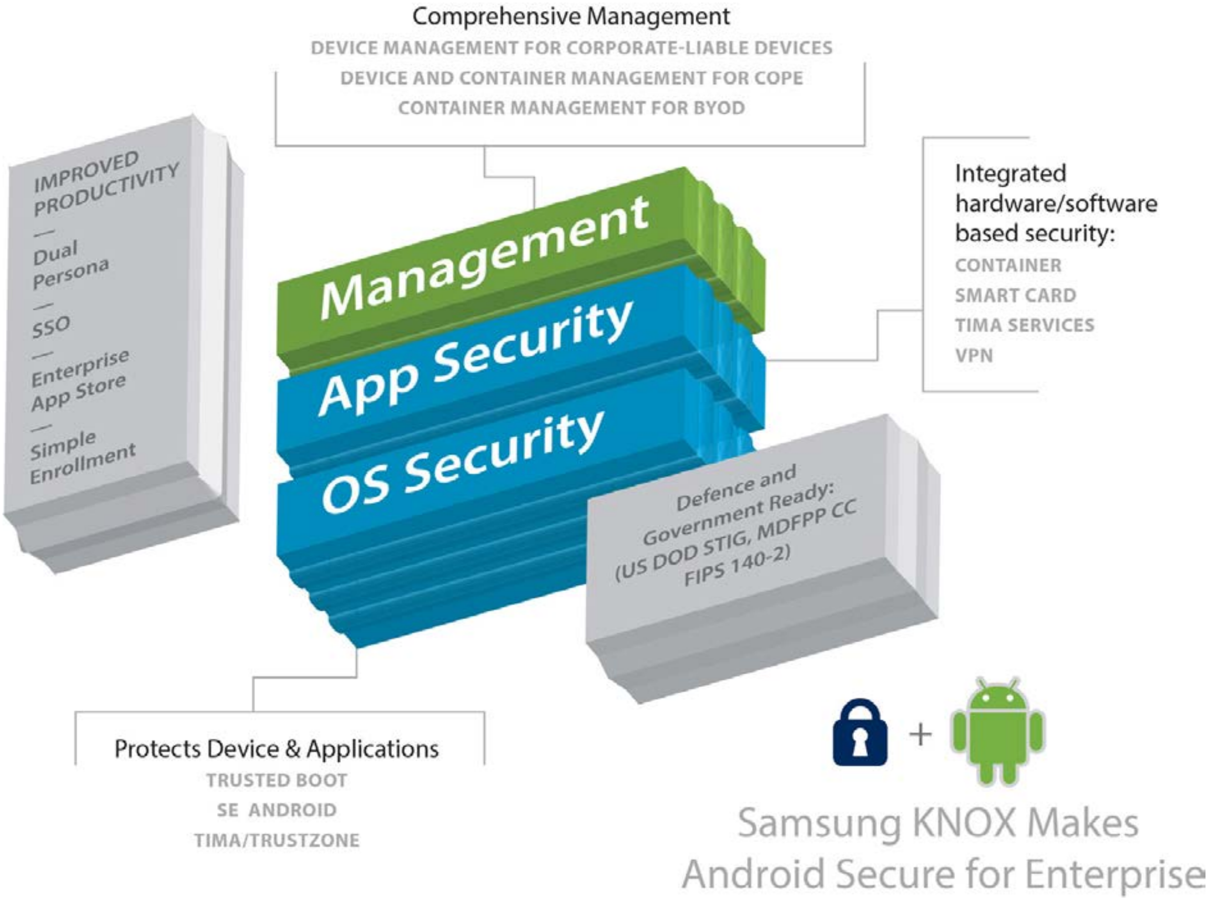
Comprehensive Management
DEVICE MANAGEMENT FOR CORPORATE-LIABLE DEVICES
DEVICE AND CONTAINER MANAGEMENT FOR COPE
CONTAINER MANAGEMENT FOR BYOD
IMPROVED PRODUCTIVITY
—
Dual Persona
—
SSO
—
Enterprise App Store
—
Simple Enrollment
Management
App Security
OS Security
Integrated hardware/software based security:
CONTAINER
SMART CARD
TIMA SERVICES
VPN
Defence and Government Ready: (US DOD STIG, MDFPP CC FIPS 140-2)
Protects Device & Applications
TRUSTED BOOT
SE ANDROID
TIMA/TRUSTZONE
+
Samsung KNOX Makes Android Secure for Enterprise

Figure 1 - Samsung KNOX overview

Samsung KNOX mobile security solution is highly suited to Government and Public Sector deployments of mobile platforms for remote working, and is designed to meet the stringent requirements demanded by Government organisations.

Samsung works closely with Government Information Assurance and Security organisations on a continuous basis to ensure our products and solutions meet and exceed these requirements.

In the UK, the Cabinet Office has introduced the End User Devices Strategy[1], which aims to enable public sector workers to work from any location using any suitable device. Adoption of the strategy enables central government and public sector organisations to access the latest technology meeting certain standards, and deploy cost effective commercial devices.

As part of this strategy, CESG, the National Technical Authority for Information Assurance, has produced a security framework for End User Devices working with OFFICIAL information, and defines controls for devices used for both OFFICAL and OFFICAL-SENSITIVE[2].

CESG assess suitable End User Devices against the security framework requirements, producing guidance for UK Public Sector organisations describing how best to configure the device to meet the requirements, highlighting any areas where the platform does not meet the security framework requirements and indentifying risks that should be considered when deploying the platform in their systems[3].

Samsung as a world leading Smartphone and Tablet manufacturer with a broad range of consumer devices, coupled with Samsung KNOX mobile security solution, is a natural fit for the UK Government End User Devices Strategy, meeting the needs of the public sector in both security and functionality. As such, CESG has assessed the Samsung KNOX platform, producing platform security guidance for public sector deployments[4].

This whitepaper explains how the features of Samsung KNOX allow public sector organisations to deliver market leading devices to their users, as part of a cost effective solution meeting the standards for the End User Devices Strategy, with minimal deployment risk, as shown in the CESG platform guidance for Samsung KNOX enabled devices.

[1] https://www.gov.uk/government/publications/end-user-device-strategy

[2] https://www.gov.uk/government/publications/end-user-device-strategy-security-framework-and-controls

[3] https://www.gov.uk/government/collections/end-user-devices-security-guidance

[4] https://www.gov.uk/government/publications/end-user-devices-security-guidance-samsung-devices-with-knox-2x

2 End User Devices Security Framework

The End User Devices Strategy: Security Framework and Controls document[5] defines a set of security requirements and controls for End User Devices working with OFFICIAL information.

The framework defines 12 areas that require security controls, with requirements and controls for each area detailed in the document.

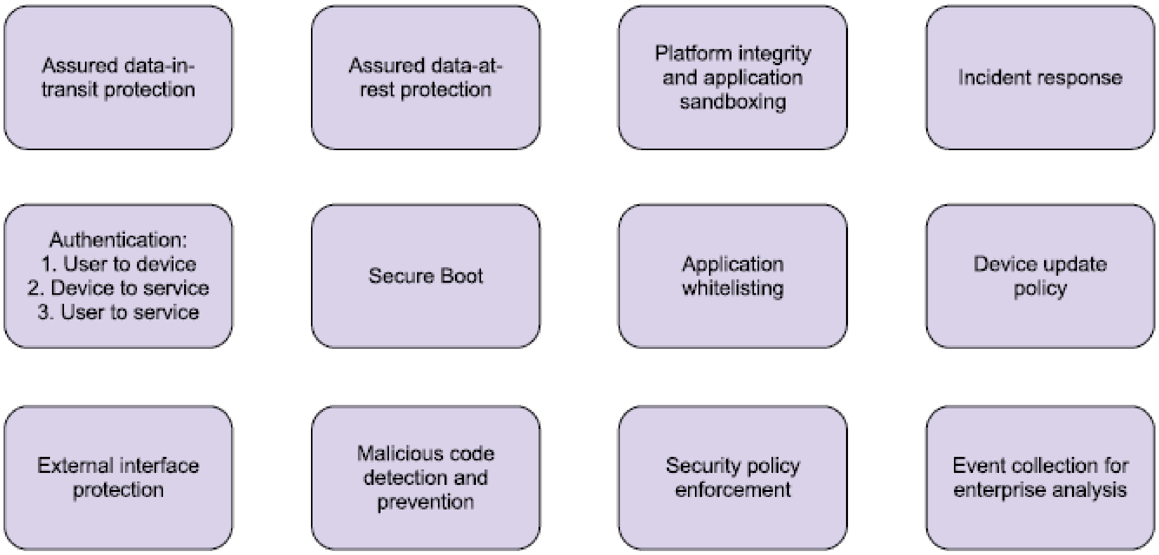
Assured data-in-transit protection
Assured data-at-rest protection
Platform integrity and application sandboxing
Incident response
Authentication:
1. User to device
2. Device to service
3. User to service
Secure Boot
Application whitelisting
Device update policy
External interface protection
Malicious code detection and prevention
Security policy enforcement
Event collection for enterprise analysis

Figure 2 - EUD Security Framework Requirements

CESG assess platforms such as Samsung KNOX against the 12 areas, identifies any risks, and defines configuration guidance for the platform which outlines who best to deploy the platform to meet the standards expected when handling OFFICIAL classification data.

Specific per-platform guidance, along with general security recommendations and enterprise considerations are published on the UK Government web portal.

The CESG assessment is independent. This whitepaper takes the EUD guidance for KNOX and aims to highlight the exact features of the platform and how they can be used to meet the standards required by the public sector.

[5] https://www.gov.uk/government/publications/end-user-device-strategy-security-framework-and-controls

3 Samsung KNOX UK Public Sector Usage Scenario

The EUD Guidance presents a usage scenario for Samsung KNOX enabled devices, where devices will be used remotely over 3G, 4g and non-captive WIFI networks to enable remote working in the form of accessing OFFICIAL classification email, reviewing and commenting on OFFICIAL documentation, and accessing the intranet and other corporate resources.

It is advised that due to the enhanced security features of the Samsung KNOX Container, sensitive enterprise data should be stored in the container, and corporate resources accessed via the container. Non-sensitive work can be carried out outside the container, with the user accessing the container for access to sensitive data.

All data-in-transit from the device should be routed over a VPN for confidentiality and integrity of device traffic, and to allow devices to be protected by enterprise monitoring solutions.

Arbitrary installation of third-party applications by user should not be permitted. Application whitelisting should be employed and approved enterprise applications distributed to devices. Unnecessary applications should be removed or managed using whitelisting.

This usage scenario defines how to best make use of Samsung's differentiating security features and is used as a basis for the recommended configuration presented in the guidance.

4 How Samsung KNOX can meet the EUD Security Framework Requirements

The EUD platform guidance for Samsung KNOX includes a section describing how the platform can best satisfy the security recommendations. Below we take this further and describe the specific features of Samsung KNOX enabled devices that align with the EUD security framework, and clearly differentiate Samsung KNOX from other available platforms.

Table 1 provides a summary of the technical features and controls which Samsung KNOX enabled devices provide to meet the EUD Security Framework requirements.

	Requirement		Mitigation
1	Assured Data-in-transit protection		- KNOX Enterprise IPSec VPN
2	Assured Data-at-rest protection		- On Device Encryption - SD Card Encryption - KNOX Container Encryption
3	Authentication	User to Device	- Android device lock screen - KNOX Container lock screen
		User to Service	- SSO Support
		Device to Service	- Mutual authentication established by IPSec VPN client - TIMA attestation
4	Secure Boot		- Secure Boot mechanism - Trusted Boot mechanism
5	Platform Integrity and Application Sandboxing		- SE For Android - TIMA - KNOX Application Container
6	Application Whitelisting		- Application whitelisting for device - Application whitelisting for KNOX Container
7	Malicious code detection and prevention		- 3rd party anti-malware products - Integrity Monitoring services
8	Security policy enforcement		- KNOX Standard and Premium MDM APIs
9	External interface protection		- MDM Restriction Policies - MDM Firewall Policies
10	Device update policy		- OTA device firmware updates - SE for Android policy updates
11	Event collection for enterprise analysis		- KNOX Audit Logging capability
12	Incident response		- MDM capabilities for remote lock remote wipe of device, and certificate management

Table 1 - Mapping of Samsung KNOX functionality to EUD Security Framework Requirements

Assured Data-In-Transit Protection

Samsung KNOX offers comprehensive support for VPN, both IPSec and SSL. The KNOX platform provides a VPN framework which allows third-party vendors to provide their clients as plug-ins to the framework. The framework enables these clients to be configured and managed via KNOX MDM policies.

The EUD Security Framework mandates the use of an IPSec based VPN, using Certificate based authentication.

The KNOX platform currently supports IPSec VPN functionality via the Mocana KeyVPN IPSec client plug-in integrated into the KNOX VPN framework. The client supports the following features:

- Includes FIPS 140-2 Level 1 certified cryptography module
- Internet Key Exchange IKE v1 (Aggressive and Main Mode) IKE v2 / IPv4 / IPv6 / XAUTH / NAT Traversal
- IPsec (ESP) using Data Encryption Standard (DES)/Triple DES (3DES) (56/168-bit) or AES (128/256-bit) with MD5 or SHA
- RSA, Diffie-Hellman, Elliptic Curve and full support for NSA Suite B Cryptography
- X.509 v3 certificate support

Support for additional IPSec based clients is planned for the near future, including integration of the Strongswan based device client into the KNOX framework (a number of different third-party SSL client are already supported).

The KNOX VPN framework and management APIs allow VPN configurations to be for full device, per container, and also per-app mode. The per-app mode allows an MDM to select applications (inside or outside the container) to connect to the network via a specified VPN profile. All applications inside the container and outside the container can be added. Up to 5 simultaneous VPN connections are allowed, allowing an administrator to define groups of applications to connect to different VPNs.

Once the VPN is configured in per-app or per-container mode, tunnel establishment is automatic. If the VPN is not connected, all outbound traffic from application is blocked from leaving the device. When connected, traffic is routed via the VPN, depending on how the devices have been configured (full device VPN, Container, per-app etc.). VPN profiles are provisioned by the MDM; they cannot be disabled or modified by the user.

These features are highly suited to the EUD deployment use case, allowing all device traffic to be tunnelled automatically, without user interaction, in an ‘always-on’ type configuration, preventing data leakage, and allowing traffic monitoring and filtering inside the customer network if desired.

The EUD guidance for KNOX recommends the use of the per-app VPN configuration, with all applications inside the KNOX container and all applications outside the KNOX container added to a VPN profile, to ensure all traffic is routed through the enterprise VPN. The flexibility of the Samsung solution allows administrators to configure separate VPN tunnels for applications inside and outside the container, so separating enterprise and less-trusted non-enterprise traffic, but still being able to monitor and control all traffic from the device as required.

Assured Data-At-Rest Protection

Data at Rest protection is a core part of the Samsung KNOX layered security solution.

The KNOX container (an isolated environment for enterprise applications and data, described later in this whitepaper) has its own AES256 encrypted file system, which automatically protects all data within the container.

A comprehensive key management solution has been implemented to meet the needs of Government customers, which includes the use of TrustZone based mechanisms with device-unique hardware keys to protect encryption keys, as well as user passcodes. The KNOX platform stores cryptographic values within TrustZone, protected by hardware, which the platform only releases if the integrity of the platform has been verified during boot. If the integrity of the device has been compromised, the values required to derive the container encryption keys, meaning sensitive data cannot be decrypted, protecting it from potential compromise.

In addition, full On Device Encryption (ODE) can optionally be enabled or enforced by the administrator to encrypt the entire device data partition, thus protecting data outside the container as well. Further, if the use of external SD Cards is permitted, encryption can also be enabled and enforced for files stored on this media.

TrustZone protection for ODE can be optionally enabled by the administrator. If this is enabled, the ODE mechanism encryption key derivation requires both the correct user passcode to be entered before the operating system is booted, but also the integrity of the system to be verified before cryptographic keys are released from TrustZone. This means ODE mechanism is afforded the same hardware based protection as the KNOX container encrypted file system.

The EUD guidance for KNOX recommends that sensitive enterprise data is only stored within the KNOX Container, and therefore encrypted by default. The guidance also recommends that ODE for the entire device is enforced, and that TrustZone protection for ODE is enabled.

Authentication

User to Device

In terms of authentication of the user to the device, Samsung KNOX enabled devices offer a variety of authentication mechanisms, which the administrator can enforce via MDM policy.

Device authentication is via the device lock-screen. The device authentication mechanisms available are Pattern, PIN, Password, and also Fingerprint swipe on compatible devices. These can be enforced by the administrator via MDM policy. Comprehensive policies are available to configure the authentication mechanisms to meet organisational policies, such as, passcode length, complexity, age, history, maximum failed attempts, allowable password policies (character sequence policies, number of characters needed to be changed when password is updated etc.) and more.

The Samsung KNOX Workspace container has a separate authentication mechanism. The container must have an authentication mechanism selected, and as with the device authentication, the mechanism to be used can be enforced by the administrator. Authentication mechanisms available for the container include Pattern, PIN, Password, Fingerprint and also two-factor authentication using the fingerprint scanner in addition to Patter, PIN or Password. Again, comprehensive policies are available to configure the authentication mechanisms to meet organisational policy, and enforce which mechanisms can and cannot be used.

As described in the Data-at-Rest Protection section, if ODE is enabled the user will need to authenticate to the device using their passcode during device boot. The passcode is used as part of the encryption key derivation process to decrypt the device. For the KNOX Container, the container passcode is used as part of the key derivation process for the container encrypted file system, together with TrustZone based mechanisms for additional protection.

The EUD guidance for KNOX leaves it open to the organisation deploying the devices to choose a device authentication policy most suited to their needs, but presents two usage scenarios:

- A numeric PIN to access the device, then a strong password to access the KNOX container
- A strong password to access the device, then a shorter password or token to access the KNOX container

The administrator should determine a policy based on where sensitive enterprise data is stored on the device, with the guidance stating that in most cases, enterprise data should be exclusively kept within the KNOX Container.

Samsung KNOX devices give organisations the flexibility to configure an authentication that best meets their operational needs and meets the security recommendations for UK Government deployments.

User to Service

The Samsung KNOX platform supports Single Sign On and Active Directory integration functionality to allow centralised authentication to enterprise services and infrastructure from within the KNOX container environment. SSO support has been enhanced to support Kerberos based authentication as well as cloud based services.

The device SSO service is configured via MDM policy, and the enterprise is required to have the necessary Active Directory infrastructure and services to take advantage of this functionality.

Device to Service

This area of the EUD Security Framework is met by having the ability to establish mutually authenticated IPSec VPN connections to access the enterprise network and services.

Samsung KNOX also has a further differentiating feature in device to service authentication, in the form of Remote Attestation.

The TIMA remote attestation feature enables the device to attest to its own device integrity to a remote service. The foundation of remote attestation is a device-unique public/private key pair that is installed in the TrustZone secure world at device manufacture time.

The attestation private key is only accessible inside the TrustZone secure world by the TIMA attestation app. Due to the security protection offered by TrustZone and the device unique public/private key pair, TIMA attestation enables the device to authenticate itself along with the key boot loader and kernel integrity to a remote service.

A number of MDM vendors have included the use of the TIMA Attestation functionality in their services, allowing administrators to optionally enforce that device attestation passes before allowing creation of the KNOX container. The device attestation verdict can be requested at on-demand at any time by the remote service and thus be used to determine action to be taken as determined by organisational security policy, such as 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.

Secure Boot

The security of the device boot process is a core part of Samsung's layered security approach to the KNOX platform.

The startup process for Android begins with the *primary* bootloader, which is loaded from ROM. This code performs basic system initialization and then loads another bootloader, called a *secondary* bootloader, from the file system into 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 next bootloader in the sequence using a certificate chain that has its root-of-trust resident in the hardware. The boot process is terminated if verification fails at any step.

Typically, the bootloader verification process is only performed until aboot is loaded, which itself does not verify the Android operating system. This allows users to install and boot customized versions of Android OS kernels. As a result, there is no guarantee for enterprise users that their Android system is enforcing OS-level security protection, such as SE for Android, which is essential for protecting enterprise apps and data.

Samsung KNOX 2.0 implements Trusted Boot to address this limitation of Secure Boot. 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 security keys, 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.

Platform Integrity and Application Sandboxing

Samsung KNOX introduces a number of significant platform enhancements which provide assurance of platform integrity, data isolation and application sandboxing which meet the EUD Security Framework requirements.

SE for Android

Samsung KNOX utilises SE for Android to enforce Mandatory Access Control (MAC) policies to isolate applications and data within the platform. While Google also introduced SE for Android in version 4.4 of the Android platform, Samsung's implementation provides significant enhancements in the level of protection offered to applications and system services. KNOX SE for Android Policy defines over 100 security domains that strictly enforce security policies.

The KNOX 2.0 platform introduces a new feature called SE for Android Management Service (SEAMS) that provides controlled access to the SELinux policy engine. SEAMS is used internally by the KNOX 2.0 container, and is also available to third-party vendors to secure their own container solutions. For security considerations, the domains for third-party containers are defined *a priori* by Samsung and activated on-demand when the container application is first invoked.

TrustZone-based Integrity Measurement Architecture

The system protection offered by SE for Android relies on the assumption of 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 pre-empted or disabled by malicious software.

TIMA Periodic Kernel Measurement (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 prevent malicious attacks from corrupting them and potentially disabling SE for Android.

TIMA Real-time Kernel Protection (RKP) performs ongoing, strategically-placed real-time monitoring of the operating system from within TrustZone to prevent tampering of the kernel. RKP intercepts critical events happening inside the kernel, which are 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 attestation verdict that tampering is suspected, which is sent to the MDM. This protects against malicious modifications and injections to kernel code, including those that coerce the kernel into corrupting its own data.

As mentioned earlier in this document, the KNOX platform also includes a remote attestation feature to allow remote services to determine the integrity of the mobile device in a highly secure manner. The EUD guidance recommends that Remote Attestation should be enabled by the administrator to verify the integrity of the platform.

KNOX Container

The Samsung KNOX container provides a separate Android environment within the mobile device, complete with its own home screen, launcher, applications, and widgets.

Applications and data inside the container are isolated from applications outside the container, that is, applications outside the container cannot use Android inter-process communication or data-sharing methods with applications inside the container. For example, photos taken with the camera inside the container are not viewable in the Gallery outside the container. The same restriction applies to copying and pasting. Note that the contacts and calendar apps represent an exception, since container contacts and the calendar can be made visible inside the KNOX container and in the personal work space. The end user can choose whether to share contacts and calendar notes between the container and personal space, however, IT policy ultimately controls this option. Sharing of files between inside and outside the container is also configurable and controllable by the administrator.

The enterprise can manage the container like any other IT asset using an MDM solution; this container management process is called Mobile Container Management (MCM). MCM is affected by setting policies in the same fashion as traditional MDM policies. The Samsung KNOX container includes a rich set of policies for authentication, data security, VPN, e-mail, application blacklisting, whitelisting, and so on.

The KNOX 2.0 platform features major enhancements to the KNOX container in the KNOX 1.0 platform. The most significant enhancement is elimination of application wrapping. This is achieved by leveraging technology introduced by Google in Android 4.2 to support multiple users on tablet devices. Due to this the KNOX container supports any Android application that is compatible with the Multi User Framework. Applications no longer need to be wrapped and signed by Samsung to be installed in the container, and can be installed completely unmodified. As well as being able to use applications available in Google Play in the container (note, access to Google Play is disallowed in the container by default), enterprise can easily deploy in-house custom applications into the container without going through any wrapping process.

The administrator can tightly control the applications which can be deployed in the container by a rich set of Application management policies

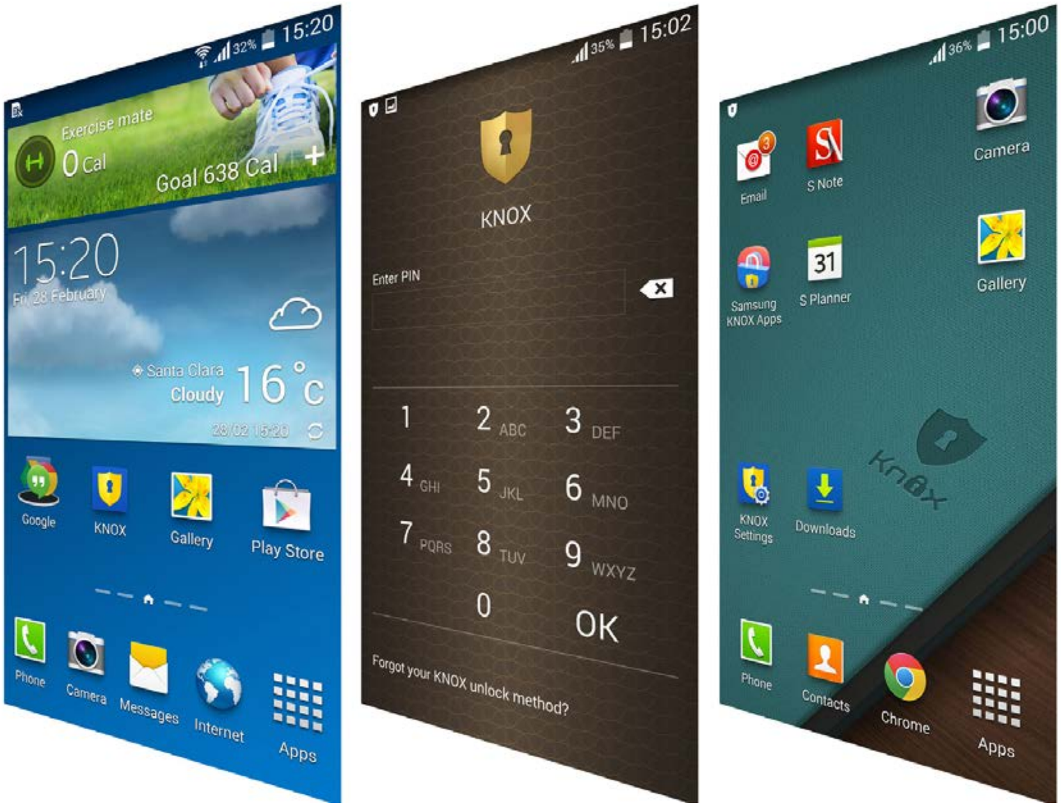

Figure 3 - Samsung KNOX Container

The administrator can control the flow of information between the container and the rest of the device, such as sharing contacts and calendar events. The administrator can entirely lock down the container if required by organisational policy.

The EUD Guidance for KNOX recommends that all enterprise applications and data reside within the KNOX container. Sharing of files between the container and the personal side of the device is disabled, and that sharing of contacts and calendar events is also disabled.

Application Whitelisting

Samsung KNOX has comprehensive application management capabilities, which allow the administrator to be able to strictly control applications which can be used and installed on the device, including inside and outside of the KNOX container.

A rich set of MDM policy APIs are available to enable application management to configure via MDM. This includes application installation whitelisting and blacklisting by package name and signature, application permission whitelisting and blacklisting, disabling of installed applications, silent installation and un-installation of applications.

All of the application management policies can be applied individually to both the device and the container.

For the KNOX container some additional specific policies have been included:

- Allow applications to moved into the container

- Enable Google Play store

‘Allow applications to be moved into the container’ policy controls if the user is allowed to install applications that are installed on the personal persona of the device into the KNOX container. If this is enabled the Container application installation whitelist can be applied to control what the user can install. The default setting for this policy is to not allow applications to be moved into the container by the user, meaning applications can only be installed via MDM or via application stores accessible in the container (Samsung KNOX apps for example, if enabled by the administrator).

‘Enable Google Play store’ policy allows the store to be used from inside the container. Container application whitelists can be used to control what the user can install. By default Google Play store is not enabled in the container. The Google Play store can also be disabled in the personal persona as required.

The application management policies allow the administrator to lock down the device and container as much as the enterprise policy requires. The EUD Guidance recommends full isolation of the container, preventing sharing of files, contact and calendar events between the container and the rest of the device. Application Whitelisting should be used to control which applications the user can install both inside and outside the container.

Malicious Code Detection and Prevention

The administrator can use the rich set of applications management policies Samsung KNOX offers to control what can be installed on the device to mitigate the threat from malicious applications.

In addition the data isolation and platform integrity mechanisms described earlier in this document are designed to protect against damage that could be caused by a malicious application.

Administrators can also deploy third-party anti-malware tools if desired also.

Security Policy Enforcement

Samsung KNOX provides a large comprehensive set of management policies that can be configured via MDM. These policy mechanisms are built into the device software and configuration achieved though management APIs accessible by MDM agents on the device.

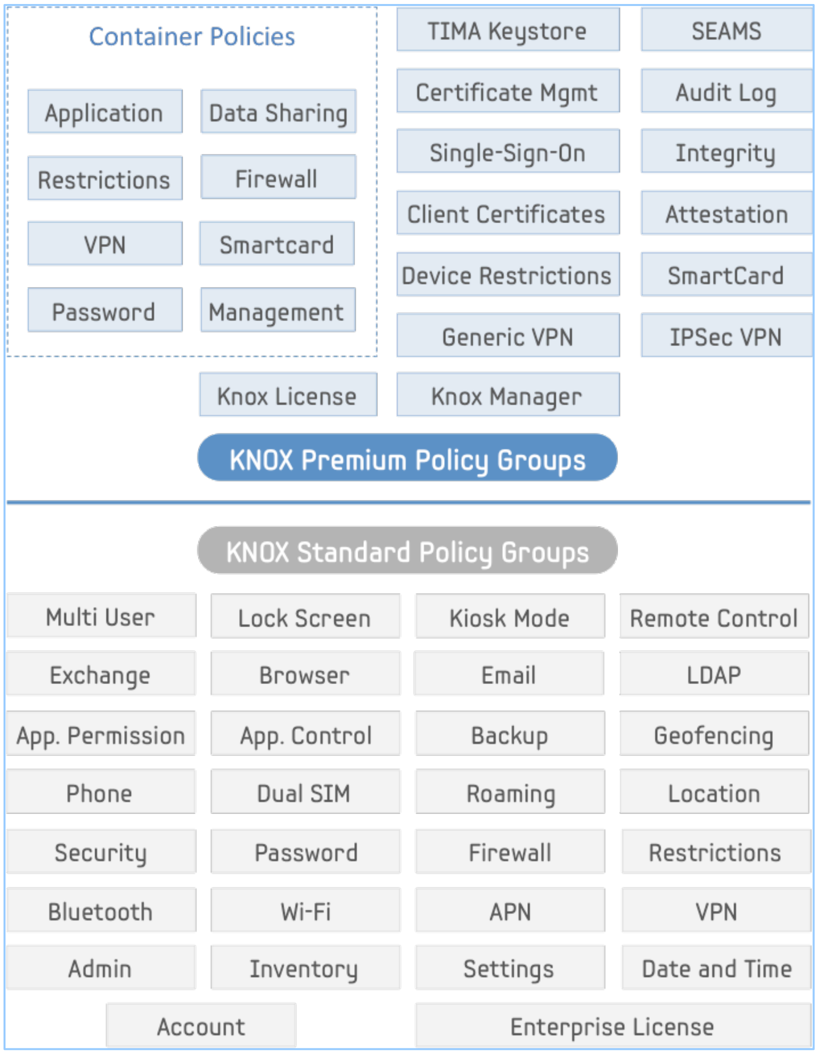

Figure 4 - Overview of Samsung KNOX MDM policies

Comprehensive management policies are available for the device as a whole, the personal side of the device and the KNOX container.

The KNOX Standard and KNOX premium API access is controlled by a licensing mechanism. An SDK is provided to MDM vendors in order for them to develop device management agents.

The administrator can prevent the user removing the device administrator by policy, as well as preventing installation and enabling of another device administrator.

Multiple device administrators can co-exist on the device, but cannot override each other's policies. Up to two KNOX containers can be provisioned on the device and managed by separate MDMs.

The management policies consist of 'global' and 'user' based policies. Global policies (for example enable/disable Bluetooth) are applied across the entire device. User based policies can be applied individually for container and personal personas (for example application management policies).

External Interface Protection

Samsung KNOX devices include MDM restriction policies to allow an administrator to control and protect external interfaces on the device. All external interfaces can be configured, enabled/disabled via MDM policy, which cannot be overridden by the user.

The device and container Firewalls can also be configured via MDM policy. Configuration includes Allow, Deny and Reroute rules for IP addresses and ports (including ranges), configuration of Proxy's, URL filtering.

In the KNOX container, access to external storage (SDCard and USB) is disabled to ensure isolation of enterprise data. As described previously, sharing of data between inside and outside the container can be strictly controlled by the administrator.

Device Update Policy

Samsung actively updates devices with new features, and also addressing issues, both functional and security related.

Device firmware updates are applied to devices either OTA pushed by Samsung servers or via USB using the Samsung Kies PC application.

Samsung KNOX devices have an extensive set of device audit policies allowing an administrator to monitor device software and status including installed applications, and enabling them to take an appropriate response as necessary, such as locking the KNOX Container until device firmware has been updated.

There are no specific MDM policies to be able to push device firmware updates; however an administrator can manage how updates are applied to a device, by for example disabling OTA updates.

Samsung can also update the device SE for Android policies independently of firmware updates in a secure manner via Samsung Policy Distribution servers. Samsung continually maintain device SE for Android policies to ensure overall security and enterprise data isolation.

The Application MDM policy includes an API to be able to silently update applications without the need for user interaction.

Event Collection for Enterprise Analysis

Samsung KNOX provides an enterprise audit logging capability, separate from the normal device logging functionality. The audit logging capability can be enabled, managed and logs retrieved via compatible MDM.

Audit logging covers device wide enterprise security related events including failed unlock events, application installation/uninstallation, and interface events.

Incident Response

Samsung KNOX devices support incident response in a number of ways.

The device and KNOX container can be remotely locked, disabled and wiped via the MDM, either manually by the administrator, or in some cases in response to a specific event such as a number of incorrect passcode's entered. Samsung KNOX provides the ability to wipe the container, the whole device, and also any SD Card that may be in use (if allowed by organisational policy). Many MDM solutions offer compliance services which can take administrator defined actions based on events or device state.

In addition to this, Samsung KNOX offers a device attestation mechanism, enabling a device to attest its integrity to the MDM, or include tamper incident logs which can then be responded to.

The EUD Guidance additionally recommends revoking VPN Client certificates in response to incidents such as device loss. It also recommends revoking certificates for other services, such client certificates for email. Samsung KNOX provides the ability to remove certificates that have been provisioned by the enterprise.

5 Samsung KNOX Configuration Guidance

As part of the CESG assessment of Samsung KNOX enabled devices, a recommended configuration has been devised which allows the solution to best meet the Security Framework requirements, and allow administrators to best manage and mitigate risks.

The EUD guidance recommended configuration is reproduced below, along with explanation of the settings. Administrators should consult the EUD guidance for Samsung KNOX through the UK Government web portal to ensure that the latest configuration guidance is followed.

Policies are applied and managed using a compatible MDM solution, and cannot be overridden by the user, ensuring the enterprise has as much control over the device as required by organisational policy.

Configuration

Policies for Samsung KNOX Enabled Device

These policies cover the configuration of the device as a whole and outside of the KNOX container. A KNOX container specific configuration is provided in the subsequent table.

Configuration Rule	EUD Recommended Setting	Notes
App Stores	Disable or remove the Google Play and Samsung Galaxy App store, and prevent the installation of applications from unknown sources.	App stores can be disabled via MDM policy in order to prevent arbitrary installation of applications. This can alternatively be managed using the installation whitelisting capabilities provided by Samsung. Installation from Unknown Sources can be disabled by the administrator, preventing the user from side-loading applications where the origin may be unknown.
Whitelist	Disable or remove unnecessary applications. If the Google Play store is permitted, allow only applications in the white list to be installed.	Samsung's application management policies allow the administrator to disable applications that are currently installed on the device as required, and create an installation whitelist of approved applications that user can install from application stores outside the container
Developer Mode	Prevent all developer mode settings, including USB debugging and USB storage mode.	This prevents the user from accessing the Android developer options, and preventing them from using ADB, which should be unnecessary for a corporate user. Samsung provides additional USB management options to prevent the device from being used in mass storage mode, or use of USB connectivity at all.
Encrypted Storage	Enforced internal encryption	On Device Encryption can be enforced by the administrator, protecting all user data on the device.

SD Card	Disable access to the SD Card	Use of SD Card slot on the device can be disabled to prevent data being copied from the device onto external storage.
Password	Require Password: True Minimum length: 8 characters Maximum failed attempts: 5 Require complex password: True Password must contain uppercase, lowercase and symbols Passcode history: 8 Maximum passcode age: 90 days Wipe external storage during device wipe: True	This is the EUD recommended password configuration policy for the device using Samsung's comprehensive password management policies. The guidance does however state that organisation can alter password complexity according to organisational requirement, for example have reduced complexity to access the device and increased complexity to access the KNOX container where enterprise data and applications are stored.
Lock Timeout	10 minutes	Timeout for when screen locks automatically when not being used.
VPN	Apply the per-app VPN to all applications outside the KNOX container.	This is to allow all device traffic to be tunnelled and to take advantage of the Samsung KNOX per-app VPN properties such as always-on type operation preventing potential data leakage if the VPN is disconnected.
Certificates	Enable certificate validation at install. Install enterprise certificates.	Samsung provides device certificate management MDM APIs to allow provisioning and management of client and CA certificates, including enabling certificate validation upon installation.
Interfaces	Disable unnecessary interfaces unless there is an overriding business need, e.g. USB interface, Bluetooth, NFC.	Administrators can manage and disable all device interfaces via MDM as per organisational policy
Attestation	Verification of KNOX attestation status should be enabled	As discussed earlier in this whitepaper, Samsung KNOX enabled devices have a secure remote attestation feature, enabling the integrity of devices to be determined. Enabling this is compatible MDMs can allow enterprise features such as KNOX container to only be provisioned to devices that can attest to having a good known state.
TIMA Key Store	Enable	Enabling this feature allows applications to store keys in Samsung KNOX TrustZone protected Key Store using the standard Android Key Storage APIs with little or no modification
ODE Trusted Boot Verification	Enable	As discussed earlier in this whitepaper, enabling the feature will mean that ODE cryptographic keys will only be released from TrustZone upon device boot, if the device integrity is valid, as well as the user entering their valid passcode. Both must be correct to allow decryption of device data. TrustZone protection enhances defence against offline attacks.

Table 2 - MDM policy configuration for Samsung KNOX enabled device

Policies for Samsung KNOX Container

These policies cover configuration of the KNOX container. Policies are independent to that applied outside of the container.

Configuration Rule	EUD Recommended Setting	Notes
App Stores	Disable the Samsung KNOX and Google Play app stores. Applications from these stores that are required may be installed using the out-of-container store app, then installed inside the container using KNOX settings utility.	Google Play is disabled by default in the KNOX Container, but can optionally be enabled by the administrator. As with outside the container, Samsung provides a comprehensive set of application management policies, such as installation whitelisting.
Allow applications to be moved into the container	Enable Applications moved into the container are restricted by the whitelist	Samsung KNOX provides the ability to move applications installed outside the device into the KNOX container. This is disabled by default, but can be enabled via MDM. The application can then execute in the container, with all application data for that instance isolated from applications outside the container and protected by the KNOX container DAR mechanism. Moving of applications in the container is subject to any application management policies applied to the container, such as a whitelist. This means that an administrator can allow an application to installed on the device outside of the container, but only allow a subset to be installed into the container by the user.
Whitelist	White list essential applications for accessing and manipulating corporate data only, e.g. mail client, browser, and office suite. If the KNOX Store or Google Play stores are permitted, allow only applications in the whitelist to be installed.	As discussed above, comprehensive application management policies can be applied to the Samsung KNOX Container, allowing only essential enterprise applications to be used in the container.
Browser	Enable	Allows the administrator to control whether or not the user can use web browser applications in the KNOX Container
VPN	Apply the Per-App VPN to all applications in the KNOX container, including background services and widgets.	This is to allow all container traffic to be tunnelled and to take advantage of the Samsung KNOX per-app VPN properties such as always-on type operation preventing potential data leakage if the VPN is disconnected.
Email	Configure the email client to connect to the enterprise server using client certificate authentication.	The container email client configuration can be configured by MDM. The EUD guidance that certificate authentication should be used to access the enterprise server.
Email Account	Disable	This prevents users adding additional account within the KNOX Container. Depending on

Addition		organisational policy, user can personal or non-sensitive email accounts outside of the KNOX Container.
Password	Enable KNOX Password Policy: True KNOX Timeout: 30 minutes Maximum failed attempts: 5 Minimum length: 8 characters Quality: Alphanumeric Password history: 8 Maximum passcode age: 90 days Minimum character changes: Set to greater than 1 to prevent incremental password change	This is the EUD recommended password configuration policy for the container using Samsung's comprehensive password management policies. The guidance does however state that organisation can alter password complexity according to organisational requirement, for example have reduced complexity to access the device and increased complexity to access the KNOX container where enterprise data and applications are stored.
Credentials	Required client certificates should be installed via policy.	Samsung provides container certificate management MDM APIs to allow provisioning and management of client and CA certificates, including enabling certificate validation upon installation.
Permit Moving Files into the Container	False	The Samsung KNOX Container implementation allows administrators to control movement of data inside and outside of the container. The EUD guidance states that data inside the container should be isolated, and moving files from outside of the container into the container is prohibited. This action is disabled by default.
Permit Moving Files out of the Container	False	The Samsung KNOX Container implementation allows administrators to control movement of data inside and outside of the container. The EUD guidance states that data inside the container should be isolated, and moving files from the container out to the personal side of the device is prohibited. This action is disabled by default. The KNOX container has a separate isolated file system which cannot be accessed from outside the container.
KNOX Container Data Synchronisation	The following settings should be set to 'disallow' to prevent data being moved between the KNOX container and the device • Preview KNOX notifications • Export contacts to personal mode • Export calendar items to personal mode	In addition to files, Samsung KNOX allows an administrator to control if KNOX container contacts and calendar events can be shared with the personal side of the device. This is disabled by default, and the EUD guidance states that they should not be enabled. In addition, by default, notifications by KNOX Container applications are not previewed in the notification panel. Preview of KNOX notifications can be optionally enabled by the administrator, but the EUD guidance states this should be disallowed.

Table 3 - MDM policy configuration for the Samsung KNOX container

VPN Configuration

The EUD guidance usage scenario for Samsung KNOX states that all device traffic should be routed over an enterprise VPN.

The Samsung KNOX IPSec VPN client should be used, as discussed earlier in this whitepaper, and configured via MDM policy.

The Samsung KNOX per-app configuration should be used. It should be noted that the Samsung per-app VPN feature allows administrators to have fine grained control over which applications access a given VPN connection (with up to 5 different VPN connections possible at one time). The administrator can configure just a single application to have its traffic routed over VPN, a group of applications, or in fact all applications.

In this case, for each of the two VPN configurations, all application packages should be added, to ensure that all container traffic and all device traffic are sent via the VPN tunnel(s). In this configuration VPN establishment is automated, and traffic is prevented from leaving the device until the VPN connection has been established.

The VPN profiles for both tunnels should be configured in-line with CESG guidelines or as per organisational policy depending on the enterprise infrastructure and network connectivity requirements (such as connecting to PSN).

The EUD guidance additionally states that organisations may wish to set up two different VPN profiles, one for all applications on the device (outside of the container), and a second for all applications within the KNOX container. This setup would allow traffic from less-trusted applications to be separated from the applications in the KNOX container that handle OFFICIAL material.

6 Samsung KNOX Deployment Guidance

The EUD Guidance defines recommended generic network architecture for deploying mobile devices. This is shown in Figure 5.

Samsung KNOX enabled devices can efficiently deployed within CESGs recommended architecture, and designed to be easily integrated into existing enterprise infrastructure.

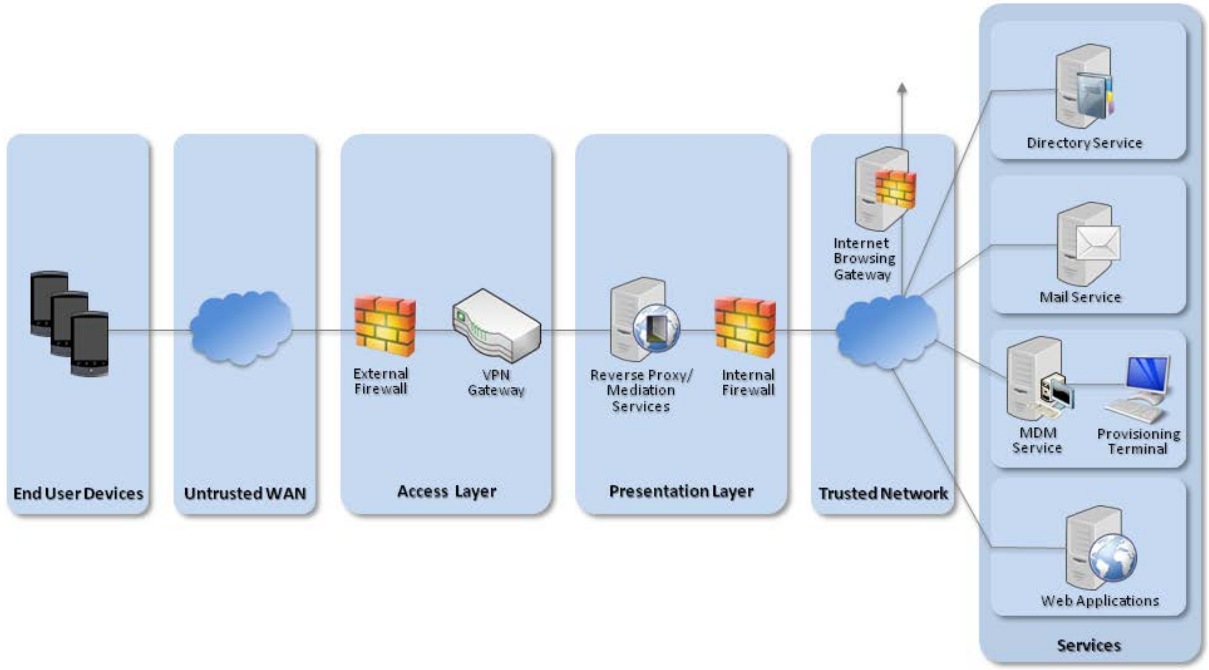

Figure 5 - CESG Recommended network architecture

MDM Support

The Samsung KNOX enabled devices contain all the necessary APIs which can be leveraged by an MDM solution to provide full management of the device and KNOX Container.

This approach allows an enterprise to choose an MDM solution that best suits their requirements. Samsung have partnered with the major MDM solution vendors for Samsung KNOX integration. Information on MDM vendors which support Samsung KNOX can be found on the Samsung KNOX website[6].

[6] https://www.samsungknox.com/en/products/knox-workspace/technical/knox-mdm-feature-list

Samsung also produces KNOX EMM; a cloud based management solution for Samsung KNOX devices, and in addition can manage Android and iOS devices from the same management system.

KNOX License Management

The deployment of devices with a KNOX configuration requires a valid KNOX license.

The licensing mechanism requires access to the network and Samsung licensing servers in order validate licenses upon initial registration of licensable services, and periodic connection to the license server for license validation.

Other Samsung network services are required for correct device operation, these include SE for Android Denial Logging uploads, SE for Android policy updates, and OTA device firmware updates.

Samsung can also provide an on-premise license system, which maybe a requirement for some public sector deployments. This will allow an enterprise to configure devices to be directed to an enterprises own licensing server (software provided by Samsung) rather than Samsung servers. The enterprise will also be able to configure the device to not connect to other Samsung services such as SE for Android denial logging, policy updates and FOTA.

Recommended Provisioning Steps

An enterprise is recommended to follow the steps below to provision their devices in line with the configuration presented in this document.

1. Enroll the device with the deployed enterprise MDM solution. Installation from unknown sources may need to be enabled on the device at this stage to enable the device administration application to be installed, dependent on MDM product.
2. Provision device with KNOX container via MDM.
3. Provision device with enterprise certificates (CA and user certificates). Both device and container certificates can be provisioned separately on the device. Provision container SSL certificates. Container certificates need to be provisioned via the MDM.
4. Deploy device security policy via MDM as per recommended configuration
5. Deploy device application whitelist and list of packages to disable on the device via MDM
6. Deploy KNOX container configuration via MDM as per recommended configuration
7. Deploy KNOX container application whitelist and list of container packages to disable via MDM
8. Install required enterprise applications into the container via MDM
9. Deploy enterprise email configuration for the KNOX container via MDM
10. Deploy KNOX per-app VPN configuration for device and container via MDM

Not that most MDMs will automate these step when the administrator has configured all the MDM policies. When a device is enrolled, the MDM agent will then automatically apply the policies listed above without the need to go through the steps manually.

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.samsungknox.com.

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